Watermarking approaches for images authentication in applications with time constraints

Musab Qassem Al-Ghadi

▶ **To cite this version:**

Musab Qassem Al-Ghadi. Watermarking approaches for images authentication in applications with time constraints. Cryptography and Security [cs.CR]. Université de Bretagne occidentale - Brest, 2018. English. NNT : 2018BRES0029 . tel-01967625

HAL Id: tel-01967625
https://theses.hal.science/tel-01967625

Submitted on 1 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITE BRETAGNE LOIRE / MATHSTIC

UBO
Université de Bretagne Occidentale

THESE DE DOCTORAT DE

L'UNIVERSITE
DE BRETAGNE OCCIDENTALE
COMUE UNIVERSITE BRETAGNE LOIRE

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Informatique*

Par

Musab Qassem AL-GHADI

Approches de tatouage pour l'authentification de l'image dans des applications à contraintes temporelles

Thèse présentée et soutenue à l'Université de Bretagne Occidentale, le 18 juin 2018
Unité de recherche : Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance (Lab-STICC / UMR CNRS 6285)

Rapporteurs avant soutenance :

Ismaïl BISKRI, Professeur, Université du Québec à Trois-Rivières
Philippe CARRÉ, Professeur, Université de Poitiers

Composition du Jury :

Ismaïl BISKRI, Professeur, Université du Québec à Trois-Rivières

Philippe CARRÉ, Professeur des Universités, Université de Poitiers

Gouenou COATRIEUX, Professeur, IMT Atlantique, Président

Caroline FONTAINE, Chargée de Recherche, CNRS, IMT Atlantique

Kamel KAROUI, Maître de Conférences, Université de Carthage

Lamri LAOUAMER, Maître de Conférences, Université de Al-Qassim, Co-encadrant de thèse

Laurent NANA, Professeur des Universités, Université de Brest, Directeur de thèse

Anca PASCU, Maître de Conférences HDR Emérite, Université de Brest, Co-directrice de thèse

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my thesis supervisors Laurent Nana, Anca Pascu and Lamri Laouamer. Thank you very much for the high quality and remarkable supervision during 4 years. Thank you for reviewing my work and giving me valuable guidances and advices. I have learned a lot from you not only about research and academic but also about attitude in life.

I present my thanks to Ismaïl Biskri and Philipe Carré for taking their time to review my dissertation. I also thank Caroline Fontaine, Gouenou Coatrieux and Kamel Karoui for accepting to be examiners. It was an honor to have you as jury members. Your attentions and comments really help me to improve the quality of the dissertation.

My sincere thanks also goes to Ismaïl Biskri, who provided me an opportunity for a mobility stage and gave access to the laboratory and research facilities at the Université du Québec à Trois-Rivieres.

I also expresses thanks to T. Moulahi, S. Zidi, J. Eleuchi, A. Elomri, M. Yehya and R. Anshasi for encouraging me and supporting everything I did.

I would like to present my thanks to all of my colleagues at Lab-STICC and Université de Bretagne Occidentale. In particular, I would like to thank M. Jabnoun, A. Benzerbadj and H. Aissaoua for their generous help when I arrived in Brest. Furthermore, I present my thank to D. Massé who I have an opportunity to work with.

I also want to send my thanks to my friends and colleges in Brest: Amine, Ayoub, Farid, Hamza, Libey, Maeen, Massinissa, Mohammed Bey, Molham, Mourad, Zakaria. Thank you very much for all the events, trips and memories that we have together. I really appreciate your help during the preparation of my defense.

Last but not least, I present my deepest gratitude to my mother Nahlah alMomani, my father Qassem alGhadi, my sisters (Um Qais, Um Anas, Um Karam, Eng. Tasneem, Esra'a, Ala'a and Batool) and my brothers (Dr.Muath, Eng.Mohammed and Baraa) for supporting and encouraging me since the beginning. I would like to thank my wife Ala'a and my son Qassem for always staying by my side, for their love and caring over these years.

PUBLICATIONS

Journals

1. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2018) A Novel Blind Spatial Domain-Based Image Watermarking Using Texture Analysis and Association Rules Mining. *Submitted to Journal of Multimedia Tools and Applications, Springer*.

2. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2016) A Novel Zero-Watermarking Approach of Medical Images based on Jacobian Matrix Model. *Security and Communication Networks, Wiley*, 9(18):5203-5218. doi: 10.1002/sec.1690.

3. *Musab Ghadi*, Lamri Laouamer, Tarek Moulahi. (2016) Securing Data Exchange in Wireless Multimedia Sensor Networks: Perspectives and Challenging. *Multimedia Tools and Applications, Springer*, 75(6):3425-3451. doi: 10.1007/s11042-014-2443-y.

4. *Musab Ghadi*, Lamri Laouamer, Tarek Moulahi. (2015) Enhancing Digital Image Integrity by Exploiting JPEG BitStream Attributes. *Journal of Innovation in Digital Ecosystems, Elsevier*, 2(1-2):20-31.
doi: https://doi.org/10.1016/j.jides.2015.10.003.

International Conferences

1. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2017) A Robust Watermarking Technique in Spatial Domain using Closeness Coefficients of Texture. In *Proceedings of the 8th International Conference on Information, Intelligence, Systems and Applications, Cyprus*. doi: 10.1109/IISA.2017.8316393.

2. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2017) A Joint Spatial Texture Analysis/Watermarking System for Digital Image Authentication. In *Proceedings of the 12th IEEE International Workshop on Signal Processing Systems, Lorient, France*. doi: 10.1109/SiPS.2017.8109968.

3. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2017) A Robust Watermarking System Based on Formal Concept Analysis and Texture Analysis. In *Proceedings of the 30th International FLAIRS Conference. Marco Island, Florida, USA*: 682-687.
doi: https://aaai.org/ocs/index.php/FLAIRS/FLAIRS17/paper/view/15484.

4. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2016) A Robust Associative Watermarking Technique Based on Frequent Pattern Mining and Texture Analysis. In *Proceedings of the 8th International ACM Conference on Management of computational and collective IntElligence in Digital EcoSystems. Hendaye, France*: 73-81. doi: 10.1145/3012071.3012101.

5. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2017) Fuzzy Rough Set Based Image Watermarking Approach. In *Proceedings of the 2nd International Springer Conference on Advanced Intelligent Systems and Informatics, AISI 2016, Cairo, Egypt*, 533:234-245. doi: 10.1007/978-3-319-48308-5_23.

6. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2015) JPEG Bitstream Based Integrity with Lightweight Complexity of Medical Image in WMSNS Environment. In *Proceedings of the 7th International ACM Conference on Management of computational and collective IntElligence in Digital EcoSystems. Caraguatatuba, Sao Paulo, Brazil*: 53-58. doi: 10.1145/2857218.2857227.

Book Chapter

1. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2018) Robust Image Watermarking Based on Multiple-Criteria Decision-Making (MCDM). In: *(S. Ramakrishnan, Ed.). CRC Press, Taylor and Francis Group*.

2. *Musab Ghadi*, Lamri Laouamer, Laurent Nana, Anca Pascu. (2018) Rough Set Theory Based Robust Image Watermarking. In: *Hassanien A., Oliva D. (eds) Advances in Soft Computing and Machine Learning in Image Processing. Studies in Computational Intelligence. Springer, Cham*, 730:627-659. doi: 10.1007/978-3-319-63754-9_28.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ABC Artificial Bee Colony

AC Alternating Current

AHP Analytical Hierarchy Process

AI Artificial Intelligence

ANN Artificial Neural Network

ARM Association Rule Mining

BER Bit Error Rate

BKF Bessel K Form

BPANN Back Propagation Artificial Neural Network

BPNN Back Propagation Neural Network

bpp Bit Per Pixel

CI Computational Intelligence

CMY Cyan-Magneta-Yellow

CMYK Cyan-Magneta-Yellow-Key

CSF Contrast Sensitivity Function

CT Computerized Tomography

DC Direct Current

DCT Discrete Cosine Transform

DPSO Dynamic-Particle Swarm Optimization

DQT Define Quantization Table

DTCWT Dual Tree Complex Wavelet Transform

DWT Discrete Wavelet Transform

ECC Error Correcting Code

EPR Electronic Patient Record

ER Embedding Rate

FC Formal Concept

FCA Formal Concept Analysis

FDCuT Fast Discrete Curvelet Transform

FIS Fuzzy Inference System

FLS-SVM Fuzzy Least Squares Support Vector Machine

FPM Frequent Pattern Mining

GA Genetic Algorithm

GLCM Gray-Level Co-occurrence Matrices

HH High-high (diagonal detail) sub-band

HL High-low (vertical detail) sub-band

HSV Hue, Saturation, and Value

HTML Hypertext Markup Language

HVS Human Visual System

HVS Human Visual System

IQDFT Inverse Quaternion Discrete Fourier Transform

JM Jacobian matrix

JND Just-Noticeable Difference

JPEG Joint Photographic Experts Group

JPEG Joint Photographic Experts Group

JPW Just Perceptual Weighting

LATESTRNDDIST Latest Small Random Distortions attack

LBP Local Binary Pattern

LH Low-high (horizontal detail) sub-band

LL Low-low (approximation) sub-band

LSB Least Significant Bit

LSB Least Significant Bits

LS-SVM Least Squares Support Vector Machine

MADM Multi-Attribute Decision Making

MCDM Multi-Criteria Decision Making

MD5 Message-Digest Algorithm 5

MDD Minimum Distance Decoder

MODM Multi-Objective Decision Making

MRI Magnetic Resonant Imaging

MSE Mean Square Error

MSE Mean Square Error

mSSIM mean Structure SIMilarity

NC Normalized Correlation

NURP Non-Uniform Rectangular Partition

NVF Noise Visibility Function

OR Operational Research

PCA Principal Components Analysis

PCET Polar Complex Exponential Transform

PN Pseudo Noise

PSAM Partly Sign-Altered Mean modulation

PSNR Peak Signal-to-Noise Ratio

QDFT Quaternion Discrete Fourier Transform

QEMs Quaternion Exponent Moments

QIM Quantization Index Modulation

QM Quantization Matrix

QWT Quaternion Wavelet Transform

RGB Red Green Blue

RML Remove lines attack

ROI Region of Interest

ROI Regions of Interest

RONI Region of Non Interest

RSA Rivest, Shamir, & Adleman

SC Soft Computing

SIRD Simple Image Region Detector

SSIM Structure SIMilarity

SURF Speed-Up Robust Features

SVD Singular Value Decomposition

TOPSIS Technique for Order of Preference by Similarity to Ideal Solution

US Ultrasound

WGN White Gaussian Noise

WV Weight Vectors

INTRODUCTION

Digital data (images, audio and video) sharing over the Internet has quickly risen. Digital data transmissions are present in many applications of our daily life. Their usage ranges from individual services such as sharing files or information with friends, family, to professional and administrative systems, such as tele-medicine, environment monitoring, military and law-enforcement. These systems combine many specific functions and use limited resources.

Digital data protection is needed for reasons such as preventing the generation of identical but unauthorized digital data and preventing manipulation, transmission and copying of digital data by unauthorized users. Three generic techniques are proposed to protect multimedia data: cryptography, steganography and watermarking. Cryptography is the most common method used for protecting digital content. It involves transforming the original data D into another form Dc such that only the authorized user can recover D from Dc. Steganography and watermarking are two information hiding techniques that involve hiding a secret information called watermark into a digital data such that watermark can be detected or extracted later. Steganography hides the important secret watermark in a carrier signal in such a way that no one apart from the authorized recipient knows the existence of the information (i.e. the existence of watermark in digital data is concealed), whereas for watermarking, the hidden watermark may be visible and the carrier signal is the important information. Formally, watermarking can be defined as a process that hides secret information called watermark within the digital data, such that the embedded watermark can be detected or extracted later to produce a confirmation of the data validity [82]. Watermarking has been recognized as a key approach for identification, authentication and integrity of digital data.

Two major issues are solved using information hiding techniques including: protection of multimedia data from malicious use and avoiding the observation of secret data by unintended recipients. Digital watermarking has much interest than other protection techniques due to the increase in concern over authenticity, integrity and copyright protection of digital content. In digital watermarking, the original data is visible and readable from all users, while the secret information is changeable and readable by the authorized user only. Cryptography techniques cannot help the owner of digital content to monitor how a legitimate user handles the content after decryption, but the digital watermarking can protect content even after it is decrypted. On the contrary, digital watermarking

alone is not a complete solution for access/copy control or copyright protection and it cannot survive every possible attack.

Sharing and archiving the patient's medical images efficiently through diverse e-healthcare applications has become an urgent requirement [106]. Medical images can be transmitted between hospitals, which are located at various locations, for many reasons, such as tele-diagnosis, teleconferences between clinicians and medical consultation, remote learning and training. As well, remote sensing system can transmit images between different administrative organizations, which are located at various locations, for many purposes, such as decision making, criminals discovering and forecasting about some actions by the experts. Medical and remote sensing images can be intentionally and unintentionally manipulated by unauthorized users [82]. Protecting these images by alleviating fraudulent activities and resisting against different illegal manipulations is important need to obtain right treatments and decisions [25].

Encryption and other access control techniques are difficult to conform to the constraints of the medical and remote sensing images security and protection [95]. Digital watermarking is an effective solution for this problem. It can efficiently address the essential requirements of the medical or remote sensing images protection including the issues of unique identification, authentication, copyright protection and integrity verification during transmission through insecure networks and storage in large databases [95].

An authentication scheme based digital watermarking have to be developed and be convenient with limited resources in an e-healthcare and public networks, rather than those based on conventional cryptographic approaches [134][135].

The first scheme could be a zero-watermarking; the need for zero-watermarking system in tele-medicine becomes essential to transmit the medical images through an e-healthcare network authentically.

The second scheme could be spatial domain based image watermarking. The core of this scheme involves understanding and analyzing the spatial characteristics of host images to identify significant visual locations for embedding watermark using spatial domain. The principles of HVS confirm that embedding watermark in significant visual locations in host image leads to high imperceptibility and robustness [61]. Additionally, embedding watermark in spatial domain leads to low computational complexity comparing with embedding watermark in frequency domain.

CONTEXT

The context of this thesis is zero-watermarking and texture analysis based image watermarking using spatial domain.

Authentication of digital image

The authentication of digital image involves the proof of image origins and attachments to one user. Watermarking allows associating a watermark with the image data to be protected, in such a way the attacker cannot modify, remove, or replace the watermark in the image data. Watermarking can be applied to image data by using its primary or secondary elements. These elements are the image pixels or its transformed coefficients. The pixels are obtained directly from the image data without any transformation, while the transformed coefficients are obtained after applying one of the transformation schemes such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Singular Value Decomposition (SVD). Imperceptibility and robustness are the most desirable properties for any watermarking approach. But, also the computational complexity is significant requirement due to limited resources in most critical systems.

Accordingly, proposing image watermarking approach that provides high level of imperceptibility and robustness with low computational complexity is very desirable to authenticate transmitted images. This requirement can be met by developing either zero-watermarking approaches or spatial domain based image watermarking approaches. Zero-watermarking scheme changes nothing in the original image (i.e. the perceptual quality of image data does not degrade) and requires less computational complexity. As well as, analyzing spatial characteristics of digital image and extracting from it some hidden knowledge that are correlated to the Human Visual System (HVS) helps to identify significant visual locations for watermark embedding. Embedding watermark in significant visual locations of host image using spatial domain has beneficial impact on imperceptibility, robustness, and computational complexity. The color representations, the texture nature, and the structure of image's surface/background are the most important characteristics of digital images.

Zero-Watermarking

The need for a zero-watermarking system in tele-medicine becomes essential to transmit the medical images through an e-healthcare network authentically. The medical images are not subject to any degradation in term of visual quality and also help to avoid any risk of misdiagnosis [106]. A zero-watermarking algorithm does not make any modification in the original image and keeps the same size of the original image [114]. This has positive impact on decreasing the computational complexity. The conflicting requirements in the frequency and the spatial digital watermarking like capacity and perceptual similarity are not taken into consideration in zero-watermarking [114]. Building a watermark in a zero-watermarking scheme is based on extracting key features from the host

image that could be used as image's identification. This does not provide any information that the attacker can use to affect the watermark [114].

Texture Analysis Based Image Watermarking in Spatial Domain

Texture is a complex visual pattern, composed of spatial arrangement entities that describe the color, intensity level, brightness/darkness of overall image or selected region of an image. Any sub-pattern of texture is characterized by given contrast, regularity, roughness, uniformity, frequency, direction and density features. These features play an important role in describing texture in an image and they are correlated to the principles of HVS [66]. Different lightweight intelligence and knowledge discovery methods are used to solve the intangibility of texture property and exploit it to achieve image authentication, through the identification of significant visual locations for embedding the watermark. Indeed, modifications in highly textured blocks in host image due to embedding of the watermark lead to enhance the robustness and imperceptibility ratios [61].

PROBLEM STATEMENT

There are three problems that are addressed in this thesis.

1. The first problem is regarding the design of robust image watermarking approaches with low computational complexity in the spatial domain. The most desirable requirements of image watermarking taken into account in previous literature are the imperceptibility and the robustness. Of course, these requirements are important for any image watermarking approach, but the computational complexity is also a significant requirement due to limited resources of the networks and systems.
2. The second problem is solving the intangibility of texture property for the authentication of images using watermarking. Texture property has many different dimensions and there is no standard method for the texture representation that is adequate for all of its dimensions. Structural, statistical and wavelet transform are three main approaches used to characterize texture. The simplest approach for describing texture is using the statistical features of the intensity histogram of an image or region.
3. The third problem is finding a practical way to measure the importance and the effect of each of used texture features on the results of texture analysis. Identifying the significance of each of used texture features is important process that decides which feature is more preferable and may be recommended to other researchers. Some of knowledge discovery and data mining methods make it possible to measure the significance of each feature by using diverse

Weighting Vectors (WVs) and then defines which WV is more preferable for texture analysis process.

SOLUTION OVERVIEW

In this thesis, we target the design of efficient image watermarking approaches to maintain the authentication of transmitted images over public networks. In most applications, the main requirements of image authentication based on watermarking are the imperceptibility, the robustness and the computational complexity. In order to manage these requirements, the proposed solution is, on the one hand, to extract robust features of host image that allow the design of an efficient zero-watermarking approach, and, on the other hand, to analyze various image characteristics including texture nature, color representations, and relationships between spatial pixels to identify significant visual locations for embedding watermark.

CONTRIBUTION SUMMARY

In this thesis, we study the JPEG file structure and the texture characteristic of digital images. The file structure of JPEG image has a robust feature that could be used to generate a verification watermark in zero-watermarking approach, while texture property is correlated to the HVS. Furthermore, we employ our understanding to address the three problems presented above. The solution proposed in this thesis is the result of work that leads to the following contributions.

1. **Spatial domain based image watermarking**:

   To address problem 1, we propose one zero-watermarking approach and six image watermarking approaches using spatial domain while taking into consideration imperceptibility, robustness and computational complexity. To develop a zero-watermarking approach, a robust image feature and the spatial pixels are used to generate a verification watermark that is able to maintain image authenticity. While, for developing image watermarking approaches, the texture property of image is exploited to identify significant visual image locations for embedding watermark.

   According to the chosen solution, the computational complexity becomes low and the results in terms of imperceptibility and robustness are high. The performance and efficiency of the proposed zero-watermarking solution is evaluated on medical and gray-scale images. While, for the other solutions the performance and efficiency are evaluated on RGB and gray-scale images.

2. **Texture analysis based on intelligence, knowledge discovery and data mining techniques**:

   To address problem 2, we use various lightweight intelligence, knowledge discovery and data mining techniques to solve the intangibility of the texture property and exploit it to achieve image authentication, through the identification of significant visual locations for embedding the watermark. These techniques help to analyze the relationships between the features of texture property and then to define the strongly textured blocks for embedding watermark. This scheme enhances the imperceptibility and the robustness ratios. To accomplish the analysis process, these techniques use a transaction matrix built by computing the values of the texture features, as well as a Boolean matrix built from the transaction matrix by identifying some thresholds representing the texture level corresponding to each texture feature.

3. **Using weight vectors used to measure the importance of texture features**:

   To address problem 3, one of knowledge discovery and data mining techniques makes it possible to measure the significance of each feature by using diverse Weighting Vectors (WVs) for the used texture features. This process defines which WV is more preferable for texture analysis process or which feature is more preferable and may be recommended to other researchers.

THESIS ORGANIZATION

This thesis is organized as follows. Chapter 1 covers key digital image processing fundamentals. Chapter 2 discusses the motivations, the requirements, the framework and the classifications of digital watermarking systems. In addition, the different digital image watermarking techniques, the principles of various attacks on digital image watermarking systems and the performance metrics of digital image watermarking are also presented in this chapter. Chapter 3 reviews several existing image watermarking approaches that are proposed in the literature and aim to provide images authentication and identification. The main contributions of this thesis are presented in chapters 4, 5 and 6. Chapter 4 proposes a zero-watermarking approach, which aims to ensure the authenticity of the transmitted medical and gray-scale images through e-healthcare and public networks based on a robust feature extracted from the host image. Chapter 5 proposes a robust image watermarking approach based on HVS characteristics and rough set theory to authenticate RGB images. Chapter 6 presents five image watermarking approaches exploiting the correlation between texture characteristic and HVS to authenticate gray-scale images. These approaches use different lightweight intelligence and knowledge discovery methods for analyzing texture characteristics. Chapter 7 concludes the thesis and outlines future work.

Part I

BACKGROUND

Chapter 1

DIGITAL IMAGE PROCESSING FUNDAMENTALS

Contents

1.1 INTRODUCTION

Image data processing for storage, transmission and representation for autonomous machine perception is the main essence in digital image processing. Image analysis involves several stages starting from low-level image processing, passing by mid-level image processing and ends with high-level image processing (computer vision). Each level in image processing provides a set of tasks for getting acquainted with basic properties of images, getting acquainted with various representations of image and acquire fundamental knowledge in processing and analysis of digital images.

Low-level image processing involves image acquisition, representation, compression, and enhancement. Mid-level image processing involves pattern recognition, image segmentation and classification. High-level image processing involves image understanding to improve pictorial information for Human interpretation.

All of previous levels require understanding the basic conception of digital image, the representation forms and digital images models, the various image characteristics, intelligent methods and techniques in image processing. Coding

(compression-decompression), image enhancement, restoration, classification, segmentation, geometric correction and digital watermarking are main functions related to image processing tasks.

This chapter introduces a discussion on these issues. The basic concept of digital image and image digitization are presented in section 1.2. Section 1.3 presents the different representation of digital images. The main characteristics of digital image are presented in 1.4. Section 1.5 presents a collection of intelligent methods and knowledge discovery techniques that are used to provide efficient solutions for some tasks related to image analysis. Some of image processing tools are presented in section 1.6 and the chapter ends with conclusion in section 1.7.

1.2 CONCEPTION OF DIGITAL IMAGE

Image is one of the significant information forms that human can perceive visually. Vision allows humans to perceive and understand the world surrounding us.

Basically, information can be represented either in analog way or digital way. Analog refers to information that is continuous and have an infinite number of values in range, while digital refers to information that have discrete state and have only limited number of values.

A flat image is a two-dimensional signal captured from a real-world scene that represents a momentary event from the 3D spatial world and can be observed by Human Visual System (HVS). In other words, a flat image is a projection of 3D scene into a 2D projection plane.

The digital image is a discrete representation of images after a digitization process. Digitizing process aims to digitize a monochromatic $M \times N$ image by defining a discrete representation of analog data suitable for storage and manipulation by a digital computer. Figure 1 presents digitization process of an image.

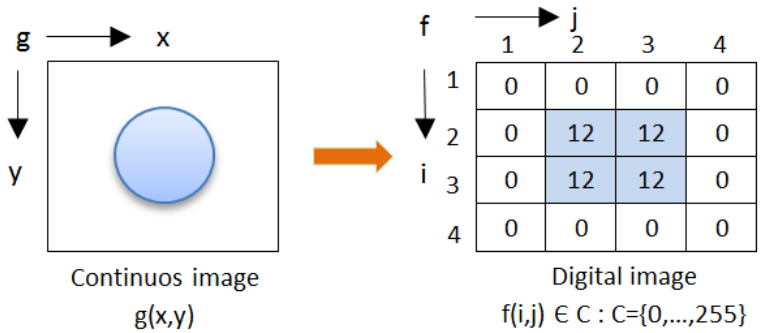


Figure 1: Image digitization process

From figure 1, the digitizing process involves two operations: sampling and quantization. The two operations are illustrated below.

- Sampling operation
  In this operation, when a continuous scene is imaged on the sensor, the continuous image is partitioned into a finite discrete elements called picture elements (pixels). Figure 2 presents the image sampling operation.

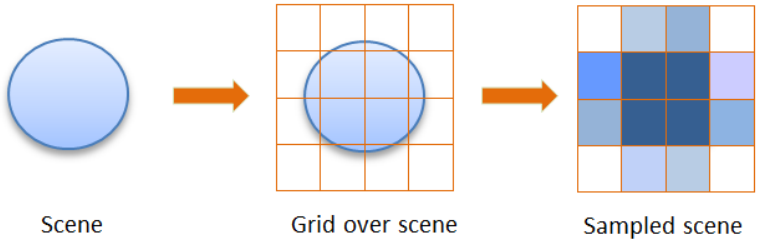


Figure 2: Image sampling.

- Quantization operation
  This operation corresponds to a discretization of the intensity values (number of bits per pixel). The number of gray-levels corresponds to the number of assigned bits per pixel.

  Several quantization approaches are used to achieve image quantization such as uniform quantization and non-uniform quantization (Weber's law) approaches. The uniform quantization approach is applicable when the signal is in a finite range ($f_{max} - f_{min}$). The entire data range is divided into L equal intervals of length Q known as quantization interval. Where Q=$\frac{(f_{max}-f_{min})}{L}$.

  Then, interval i is mapped to the middle value of this interval. The index of quantized value $Q_i(f) = \lfloor \frac{f-f_{min}}{Q} \rfloor$ and the quantized value $Q(f)$=$Q_i(f)Q + Q/2 + f_{min}$. The uniform quantization is optimal for uniformly distributed signal and it is not practical for quantization of signals concentrated near zeros.

  In Weber's law approach, the input data is not uniformly distributed and is quantized according to the human visual sensitivity (high visual and low visual sensitivities). The Weber's law studied responses of humans to physical stimulus in quantitative manner. Figure 3 presents an image quantization operation.

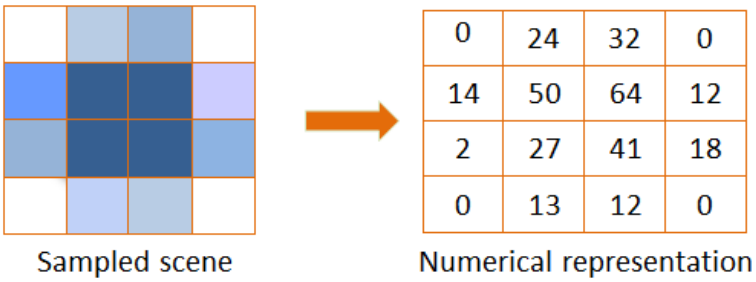


Figure 3: Image quantization.

Figure 3 shows that the digital image of size $M \times N$ is represented by $M \times N$ matrix such as presented below. Each element of this matrix is called *pixel* (picture element), which is a discrete point of light (color) in an image.

Indeed, the digital image can be represented as a scalar function, f from N^2 to N: $f_{i,j}$ gives the intensity (gray-level) value at position (i,j), i and j are two space variables, $i=0,1,\ldots,M-1$ and $j=0,1,\ldots,N-1$. More f_{ij} is large, more corresponding point in image is bright. The function f can take discrete values $x=0,1,\ldots,G-1$, where G is the total number of intensity levels in the image. The total number of intensity levels is $L=2^B$ where B is the number of bits.

$$F = \begin{bmatrix} f_{00} & f_{01} & f_{02} & \cdots & f_{0(N-1)} \\ f_{10} & f_{11} & f_{12} & \cdots & f_{1(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{(M-1)0} & f_{(M-1)1} & f_{(M-1)2} & \cdots & f_{(M-1)(N-1)} \end{bmatrix}$$

Typically, 256 levels (8 bits/pixel) suffice to represent the intensity. For color images, 256 levels are usually used for each color intensity.

Table 1 shows a description for three different bit numbers and corresponding intensity level.

number of bits (B)	intensity level (L)	description
1	2	Binary image (black or white)
6	64	64 levels, limit of human visual system
8	256	Typical gray-level resolution

Table 1: A description for three bit numbers and corresponding intensity levels.

A color image has three channels (red, green and blue) as illustrated in figure 4. The common color resolution for high quality images is 256 levels for each channel, or $256^3=16777216$ colors.

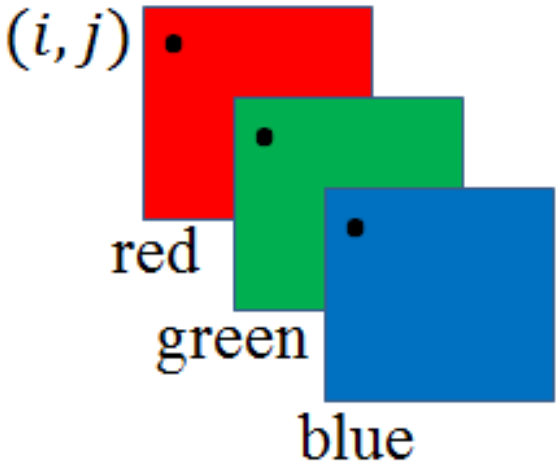


Figure 4: A color image representation.

A color image can be represented as three functions pasted together and can be written as a vector-valued function as follows:

$$F = \begin{bmatrix} red(i,j) \\ green(i,j) \\ blue(i,j) \end{bmatrix}$$

1.3 DIGITAL IMAGE REPRESENTATION

A digital image can be represented in three forms:

- **Binary image (black or white)**
  A binary image has a single plane with 1 bit and 2 intensity levels. In this form $f(i,j) \in \{0,1\}$. Figure 6 presents an example of binary image.

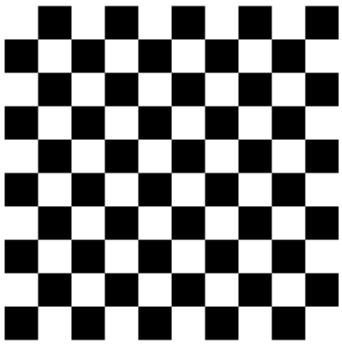


Figure 5: Binary image.

- **Gray-scale image**
  A gray-scale image (monochromatic image) has a single plane with 8 bits and

256 intensity levels. Gray-scale image contains no color information, all shades vary from white to black. In this form $f(i,j) \in C$: $C=\{0,...,255\}$. Figure 6 presents an example of gray-scale Lena image.

Figure 6: Gray-scale Lena image.

- **Color image**
  A color image (chromatic image) has three color planes (red, green and blue), each with 8 bits and 256 intensity levels. In this form $f_{\mathrm{red}}(i,j) \in C$, $f_{\mathrm{green}}(i,j) \in C$, *and* $f_{\mathrm{blue}}(i,j) \in C$: $C=\{0,...,255\}$. Figure 7 presents an example of RGB Lena image.

Figure 7: RGB Lena image with three color planes.

Any color image is represented by many models; RGB, CMYK, HEX, HSV, LAB, and YCbCr are examples of color models.

RGB color model is based on the additive mixture of three monochromatic lights: red, green and blue. This model represents how the computer sees colors. According to the RGB model, each of the three colors (red, green and blue) is represented by a number ranging from 0 to 255. As example, the black color is represented by the '0 0 0' RGB value (red=0, green=0, and blue=0) while the white color is represented by the '255 255 255' RGB value (red=255, green=255, and blue=255). The RGB model can represent more than 16 millions of colors by combinations of RGB values.

CMYK (Cyan-Magenta-Yellow-Key) color model is a subtractive model using blue (cyan), red (magenta), and yellow to mix all colors and adds black (key) as a fourth color. Each of the colors are calculated in percentage from 0 to 100.

CMYK colors are used specifically for printed materials and physical media and are created by combinations of the primary colors, like blending colors on white paper. Given a color in a normalized RGB space as (red, green and blue), the same color in CMY space is given as (Cyan, Magneta, and Yellow). The Key is created from mixing CMY. The following matrix represents the Conversion from RGB to CMY.

$$\begin{bmatrix} C \\ M \\ Y \end{bmatrix} = \begin{bmatrix} 1 - Red \\ 1 - Green \\ 1 - Blue \end{bmatrix}$$

Any color can be decomposed into a brightness component and color component. A brightness component corresponds to the gray-scale version of the color and all other information is 'color' or 'chroma'. In RGB and CMYK models, the brightness and chroma are distributed over each of the three components.

HEX color model is an extension of the RGB model, using hexadecimal numbers to define colors for Hypertext Markup Language (HTML) code. Colors in HEX model are created by combing parts of the three primary colors (red, green and blue). Each of the primary colors can have a value in the range *00* as minimum to *FF* as maximum in hexadecimals. HEX is used specifically for online material and websites and used combinations of the primary colors similar to RGB.

HSV (Hue, Saturation, and Value) color model is the most common cylindrical-coordinate representation of points in an RGB color model. HSV describes the chromaticity or pure color (hue) in terms of their shade (saturation or amount of gray) and their brightness (value of luminance). Saturation range from 0 to 100, the low saturation of a color, the more grayness is present and the more faded in color will appear. Hue is an angular value that ranges from 0 to 360 that is often normalized to be ranged from 0 to 100, where 100 corresponds to 360 degrees. Brightness value is ranged from 0 to 100, 0 represents the white color and 100 represents the black one.

LAB color model stands for Luminance (or lightness) and A, B (which are chromatic components). In this model, A ranges from green to red, and B ranges from blue to yellow. The Luminance ranges from 0 to 100, the A component ranges from -120 to +120 (from green to red) and the B component ranges from -120 to +120 (from blue to yellow). This model was designed to be device independent. In other words by means of this model, colors are handled regardless of specific devices (such as monitors, printers, or computers).

YCbCr color model separates colors into luminance (Y) and chrominance (Cb and Cr) channels. *Y* is luminance, *Cb* is a measure of 'blueness', and *Cr* is a measure of 'redness'.

To convert from RGB to YCbCr, given a color in normalized RGB space [14]. The RGB colors are normalized to values range from 0 to 1. The corresponding 8-bit YCbCr color is given as <Y, Cb, Cr> where

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 65.481 & 128.553 & 24.966 \\ -37.797 & -74.203 & 112.000 \\ 112.000 & -93.786 & -18.214 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix}$$

It is worth to note that *Y* is in range of 16 to 235, while *Cb* and *Cr* are in range of 16 to 240. In practice, scaling is often used to convert into the full dynamic range of 0 to 255. YCbCr color model is used in the JPEG file format and video systems.

1.4 DIGITAL IMAGE CHARACTERISTICS

Digital image processing is done through computerized routines that perform some operations on an image, in order to get an enhanced image (low-level image processing) or to extract some useful information from it (high-level image processing). Particularly, low-level image processing involves transform of one image to another, while high-level image processing involves image understanding and imitating human cognition to make decisions according to information in image.

The digital images have many characteristics that are correlated to the Human Visual System (HVS), these characteristics include: resolution, contrast, color, brightness/darkness, and texture. Human perception of image provokes many illusions, whose understanding provides valuable clues about visual mechanisms.

Understanding digital images and analyzing their characteristics are an important tasks that could be exploited to perform several functions related to image processing. Image characteristics are illustrated in this section.

- **Image resolution**

  Image resolution refers to the number of pixels per inch that determines the quality of the image. This is called *dots per inch* (dpi). In most cases higher resolution (higher dpi) result in better image quality and represents the details contained in an image. Image resolution can always be reduced. Increasing resolution will not improve image quality.

- **Image contrast**

Contrast is the local change in brightness and is defined as the ratio between average brightness of an object and the background brightness. The human eye is logarithmically sensitive to brightness.

- **Image color**

  The color feature deals with the degree of sensitivity of each color space of the host image to the human eyes. The importance of color feature to human visual perception comes due to the biological structure of the human retina. Color refers to the ability of objects to reflect electromagnetic waves of different wave lengths. Human eye can detect colors as combination of the primary colors (red, green and blue). The wave length for red is 700 nm (nano-meters), for green is 546.1 nm, and for blue is 435.8 nm.

- **Image brightness/darkness**

  The brightness/darkness is a relative property of the host image that depends on object surface orientation with respect to the visual perception of the viewer and light source. It expresses the amount of energy output by a source of light and it can be measured by calculating the mean intensity of pixels (higher intensity expresses higher brightness).

- **Image intensity**

  Image intensity is the light energy emitted from a unit area in the image. The gray-scale intensity levels are related to the varying of gray-scale values of neighboring pixels in the host image. This variation in pixel values of neighbored regions has imperfect perceptibility due to the deficiency of contrast. In terms of HVS, the uncertainty and vague gray-scale values may adversely affect image's contrast, then it may weaken the perceptual quality of the image.

- **Image Texture**

  Texture is a complex visual pattern, composed of spatial arrangement entities that describe the color, intensity level, brightness/darkness of overall image or selected regions. Any sub-pattern of texture is characterized by given contrast, regularity, roughness, uniformity, frequency, direction, and density features. These features play an important role in describing texture in an image and they are correlated to the principles of HVS [66].

  Texture property has many different dimensions and there is no standard method for the texture representation that is adequate for all of its dimensions. Texture is usually found in digital images that contain natural scenes or user-made objects. Leaves, grass, stones, twigs, sand, and many other objects create a textured appearance in images. Figure 8 presents some of texture natural images. These images are collected from the USC-SIPI image database[1].

1 USC-SIPI image database, http://sipi.usc.edu/database//

Figure 8: Textured natural images from the USC-SIPI image database.

Texture analysis refers to the characteristics of regions in an image by their texture content. Feature extraction, texture discrimination, and texture classification are three major stages in texture analysis. The feature extraction involves computing the characteristic of digital image able to numerically describe its texture properties. Texture discrimination involves partitioning a textured image into regions, each corresponding to a perceptual homogenous texture. Texture classification determines to which class a homogenous texture region belongs.

Structural, statistical, and wavelet transform are three main approaches used to characterize texture.

Structural approach builds a hierarchy structure of spatial pixels in order to find a set of repetitive texture elements called *texel* occurring in some regular or repeated pattern. Texels are basic texture elements that are determined through some features like gray-levels, shape, edge, orientation, etc.

Statistical approach characterizes the texture through non-deterministic features that govern the distributions and relationships between the gray-scale intensities of an image based on first-order histogram measures or co-occurrence metrics [66][22]. All of these techniques aim to analyze the spatial relations between neighborhood pixels in image regions.

Wavelet transform is a multi-resolution analysis approach, which involves decomposing the image into low and high frequency regions and then extracting the energy values of image regions to characterize the image texture.

Table 2 presents the foundation, description and classification of structural, statistical, and wavelet transform approaches.

	Structural	Statistical	Wavelet transform
Foundation	Human perception and cognition	Statistical decision theory	Multi-resolution analysis
Description	– Morphological primitives – Variable number of primitives – Captures primitive relationships – Semantics from primitive encoding	– Quantitative features – Fixed number of features – Ignores feature relationships – Semantic from feature position	– Based on properties of the Fourier spectrum by identifying high-energy, narrow peaks in the spectrum – Primarily to detect global periodicity
Classification	Parsing with syntactic grammars	Statistical classification	Energy values calculation

Table 2: Foundation, description and classification of structural, statistical, and wavelet transform approaches.

Table 2 shows that the structural approach can work well for regular patterns. It requires the setting of morphological primitives and their relationships. The statistical approach can work well for random patterns (edge density, histogram features, etc) and is used more often in practice. It depends on image intensity domain to calculate some features that help to define texture semantics. The wavelet approach work well for texture analysis with random nature based on Fourier spectrum properties to detect global periodicity.

The simplest approach for describing texture is using the statistical features of the intensity histogram of an image or region. Using first-order histogram measures will result in measures of texture that carry only information about distribution of intensities, but not about the relative position of pixels with respect to each other in that texture. The co-occurrence matrix helps to provide significant information about the relative position of the neighboring pixels in an image [27]. Gray-Level Co-occurrence Matrices (GLCM) is a method used for texture feature extraction. It represents the distributions of the intensities and the information about relative positions of neighboring pixels of an image [91].

1.5 INTELLIGENT METHODS AND TECHNIQUES IN DIGITAL IMAGE PROCESSING

A collection of methodologies, complementary and synergistic, which are capable to identify simple algorithms to produce efficient solutions for various problems are becoming the focus of attention for researchers in different fields.

The concepts and paradigms of Computational Intelligence (CI), Soft Computing (SC), Artificial Intelligence (AI), knowledge discovery and data mining [9][40][5][99][4] provide intelligent techniques to develop simple algorithms with efficient solutions for various issues, especially those related to system optimization, pattern recognition and intelligent control systems.

Substantially, all CI, knowledge discovery and data mining techniques are iterative and interactive. Indeed, all of these techniques work in multiple passes and require human interaction in the loop.

CI has a close relation with AI. The difference between them is that CI employs a sub-symbolic knowledge to design a simple algorithm to provide an efficient solution for a given problem, while AI uses symbolic knowledge that focuses on finding the best output ignoring the complexity of the proposed algorithm. From the viewpoint of vague and uncertainty concepts, CI is based on numerical and partial set of knowledge (uncertain and incomplete knowledge) that is produced from a given problem, while AI is based on a full knowledge representation decomposed into semantic concepts and logic that are close to the human reasoning. Problems connected with mining, clustering, reduction and associations are usually solved by CI and knowledge discovery techniques, while speech recognition, robots, handwriting recognitions and gaming problems are solved by AI techniques [9][40].

The SC principle involves all algorithms that are designed to provide a foundation for the conception, design and deployment of intelligent systems. The soft computing methodologies are designed to find efficient solutions for intelligent systems based on uncertain and vague knowledge [9].

The CI combines mainly three techniques including Artificial Neural Networks (ANNs), evolutionary computing, and fuzzy systems. ANNs are inspired by the biological nervous systems, and are learning and adaptive structures used for information processing when it is difficult or not possible to define a set of rules related to a specific problem. The learning task in ANNs is classified into three paradigms; supervised, unsupervised and reinforcement learning. The Back Propagation ANN algorithm (BPANN) [50] is a supervised learning algorithm that learns by processing the training sets to find approximately optimal network's weight, which is used in turn to enable the algorithm to produce desired output with minimum error. In unsupervised learning methods there is no desired output associated with the training set. It is used usually in clustering

and compression applications. The reinforcement learning paradigm is close to supervised learning, except that the change of the network's weight is not related to the error value. Commonly, ANNs-based techniques are applied in classification, frequent pattern and approximation functions to solve many application problems such as medical diagnosis, image processing, pattern recognition and data mining.

Evolutionary algorithms are based on the techniques of natural selection and biological evolution. These techniques involve representable and objective functions. Evolutionary algorithms are used when brute-force search is not practical. They are useful for multi-parameter optimizations. The Genetic Algorithm (GA) is one of the important kinds of evolutionary algorithms.

The fuzzy theory is a heuristic-based approach aiming to introduce efficient solutions based on a set of rules and fuzzy membership function. The fuzzy rules deal with incomplete and inexact knowledge such as the concepts of bigger, taller or faster. Fuzzy sets, fuzzy logic, and rough sets are the most important techniques in the CI, and they can be combined to give a definition for vagueness and imprecise knowledge in different fields [79][128][132]. Extracting hidden patterns from data, medical diagnosis, pattern recognition, image classification and intelligent dispatching are set of application whose design can be based on fuzzy sets, fuzzy logic and rough sets techniques.

Knowledge discovery and data mining is the automatic extraction of valid, useful, understandable knowledge from large volumes of data. The extracted knowledge could be patterns, models, rules, etc. Generally, data is represented as a string of bits, numbers and symbols, while information are data stripped of redundancy, and reduced to the minimum necessary to characterize the data. Knowledge is an integrated information, including facts and their relations, which have been perceived, discovered, or learned in human mental view. Multi-Criteria Decision-making (MCDM), Formal Concept Analysis (FCA), Frequent Pattern Mining (FPM), and Association Rule Mining (ARM) are the most important techniques in knowledge discovery and data mining that help end users to extract useful knowledge from large databases.

MCDM is a branch of Operational Research field (OR) whose aim is to provide solutions for many complex decision-making problems that are characterized as a choice among many alternatives to find the best one based on different criteria and decision-maker's preferences [21]. The importance of this study comes due to the difficulty to deal with traditional paradigm in analyzing decision making which is based on uni-dimensional and only one criterion to make a decision. Many problems in our life involve multiple objectives and criteria. These problems are related to the fields of engineering, industry, commercial, and human resource management.

FCA is a technique used to analyze, investigate and process explicitly given information, to allow for meaningful and comprehensive interpretation [81][5]. FCA studies how objects can be hierarchically grouped together according to their common attributes. A concept is a cognitive unit of meaning or a unit of knowledge. FCA has been applied to solve many problems related to automatic modularization, management of component repositories, reverse engineering and program understanding.

FPM is one of the most important search approaches in computational and algorithmic development. It deals with finding the maximal relevant items that are frequently occurring together within a transaction database. One of the popular examples that uses the frequent pattern mining is the basket data analysis, where the mining method is normally used to analyze the regularities of shopping behavior of customers and then to find sets of relevant products that are often purchased together. The extracted frequent patterns may then be expressed as an association rule, which has a valuable role to improve the arrangement of products in the shelves, and helps decision makers in advantageous actions regarding shelf stoking or any recommendations to add other products [4].

ARM is a data mining technique that aims to discover implicit knowledge and hidden relations between data items in large databases. Primarily, the association rules were used in the marketing field to discover set of hidden frequent patterns of products that are purchased together by customers. The extracted hidden patterns support the decision-makers to enhance the marketing process through useful actions for shelf stocking and recommendations to add other products [102].

CI, knowledge discovery and data mining techniques exhibit many capabilities to adapt and provide multimodal solutions for many complex systems. Although many CI, knowledge discovery and data mining-based models are developed in the fields of fault diagnosis, image classification, recommendation system and intelligent control system, the employment of these techniques in the field of security and authentication of transmitted multimedia data over the networks is confined, in spite of their significance.

1.6 DIGITAL IMAGE PROCESSING TOOLS

The different image processing tasks such as image enhancement, feature extraction, pattern recognition, image classification, geometric correction, and multiscale signal analysis are applied through set of image processing tools. This section presents some of these tools.

1. MATLAB (Matrix Laboratory)

MATLAB is a multi-paradigm numerical computing environment, where a proprietary programming language is developed by MathWorks. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, C#, Java, Fortran and Python.

The image processing Toolbox in Matlab provides a comprehensive set of standard reference algorithms and applications for image processing, analysis, visualization and algorithm development. The operations you can perform include image segmentation, image enhancement, geometric transformations, image registration, and 3D image processing.

Via Matlab the user can interactively segment image data, compare image registration techniques, and batch process large amounts of data. Applications and visualization capabilities are provided to explore images, 3D volumes, and videos, adjust contrast, create histograms, and manipulate Regions of Interest (ROI).

2. Concept Explorer (ConExp)

   ConExp was first developed as a part of master thesis under the supervision of Professor *Tatyana Taran* at the National Technical University of Ukraine (KPI) in 2000 [129]. Through the following years, ConExp was extended and became an open source project on Sourceforge[2].

   ConExp is mainly developed to implement basic functionality needed for study and research of Formal Concept Analysis (FCA). FCA takes as input a matrix specifying a set of objects and attributes, and then finds both all the clusters of attributes and all the clusters of objects in the input data in order to allow for meaningful and comprehensive interpretation.

   Generally, ConExp provides several functionality including: context editing, building concept lattices from context, finding bases of implications that are true in context, finding bases of association rules that are true in context and performing attribute exploration.

1.7 CONCLUSION

Digital image processing relies on computerized routines for information extraction from images to obtain categories of information about specific features. Digital image processing provides different functions including: coding, image enhancement, restoration, classification, segmentation, geometric correction and digital watermarking.

2 SourceForge is an Open Source community resource, http://www.sourceforge.net

The different representation forms of digital images and the various image characteristics are main requirements to define set of parameters that can be manipulated by several intelligent techniques to achieve different functions of image processing.

The basic conception of digital image, the representation forms of digital images, the various image characteristics, the intelligent methods for image processing have been discussed in this chapter. As well as, two of common image processing tools that are used in implementation of different algorithms of digital image processing functions have been presented in this chapter.

Chapter 2

DIGITAL IMAGE WATERMARKING

Contents

2.1 INTRODUCTION

The rapid growing of digital media (images, audio and video) has urged for the need of protection. Three generic techniques are proposed to protect multimedia data: cryptography, steganography and watermarking. Cryptography is the most common method used to protect digital content, it involves transforming the original data D into another form Dc such that only the authorized user can recover D from Dc. Steganography and watermarking are two information hiding techniques, steganography aims to hide the important secret information called watermark in a carrier signal in such a way that no one apart from the authorized recipient knows on the existence of the information (i.e. the existence of watermark in digital data is concealed), whereas for watermarking, the hidden information (watermark) may be visible and the carrier signal is the important information.

Information hiding techniques involve hiding a watermark w in the original data D (the result is a watermarked data denoted Dw) such that in case of water-

marking, an attacker can not remove or modify or replace the watermark w in Dw, whereas for steganography, an attacker can not detect the presence of watermark in the watermarked data. Two major issues are solved using information hiding techniques including: protection of multimedia data from malicious use and avoiding observing secret data by unintended recipients.

Digital watermarking has much interest than other protection techniques due to the increase in concern over authenticity, integrity and copyright protection. In digital watermarking, the original data is visible and readable from all users, while the secret information is changeable and readable by the authorized user only. Cryptography techniques cannot help the owner of digital content to monitor how a legitimate user handles the content after decryption, but the digital watermarking can protect content even after it is decrypted.

This chapter introduces a discussion on the motivations of digital watermarking in section 2.2, then the requirements of digital watermarking systems are presented in section 2.3. The framework of digital watermarking is illustrated in section 2.4, and the classifications of digital watermarking are presented in section 2.5. Section 2.6 presents the different digital image watermarking techniques and section 2.7 introduces the principles of various attacks on digital image watermarking systems. The performance metrics of digital image watermarking are presented in section 2.8 and section 2.9 presents one benchmark of digital image watermarking. This chapter ends with conclusion in section 2.10.

2.2 MOTIVATIONS FOR DIGITAL WATERMARKING

Due to many dilemmas, digital watermarking has become an urgent need for multimedia data protection. Two of these dilemmas are presented below:

- digital data are rapidly revealed and generating identical but unauthorized digital data becomes more easy to be falsified.
- digital data can be manipulated, transmitted and copied easily by anonymous users with no way to identify the malefactors.

These dilemmas are related to many applications like tele-medicine and remote sensing imaging. Medical data can be transmitted between hospitals, which are located at various locations, for many reasons, such as tele-diagnosis, teleconferences between clinicians and medical consultation, remote learning and training. As well as, remote sensing system can transmit multimedia data between different administrative organizations, which are located at various locations, for many purposes, such as decision making, criminals discovering and forecasting about some actions by the experts.

Medical data and remote sensing data can be intentionally and unintentionally manipulated by unauthorized users [82]. Protecting these data is an important

need to obtain right treatments and decisions. Inserting watermark in original data may cause loss of important details that have impact on the decisions of doctors and the experts [115].

Encryption and other access control techniques are difficult to conform to the constraints of the medical data security and protection [95]. Digital watermarking is an effective solution for this problem. It can efficiently address the essential requirements of the medical or remote sensing data protection including the issues of unique identification, authentication, copyright protection and integrity verification during transmission through insecure networks and storage in large databases [95].

2.3 DIGITAL WATERMARKING REQUIREMENTS

Several requirements are essential for designing a general watermarking approach. These requirements include: security, reliability, imperceptibility, robustness, data payload, computational complexity and reversibility. This section describes these requirements as follows:

1. Security

   Security requirement involves that the watermarking approach has the capability to resist to intentional attacks. These attacks can be classified into three groups: unauthorized removal, unauthorized embedding and unauthorized detection. Eliminating, masking and collusion attacks are examples of unauthorized removal attacks, while embedding forgery watermark in multimedia data that should not contain watermark is an example of unauthorized embedding attack. Unauthorized detection attack involves that unauthorized user can extract the watermark without having a full knowledge about the embedding algorithm. The watermarking approach should guarantee that only the authorized user can extract or remove the embedded watermark. As well, the watermarking approach should prevent false-positive alarm, which involves watermark detection in a digital data that is actually unmarked.

2. Reliability

   This requirement encompasses two principles: the authentication and the integrity. The authentication involves the ability to proof the origin of data and its attachments to one user, while the integrity involves the capability to proof that the data has not been altered or modified either maliciously or accidentally by unauthorized user.

3. Imperceptibility

   Imperceptibility, referred to invisibility, which is one of the most desired requirements in watermarking approaches. The watermark should be embed-

ded with least content quality degradation and in an invisible way as much as possible to the human eye. The imperceptibility rate is expressed by computing the perceptual similarity between the original data and the watermarked data. High imperceptibility ratio expresses low distortion in the perceptual quality of the original data.

4. Robustness

   This requirement involves the ability of watermarking approach to extract the embedded watermark after common signal processing operations. These attacks can be classified into two groups: intentional (malicious) and unintentional attacks. These attacks aim to remove or destroy the embedded watermark or even to prevent the watermark from fulfilling its expected purpose. Not all digital watermarking applications require to withstand all signal processing attacks. An example of watermarking approach where robustness is undesirable is fragile watermarking approach.

5. Data Payload (Capacity)

   This requirement refers to the number of watermark bits that can be embedded in the original data without affecting the original data quality and can be detected. Embedding multiple watermarks implies more data payload and more robustness to avoid the risk caused by easily changing watermarks since watermarks can be replicated.

6. Computational Complexity

   This requirement refers to the number of steps and the amount of computation required for embedding and extraction processes. For real-time application both fast (low complexity) and efficient algorithms are required.

7. Reversibility

   This requirement guarantees the extraction of watermark along with exactly reconstructing of the unmodified original data. To achieve this requirement, the watermarked should be distortion-free and the extraction process should be reversible. This requirement is important for some applications like telemedicine or remote sensing systems. Indeed, the medical data should not be altered for tele-diagnosis and treatment purposes, as well the remote sensing data should not be altered for right decision making.

2.4 DIGITAL WATERMARKING FRAMEWORK

The basic model of the digital watermarking scheme consists of three components: watermark generation, watermark embedding and watermark extraction [82]. The watermark generation are showed in figure 9, while the watermark embedding and extraction are presented in figure 10.

2.4.1 *Watermark generation*

This function creates a suitable watermark according to the desired applications. In simple applications, the watermark can be a text, logo or binary code. In the sophisticated applications, the watermark may have particular properties based on the desired objectives. For example, in medical application, the watermark may need to combine the patient information or some features of medical data to ensure the identification, authentication and integrity of the watermarked data.

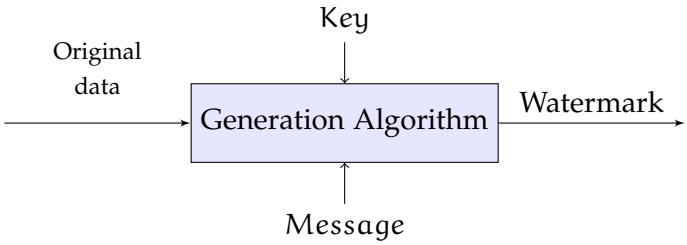


Figure 9: Watermark generation components.

Figure 9 shows that the original data, specific user message and secret key are three parameters that may be used in the generation algorithm of watermark. Some or all of these parameters are required to generate the watermark; the selection of required parameters depends on the application targeted.

2.4.2 *Watermark embedding*

The watermark embedding process is achieved at the sender side. In this step, the watermark is added to the original data (image, audio and video) by applying a certain algorithm and using a secret key. The result of watermark embedding process is a watermarked data.

2.4.3 *Watermark extraction*

The watermark extraction process is achieved at the receiver side. In this step, the reverse implementation of watermark embedding algorithm is applied to extract the embedded watermark from watermarked data or to identify whether any other watermark is embedded in the data. The watermark extraction algorithm use the secret key and/or the original data to detect/extract the embedded watermark.

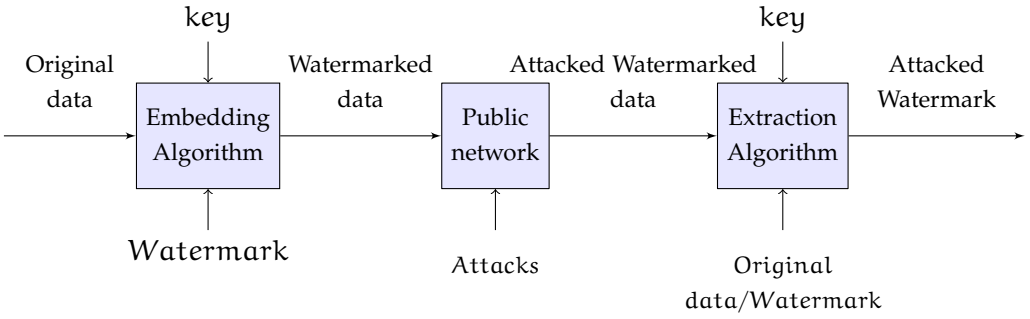


Figure 10: Main components of watermarking schemes.

Based on figure 10, the watermark embedding deals with three elements: original data (*D*), watermark (*W*) and secret key (*K*) to generate the watermarked data (*Dw*) (i.e. watermark embedding (D, W, K)=Dw). The watermark extraction algorithm deals with two or three elements including: attacked watermarked data (Dw'), secret key (K) and/or original data (D) or watermark to extract the watermark (W') after attack (i.e. watermark extraction (Dw', K, D or W)=W'). The extracted watermark *W'* is compared with the original watermark *W* to find correlation and to ensure the reliability of digital data.

2.5 DIGITAL WATERMARKING CLASSIFICATION

Digital watermarking approaches can be classified into many categories including: data type, embedding domain, human perception and reversibility. These categories are presented in figure 11. Digital watermarking can be applied on different data types such as text, image, audio and video. The digital watermarking approaches can be designed in spatial, transform or spread-spectrum domains. According to the human perception, digital watermarking can be classified into visible, invisible and dual approaches. Invisible watermarking approaches can be further classified, based on their robustness, into four categories: fragile, semi-fragile, robust and hybrid. In addition to the previous classifications, digital watermarking approaches can be classified into reversible and irreversible categories. The reversibility are in relationship with lossy and lossless feature of digital watermarking approaches.

The main classification of digital watermarking approaches are discussed in the following subsections.

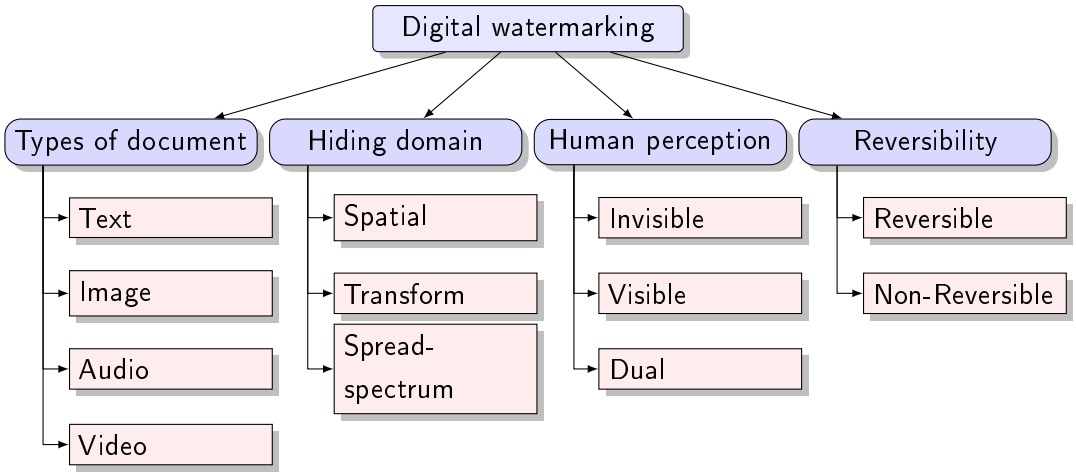


Figure 11: Digital watermarking approaches classification based on the data type, domains of hiding the watermark, human perception and reversibility aspects.

2.5.1 *Data type based categorizations*

Text, image, audio or video watermarking refers to embedding watermarks in text/image/audio/video in order to protect the data content from copying, transmitted or manipulated anonymously.

In text watermark, the varying spaces after punctuation, spaces between lines and the spaces at the end of sentences could be significant features used to generate the watermark or to find proper locations in text for embedding watermark. In audio, image and video watermarking, the watermark could be embedded in the low/high frequency coefficients of frequency domain or could be embedded directly in the least significant bits of spatial data.

2.5.2 *Human perception based categorizations*

Based on human perception property, digital watermarking approaches are classified into three categories: visible, invisible and dual approaches. In visible watermarking, the watermark is inserted into the original data in such a way that it is visible to the human eye. Visible watermark is used to indicate the ownership of multimedia data. The logo or seal of the organizations, which are stamped on the documents, images, video or TV channels for content and ownership identification are the most popular examples of visible watermarks.

In invisible watermarking, the watermark is inserted into the original data in such away that is intended to be imperceptible to the human eye. Invisible watermark can be detected only though watermark extraction algorithm and is suitable for many purposes including: ownership identification, authentication and integrity verification.

In some applications, visible and invisible watermarks can be applied together. This procedures is called the dual watermarking, and in this situation, the invisible watermark is assumed as a backup for the visible one.

2.5.3 *Robustness based categorizations*

Based on the robustness of digital watermarking, the invisible watermarking approaches can be divided into four categories: robust, fragile, semi-fragile and hybrid techniques.

Robust watermarking approaches are intended to survive various manipulations on data content via unauthorized removal, unauthorized embedding and unauthorized detection attacks as well as to fulfill their expected purpose. Robust approaches are typically used to detect misappropriated data for data authentication and integrity.

In fragile watermarking approaches, the watermark is intolerant to slight modifications. This approaches are usually used to verify the integrity of data. The tamper proof is one benefit of fragile watermarking; losing watermark implies tampering occurred.

The semi-fragile watermarking approaches achieve moderate robustness against designated class of attacks. In these approaches, the watermark resist unintentional modifications, but it fails after intentional malicious modifications. This kind of approaches can be used to verify the reliability (authentication or integrity) of data content. Some watermarking approaches may combine the fragile and robust methods to achieve the authenticity, integrity and ownership protection simultaneously.

Generally, invisible robust watermarks are used to detect misappropriated data, data authentication such as evidence of ownership, while the invisible fragile watermarks are used to verify the integrity of data content.

2.5.4 *Extraction based categorizations*

The digital watermarking approaches, based on extraction techniques, can be classified into three categories: blind, semi-blind and non-blind watermarking. The blind watermarking approaches need only robust key to extract the watermark from the attacked watermarked data. These approaches are known as public approaches, since they use a public key in the extraction process. Comparing with other types of watermarking approaches, the blind approaches require less information storage at receiver side. The source end will send only the public key and the watermarked data.

The semi-blind watermarking approaches require the original watermark and the key to extract the embedded watermark from the watermarked data. These

approaches are known as semi-private approaches, because the original watermark is shared between the sender and the receiver.

The non-blind watermarking approaches require the original watermark, the key and the original data to extract the embedded watermark from watermarked data. These approaches are known as private approaches, where the watermark is usually generated from the original data itself. This kind of watermarking is more preferable for tamper-proof application.

2.5.5 *Reversibility based classification*

The reversibility is an important requirement for some applications that deal with sensitive digital data such as medical, military and law-enforcement applications. The reversible watermarking approaches guarantee extraction of both the embedded watermark and the original data exactly from the watermarked data. For tele-diagnosis purpose, the medical data should not be altered and for decision making purposes the military and law-enforcement data should not be changed. The reversibility requirement is met in lossless scheme of digital watermarking.

In contrast, the irreversibility refers to extract the embedded watermark and the original data from watermarked data but not exactly as to the original ones. The irreversibility requirement is met in lossy scheme of digital watermarking. The lossless and lossy schemes of digital watermarking are discussed below.

- Lossless watermarking

  In lossless watermarking schemes the original data can be recovered in exact after the process of removing the hidden data (like text, logo, patient's record, etc.) [105]. Zero data loss when no attacks are applied on watermarked data proves lossless property [95]. This type of watermarking schemes is very desirable in some applications like medical and military systems since slight change in the original data may affect the decision making process [13].

  To protect the copyright of these kinds of data, lossless watermarking scheme are proposed to embed the watermark in the original data without changing data content or in other words with less data quality distortion. Lossless watermarking schemes can be divided into two categories: zero-watermarking and reversible watermarking [33]. Zero-watermarking schemes have good lossless feature and better robustness than the reversible watermarking schemes. Zero-watermarking approaches utilize unique features of original data to build the watermark, they do not make any modification in the content of the original data. The unique features of original data should not be significantly affected with different attacks and they should enable to reconstruct the watermark.

Most of the reversible watermarking approaches require lossless environment to transfer the watermarked data because any change on the watermarked data due to intentional or unintentional attacks can destroy the hidden watermark. The reversible watermarking scheme should have the ability to recover the watermark even if the watermarked data is exposed to attacks. For any reversible watermarking approach the attacks should be unintentional attacks. The reversible watermarking approaches that can convey the embedded watermark through lossy environment are called robust.

- Lossy watermarking

  In lossy watermarking schemes, the watermark is embedded in the original data by replacing or altering some data details like replacing Least Significant Bits (LSB) or altering the transform coefficients of frequency domain [13]. In this case, the original data can not be reversed due to the modifications caused by the inserted watermark. This type of watermarking is usually designed to authenticate data, verify the integrity and identify data ownership [84]. Embedded watermark in lossy watermarking schemes usually impairs the data quality, but is more robust than lossless watermarking schemes. This can be explained due to embedding watermark around the edges or in other significant visual locations of original data.

2.6 DIGITAL IMAGE WATERMARKING TECHNIQUES

Embedding watermark in original data takes place in three main domains: spatial, transform and spread-spectrum. The different techniques for embedding watermark in each domain and the properties of each technique are presented in this section. One can note that this section concentrates more on the significant properties of each technique to success digital image watermarking (i.e. fulfilling most requirements of digital image watermarking).

2.6.1 *Spatial domain techniques*

In theses techniques, the watermark is embedded in the original data by directly modifying the pixels values. The algorithms related to this domain are fast, simple and offer wide embedding capacity. As well, this domain allows embedding watermark many times to provide additional robustness against different attacks, especially the geometric attacks like cropping, translation and rotation, because the possibility of removing all watermark becomes low. The main drawback of spatial domain based watermarking approaches is that they can not survive against many removal attacks like noise addition, sharpening, blurring and median filtering. Additionally, discovering the used embedding technique

allows the attacker to change or alter the hidden watermark more easily. The different techniques for embedding watermark in spatial domain are presented below:

A *Least Significant Bit (*LSB*)*

Least Significant Bit (LSB) uses the least significant bits of each pixel in one image to hide the most significant bits of another. Pixels may be chosen randomly according to a key. LSB based image watermarking approach starts by loading up both the host image and the watermark you need to hide, then the LSB of the host image is replaced with the watermark bits. LSB method results in watermarked image that contains hidden watermark that appears to be high imperceptible. LSB method provides an effective transparent embedding technique and good correlation properties for watermark detection, but with high sensitivity to removal attacks. Additionally, LSB method is inexpensive computationally.

B *Local binary pattern*

Local Binary Pattern (LBP) is a feature used in 2D texture analysis and object/-pattern detection. The basic idea of LBP is to summarize the local structure of an image by comparing each pixel with its neighborhood pixels. Initially, the host image is partitioned into non-overlapping square blocks. Then, the local pixel differences between the central pixel and its circularly neighborhood in each block are calculated. Using the center pixel as a threshold, the neighborhood pixel is labeled as 1 if its intensity is greater than the threshold, else labeled as 0. In the end of this process, LBP produces a binary code of 8 bits from 0-255 just like '10011010'. With 8 surrounding pixels, there are 2^8 possible combinations. These codes are called LBP codes. The produced LBP code represents a texture spectrum of an image block with 256 gray-levels, this code is often used to extract image features for classification or recognition [121].

LBP method could be used to measure the local contrast between the neighborhood pixels and to ensure the authenticity of digital image. The LBP codes are utilized for embedding the watermark bits. LBP based methods are robust against luminance variation and contrast adjustment, but fragile against other operations like blurring and filtering. In other words, this technique is suitable for semi-fragile watermarking applications.

C *Histogram modification*

Histogram modification method is based on the pixel values to build the histogram of image and utilizes the redundancy of the host image statistical information to hide secret data. This method hides the watermark by shifting the peak and zero points of the image histogram. This method can be implemented

easily, but the capacity is limited to the number of peak and zero points in the histogram.

The histogram modification method is extended by pixels differences model or multi-layer embedding model to improve its performance. The pixels differences are calculated, then the histogram of pixel differences is generated. The histogram is shifted by embedding the secret data and the marked pixel difference is generated. The extraction process is performed in the reverse order of the embedding process and the information about the peak and zero points should be sent to the receiver for reversible recovery.

2.6.2 *Transform domain techniques*

There are various methods used to process 1D or 2D signals, these methods divide the signal into frames and for each frame invertible transform is applied to compresses the information into set of coefficients. The transformation methods introduce many benefits including: fast computation, efficient storage and transmission due to energy compaction or pick a few representatives as a basis for processing. As well, the transformation methods allow better image processing by taking into account the correlations of pixels in space and conceptual insights in spatial-frequency information.

Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) are common transformation methods. This section presents the basises of these methods.

A *Singular Value Decomposition (*SVD*)*

Singular value decomposition on a matrix A of rank ρ and of dimension $M \times N$ creates a diagonal matrix S and unitary orthogonal matrices U and V whose column vectors are u_i and v_i, correspondingly [7].

The columns of U are orthogonal eigenvectors of AA^T and the columns of V are orthogonal eigenvectors of A^TA. The orthogonal matrix U has dimension as $M \times M$, while the orthogonal matrix V has dimension as $N \times N$. The eigenvalues $(\lambda_1,...,\lambda_r)$ of AA^T are the eigenvalues of A^TA, where $r=N \times N$.

For A with rank ρ, the singular value $S = diag(\sigma_1,\sigma_2,...,\sigma_\rho)$ satisfies $\sigma_1 \geqslant \sigma_2 \geqslant ... \sigma_\rho \geqslant \sigma_{\rho+1}=...= \sigma_n=0$, where $\sigma_i = \sqrt{\lambda_i}$: $i=1,...,n$ and $n=M \times N$. The matrix S contains non-negative diagonal elements in descending arrangement and has similar dimensions as A. All eigenvalues of a positive matrix are non-negative.

The three matrices after SVD decomposition of $M \times N$ matrix are illustrated as follows.

$$SVD(A) = USV^T = \begin{bmatrix} u_1, u_2, ..., u_n \end{bmatrix} \begin{bmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & \ddots & \\ & & & \sigma_n \end{bmatrix} \begin{bmatrix} v_1, v_2, ..., v_n \end{bmatrix}^T$$

As example let us take

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$$

where M=3 and N=2, then

$$SVD(A) = \begin{bmatrix} 0 & 2/\sqrt{6} & 1/\sqrt{3} \\ 1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 1/\sqrt{2} & 1/\sqrt{6} & -1/\sqrt{3} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{3} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

SVD has many algebraic properties that are very much desirable for different image processing functions like image coding, image enhancement and image reconstruction. These properties are explained as follows:

- Transpose.

  A matrix A and its transposed A^T have the same non-zero singular values.

- Translation.

  A matrix A and its translated counterpart A_{tr} have the same non-zero singular values. A_{tr} is obtained from A after adding some rows and columns of zero (black) pixels.

- Flipping.

  A matrix A and its flipped counterpart A_f have the same non-zero singular values. A_f is obtained from A after flipping around vertical axis and horizontal axis.

- Rotation.

  A matrix A and its rotated counterpart A_r have the same non-zero singular values. A_r is obtained from A after rotation in arbitrary angle θ.

- Scaling.

  For a matrix A of dimension $M \times N$ that has the singular values (σ_1,σ_2,...,σ_n); its scaled counterpart A_s has the singular values equal to ($\sigma_i^* \sqrt{S_{row} S_{column}}$) where S_{row} is the scaling factor of rows and S_{column} is the scaling factor of columns.

- Stability.

  Let A and B are two matrices each of dimension $M \times N$ and their corresponding singular values are $(\sigma_1,\sigma_2,...,\sigma_n)$ and $(\nu_1,\nu_2,...,\nu_n)$, respectively. Then, a relation of $|\sigma_i\text{-}\nu_i| \leqslant \|\text{A-B}\|_2$. This relation indicates that the singular values of a matrix have high stability; the variation of its singular values due to little disruption is not grater than 2-norm of disturbance matrix.

Moreover, SVD provides many attractive properties correlated to HVS. Singular values stand for the luminance of the image while variance measures the relative contrast and smoothness of the intensity in the image [7].

All of the mentioned properties of SVD are desirable for designing watermarking algorithms that are particularly preserving perceptual quality of host image and watermarking robustness to geometric attacks. Little disruption in singular values do not cause noticeable image quality distortion, as well the geometric properties of singular values do not get modified after exposing to different kind of geometric image processing attacks [7][60].

B *Discrete Wavelet Transform (*DWT*)*

Wavelet transform decomposes a signal into a set of basic functions called wavelets. Wavelet is a finite interval function with zero mean suited to analysis of transient signals. Wavelets are general way to represent and analyze multi-resolution images, and are as well applied to 1D signals. In signal processing and especially in the domain of medical applications, wavelets make it possible to remove noise and to recover weak signal from noise. As well, in the domain of the Internet communication, wavelets are useful for image compression.

The discrete wavelet transforms a discrete time signal to a discrete wavelet representation. Indeed, it converts an input series $(x_0,x_1,...,x_n)$, into one low-pass wavelet coefficient series (L) and one high-pass wavelet coefficient series (H) of length $n/2$ for each. These chains are given according to the equations 1 and 2, respectively.

$$L_i = \sum_{n=0}^{k-1} x_{2i-n} \times t_n(z) \tag{1}$$

$$H_i = \sum_{n=0}^{k-1} x_{2i-n} \times s_n(z) \tag{2}$$

where $t_n(z)$ and $s_n(z)$ are called wavelet filters, k is the length of the filter, and $i=0, ..., [n/2]-1$. The choice of the filter determines the shape of the wavelet that uses to perform the analysis.

DWT has gained widespread use in image processing and image compression due to their inherent multi-resolution decomposition. The multi-resolution analysis involves analyzing the signal at different frequencies and giving different

resolutions. The multi-resolution analysis gives good frequency resolution and poor time resolution for low frequency components of the signal, while it gives good time resolution and poor frequency resolution for high frequency components of the signal.

For multi resolution decomposition of an image A of dimension $M \times N$, the DWT decomposes down an image into four sub-bands LL, HL, LH and HH in first level. Each sub-band has dimension $M \times N$, such as LL={LL(i,j): $0 \leqslant i \leqslant M$, $0 \leqslant j \leqslant N$}. LL(i,j) represents a pixel value located in *i-th* row and *j-th* column in sub-band LL.

The LL is the Low-Low (approximation) sub-band. It indicates the major energy of an image that is concentrated in the lowest frequency coefficients. While, LH is Low-High (horizontal detail) sub-band, HL is High-Low (vertical detail) sub-band and HH is High-High (diagonal detail) sub-band give the missing details (finest scale) coefficients. The approximation band (LL) has high-scale, low frequency components of the signal, while each of the details sub-bands (HL, LH and HH) has low-scale, high frequency components of the signal.

If further decomposition is desired, the sub-band LL can be further decomposed down into four sub-bands LL2, HL2, LH2 and HH2. The progression is sustained until a preferred level is reached. The two-level wavelet decomposition of gray-scale Lena image is shown in figure 12.

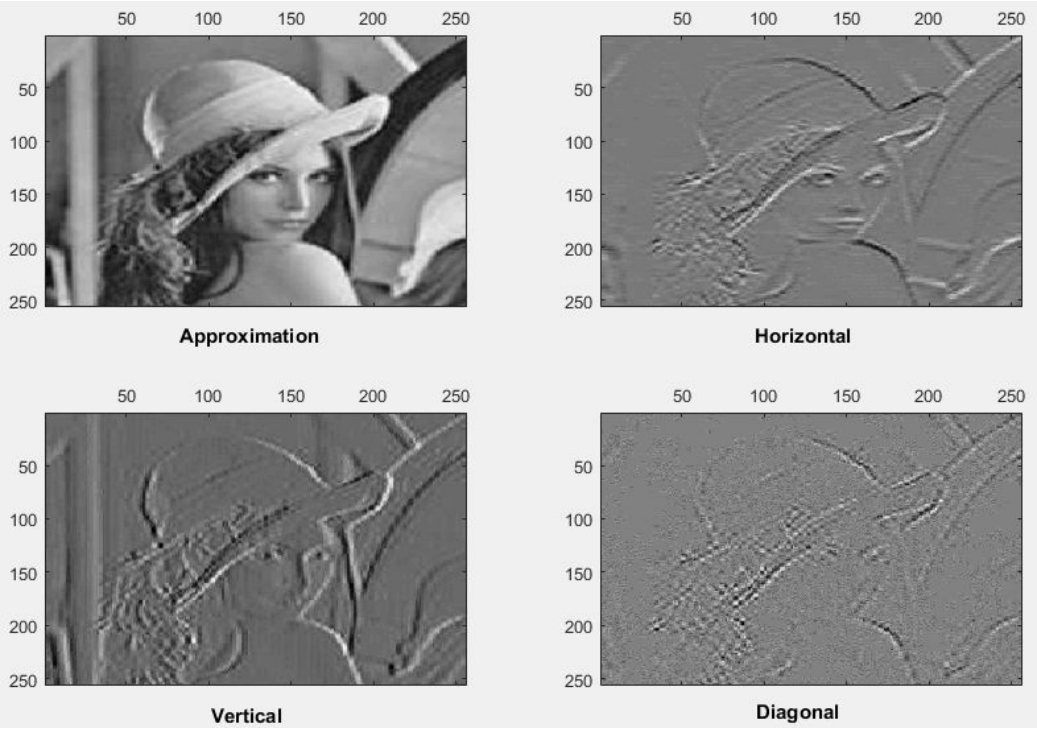


Figure 12: The single-level 2-D discrete wavelet transform (DWT) of gray-scale Lena image.

For the purpose of analyzing and synthesizing a host signal, DWT offers adequate information and needs a reduced amount of computation time. For decomposition, Haar wavelet has been used. The Haar wavelet transform has numerous benefits. It is abstractly easy, fast, memory competent and accurately reversible without edge effects that are issues with other wavelet transforms. Haar transform is executed in two step: horizontal separation and vertical separation.

- Horizontal separation.

  In horizontal separation the low band (L) and the high band (H) are constructed. The (L) band is computed by adding the values of adjacent pixels, while the (H) band is computed by subtracting the values of adjacent pixels. The process of computing band (L) and band (H) is illustrated in figure 13.

- Vertical separation.

  In vertical separation the Low-Low band (LL), High-Low band (HL), Low-High band (LH) and High-High band (HH) are constructed. The (LL) band is computed by adding the values of adjacent results in band (L) that is generated in horizontal separation step, as well the (LH) band is computed by subtracting the values of each adjacent results in the band (L). The (HL) band is computed by adding the values of adjacent results in band (H) that is generated in horizontal separation step, as well the band (HH) which is computed by subtracting the values of each adjacent results in band (H). The process of vertical separation is illustrated in figure 13.

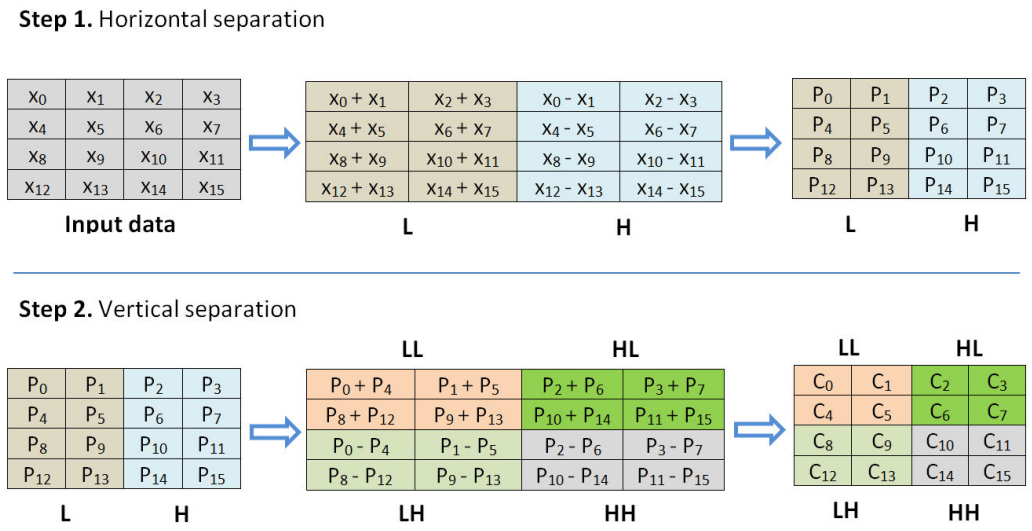


Figure 13: Harr wavelet transform steps.

As example, let A is a host image of dimension 4×4

$$A = \begin{bmatrix} 20 & 21 & 32 & 65 \\ 12 & 43 & 45 & 55 \\ 32 & 17 & 53 & 34 \\ 23 & 12 & 32 & 21 \end{bmatrix}$$

Then, the first horizontal separation (H) and first vertical separation (V) are illustrated as follows:

$$H = \begin{bmatrix} 41 & 97 & -1 & -33 \\ 55 & 100 & -31 & -10 \\ 49 & 87 & 15 & 19 \\ 35 & 53 & 11 & 11 \end{bmatrix}$$

$$V = \begin{bmatrix} 96 & 197 & -32 & -43 \\ 84 & 140 & 26 & 30 \\ -14 & -3 & 30 & -23 \\ 14 & 34 & 4 & 8 \end{bmatrix}$$

Thus, the 2^{nd} level DWT of A is illustrated as follows:

$$A_{DWT} = \begin{bmatrix} 517 & -157 & -32 & -43 \\ 69 & -45 & 26 & 30 \\ -14 & -3 & 30 & -23 \\ 14 & 34 & 4 & 8 \end{bmatrix}$$

Wavelet domain is a promising domain for watermark embedding as it allows good localization both in time and spatial domain. Those regions make it easier to enhance the robustness of the watermark are selected for the embedding purpose. Some parameters of the multi-resolution decomposition of the image using DWT are correlated to the HVS. DWT provides a proper spatial localization and decomposes an image into horizontal, vertical and diagonal dimensions representing low and high frequencies [82]. The energy distribution is concentrated in low frequencies, while the high frequencies cover the missing details. Since the human eye is more sensitive to the low frequency coefficients, so embedding the watermark on high frequency coefficients causes less visual distortion in image.

c *Discrete Cosine Transform (*DCT*)*

DCT is another kind of transform domain method, that it uses the cosine function as a kernel. DCT transforms an image from spatial domain to frequency

domain by 2D DCT allowing also to restore from DCT domain to frequency domain by applying inverse 2D DCT.

For an image A of dimension $M \times N$, that is represented as a function $f(i,j)$ of two space variables i and j: ($i=0,1,...,M-1$, $j=0,1,...,N-1$), the 2D DCT is obtained according to equation 3, while the inverse is obtained according to equation 4.

$$C(u,v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i,j) \cos\frac{\pi(2i+1)u}{2M} \times \cos\frac{\pi(2j+1)v}{2N} \tag{3}$$

$$f(i,j) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \alpha_u \alpha_v C(u,v) \cos\frac{\pi(2i+1)u}{2M} \times \cos\frac{\pi(2j+1)v}{2N} \tag{4}$$

Where $C(u,v)$ is DCT coefficient of image $f(i,j)$ at position (u,v), $M \times N$ is the dimensions of image $f(i,j)$, u and v are the horizontal and the vertical positions ($u=0,1,...,M-1$, $v=0,1,...,N-1$). The values of α_u and α_v are obtained according to equations 5 and 6, respectively.

$$\alpha_u = \begin{cases} \sqrt{1/M}, u = 0 \\ \sqrt{2/M}, 1 \leqslant u < M-1 \end{cases} \tag{5}$$

$$\alpha_v = \begin{cases} \sqrt{1/N}, u = 0 \\ \sqrt{2/N}, 1 \leqslant u < N-1 \end{cases} \tag{6}$$

Basically, the 2D DCT process transforms the spatial pixels of an image block sized $n \times n$ into frequency domain coefficients. The result is $n \times n$ coefficients matrix consisting in one coefficient called DC and 2^n-1 coefficients called ACs. Figure 14 presents the location of DC coefficient and the locations of ACs coefficients in the resulted matrix.

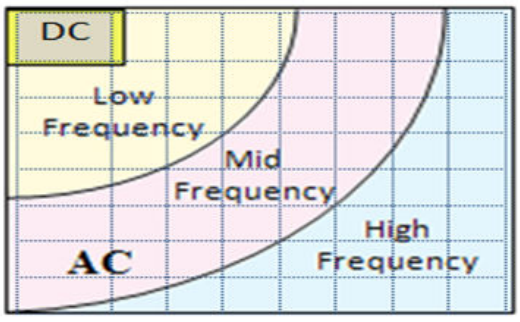


Figure 14: Elements of 2D DCT process.

The DC coefficient for each 8×8 sub-block can be computed in spatial domain according to equation 7 [97].

$$DC = \frac{1}{\sqrt{M \times N}} \sum_{i=1}^{M} \sum_{j=1}^{N} f(i,j) \tag{7}$$

where a partitioned block is represented as a function *f(i,j)* of two space variables *i* and *j (i=1,2,...,8 , j=,2,...,8)*; *f(i,j)* represents the value of pixel at position *(i,j)*.

The value of DC coefficient in 8-bit depth image depends on the size of the processed block. For a 8×8 block, the DC coefficient ranges [-1024-1016] after shifting the pixels values by 128.

The properties of DCT coefficients create new space of features for object description, where DCT process organizes information by order of importance to the Human Visual System (HVS). The most important values to human eyes will be placed in the upper left corner of the coefficients matrix, while the least important values will be mostly in the lower right corner of the coefficients matrix. From the perspectives of texture analysis and HVS, the DC coefficient expresses the average information of the overall magnitude of the processed block and used as a fine property to define the energy of a given block [97]. A high-energy block is more textured than a low-energy block.

2.6.3 *Spread-spectrum domain*

Spread-spectrum method refers to the transmission of a narrow-band signal over a much larger bandwidth. The signal strength is expressed by the frequency of signal; low frequency signal has much energy than high frequency signal. In spread spectrum based-watermarking, the watermark is embedded in perceptually significant spectrum to enhance the robustness. As well, long random vector of low energy are used as watermark to avoid artifacts, to enhance the imperceptibility, robustness and security. In the watermark embedding process the watermark is spread over many frequency bins in such a way the change of energy in any bin will be very small and almost undetectable. In watermark extraction, these many weak signals are combined and result with single watermark. Usually, the watermark verification process knows the locations and the content of the embedded watermark. Spread-spectrum can be used for both spatial and frequency domains.

2.7 ATTACKS ON DIGITAL IMAGES

Various attacks can be applied on digital watermarking system. These attacks can be classified mainly into two categories: unintentional and intentional (malicious) attacks. The unintentional attacks combine all attacks that aim to remove or destroy the watermark from watermarked data. These attacks can be divided into two groups: removal and geometric attacks.

The intentional attacks combine all attacks that aim to alter the embedded watermark, to embed another watermark in watermarked data, to disable the watermark from fulfilling its purpose or to destroy the secret key that is used in watermarking scheme. These attacks can be divided into two groups: property and cryptographic attacks.

Most of unintentional attacks are simulated by StirMark benchmark [80]. This software introduces most kind of attacks that may be applied on images. More clarification about these attacks is illustrated in this section.

2.7.1 *Removal Attacks*

- JPEG compression

  JPEG compression involves a lossy representation of the processed pixels; less memory is needed to represent these pixels, with quality factors ranging from 0-100 [51]. The compression ratio is calculated using equation 8.

$$\text{compression ratio} = \frac{\text{pixel's value}}{\text{quality factor}} \tag{8}$$

  The JPEG compression leads to a general loss in sharpness, reducing edge clarity, loss of color detail when the quality factors tend to 0. As example, JPEG(8) is a lossy representation of the processed pixels by quality factor=8.

- Median filtering

  Median filter attack operates over $M \times N$ pixels to replace each pixel's value with the median intensity of its region. As example, Median(5) operates over 5×5 pixels to replace each pixel's value with the median intensity of its region.

- Gaussian noise

  Gaussian noise manipulates the variations of the intensity drawn from a Gaussian normal distribution. The noise value is added to the pixels of the input image. Its amount can be adjusted by a single parameter ranging from 0 to 100 where 0 means no noise and 100 means completely random image [51]. As example, Noise(20) adds the noise value=20 to the pixels of the host image.

- Histogram equalization

  Histogram equalization involves transforming the intensity values so that the histogram of the output image approximately matches a specified histogram (enhancing the contrast of image to cover all possible gray levels). The ideal histogram flat same number of pixels at each gray-level. The ideal number (*Id*) of pixels at each gray-level is calculated according to equation 9.

$$\mathrm{Id} = \frac{\mathrm{M} \times \mathrm{N}}{\mathrm{L}} \tag{9}$$

where $M \times N$ is the size of image and L is the number of gray-levels.

The contrast of image is the difference between maximum and minimum pixel intensities (pixel's value) in an image, and it expresses the separation between the darkest and the brightest areas of the image. Increasing contrast increases the separation between dark and bright, making shadows darker and highlights brighter.

- Sharpening

  Sharpening refers to an enhanced version of gray-scale or RGB image. Increasing sharpness, increases the contrast only a long/near edges in the image while other areas are left without any change.

- Blurring

  Blurring attack is an opposite process of sharpening, the effect of blurring attack is to attenuate the high spatial frequencies. Basically, blurring process involves spreading out the information from each point into the surrounding points. The high-frequency components of the image were removed after this process. This process called convolution, where the mathematical operation of convolution corresponds to multiply the Fourier transform of the image with that of the convolution kernel. So convolution in ordinary space corresponds to multiplying the various frequency components of the image by a filter function (in frequency space).

2.7.2 *Geometric Attacks*

- Rotation

  This attack rotates a set of pixels by an angle θ either counterclockwise or clockwise about the origin. The function form of rotation is $x'=x\cos\theta + y\sin\theta$ and $y'=-x\sin\theta + y\cos\theta$. Theses functions can be written as a matrix form as follows:

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x\cos\theta + y\sin\theta \\ -x\sin\theta + y\cos\theta \\ 1 \end{bmatrix}$$

  where θ specifies the angle of rotation. As example, Rot(10) rotates a set of pixels clockwise by an angle θ=10 about the origin.

- Translation

  Translation moves a set of pixels as fixed distance in x and y directions. The function form of translation is $x'=x+a$ and $y'=y+b$, and written in a matrix form as follows:

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x+a \\ y+b \\ 1 \end{bmatrix}$$

where a specifies the displacement along the x-axis and b specifies the displacement along the y-axis. As example, translation(5) moves a set of pixels at fixed distance (5) in (y) direction.

- Scaling

  This attack scales a set of pixels up or down in the x and y directions. The function form of scaling is x=$S_x x$ and y'=$S_y y$, and written in a matrix form as follows:

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} S_x & 0 & 0 \\ 0 & S_y & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} S_x x \\ S_y y\theta \\ 1 \end{bmatrix}$$

  where S_x specifies the scale factor along the x-axis and S_y specifies the scale factor along the y-axis. As example, scale(0.2) scales a set of pixels up and down in the x and y directions by 0.2.

- Affine transformation

  Affine transformation involves twisting the image vertically and horizontally, where the transformations convert the pixels between the x and y directions. The function form of Affine transformation is x'=$a_{11}x$+$a_{12}y$+a_{13} *and* y'=$a_{21}x$+$a_{23}y$+a_{23}, and written in matrix form as follows:

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = T. \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} a_{11}x + a_{12}y + a_{13} \\ a_{21}x + a_{22}y + a_{23} \\ 1 \end{bmatrix}$$

  where T is the transformation matrix, where a_{11}, a_{12},a_{13}, a_{21}, a_{22}, a_{23} are real numbers.

  An affine transformation ensures two principles: (1) the co-linearity, where all pixels lying on a line initially still lie on a same line after the transformation and (2) the relative amount of distances, where a midpoint of a line remains the midpoint of same line after the transformation. In StirMark [80], the used parameter configurations are from [1-8]. These parameters represent the lists of the parameter configurations for the inverse transformation matrix used for the StirMark test stretching in x-direction.

- Cropping

  This attack crops the image by defining four elements that represent the position vector of the form [xmin, ymin, width, height] that specifies the size and the position of the crop rectangle. The function of cropping includes row/column removal. As example, in Crop(50) the processed image is cropped to 50% of the original size.

- Remove Lines (RML)

  This attack removes lines in both vertical and/or horizontal directions. This manipulation removes set of pixels in distinct rows/columns of the processed image. The amount of removed rows/columns can be adjusted by a parameter α ranged from 10 to 100, which corresponds to the frequency of removing lines, where α means remove one line in the entire α lines and then the dimensions of the output image are reduced [51]. As example, RML(10) removes one line in the entire 10 lines horizontally and vertically.

- Latest Small Random Distortions (LATESTRNDDIST)

  LATESTRNDDIST attack applied a bilinear transformation to the image by moving its corners by a small random amount. Experiment transforms on the host image can be achieved with different parameters. With the actual version of StirMark, also here in Latest Small Random Distortions a single parameter, representing a multiplier for the default parameters, is used to adjust the intensity of the attack. The parameters can be chosen as the set {0.6,1.0,1.4,1.8,2.2,2.6,3.0,3.4,3.8,4.2}.

2.7.3 *Property Attacks*

- Collusion

  In this attack, the attacker uses several copies of one part of digital data, each with a different watermark, to construct a copy of digital data with no watermark. This attack can be defined as unauthorized removal attack.

- Forgery

  The attacker tries to embed a new watermark of their own rather than remove the embedded one. This attack can be defined as unauthorized embedding attack.

- False-positive

  This attack involves that the attacker can extract the watermark without having a full knowledge about the embedding algorithm. Indeed, the attacker can detect watermark in digital data that is actually unmarked and has not actually belonged to the authorized owner. This problem encourages malicious

owner in claiming other unauthorized data by generating his own watermark easily. This attack can be defined as unauthorized extraction attack.

2.7.4 *Cryptographic Attacks*

One of the main cryptographic attacks that affects on digital watermarking systems is the brute-force. This attack is trial-and-error method used to recognize some information related to the digital watermarking system. It generates all guesses as to the value of desired information until finding the correct guess. Digital watermarking system fails if the attacker is able to guess the secret or public key is used in embedding/extraction processes. The resistance of watermark against brute-force attack depends on the length of used key or other information. Longer key is more resistant.

2.8 DIGITAL IMAGE WATERMARKING PERFORMANCE METRICS

The performance of any image watermarking system in terms of imperceptibility, robustness and embedding rate is expressed using well-known metrics, namely: Peak Signal-to-Noise Ratio (PSNR), Structure SIMilarity (SSIM), Normalized Correlation coefficients (NC), Bit Error Rate (BER) and Embedding Rate (ER) [106][133]. The description of these metrics are illustrated in this section.

2.8.1 *Imperceptibility*

The PSNR and SSIM are two common metrics used to express the performance of an image watermarking approach in term of imperceptibility.

- PSNR measures the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation using Mean Square Error (MSE). In image watermarking the PSNR expresses the perceptual quality of the watermarked image with respect to the original image. Higher PSNR proves that the embedded watermark is highly imperceptible and cause less quality degradation in the original image. MSE is computed according to equation 10 and the PSNR in decibels (dB) is calculated according to equation 11.

$$MSE(I, \bar{I}) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I_{ij} - \bar{I}_{ij})^2 \tag{10}$$

$$PSNR(I, \bar{I}) = 10\log_{10}\left[\frac{255^2}{MSE}\right] dB \tag{11}$$

Where I_{ij} is the pixel *(ij)* in the original image I and $\bar{I}_{ij}$ is the pixel *(ij)* in the watermarked image $\bar{I}$, $M \times N$ is the size of image.

- SSIM measures the similarity between two images in a perception-based model that considers image degradation as perceived change in structural information. The structural information is the carried information from the inter-dependencies between the adjacent spatial pixels of image. These inter-dependencies between adjacent spatial pixels have much information about the structure of objects in the visual perception scene. SSIM is calculated by incorporating important perceptual characteristics including the luminance masking and the contrast masking. Luminance masking whereby image distortions tend to be less visible in bright regions in the image, while contrast masking whereby distortions become less visible in highly significant activity or textured regions in the image. The SSIM is computed according to equation 12 and the mean of SSIM also computed according to equation 13.

$$SSIM(I, \bar{I}) = \frac{(2\mu_I\mu_{\bar{I}} + C_1)(2\sigma_{I\bar{I}} + C_2)}{(\mu_I^2 + \mu_{\bar{I}}^2 + C_1)(\sigma_I^2 + \sigma_{\bar{I}}^2 + C_2)} \tag{12}$$

$$mSSIM(I, \bar{I}) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} SSIM(I_{ij}, \bar{I}_{ij}) \tag{13}$$

Where μ_I is the average of original image I, $\mu_{\bar{I}}$ is the average of watermarked image $\bar{I}$, $\sigma_{I\bar{I}}$ is the covariance of I and $\bar{I}$, σ_I^2 is the variance of I, $\sigma_{\bar{I}}^2$ is the variance of $\bar{I}$; $C_1=(K_1L)^2$, $C_2 = (K_2L)^2$ are two variables to stabilize the division with weak denominator (L the dynamic range of the pixel-values (typically is $2^{\#\,bits\,per\,pixel}$-1), K_1=0.01 and K_2=0.03) [120], $M \times N$ is the size of image.

The PSNR and the MSE present an inconsistency with the principles of HVS; they only estimate absolute errors between two images. Using SSIM is more useful to measure the imperceptibility performance of any image watermarking approach.

2.8.2 *Robustness*

NC and BER are two common metrics used to express the performance of an image watermarking approach in terms of robustness.

- NC measures the similarity (or distance) between the original watermark and the extracted one. To compute the similarity between two images that varies in

brightness and template, both images are initially normalized by subtracting the mean value and then each one is divided on its variance. The NC ranges between [1,-1]; if NC=1 this means that two images are absolutely identical, if NC=0 this means that two images are completely dissimilar, if NC= -1 this means that two images are completely anti-similar. NC is computed according to equation 14.

$$NC(w,\bar{w}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(w_{ij}-\mu_w)\times(\bar{w}_{ij}-\mu_{\bar{w}})}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(w_{ij}-\mu_w)^2}\sqrt{(\sum_{i=1}^{M}\sum_{j=1}^{N}(\bar{w}ij-\mu_{\bar{w}})^2}} \tag{14}$$

Where w_{ij} is the *(ij)* pixel in the original watermark w, $\bar{w}_{ij}$ is the *(ij)* pixel in the extracted watermark $\bar{w}$, μw is the mean of the original watermark w, and $\mu_{\bar{w}}$ is the mean of the extracted watermark $\bar{w}$, $M\times N$ is the size of watermark image.

- BER: measures the percentage of erroneous extracted watermark bits to the total number of original watermark bits. Lower BER expresses high robustness of watermark against different attacks. BER is computed according to equation 15.

$$BER(w,\bar{w}) = \frac{1}{M\times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(w(i,j)\bigoplus\bar{w}(i,j)\right]\times 100 \tag{15}$$

Where *w(i,j)* represents the pixel *(i,j)* in the original watermark w, *$\bar{w}$(i,j)* represents the pixel *(i,j)* in the watermarked image *($\bar{w}$)* and $M\times N$ is the size of watermark.

2.8.3 *Embedding Rate Measures*

- Embedding rate (ER), which is also called watermark payload, measures the percentage of the embedded data (i.e. watermark bits or watermark coefficients) in the whole host image [133]. An ideal algorithm exhibits excellent performance if it achieves higher watermark payload, higher imperceptibility and higher robustness. Moreover, higher watermark payload usually result in a better resolution of tamper localization. The embedding payload is computed according to equation 16.

$$ER = \frac{T}{M\times N} \tag{16}$$

In equation 16, T is the total number of embedded secret bits and M×N is the size of the host image.

2.9 DIGITAL IMAGE WATERMARKING BENCHMARK

Stirmark Benchmark is a generic tool for simple robustness testing of image watermarking algorithms [80]. It introduced removal and geometric distortions to de-synchronize image watermarking algorithms. The first version of StirMark was published in 1977, then several versions followed improving the original attack by introducing a longer lists of tests. The goal of StirMark is introducing automated independent public service with extended evaluation profiles to evaluate quickly watermarking libraries. StirMark Benchmark 4.0 is freely available as binary and C/C++ source code. This program can easily be compiled using the freely available Microsoft Visual Studio Express[1].

2.10 CONCLUSION

Three generic techniques are proposed to protect multimedia data: cryptography, steganography and watermarking. Cryptography techniques cannot help the owner of digital content to monitor how a legitimate user handles the content after decryption, where digital watermarking can protect content even after it is decrypted. Steganography and watermarking are the main techniques in information hiding field. Each involves hiding secret information called a watermark into a digital data such that watermark can be detected or extracted later. In watermarking, the important information is the digital data itself and the watermark is used as an assertion about the digital data. Thus, any digital watermarking approach must prevent an attacker from removing or modifying or replacing watermark in the watermarked data. Whereas for steganography, the watermark is the important information, thus any steganography approach must hide the presence of watermark in the watermarked data.

Digital watermarking has much interest than other protection techniques due to the increase in concern over authenticity, integrity and copyright protection of digital content. The motivations toward digital watermarking, the requirements of digital watermarking systems and the framework of digital watermarking are illustrated in this chapter. As well, classification of digital watermarking, the different digital image watermarking techniques, the principles of various attacks on digital image watermarking systems, the set of metrics that are used to evaluate the performance of digital image watermarking and the common benchmark are also presented in this chapter.

1 Microsoft Visual Studio Express, https://www.visualstudio.com/

Chapter 3

LITERATURE REVIEWS

Contents

3.1 INTRODUCTION

We introduce through this chapter several image watermarking approaches that are proposed in the literature aiming to provide images authentication and identification. The proposed watermarking approaches are designed either in spatial, transform and hybrid domains.

Some of these approaches are especially designed to provide images authentication and identification in sensitive types of applications such as telemedicine applications or remote sensing imaging systems. In these applications, image authentication and identification require no significant change on the original data for diagnosis purposes in case of telemedicine applications or for decision making in case of remote sensing imaging systems. The destining of any of the proposed zero-watermarking approaches is based on extracting robust and unique features from host images to build a zero-watermark.

The other types of the proposed watermarking approaches are used to provide medical, natural gray-scale or color images authentication. Any of the proposed approaches is based on analyzing various image characteristics that are correlated to the HVS to define significant visual locations/coefficients in host image for embedding watermark with high imperceptibility and robustness. As well, different AI techniques are used in some of the proposed watermarking approaches to optimize some parameters that are used to the watermark embedding process and the related issues. These parameters have significance in

identifying the best location/coefficients among many alternatives to hold watermark, and to control the amount of watermark bits that can be embedded in different locations/coefficients without causing noticeable image quality distortion or fragility against different attacks.

The focus of each of the proposed approaches, the images features that can be used either to build a zero-watermark or to define significant visual locations/-coefficients in host image. The experiments result are discussed in this chapter. At the end of each section, several aspects are considered to synthesize the specification of each approach. These aspects including the type of images tested, the approach target, the domain based, the robustness ratio, the lossy/lossless, the computational complexity and the execution time. For analyzing the computational complexity of each approach, the O-notation is mostly considered because it gives an upper limit of the execution time (i.e. the execution time in the worst case). The performance of each approach is tested on host images I of dimensions $M \times N$, where M is the height of image and N is the width of image.

This chapter is organized as follows. Section 3.2 presents several zero-watermarking approaches and then section 3.3 presents many digital watermarking approaches that aim to provide an authentication and an identification for medical images and other kinds of images. Finally, we conclude this chapter in section 3.4.

3.2 ZERO-WATERMARKING BASED APPROACHES

Many zero-watermarking approaches have been proposed to address the issues of identification, authentication and integrity control. Designing any zero-watermarking approach is based on extracting robust and unique features from host images to build a zero-watermark. These features are inferred from the properties of spatial or frequency domains and most of them are correlated with the principles of HVS. The texture property, the singular values in SVD transform, the energy distribution of DWT low frequency and the importance of image information expressed by means of DCT coefficients are examples of images features that are used to generate a zero-watermark. Additionally, Polar Complex Exponential Transform (PCET), Quaternion Exponent Moments (QEMs), and Bessel-Fourier moments [123] are three transformation methods that provide some robust features that are exploited to build a zero-watermark for image authentication.

In the following paragraphs, some of zero-watermarking approaches, the extracted features that are used to build a zero-watermark and the experiments results are presented. At the end of this section, several aspects are considered to synthesize the specificity of each approach.

Authors in [115] proposed a robust zero-watermarking based on Polar Complex Exponential Transform (PCET) [83] and logistic mapping [119]. The pro-

posed approach started by scrambling the watermark image W using Arnold scrambling method [52] and seed S to improve the robustness, the result is W_S. Then, the PCET is applied on the original image I to obtain the PCET coefficients. The logistic map is then used to select randomly a set of PCET coefficients to construct a feature vector $\vec{A}$. The vector $\vec{A}$ is converted into 1D-binary sequence, and the resulted sequence is reshaped as 2D feature image I_F. XOR operation between the feature image I_F and the scrambled watermark image W_S is applied to generate a verification zero-watermark image W_V. The hash value H_{VSK} of the W_V, the seed S, and the secret key K that is used in the logistic mapping method, is computed using Message-Digest 5 (MD5) algorithm [110]. Subsequently, the timestamp T is added to H_{VSK} to generate H_{VSKT}. The H_{VSKT} becomes a unique identification for generating zero-watermark and is sent to a trusted third-party via secure channel. The zero-watermark verification process starts by verifying the validity of the security parameters: W_V, seed S, and secret key K. If these parameters are validated, then the feature vector $\vec{A^*}$ from the attacked image I^* is constructed using PCET method and logistic map key K. The 1D-binary sequence of the extracted feature vector A^* is reshaped into 2D-feature image I_F^*. XOR operation between I_F^* and W_V is applied to generate a scrambled watermark image W_S^*, and a reverse Arnold transformation using seed S is applied to obtain the verified watermark image W^*. The bit error rate between the original watermark W and the extracted one W^* is calculated to verify the robustness of the zero-watermark. The BER is ranged between 6.9-10.2% against cropping and rotation attacks, while it is ranged between 1.2-6.4% against scaling, compression, noise, sharpening and blurring attacks.

In [95], the authors proposed a zero-watermarking technique to provide unique identification, authentication and integrity verification of medical images. The proposed technique involves extracting robust features from DWT and SVD coefficients to generate a unique identification code from fundus images. The approximation sub-band LL of DWT process is more robust against image processing attacks compared to the details sub-bands (LH, HL and HH). The coefficients values of LL sub-band change less comparing with other sub-bands. As well, the singular values of any matrix are unique and they are less affected by image processing attacks. These unique features of DWT coefficients and singular values are used to build a unique identification code, which after is combined with the patient ID strategically to produce the master share. The proposed technique is implemented in three forms. In the first form, the host image is transformed by 1-level DWT to generate (LL, LH, HL and HH) sub-bands. Then, the LL sub-band is partitioned into set of non-overlapping blocks, and for each block the first singular value is selected to build a matrix M. X-OR function is performed between the encrypted form of matrix M and the binary watermark to generate a new matrix, which will be encrypted using Arnold Cat Map [55] to generate

a master share K. In the extraction process, a unique identification code is also generated from unique features of the host image. The generated code and the received master share are combined to obtain the patient's details. The host image is transformed using 1-level DWT, then the LL sub-band is partitioned into set of non-overlapping blocks. For each block the singular values are extracted, and the first singular value in each block is selected to build a matrix M^*. X-OR function is performed between the matrix M^* and the decrypted master share K^* to extract the watermark, related to the patient's details. The implementation of the second form of the proposed technique is similar to the first form, the difference is in the first step where the host image is initially divided into set of non-overlapping blocks and for each block the DWT is applied. The third form of the proposed technique partitioned the host image into set of non-overlapping blocks and for each block the singular values are computed to build the matrix M. The same implementation as in the first form of the proposed technique is implemented. The proposed approach is tested to measure its performance in terms of robustness against different attacks. In case of blurring attack, the NC was 0.69 and the BER was 7.3%. In cases of sharpening, histogram equalization, filtering and JPEG compression, the NC was ranged 0.85-1 and the BER did not exceed 2.6%.

In [94], the authors proposed a zero-watermarking approach based on Non-Uniform Rectangular Partition (NURP) [100]. In NURP domain, the host image is partitioned into different rectangle grids and some bivariate polynomials over partitioned grids are obtained to represent the pixels of host image. The NURP is a useful technique to describe the image texture property, where the rectangle number in each partitioned grid expresses image texture. In the proposed approach, a zero-watermark is constructed by performing NURP on the host image to obtain the rectangles numbers of each 8×8 block. These numbers are stored in a feature matrix, which is then used as a zero-watermark. The generated zero-watermark and the original binary watermark are used in the extraction process. To enhance the robustness, the Arnold scrambling method [52] is applied. In the extraction process, the Speed-Up Robust Features (SURF) algorithm [10] is applied on attacked host image to recover the host image. Then, the NURP is applied on the recovered image to get the attacked feature matrix. This matrix is scrambled inversely using the same Arnold key k and a comparison between it and the original one is held to extract the scrambled binary watermark W'. Finally, W' is scrambled inversely using the same Arnold key k to recover the attacked binary watermark. The proposed approach is tested in terms of robustness against different attacks. The NC was ranged 0.86-0.98 and the BER did not exceed 10.9%.

The authors in [114] proposed a color image zero-watermarking approach based on Quaternion Exponent Moments (QEMs) algorithm [118]. The proposed

approach aims to extract a set of robust features from the original color image I to build a zero-watermark image. The proposed approach consists of two main processes. The first process is zero-watermark generation and the second process is zero-watermark verification. In the first process, the original watermark W is scrambled using quasi-affine transform [136] and seed S_1 to enhance the robustness of the whole watermarking system, the result is W_S. Then, the QEMs of the original image is computed and a set of extracted moments are selected randomly using a secret key S_2. The magnitude of the selected moments are represented as $\vec{A}$. $\vec{A}$ is rearranged into two-dimensional feature image I_A and a binary feature image I_F from I_A is obtained based on a defined threshold using Otsu's method [126]. XOR operation between the feature image I_F and the scrambled watermark image W_S is applied to generate the zero-watermark image Z_W. For copyright protection, the digital signature for Z_W, S_1 and S_2 is computed using the digital signature function ($Sign_{OSK}$) [19] and it is sent to a trusted third-party via secure channel. In the second process, zero-watermark verification is started by verifying the digital signature and validating the security parameters Z_W, S_1 and S_2. Once these parameters are validated, then the QEMs for the attacked image I^* is computed. After that, a set of robust QEMs are selected randomly using the secret key S_2. These moments are represented as $\vec{A}^*$. $\vec{A}^*$ is rearranged into two-dimensional feature image I^*_A, then a binary feature image I^*_F is obtained. XOR operation between I^*_F and Z_W is applied to extract the scrambled watermark image W^*_S. The retrieved watermark image W^*_S is inversely scrambled to obtain the attacked watermark image W^* using seed S_1. The proposed approach resisted against various attacks and worked properly with different geometric attacks except cropping large scale of original images. The BER ranged 0-1.8% against non-geometric attacks, 1.2-7.5% against rotation attack and 12.4% against cropping attack.

In [33], a new zero-watermarking copyright authentication approach based on Bessel-Fourier moments [123] is proposed. In this approach, the host image I is normalized for its translation and scaling, then the Bessel-Fourier moments of the normalized image is computed. The magnitudes of the computed Bessel-Fourier moments are used to construct a feature vector $\vec{F}$, which is then converted into 1D-binary sequence F. The binary sequence F is reshaped into 2D-matrix to generate the feature image I_F. For security reason, I_F is scrambled using composite chaos method [32] and using seed S. XOR operation between I_F and the original watermark W is applied to generate the verification image I_V. For copyright protection, the hash value of the generated verification image I_V and the seed S is computed using unidirectional hash function [71] and then combined with the timestamp T. The result is H_{VST} that is sent to a trusted third-party via secure channel. In the verification process, the H_{VST} is requested from the trusted third-party to validate the security parameters: I_V, S and T. Once these

parameters are verified, then the magnitudes of the computed Bessel-Fourier moments of the attacked image I^* are used to construct a feature vector $\vec{F^*}$. $\vec{F^*}$ is converted into 1D-binary sequence F^* and then is reshaped into 2D-matrix to generate the scrambled feature image I^*_{SF}. The I^*_{SF} inversely scrambled using composite chaos method [32] and using seed S to generate the feature image I^*_F. XOR operation between I^*_F and I_V is implemented to extract the attacked watermark W^*. The consistency rate between the original watermark W and the extracted one W^* is computed in term BER against different attacks. The BER results are reported in [114], it ranged 1.3-8.9% against rotation attack and reached 21.1% against cropping attack. In case of scaling, noise, compression, blurring and sharpening attacks the BER ranged 0-1.9%.

The authors in [86], proposed two zero-watermarking approaches based copyright protection using DWT and SVD. The rightful ownership using these approaches is proved mainly by generating two shares: the master share M and the ownership share O. The first approach divides the host image I into overlapping blocks of size 8×8 and then the first level of DWT is applied for each block. The LL sub-band of each transformed block is selected and followed by *SVD* transform to extract a set of robust features of host image that are used to construct the master share M. Indeed, the higher singular values of each transformed block are used to form a matrix S. Afterward, four random numbers are generated using Mersenne twister algorithm [67] to pick up two singular values from matrix S and then the differential classification of randomly picked singular values is used to build the master share M. If the difference between the picked singular values is higher than 0 then 1 is placed in matrix M, otherwise 0 is placed. The ownership share O is generated by applying *X-OR* operation between the matrix M and the watermark W. The rightful ownership is proved by extracting the watermark W_a from the attacked image I_a. W_a is extracted by applying *X-OR* operation between the extracted master share M from I_a and the ownership share O provided by trusted third-party. The second approach is almost similar to the first approach, except that it initially transforms the host image by DWT and then SVD transform is applied on the partitioned 4×4 blocks of LL sub-band. The SVD process is applied for each block to generate the master share M in the same manner than the first approach. The proposed watermarking approaches do not embed the watermark in the host image, but rather they work as encrypting watermark in the host image without any addition or alteration on the data of the original image. Additionally, the proposed approaches based on the singular values of LL sub-band as robust features in the host image to build the master share M, since these elements are least effected with various attacks. The proposed approaches are tested for their performance in terms of robustness against different attacks. The NC ranged 0.83-1 in the first approach and ranged 0.50-0.99 in the second approach.

The robust features used to build zero-watermark and its impact on the performance of the illustrated zero-watermarking approaches are presented in table 3. The specifications of the illustrated approaches are presented in table 4. The computational complexity and the execution time of the illustrated zero-watermarking approaches are presented in table 5. The presented execution time in table 5 represents to the overall running time for each of the illustrated approaches, as well the presented overall computation complexity in table 5 is computed after considering the computational complexities for the set of functions or algorithms that are used in the given approach.

Proposed approach	The robust feature that is used to build a zero-watermark	The significance of the robust feature on the performance of the proposed approach
Wang et al., 2017 [115]	The PCET coefficients encompasses the features of orthogonality and geometric invariance	These features helps to improve the robustness of the zero-watermarking algorithm against geometric attacks; the orthogonality allows for image reconstruction, while the magnitude of PCET coefficients are invariant to image rotation and scaling
Shen et al., 2017 [94]	The rectangles numbers of host image blocks after NURP transformation	The rectangles of host image blocks numbers describe the texture property for each block, this property helps to improve the robustness of the zero-watermarking algorithm against different attacks
Chun-peng et al., 2016 [114]	The quaternion exponent moments	The stability of quaternion exponent moments against rotation and scaling attacks; the QEMs are invariant to image rotation and scaling
Gao et al., 2015 [33]	The magnitude of Bessel-Fourier moments	The magnitude of Bessel-Fourier moments have rotation invariance, this help to improve the robustness of zero-watermarking against rotation attack
Singh et al., 2017 [95] and Rani et al., 2015 [86]	The geometric properties of singular values and low frequency sub-band of DWT of host image	The LL sub-band of DWT and the uniqueness singular values of host image affect less with image processing attacks; the singular values and the low frequency sub-band of DWT do not get modified after exposing to different kind of geometric image processing attacks

Table 3: Robust features used in building zero-watermark and their impact on the performance of the proposed zero-watermarking approaches.

Proposed approach	Types of images tested	Objective	Domain based	Robust or Fragile	Robustness ratio	lossy or lossless
Wang et al., 2017 [115]	Natural and medical (CT) gray-scale images	Copyright verification	PCET	Robust	BER ranged 1.2-10.2%	Lossless
Singh et al., 2017 [95]	Fundus (medical) images	Image identification and authentication	DWT and SVD	Robust against non-geometric attacks	NC ranged 0.69-1 and BER<7.3%	Lossless
Shen et al., 2017 [94]	Natural gray-scale images	Copyright verification	NURP	Robust	NC ranged 0.86-0.98 and BER<10.9%	Lossless
Chun-peng et al., 2016 [114]	Natural color image	Copyright verification	Pure quaternion numbers [6]	Robust	BER<12.4%	Lossless
Gao et al., 2015 [33]	Natural and medical gray-scale images	Copyright verification	Bessel-Fourier transform	Robust	BER<21.1% [114]	Lossless
Rani et al., 2015 [86]	Natural gray-scale images	Copyright verification	DWT and SVD	Robust	NC ranged 0.50-1	Lossless

Table 4: Specifications of several proposed zero-watermarking approaches.

Proposed approach	Computational complexity	Overall computational complexity	Execution time (seconds)
Wang et al., 2017 [115]	• Complexity of Arnold scrambling method= *O(M×N)* [52] • Complexity of PCET= the number of multiplications in the computation of ω order PCET for *I* is $O(M\times N \times \omega^2)$ [115] • Complexity of logistic mapping = linear complexity [87] • Complexity of one-way hash function (MD5)= for (k) bytes the complexity is *O(k)* [110]	$O(M\times N \times \omega^2)$	21.84
Singh et al., 2017 [95]	• Complexity of DWT= *O(M×N)* [122] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of Arnold Cat Map= $O((M\times N)^3 \log_2 M\times N)$ [55]	$O((M\times N)^3 \log_2 M\times N)$	3.5 in the first and third algorithms and 20 in the second algorithm
Shen et al., 2017 [94]	• Complexity of NURP= *O(log b)*: b is the number of partitioned blocks of M×N [56][101] • Complexity of SURF= *O(M×N)* [26] • Complexity of Arnold scrambling method= *O(M×N)* [52]	*O(M×N)*	Not mentioned
Chun-peng et al., 2016 [114]	• Complexity of QEMs= *O(M×N)* [118] • Complexity of Quasi-affine transform= *O(M×N)* [136] • Complexity of Otsu's method= *O(M×N)* [8]	*O(M×N)*	740.51
Gao et al., 2015 [33]	• Complexity of image normalization= *O(1)* [124] • Complexity of composite chaos method= linear complexity [137] • Complexity of Bessel-Fourier transformation= $O(M^2\times N^2)$ [33], if the maximum order of Bessel-Fourier moments required by the feature vector be *N* • Complexity of unidirectional hash function= for (k) bytes the complexity is *O(k)* [71]	$O(M^2\times N^2)$	4345.64 [114]
Rani et al., 2015 [86]	• Complexity of Mersenne twister algorithm= $O(p^2)$: *p* is the degree of the polynomial [67] • Complexity of DWT= *O(M×N)* [122] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65]	$O(min(M\times N^2, M^2\times N))$	900 using the first approach and 90 using the second approach

Table 5: Computational complexity and execution time of several proposed zero-watermarking approaches.

3.3 IMAGE WATERMARKING APPROACHES USING SPATIAL PIXELS/TRANSFORMED COEFFICIENTS

Several image watermarking approaches are illustrated in this section. These approaches are presented through three categories; the first category presents a set of medical image watermarking approaches. The second category presents a set of natural gray-scale or color images watermarking approaches correlated to the HVS. The third category presents intelligent natural gray-scale or color images watermarking approaches correlated also to the HVS.

In each approach: the main idea, the image characteristics that are analyzed to identify significant visual locations/coefficients in host image to embed the watermark and the experiments results are presented in this section. At the end of each category, several aspects are considered to synthesize the specification of each approach. These aspects include: the type of images tested, the approach target, the domain based, the robustness ratio, the lossy/looseness, the computational complexity and the execution time.

3.3.1 *Medical Image Watermarking Approaches*

In [106], the authors proposed a robust blind medical image watermarking based on DWT and SVD. The proposed approach aims to provide image authentication and identification by embedding two watermarks in Region of Interest (ROI) of medical image. The first watermark is a logo image, while the second watermark is text that represents Electronic Patient Record (EPR). Initially, the 2-level of DWT is applied on the ROI of medical image to generate LL, LH, HL and HH sub-bands. The LL sub-band is partitioned into set of non-overlapping blocks and each block is transformed by SVD to generate three matrices U, S and V. A pair of elements with much closer value in the second and third rows of the first column of the left singular matrix U are modified using certain threshold to embed a bit of watermark. The watermarks are extracted blindly from the ROI of watermarked medical image by comparing the values of elements in the second and third rows of first column of the left singular matrix U. In this approach, the hamming Error Correcting Code (ECC) is applied on EPR watermark to reduce the BER and thus provides better recovery. As well, choosing appropriate threshold is important to achieve high imperceptibility and robustness. The proposed approach is tested on three types of medical images including X-ray, Computerized Tomography (CT) and mammography. The performance of this approach is evaluated in terms of imperceptibility and robustness against different attacks. The perceptual quality of watermarked image in terms of PSNR and SSIM exceeded 43 dB and 0.95 respectively. The similarity between the extracted and the original watermarks in terms of NC was ranged 0.89-1 and the BER did not exceed 4.6% against compression, filtering, noise, sharpening and scaling attacks. In case of compression and cropping attacks the NC was ranged 0.35-0.71 and the BER reached 36.0%.

In [108], the authors proposed a blind medical image watermarking approach based on Fast Discrete Curvelet Transform (FDCuT) and DCT. FDCuT is used to transform the medical image into low frequency, mid frequency and high frequency sub-bands. The high frequency Curvelet sub-band is partitioned into 8×8 non-overlapped blocks and transformed using DCT. The mid-band frequency coefficients of high frequency Curvelet sub-band are modified by inserting two

White Gaussian Noise (WGN) sequences according to watermark bit to generate a watermarked medical image. The two WGN sequences are generated using noise generator, each of size equal to the size of mid band frequency coefficients. In the embedding process, if the watermark bit is zero, then the DCT mid-band frequency coefficients are modified using WGN. Else, the DCT mid-band frequency coefficients are modified using WGN sequence for watermark bit 1. The inverse processes of DCT and FDCuT are applied to generate the watermarked image. In the extraction process, the watermark is extracted blindly using the correlation between the watermarked image and the two generated WGN sequences. FDCuT provides high embedding capacity, where the size of high frequency Curvelet sub-band that resulted after applying FDCuT is equal to the size of the host image. As well, FDCuT provides better imperceptibility compared to other transforms, since it represents the image in terms of edges. Dividing the high frequency Curvelet sub-band into 8×8 non-overlapped blocks and applying DCT process aim to enhance the robustness. The proposed approach is tested on four types of medical images including X-ray, Ultrasound (US), Magnetic Resonant Imaging (MRI) and Computerized Tomography (CT). The performance of this approach is evaluated in terms of imperceptibility and robustness against different attacks. The PSNR is calculated to obtain the perceptual quality of watermarked image, as well as NC to evaluate the similarity between the extracted watermark and the original one. The PSNR reached 55.06 dB and the NC reached 0.99 against different attacks.

In [77], the authors proposed two blind medical image watermarking approaches based on DCT. In each approach, logo image and Electronic Patient Record (EPR) watermarks are embedded in the host medical image to provide copyright protection and image identification. In the first approach, the watermarks are embedded in Region of Interest (ROI) and Region of Non Interest (RONI). While, in the second approach the watermarks are embedded in RONI only and the ROI is kept unmodified for tele-diagnosis purpose. In the proposed approaches, the 8×8 block based DCT is used to transform the selected regions and in each 8×8 transformed block two mid frequency coefficients are selected to embed watermarks. The embedding process is carried out by comparing the values of selected coefficients, and then modifying them by using a specific embedding factor for embedding bit 0 or bit 1 of the watermarks. The proposed approaches are tested for their performance in terms of imperceptibility and robustness against different attacks. The PSNR and SSIM are calculated to evaluate the perceptual quality of watermarked image, as well the NC and BER are calculated to obtain the similarity between the extracted watermark and the original one. The PSNR was ranged 36-48 dB and SSIM reached 0.99. While, the NC reached 0.99 and BER did not exceed 19.8% against different attacks.

In [68], the authors proposed a reversible fragile medical image watermarking approach based on DWT and DCT. An adaptive watermarking approach is employed to identify visual significant coefficients to embed the watermark into medical images in such a way that it is imperceptible for the HVS. The HVS is more sensitive to any change in the low frequency coefficients than the high frequency coefficients, as they represent the most significant characteristics of the host image. The high frequency coefficients give less significant characteristics of host image and any changes in these coefficients are not easily noticeable by HVS. In the proposed approach, the first level of DWT is applied on the medical image, the result is the LL, LH, HL and HH sub-bands. The high frequency band HH, which is the detailed sub-image, is transformed to DCT coefficients. The average value of the DC coefficients in each DCT block of the host image is computed and used as a scaling factor. The watermark is multiplied with this factor to get a new watermark coefficients. The new watermark coefficients is added to the DCT coefficients values to produce new coefficients values. The inverse processes of DCT and DWT are applied to generate the watermarked image. In the extraction process both the watermarked and the host images are required to extract the watermark. The DWT is applied on the watermarked and the original images, then the high frequency band of watermarked and original images after applying DWT are transformed using DCT. As well, the average value of the DC coefficients in each DCT block of host image is computed and used as a scaling factor. Subtraction process between the DCT coefficients of host image and the watermarked image are computed and multiplied by a scaling factor to create the watermark. The PSNR and NC are calculated to obtain the perceptual quality of watermarked image in comparison to the original image. The PSNR was ranged 40-45 dB and the NC reached 1.

In [96], the authors proposed a robust medical images watermarking approach based on DWT. Multiple watermarks are embedded in the DWT coefficients of medical image to obtain high robustness. In the embedding process, the host image is transformed using Haar wavelet transform to get the first and the second sub-bands coefficients. Selective coefficients in LH and HL sub-bands of each DWT level are embedded with Pseudo Noise (PN) bits depending on the value of watermark bit. The PN sequences are generated according to each watermark bit, and are embedded column wise into the selected DWT coefficients in each sub-band. The inverse process of DWT is performed to generate the watermarked image. The watermark extraction process is achieved by finding the correlation between the coefficients of LH and HL sub-bands of DWT on watermarked images and the generated PN sequences on each DWT level. The proposed approach is tested on three types of medical images including Ultrasound (US), Magnetic Resonant Imaging (MRI) and Computerized Tomography (CT). The performance of the approach is evaluated in terms of imperceptibility

and robustness against different attacks. The perceptual quality of watermarked image in terms of PSNR reached 37.75 dB, while the similarity between the extracted and the original watermarks in terms of NC reached 0.75 and the BER did not exceed 6% against compression, filtering, noise, sharpening and scaling attacks.

The set of image characteristics that are correlated to the HVS and their impact on the performance of the discussed watermarking approaches are presented in table 6 and the specifications of the illustrated watermarking approaches are presented in table 7. As well, the computational complexity and execution time of the illustrated approaches are presented in table 8. The presented execution time in table 8 represents to the overall running time for each of the illustrated approaches, as well the presented overall computation complexity in table 8 is computed after considering the computational complexities for the set of functions or algorithms that are used in the given approach.

Proposed approach	Image characteristics correlated to the HVS used	The significance of the image characteristics on the performance of the proposed approach
Thakkar et al., 2017 [106]	The geometric properties of low frequency sub-band (LL) of DWT of host image	The low frequency sub-band (LL) of DWT do not get modified after exposing to different kinds of geometric image processing attacks. Then, embedding watermark bits in left singular matrix U of SVD transform of LL sub-band of DWT improves the robustness against image processing attacks
Thanki et al., 2017 [108]	The texture and the brightness properties obtained from DCT coefficients, as well the capacity property of FDCuT transformation	FDCuT provides high embedding capacity; the size of resulted high frequency Curvelet sub-band after applying FDCuT is equal to the actual size of the host image. As well, FDCuT provides better imperceptibility compared to another transforms, because it represents the image in terms of edges. Embedding watermark in the mid coefficients of the high frequency Curvelet sub-band after applying DCT process enhances the robustness against attacks
Parah et al., 2017 [77]	The texture and brightness properties obtained from DCT coefficients	Embedding watermark in the mid coefficients of DCT of host image helps to make a balance between the imperceptibility and robustness rates
Mehto et al., 2016 [68]	The sensitivity of human eye to the representations of DWT sub-bands and the brightness property obtained from DC coefficient	Embedding watermark in the DCT coefficients of high frequency sub-band of DWT gains a balance between the imperceptibility and robustness rates. The high frequency coefficients of DWT give less significant characteristics of host image and any changes in these coefficients are not easily noticeable by HVS, while the average value of the DC coefficients in each DCT block of host image is used as a scaling factor to control the robustness of watermarking approach. The DC coefficient changes less with different attacks.
Singh et al., 2015 [96]	The correlation between the HVS and the parameters of the multi-resolution decomposition of the host image using DWT	Since the human eye is more sensitive to the low frequency coefficients (LL) sub-band of DWT, distributing the watermark on high frequency coefficients (HL and LH) of DWT causes less visual distortion in image.

Table 6: Image characteristics correlated to the HVS and their impact on the performance of several proposed medical images watermarking approaches.

Approach	Types of images tested	Objective	Domain based	Robust or Fragile	Blindness	Imperceptibility rate	Robustness rate	lossy or lossless
Thakkar et al., 2017 [106]	Medical gray-scale (x-ray, CT, mammography) and natural color images	Image authentication and identification	DWT and SVD	Robust	Blind	PSNR exceeded 43.0 dB and SSIM exceeded 0.95	BER<36% and NC ranged 0.35-1	Lossy
Thanki et al., 2017 [108]	Medical gray-scale (x-ray, US, MRI and CT) images	Copyright protection	FDCuT and DCT	Robust	Blind	PSNR reached 45 dB in average	NC reached 0.94 in average	Lossy [92]
Parah et al., 2017 [77]	Medical gray-scale (CT) images	Copyright protection and image identification	DCT	Robust	Blind	PSNR ranged 36-48 dB and SSIM reached 0.99	BER ranged 0-19.8% and NC ranged 0.44-0.99	Lossy
Mehto et al., 2016 [68]	Medical gray-scale (x-ray, MRI and CT) images	Provides patient's privacy	DCT and DWT	Fragile	Non-blind	PSNR ranged 40-45 dB and NC reached 1	Reversible watermarking	Lossless
Singh et al., 2015 [96]	Medical gray-scale (US, MRI, CT) images	Image authentication	DWT	Robust	Blind	PSNR reached 37.75 dB	BER<6% and NC<0.75	Lossy

Table 7: Specifications of several proposed medical images watermarking approaches.

Approach	Computational complexity	Overall computational complexity	Execution time (seconds)
Thakkar et al., 2017 [106]	• Complexity of 2nd-level DWT= $O(M\times N)$ [122] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of Hamming coding= $O(M\times N)^2$ [70]	$O(M\times N)^2$	1.24
Thanki et al., 2017 [108]	• Complexity of FDCuT= $O((M\times N)^2 log_2(M\times N))$ [15] • Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74]	$O((M\times N)^2 log_2(M\times N))$	29.95
Parah et al., 2017 [77]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned
Mehto et al., 2016 [68]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of 1st-level DWT= $O(M\times N)$ [122]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned
Singh et al., 2015 [96]	• Complexity of 2nd-level DWT= $O(M\times N)$ [122] • Complexity of pseudo-random sequences generation PN= $O(1)$ [46]	$O(M\times N)$	Not mentioned

Table 8: Computational complexity and execution time of several medical images watermarking approaches.

3.3.2 *Human Visual System Based Image Watermarking Approaches*

In [62], the authors proposed a robust and secure image watermarking approach based on logistic mapping and RSA algorithms. The proposed approach started by scrambling the watermark using logistic mapping algorithm, and then encrypting the scrambling parameters using RSA algorithm to guarantee the security of the hidden data. The host image is decomposed into four sub-bands (LL, LH, HL and HH) using 1-level DWT, then the low-frequency sub-band (LL) is transformed to SVD. The singular values of LL sub-band are modified by adding the scrambled watermark bits and by using proper scaling factor to control the embedding strength. The inverse DWT process is applied to generate the watermarked image. The watermarked image, the encrypted scrambled parameters and the original image are used in the extraction process (non-blind manner) to extract the watermark. The proposed approach is tested both on gray-scale and color images. In case of color image, the blue component is used for embedding watermark. This scheme guarantees least noticeable image quality distortion, since the human eye is less sensitive to any change in blue component rather than other components. The experiments results showed good performance in terms of imperceptibility and robustness. In case of gray-scale images, the PSNR reached 50 dB and the NC was ranged 0.61-1 against different attacks. While, in case of color images the PSNR reached 45.9 dB and the NC was ranged 0.60-0.97.

The authors in [131] proposed a blind image watermarking approach based on the Dual Tree Complex Wavelet Transform (DTCWT). A new visual masking model is proposed in this approach. The visual masking is built using Just Perceptual Weighting (JPW), which uses three HVS characteristics, namely: the sensitivity of spatial frequency, the local brightness masking sensitivity and the texture masking sensitivity. The Contrast Sensitivity Function (CSF) is used to calculate the spatial frequency sensitivity of each image block, and the Noise Visibility Function (NVF) is used to calculate the texture masking sensitivity of each image block. The local brightness masking sensitivity of each block is calculated according to the magnitude of the low frequency sub-bands of the DTCWT. Those functions are combined to compute a weight factor for each DTCWT coefficient. This weight describes the acceptable amount of changes on the DTCWT coefficients that corresponds to the sensitivity of the HVS. At the embedding phase, the high frequency coefficients of the transformed watermark via DTCWT are embedded in the high frequency coefficients of the transformed image via DTCWT. The amount of watermark coefficients that could be inserted in the host image coefficients with less quality distortion is maintained using the visual masking model. At the watermark detection phase, the Rao-test based detector [72] is used to verify the presence of the candidate watermark. Imperceptibility in terms of PSNR and SSIM reached 45 dB and 1, respectively. The robustness

ratio against different attacks is expressed through considering the probability of watermark detection with the probability of false alarm. The probability of watermark detection was ranged 0.80-1 with a false ratios ranged 10^{-4}–1.

The authors in [43] utilized the correlation between DCT coefficients of nearby blocks to propose a prediction based watermarking approach. The proposed approach joint Partly Sign-Altered Mean modulation (PSAM) and mixed modulation techniques for inter-block prediction. The embedding scheme adjusted a set of low frequency band DCT coefficients relatively to its predicted DCT coefficients, which gives ability to extract watermark in blind manner. The imperceptibility ratio in terms of PSNR and SSIM reached 39.5 dB and 0.96, respectively. While the BER reached 49.0% against cropping down attack and it did not exceed 12.8% against other attacks.

The authors in [44] proposed a blind image watermarking using the mixed modulation on DCT coefficients. The mixed modulation is done by integrating some favorable properties of Quantization Index Modulation (QIM) into relative modulation scheme. The QIM maps the DCT selected coefficients into a designated range according to binary values like DC category or AC category, while the relative modulation scheme modulates the DCT coefficient value by referring to its estimated one. The target of mixed modulation is to enable control over the parameters required to provide high resistance against commonly encountered attacks while maintaining less noticeable quality degradation. In this approach, the selected DCT coefficients are modified by watermark bits, which are scrambled using Arnold scrambling method [52], according to predefined boundaries given from QIM and low estimation differences between DCT coefficients from relative modulation scheme. These control parameters are intended to maintain good levels of imperceptibility and robustness. The imperceptibility ratio in terms of PSNR and SSIM reached 40.0 dB and 0.97, respectively. While, the BER against various attacks did not exceed 12.8%.

In [98], the authors proposed a color image watermarking approach based on Hessenberg transform. The largest coefficient in the upper Hessenberg matrix is used for embedding watermark. This element represents the maximum energy of a given transformed 4×4 block of the host image. In the process of watermark embedding, each layer of the color host image (R, G and B) is partitioned into non-overlapping 4×4 blocks and the Hessenberg transformation is applied on set of randomly selected blocks in each layer to embed watermark. The Hash pseudo-random replacement algorithm (i.e. based on MD5) is used to select the random blocks in order to improve the robustness of anti-cropping. The largest coefficients of the resulting upper Hessenberg matrices after applying Hessenberg transformation on the elected blocks are embedded with scrambled watermark bits by quantization technique. The Arnold transformation is applied on the watermark to ensure watermarking security. Inverse Hessenberg trans-

form is applied after the embedding process to obtain the watermarked image. The reverse processes are applied on the attacked watermarked image and the anti-Arnold transformation is applied in a blind manner to obtain the extracted watermark.

In [69], the authors proposed an image watermarking approach in YCoCg-R. The three components of YCoCg-R color space have low dependence to each other, then any change in one component has least impact on the other components. The property of YCoCg-R color space helps to enhance the robustness. In this approach, the RGB host image is converted into YCoCg-R color space. The Y component is selected for embedding watermark, and it is transformed to frequency domain using DCT in an 8×8 blocks. The complexity of each block is calculated using the variance function. The image blocks are sorted and the complex blocks are selected for embedding watermark. The complex blocks resistant more against JPEG compression attack. As well, the energy of each block is calculated using mean function in order to select proper embedding factor for each block. A block with higher energy, lower embedding factor is selected and for a block with lower energy, higher embedding factor is selected. The scrambled watermark bits using Arnold transformation (scrambling watermark helps to improve security) are embedded in five low frequency DCT coefficients in each selected block. The inverse DCT is applied to generate the watermarked. The watermark is extracted from attacked watermarked image in blind manner. The same processes that are applied on host image are applied on watermarked image to extract the watermark.

The authors in [88] proposed a DCT based-color multiple watermarking approach using Error-Correcting Codes ECC (repetition code design) method [30]. The green and blue spaces of the host image are transformed using DCT and then for each space the length (t) of a repetition code of watermark bits are used to select t-pair of DCT coefficients from middle band frequency (AC band). Each pair of DCT coefficients are swapped according to the value of watermark bit (either 0 or 1). In the extraction process, the t-pair of DCT coefficients from middle band frequency are selected from the attacked watermarked image. Then, by comparing the values of each pair of coefficients, the watermark is extracted blindly. The experiments result showed an interesting ratio of perceptual quality and robustness against common attacks. The PSNR reached 43 dB and BER was ranged 0-26%.

In [97], a spatial domain based color image watermarking approach is proposed. In the blue space of color image, the DC coefficient of a specific block is computed and adjusted by quantity value, which is choosed based on the value of watermark bit (either 0 or 1) and the quantization factor (Δ). Indeed, the DC coefficients of DCT transform are modified in the spatial domain. The input value for DC coefficients will be equal to the modified value of DC in DCT domain

that is computed by $\Delta M_{i,j}/b$; ($\Delta M_{i,j}$ is the modified value (acceptable quantity amount) of DC components and b is the size of processed block). To increase the security, the watermark is permuted using Hash pseudo-random permutation algorithm based on MD5. For the extraction process, the DC coefficients in spatial domain of the attacked watermarked image and the quantization factor (Δ) are used to extract the watermark in blind manner.

In [2], the authors proposed a spatial domain based color image watermarking. The proposed approach used Simple Image Region Detector (SIRD) method to identify the most appropriate sub-regions within image blocks to embed watermark without degrading the quality of the image. The blue space of RGB color image is used for embedding watermark due to insensitivity to the human eye comparing with red and green spaces. Indeed, the Least Significant Bits (LSBs) of blue space pixels are modified by watermark pixels and two embedding masks are used to ensure that the original color distributions are least affected. The experiment results showed good imperceptibility ratio; the PSNR was ranged 47.0-53.0 and SSIM was ranged 0.97-0.99. While, the watermarking approach showed worse robustness results against different attacks, the BER ranged 11.7-75.0 % against cropping and resizing attacks and the NC ranged 0.25-1.

The authors of [78], proposed a blind image watermarking approach based on DCT inter-block coefficient differencing. The approach utilizes the advantage of correlation between the DCT coefficients of adjacent blocks. The difference between the DCT coefficients of a block and the DCT coefficients of its subsequent block is computed to decide about the procedure for embedding watermark bits in the DCT coefficients. The watermark is encrypted using a randomly generated key to improve security. A scaling variable, embedding factor, DC coefficient and the median of first 9 AC coefficients of a given block decide the amount of modification in the DCT coefficient. The embedding factor is chosen for experimental purpose to obtain maximum robustness and least quality distortion of image. The proposed approach achieved good levels of imperceptibility and robustness. The PSNR reached 41.8 dB, while the BER did not exceed 16.0 %.

The set of image characteristics that are correlated to the HVS and their impact on the performance of the discussed images watermarking approaches are presented in table 9 and the specifications of the illustrated HVS based image watermarking approaches are presented in table 10. As well, the computational complexity and execution time of the illustrated approaches are also presented in table 11. The overall computation complexity in table 11 for each of the illustrated approaches is computed after considering the computational complexities for the set of functions or algorithms that are used in the given approach.

Proposed approach	Image characteristics correlated to the HVS used	The significance of the image characteristics on the performance of the proposed approach
Liu et al., 2018 [62]	The geometric properties of singular values and low frequency sub-band of DWT of host image	The LL sub-band of DWT and the uniqueness singular values of host image do not get modified after exposing to different kind of geometric image processing attacks, this property increases the robustness
Zebbiche et al., 2018 [131]	The sensitivity of spatial frequency, the local brightness and texture masking sensitivity properties that are inferred from the low frequency coefficients of the DTCWT	The functions of sensitivity of spatial frequency, the local brightness and texture masking sensitivity properties help to define the weight factor of each DTCWT coefficient. The weight factors decide the amount the watermark bits could be inserted in high frequency coefficients of the DTCWT with high imperceptibility ratio
Su et al., 2017 [98]	The properties of Hessenberg transform coefficients	Embedding watermark in the largest coefficient in the upper Hessenberg matrix of Hessenberg transform improves the robustness ratio, where this element represents the maximum energy of a given transformed block of the host image
Moosazadeh et al., 2017 [69]	The property of low dependency of the three components of YCoCg-R color space to each other	Embedding watermark in the low frequency DCT coefficients of one color space of YCoCg-R improve the robustness ratio. Any change in one component has least impact on the other components
Roy et al., 2017 [88]	The texture and brightness properties obtained from DCT coefficients and the sensitivity of the HVS to the color spaces	Embedding watermark in the mid DCT coefficients of green and blue components of host image helps to make a balance between the imperceptibility and robustness rates. The HVS is less sensitive to any change in the green and the blue components rather comparing with red component
Su et al., 2017 [97]	The sensitivity of the HVS to the color spaces and the average information of the overall magnitude of the processed block that is carried in DC coefficient of DCT	Embedding watermark in the low frequency coefficient (DC) of DCT of blue component of host image helps to make a balance between the imperceptibility and robustness rates. The HVS has least sensitivity to any change in the blue component comparing with the green and the red components
Abraham et al., 2017 [2]	The sensitivity of the HVS to the color spaces	Embedding watermark in LSB of blue space pixels helps to improve the imperceptibility ratio and the computational complexity
Hsu et al., 2017 [43], Hu et al., 2016 [44] and Parah et al., 2016 [78]	The correlation between the DCT coefficients of adjacent blocks expresses the texture	Embedding watermark in the low coefficients (LL) of DCT of host image helps to improve the robustness rate

Table 9: Image characteristics correlated to the HVS and their impact on the performance of several proposed images watermarking approaches.

Proposed approach	Types of targeted images	Objective	Domain based	Robust or Fragile	Blindness	Imperceptibility rate	Robustness rate	lossy or lossless
Liu et al., 2018 [62]	Natural color and gray-scale images	Image authentication	DWT and SVD	Robust	Non-blind	PSNR equal 45.9 dB in average	NC ranged 0.60-0.97	Lossy
Zebbiche et al., 2018 [131]	Natural color and gray-scale images	Image authentication	DTCWT	Robust	Blind	PSNR and SSIM reached 45 dB and 1, respectively	The probability of watermark detection ranged 0.80-1	Lossy
Hsu et al., 2017 [43]	Natural gray-scale images	Image authentication	DCT	Robust	Blind	PSNR and SSIM reached 39.5 dB and 0.96, respectively	BER reached 49.0% against cropping down attack and it did not exceed 12.8% against other attacks	Lossy
Hu et al., 2016 [44]	Natural gray-scale images	Image authentication	DCT	Robust	Blind	PSNR and SSIM reached 40.0 dB and 0.97, respectively	BER did not exceed 12.8%	Lossy
Su et al., 2017 [98]	Natural color images	Image authentication	Hessenberg transform	Robust	Blind	PSNR reached 37.6 dB and SSIM reached 0.94	NC ranged 0.63-1	Lossy
Moosazadeh et al., 2017 [69]	Natural color images	Image authentication (ownership protection)	DCT	Robust	Blind	PSNR reached 41.0 dB	BER did not exceed 12.8 % and NC ranged 0.42-1	Lossy
Roy et al., 2017 [88]	Natural color images	Image authentication	DCT	Robust	Blind	PSNR ranged 41-43 dB	BER ranged 0-26% ad NC ranged 0.82-1	Lossy
Su et al., 2017 [97]	Natural color images	Image authentication	Spatial domain	Robust	Blind	PSNR reached 50.0 dB and SSIM reached 0.99	NC ranged 0.76-1	Lossy
Abraham et al., 2017 [2]	Natural color images	Image authentication	Spatial domain	Fragile to geometric attacks	Non-blind	PSNR ranged 47.6-53.6 and SSIM ranged 0.97-0.99	BER reached 75.0 against cropping attack	Lossy
Parah et al., 2016 [78]	Natural color and gray-scale images	Image authentication	DCT	Robust	Blind	PSNR reached 41.8 dB	BER did not exceed 16.7 % and NC ranged 0.84-0.98	Lossy

Table 10: Specifications of several proposed HVS based image watermarking approaches.

Proposed approach	Computational complexity	Overall computational complexity	Execution time (seconds)
Liu et al., 2018 [62]	• Complexity of 1-level DWT= $O(M\times N)$ [122] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of logistic mapping = $O(M\times N)$ [87] • Complexity of RSA algorithm= $O(k^3)$, k is the number of digits in n :$n = p\times q$ (public key) [16]	$O(min(M\times N^2, M^2\times N))$	Not mentioned
Zebbiche et al., 2018 [131]	• Complexity of DTCWT= $O(M\times N)$ [113] • Complexity of CSF= $O(M\times N)$ [64] • Complexity of NVF= $O(M\times N)$ [111]	$O(M\times N)$	1.69
Hsu et al., 2017 [43]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned
Hu et al., 2016 [44]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of Arnold scrambling method= $O(M\times N)$ [52]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned
Su et al., 2017 [98]	• Complexity of Hessenberg transform= $O(M\times N)$ [17] • Complexity of Arnold scrambling method= $O(M\times N)$ [52] • Complexity of MD5-based Hash pseudo-random replacement algorithm= $O(k)$, k byte or bits [110]	$O(M\times N)$	0.88
Moosazadeh et al., 2017 [69]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of Arnold scrambling method= $O(M\times N)$ [52]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned
Roy et al., 2017 [88]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of Arnold scrambling method= $O(M\times N)$ [52]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned
Su et al., 2017 [97]	• Complexity of DC coefficients= $O((M\times N) log_2(M\times N))$ [74] • Complexity of MD5-based Hash pseudo-random permutation algorithm= $O(k)$, k byte or bits [110]	$O((M\times N) log_2(M\times N))$	5.99
Abraham et al., 2017 [2]	• Complexity of SIRD= $O(M\times N)$ [3]	$O(M\times N)$	Not mentioned
Parah et al., 2016 [78]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of randomly key generation = $O(1)$ [46]	$O((M\times N)^2 log_2(M\times N))$	Not mentioned

Table 11: Computational complexity and execution time of several HVS based image watermarking approaches.

3.3.3 *Intelligent Techniques and Human Visual System Based Image Watermarking Approaches*

The authors in [58] proposed a robust image watermarking approach in frequency domain based on HVS characteristics and rough set theory. The proposed approach deals with two problems that are related to the boundary of gray-

scale image's pixels and the statistical redundancy due to the shift invariance in DWT coefficients. These problems have a close relationship with the principles of HVS in terms of robustness and imperceptibility. Embedding watermark in wide range of gray-scale is uncertainty problem, since the optimal number of bits that could be embedded in the variation of gray-scale values without adversely affect the perceptual quality of image is imperfect perceptibility. In terms of HVS, this uncertainty problem may adversely affect image's contrast, then it may weaken the perceptual image quality. Moreover, the statistical redundancy ambiguity occurs due to the shift invariance problem symbolized in conventional DWT. The shift invariant problem symbolizes the variance in the energy of wavelet coefficients whenever the incoming signal is shifted, even though it's basically same signals. The statistical redundancy indicates inability and unpredictability to the actual sensitivity to the HVS. This in turn affects the perceptual quality of embedded image in case of watermarking. The rough set theory is used in this approach to deal with these problems and to design an efficient watermarking system able to ensure the imperceptibility and robustness. The proposed watermarking approach applied rough set theory on one sub-band of DWT, which is used as a reference image, to approximate its coefficients into upper and lower sets. The singular value of the watermark is embedded in the singular value of reference image. The experiments results showed that the imperceptibility in terms of PSNR reached 69.5 dB and the robustness in terms of BER and NC against different geometric and non-geometric attacks did not exceed 13% and 0.87, respectively.

In [1], the authors proposed a blind image watermarking approach using the Artificial Bee Colony (ABC) technique. The correlation between DCT coefficients of adjacent blocks is exploited to define the visual significant locations in host image. These locations are convenient for embedding watermark with maximum robustness and less image quality distortion. Indeed, the difference value between the coefficients of adjacent blocks defines the texture property of host image blocks. According to the watermark bit (either 0 or 1) and the difference value between two coefficients of adjacent DCT blocks, a single watermark bit is embedded by modifying the two coefficients of adjacent DCT blocks (one coefficient in each block). The ABC technique is used as a meta-heuristic optimization method for optimizing watermark-embedding process. The goal of this optimization is to achieve maximum level of robustness and lower level of noticeable image distortion. A new fitness function is proposed to optimize the embedding parameters in order to provide required convergence for the optimum values of robustness and imperceptibility. The imperceptibility ratio in term of PSNR was ranged 36.7-47.1 dB, while the BER was ranged 1-50%.

The authors in [75], proposed an adaptive image watermarking approach based on Fuzzy Inference System (FIS) of Mamdani type IF-THEN. The FIS is ap-

plied to calculate the orthogonal moments of the host image, and then the quantization factor for each moment is calculated. The set of orthogonal moments are embedded by watermark bits by dither modulation [18]. Indeed, the orthogonal moments describe the fine image information and can be used as significant visual moments to hold the watermark. Hence, the FIS uses the moments' quantization factors and a set of fuzzy linguistic terms to define the fuzzy membership functions, where the parameters of fuzzy membership functions are optimized using IF-THEN rules and Genetic Algorithm GA to improve the robustness and imperceptibility rates. The obtained optimized values of quantization factors are used as basis to decide the amount of bits that can be embedded in each moment without causing noticeable visual difference. The Minimum Distance Decoder (MDD) [31] is used to extract the watermark from the orthogonal moment of the attacked watermarked image in blind manner. The imperceptibility ratio reached 40.0 dB, while the BER was ranged 8-30%.

The authors in [48] proposed an optimized image watermarking approach based on HVS characteristics and integration between Fuzzy Inference System (FIS) and Back Propagation Artificial Neural Networks (BPANN). The approach can be summarized in three phases; fuzzification phase, where the approach calculates the texture and brightness sensitivity characteristics of the DCT coefficients of each image block. These characteristics are considered as an input to the fuzzy inference system of Mamdani type AND logic. The inference engine phase, where the input parameters are mapped into values between 0 and 1 based on predefined fuzzy inference rules. The result of this phase is a basis used to select some blocks, which are blocks with high texture and high luminance. After that, the centroid method based BPANN is implemented in the Defuzzification phase, where the center value and the eight neighbors elements for each image block became as input to BPANN as a training set to search for optimum weight factor to select approximately most appropriate coefficients to embed watermark bits with good robustness and imperceptibility. The efficient integration between FIS and BPANN in this approach provides the ability to optimize intensity factor (α). This factor is used in the embedding equation to balance between the ratio of robustness and imperceptibility. Additionally, the integration between FIS and BPANN introduced a fuzzy crisp set for the value of DCT coefficients that are more appropriate to embed watermark bit. The experiments result proved the efficiency of the proposed approach. The PSNR reached 48.5 dB, while the NC was ranged 0.73-1 against different attack scenarios.

The authors in [39] proposed an optimized image watermarking approach based on Genetic Algorithm (GA). The proposed approach analyzed the processed image with means of HVS characteristics to define texture regions in image, which are more appropriate to embed watermark robustly. The singular values of SVD transform, which express the contrast of image intensity, are

utilized to find the activity factor of each processed image block using a weight parameter (α). The approach selects the high activity factor blocks, which involve a good visual masking effect, to be as input in watermark embedding process. The embedding process is carried out in the DC coefficients of the transformed DCT image rather than AC coefficients, where the DC coefficients are more appropriate to embed watermark robustly. The embedding process as well uses an embedding intensity parameter (β), which controls the degree of image quality. The GA cooperates in this approach to optimize α and β parameters, which reflect both the robustness and the perceptual quality of the watermarked image. A fitness function of GA considers the PSNR, the NC and the SSIM parameters under several attacking conditions for processed images to find approximately the optimal value of α and β. The proposed watermarking approach was tested against additive noise, median filtering and JPEG loss compression (quality factor=60) attacks. The PSNR of the proposed approach with means of different capacity thresholds was ranged 31-46 dB in average and the experiments result showed that the NC was ranged 0.83-0.93.

The authors in [47] proposed an optimized digital image watermarking approach based on HVS characteristics and Fuzzy Inference System (FIS). The approach intended to find approximately best weighting factors (S1,S2,S3), which are used in the embedding watermark procedure to diminish the conflict between the imperceptibility and robustness requirements. The proposed approach uses Matlab packages to compute the set of HVS characteristics from the DCT coefficients of each processed image block. These characteristics include the luminance, texture, edge and frequency sensitivities, to be as input vector for FIS. The FIS uses three inference procedures to find three weighting factors used in the embedding watermark equation. The embedding is done in the center coefficient of each image DCT block to build the watermarked image. The experiment results showed that the PSNR reached 42.3 dB and the NC against different attacks was ranged 64-100%.

In [42], the authors proposed a joint Backward-Propagation Neural Network (BPNN) technique and Just-Noticeable Difference (JND) model to exploit the inter-block prediction and visibility thresholds in DCT to achieve effective blind image watermarking. The relative modulation scheme is used for embedding the scrambled watermark (chaotic mapping [119] method is used to scramble watermark) by adjusting the intended DCT coefficients with their BPNN predictions, and the JND value is used to decide the embedding strength. This approach achieved a balance between robustness and imperceptibility. As well, the embedded watermark was protected against several attacks. The experiment results showed that the PSNR reached 40.1 dB and the BER against different attacks did not exceed 15.3%.

The authors in [59] proposed an optimized image watermarking approach based on GA and SVD transform. Firstly, the singular matrix (S) of the transformed image (USV) is embedded with watermark using a scalar factor (α)$\in$[0,1], responsible to control robustness and the perceptual quality of watermarked image. The approach introduced an optimized technique to find approximately optimum value of scale factor using Tournament selection method [12], which is one of the most widely used selection strategies in evolutionary algorithms. The approach initially assigns scalar factor (α) to be equal 0.5 and then the fitness value is computed by means of PSNR and NC such as *fitness=robustness-imperceptibility*. The resulting fitness value is considered as reference in the optimization process. Then, the Tournament selection method involves a random selection of two individuals from a population of individuals, with values between 0 and 1, to be parent to produce four chromosomes according to Tournament selection mechanisms. These four values are used in the embedding process to find which one gains the minimum fitness value. The one with the minimum fitness is selected for successive generations, till the population evolves towards minimum fitness and then finds approximately the optimal scalar factor (α). The experiments result proved that considering this approach to find scaling factor is efficient to obtain high robustness and imperceptibility. In case of Lena image, the PSNR reached 47.5 dB, and the NC reached 0.99 against different image processing attacks.

The authors in [90] proposed a DWT-SVD-based image watermarking approach using Dynamic-Particle Swarm Optimization (DPSO) algorithm. The proposed watermarking approach works to balance between imperceptibility and robustness by controlling the scaling factor, which defines the amount of watermark bits that could be embedded into host image with less image quality degradation and high robustness. The DPSO algorithm is an efficient optimization algorithm used to find the approximately optimal value of the scaling factor for different combination of host and watermark images. Fractional principal components of watermark, which are controlled by scaling factor, is inserted in the singular values of low frequency DWT sub-band of each color space of host image. The fractional principal components of watermark are computed after applying Principal Components Analysis PCA. The experiments result showed that the PSNR reached 36.87 dB and the robustness in terms of PSNR was ranged 21.9-27.3 dB against noise addition, rotation and blurring attacks.

The authors in [116] proposed a robust color image watermarking approach that resist most against geometric attacks based on Fuzzy Least Squares Support Vector Machine (FLS-SVM) and Bessel *K* Form distribution (BKF). The FLS-SVM is a version of the LS-SVM enhanced by reducing the effect of outliers and noises in data, while the BKF is one of the efficient geometric correction methods. The idea can be organized through two phases; phase 1 involves the embedding

watermark by finding the maximal center region of the host image, where this region typically has least amount of lost data to resist more against the rotation and cropping attacks. The scrambled watermark using affine transform [52] is embedded in the low frequency coefficients of the Quaternion Discrete Fourier Transform (QDFT) of selected region to obtain high robustness and imperceptibility, and the Inverse Quaternion Discrete Fourier Transform (IQDFT) is achieved to build the watermarked image. In phase 2, the geometric correction on attacked image is applied by BKF and FLS-SVM, where the attacked image is initially converted into gray-scale image and the 2QWT (Quaternion Wavelet Transform) is applied on it. The shape and scale parameters of BKF are used to construct the feature vector. This vector is considered as training data to the FLS-SVM to predict with approximation the best value for rotation angle, scaling factor and horizontal or vertical distance. Hence, the model will be able to correct the color image. The proposed approach is tested against different attacks scenarios on many color images. The experiments result proved the efficiency of the proposed approach in terms of imperceptibility and robustness, where the PSNR reached 40 dB, while the BER was ranged 0.3-2.0% against different geometric and non-geometric attacks. In case of scaling 256×256 attack, the BER was very high and reached 43.7%.

The set of image characteristics that are correlated to the HVS and their impact on the performance of discussed images watermarking approaches using AI techniques are presented in table 12 and the specifications of the illustrated AI and HVS based image watermarking approaches are presented in table 13. As well, the computational complexity of the illustrated approaches are presented in table 14. The overall computation complexity in table 14 for each of the illustrated approaches is computed after considering the computational complexities for the set of functions or algorithms that are used in the given approach. It is worth to note that based on the available information in the illustrated approaches, the execution time aspect has not presented in table 14.

Proposed approach	Intelligent technique used	Image characteristics correlated to the HVS used	The significance of the image characteristics and AI technique on the performance of the proposed approach
Kumar et al., 2017 [58]	Rough set theory	The properties of singular values and DWT bands	Rough set approximated one DWT band into upper and lower sets. The upper and lower sets are used as weight factors in embedding process to improve image quality. Watermark is also embedded in the singular values to improve the imperceptibility and robustness rates
Abdelhakim et al., 2017 [1]	Artificial Bee Colony	The texture property obtained from the difference value between the DCT coefficients of adjacent blocks	The difference value between the DCT coefficients of adjacent blocks expresses texture characteristic. High difference value expresses more texture than low difference value. Increasing the value of a DCT coefficient according to the others enhances the imperceptibility but may not enhance the robustness. Then, optimizing two embedding parameters to maintain the maximum number of watermark bits that could be embedded in DCT coefficients led to obtain maximum level of robustness and lower level of image distortion
Papakostas et al., 2016 [75]	FIS and GA	Orthogonal moments of the spatial pixels of image that represent the fine image information	FIS generated the quantization factors of orthogonal moment to control the embedding strength of the watermark, while the GA optimized these factors to find the maximum number of bits that can be added to the image without causing visual distortion
Jagadeesh et al., 2016 [48] and Jagadeesh et al., 2015 [47]	FIS and BPANN	The texture and brightness properties obtained from DCT coefficients	FIS constructed a basis for selecting the high textured and high luminance blocks for holding watermark. BPANN optimized weight factor of embedding process to improve the robustness and imperceptibility rates
Han et al., 2016 [39] and Lai et al., 2011 [59]	Genetic algorithm	The singular values represent the luminance	SVD provides many attractive properties correlated to HVS. Singular values stand for the luminance of the image where embedding a small data to an image, large variation of its singular values does not occur. As well, singular values have many properties that are particularly robust to geometric attacks. Hence, optimizing the embedding factor to maintain the maximum number of watermark bits that could be embedded in singular values led to obtain maximum level of robustness and lower level of image distortion
Hsu et al., 2015 [42]	BPNN	The correlation between the DCT coefficients of adjacent blocks expresses the texture	BPNN explored the correlation between the DCT coefficient to increase the value of one DCT coefficient according to the other to improve the imperceptibility and robustness rates
Saxena et al., 2018 [90]	DPSO	The properties of singular values and DWT bands	Singular values stand for the luminance of the image where embedding a small data to an image, large variation of its singular values does not occur. As well, singular values have many properties that are particularly robust to geometric attacks. The energy distribution in DWT is concentrated in low frequencies and since the human eye is more sensitive to the low frequency coefficients, so embedding the watermark on high frequency coefficients causes less visual distortion in image. The DPSO algorithm is an efficient optimization algorithm used to find the approximately optimal value of the scaling factor for different host images. Controlling the scaling factor defines the amount of watermark bits that could be embedded into host image with less image quality degradation and high robustness
Wang et al., 2017 [116]	FLS-SVM and BKF	The texture property obtained from the low frequency coefficients of the QDFT transform	The property of low frequency coefficient of the QDFT allow embedding watermark with high robustness against rotation attack. The shape and scale parameters of BKF are used as an input for training data in the FLS-SVM to predict with approximation the best value for rotation angle, scaling factor and horizontal or vertical distance. Hence, the approach is able to correct the host image and be robust against rotation attack

Table 12: Image characteristics correlated to the HVS and their impact on the performance of several proposed images watermarking approaches using AI techniques.

Approach	Types of targeted images	Objective	Domain based	Robust or Fragile	Blindness	Imperceptibility rate	Robustness rate	lossy or lossless
Kumar et al., 2017 [58]	Natural gray-scale images	Image authentication	DWT and SVD	Robust	Semi-blind	PSNR reached 69.5 dB	BER and NC did not exceed 13% and 0.87, respectively	Lossy
Abdelhakim et al., 2017 [1]	Natural gray-scale images	Image authentication	DCT	Robust	Blind	PSNR ranged 36.7-47.1 dB	BER ranged 1-50%	Lossy
Papakostas et al., 2016 [75]	Natural gray-scale images	Image authentication	Orthogonal moments	Robust	Blind	PSNR reached 40.0 dB	BER ranged 8-30%	Lossy
Jagadeesh et al., 2016 [48]	Natural gray-scale images	Image authentication	DCT	Robust	Blind	PSNR reached 48.5 dB	NC ranged 0.73-1	Lossy
Han et al., 2016 [39]	Natural gray-scale images	Image authentication	DCT and SVD	Robust	Non-blind	PSNR ranged 31-46 dB in average	NC ranged 0.83-0.93	Lossy
Jagadeesh et al., 2015 [47]	Natural gray-scale images	Image authentication	DCT	Robust	Blind	PSNR reached 42.3 dB	NC ranged 0.64-1	Lossy
Hsu et al., 2015 [42]	Natural gray-scale images	Image authentication	DCT	Robust	Blind	PSNR reached 40.1 dB	BER did not exceed 15.3%	Lossy
Lai et al., 2011 [59]	Natural gray-scale images	Image authentication	SVD	Robust	Semi-blind	PSNR reached 47.5 dB	NC reached 0.99	Lossy
Saxena et al., 2018 [90]	Natural color images	Image authentication	DWT and SVD	Robust	Non-blind	PSNR reached 36.87 dB	PSNR ranged 21.9-27.3 dB	Lossy
Wang et al., 2017 [116]	Natural color images	Image authentication	QWT and QDFT	Fragile to local geometrical distortions	Blind	PSNR reached 41.7 dB	BER reached 43.7% (geometric attacks) and 7.5% (non-geometric attacks)	Lossy

Table 13: Specifications of several AI and HVS based image watermarking approaches.

Approach	Computational complexity	Overall computational complexity
Kumar et al., 2017 [58]	• Complexity of 1st-level DWT= $O(M\times N)$ [122] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of applying rough set theory= $O(M\times N)$	$O(min(M\times N^2, M^2\times N))$
Abdelhakim et al., 2017 [1]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of ABC= $O((M\times N)^2 \times k \times i)$, k is the number of attributes and i is the number of iteration [23]	$O((M\times N)^2 log_2(M\times N))$
Papakostas et al., 2016 [75]	• Complexity of Orthogonal moments calculation= $O(M\times N)$ [76] • Complexity of Minimum Distance Decoder (MDD)= $O(M\times N)$ [75] • Complexity of GA= $O(P\times G)$, where P is the population size and G is the number of generations [29] • Complexity of FIS= $O(M\times N\times p)$, where p is the size of input variables [37]	$O(M\times N\times p)$
Jagadeesh et al., 2016 [48]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of FIS= $O(M\times N\times p)$, where p is the size of input variables [37] • Complexity of BPANN= $O((M\times N)\times p\times q+p\times(M\times N)\times log(M\times N))$, p is number of input feature vectors, q is number of output vectors [36]	$O((M\times N)^2 log_2(M\times N))$
Han et al., 2016 [39]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of GA= $O(P\times G)$, where P is the population size and G is the number of generations [29]	$O((M\times N)^2 log_2(M\times N))$
Jagadeesh et al., 2015 [47]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of FIS= $O(M\times N\times p)$, where p is the size of input variables [37]	$O((M\times N)^2 log_2(M\times N))$
Hsu et al., 2015 [42]	• Complexity of 2D-DCT= $O((M\times N)^2 log_2(M\times N))$ [74] • Complexity of BPANN= $O((M\times N)\times p\times q+p\times(M\times N)\times log(M\times N))$, p is number of input feature vectors, q is number of output vectors [36]	$O((M\times N)^2 log_2(M\times N))$
Lai et al., 2011 [59]	• Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of Tournament selection method= $O(M\times N)$ [12] • Complexity of GA= $O(P\times G)$, where P is the population size and G is the number of generations [29]	$O(min(M\times N^2, M^2\times N))$
Saxena et al., 2018 [90]	• Complexity of 1st-level DWT= $O(M\times N)$ [122] • Complexity of SVD= $O(min(M\times N^2, M^2\times N))$ [65] • Complexity of PCA= $O(M\times N\times min(M,N))$ [28]	$O(min(M\times N^2, M^2\times N))$
Wang et al., 2017 [116]	• Complexity of QDFT= $O(M\times N)$ [73] • Complexity of 2nd-level QWT= $O(M\times N)$ [122] • Complexity of Arnold scrambling method= $O(M\times N)$ [52]	$O(M\times N)$

Table 14: Computational complexity of several AI and HVS based image watermarking approaches.

3.4 CONCLUSION

Several image watermarking approaches are presented in this chapter. These approaches are presented through four categories; the first category presents set of image zero-watermarking approaches. The second category presents set of medical image watermarking approaches, the third category presents set of HVS based image watermarking approaches and the fourth category presents intelligent images watermarking approaches that are correlated to the HVS.

Most of the proposed zero-watermarking approaches are based on extracting some robust features to build zero-watermark from the transformed coefficients. Each of the proposed approaches that extracts the robust feature from SVD, DCT, Bessel-Fourier transform or PCET coefficients requires high computation complexity comparing to other approaches that are based on DWT, QEMs or NURP. In addition, most of the proposed zero-watermarking approaches require applying some encryption techniques to secure the generated zero-watermarks; this consumes more execution time. The achieved robustness ratio in the proposed zero-watermarking approach is acceptable against different attacks.

In case of the other AI and HVS based image watermarking approaches using spatial/transformed domains, most of the analyzed image characteristics that are used to identify the significant visual locations/coefficients for embedding watermark are achieved in the frequency domains. This has a negative impact on the computational complexity and execution time. In spite of their low complexity, no much proposed approaches are based on the spatial pixels to analyze different image characteristics that help to identify the significant visual locations for embedding watermark. The main explanations for embedding watermark in the frequency coefficients rather than spatial pixels are the fragility against geometric attacks, and the degradation on the perceptual quality of host images. These arguments can be refuted by dealing with some uncertainty problems that are related to the spatial pixels like the uncertainty problem of embedding watermark in wide range pixels values and the effect of embedded watermark bits on the correlations of adjacent pixels. Analyzing the relationships between image pixels and HVS is an important point for designing efficient image watermarking approach based on spatial domain. As well, assigning importance scales for different features that are used in defining significant visual locations in host images is also an important factor.

The various AI techniques have a vital role to solve these issues. Indeed, they may be used to enhance watermarking approaches by (i) identifying the best locations/coefficients among many alternatives to embed the watermark and (ii) finding an optimized scaling factor to control the amount of watermark bits that can be embedded in different location/coefficients in host image without causing less image perceptual quality and less robustness against different attacks.

Part II

CONTRIBUTION

Chapter 4

ZERO-WATERMARKING APPROACH FOR MEDICAL IMAGES BASED ON JACOBIAN MATRIX

Contents

4.1 INTRODUCTION

Sharing and archiving the patient's medical images efficiently through diverse e-healthcare applications has become an urgent requirement [106]. It needs to ensure the authenticity when exchanging the patients' images, alleviating fraudulent activities and resisting against different illegal manipulations [25]. An authentication scheme has to be developed and be convenient with limited resources in an e-healthcare network, rather than those based on conventional cryptographic and frequency/spatial digital watermarking approaches, which embed the secret data within medical images [134][135]. A zero watermarking scheme aims to construct the watermark from the relevant features of the host image without any alteration [33][94]. The need for a zero watermarking system in Telemedicine becomes essential to transmit the medical images through an e-healthcare network authentically. This is due to many reasons that include: (i) a zero-watermarking algorithm does not make any modification in the original

image and keeps the same size of the original image [114]. (ii) The conflicting requirements in the conventional cryptographic and frequency/spatial digital watermarking (like capacity and perceptual similarity) are not taken into consideration in the zero-watermarking [114]. (iii) Building a watermark in a zero-watermarking approach is based on extracting the key features from the host image. This does not provide any information that the attacker can use to affect the watermark [114]. (iv) The medical images are not a subject to any degradation in term of visual quality and also help to avoid any risk of misdiagnosis [106].

Generally, two aspects should be considered when designing a new zero-watermarking approach. These aspects include proposing an approach with low complexity and building a meaningful watermark from the original image rather than frequency coefficients such as the DWT, the DCT and the SVD where the complexity increase [86][95][96][68][77][106][108]. Furthermore, it is necessary to secure the watermark when sending to the receiver.

This chapter proposes a new zero watermarking approach, which aims to ensure the authenticity of the transmitted medical images through an e-healthcare network based on a specific parameter extracted from the host image. The zero watermarking system that is implemented in this approach is based on partitioning the host image into 8×8 non-overlapping blocks, and accumulating a subtraction process between these blocks by exploring the JPEG file QM to generate the final 8×8 matrix. An average value of this matrix is computed and used as a key input to the Jacobian matrix model to construct a meaningful watermark. The proposed approach explores the Jacobian matrix principle to construct a watermark. The important parameter of the Jacobian matrix model is the average value of the medical image blocks intensity. Two metrics are used to evaluate the efficiency of the proposed approach in terms of robustness including: the measure of error's probability explained by Bit Error Rate (BER) and the measure of perceptual similarity between the original watermark and the extracted one by a Normalized Correlation Coefficient (NC). The proposed approach achieves the authentication of medical images and robustness against different geometric and non-geometric attacks. Furthermore, the proposed scheme may help the researcher to develop a new approach to control access on patient data and the relevant medical records [106]. The proposed approach is discussed in details in this chapter.

The rest of the chapter is organized as follows. Section 4.2 introduces the Jacobian matrix principle. Section 4.3 illustrates the system model including watermark generation and the proposed Jacobian matrix model. The experiment's result is illustrated in section 4.4 and the computational complexity is presented in section 4.5. The comparison study is tackled in section 4.6 and the system analysis is discussed in section 4.7. Section 4.8 concludes the chapter.

4.2 JACOBIAN MATRIX

Suppose *f:* $R^n \rightarrow R^m$ is a function with inputs x_1,x_2,...,x_n. Where the vector x = (x_1,x_2,...,x_n) $\in R^n$ and outputs $f_1(x_1,x_2,...,x_n)$, $f_2(x_1,x_2,...,x_n)$,...$f_m(x_1,x_2,...,x_n)$ such that the vector $f(x) \in R^m$. Let that (k_1,k_2,...,k_n) is a point in the domain of f such that f_1 is differentiable at (k_1,k_2,...,k_n).

The Jacobian matrix J of f at (k_1,k_2,...,k_n) is a $m \times n$ matrix of numbers whose $(i,j)^{th}$ entry is given by:

$$J = \frac{\partial f_i}{\partial x_j}(x_1, x_2, ..., x_n)_{|(x_1,x_2,...,x_n)=(k_1,k_2,...,k_n)} \tag{17}$$

Here is how the matrix looks:

$$J = \frac{\partial f}{\partial x} = \begin{bmatrix} \frac{\partial f}{\partial x_1} & \cdots & \frac{\partial f}{\partial x_n} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{\partial f_1}{\partial x_1}(x_1, x_2, ..., x_n)_{|(x_1,x_2,...,x_n)=(k_1,k_2,...,k_n)} & \cdots & \frac{\partial f_1}{\partial x_n}(x_1, x_2, ..., x_n)_{|(x_1,x_2,...,x_n)=(k_1,k_2,...,k_n)} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(x_1, x_2, ..., x_n)_{|(x_1,x_2,...,x_n)=(k_1,k_2,...,k_n)} & \cdots & \frac{\partial f_m}{\partial x_n}(x_1, x_2, ..., x_n)_{|(x_1,x_2,...,x_n)=(k_1,k_2,...,k_n)} \end{bmatrix}$$

4.3 PROPOSED ZERO-WATERMARKING APPROACH

The proposed approach aims to build a robust watermark from the original (host) image pixel values. The key value (k) is computed with means of pixels values of the original image and the QM from the JPEG bitstream. This k is considered as an input to the Jacobian matrix model to generate an 8×8 matrix. The given matrix can be written as a meaningful image. A zero-watermarking approach involves many processes that are described in detail throughout the following sections. The framework of the proposed approach is illustrated in figure 15, which combines all processes for both sender and receiver.

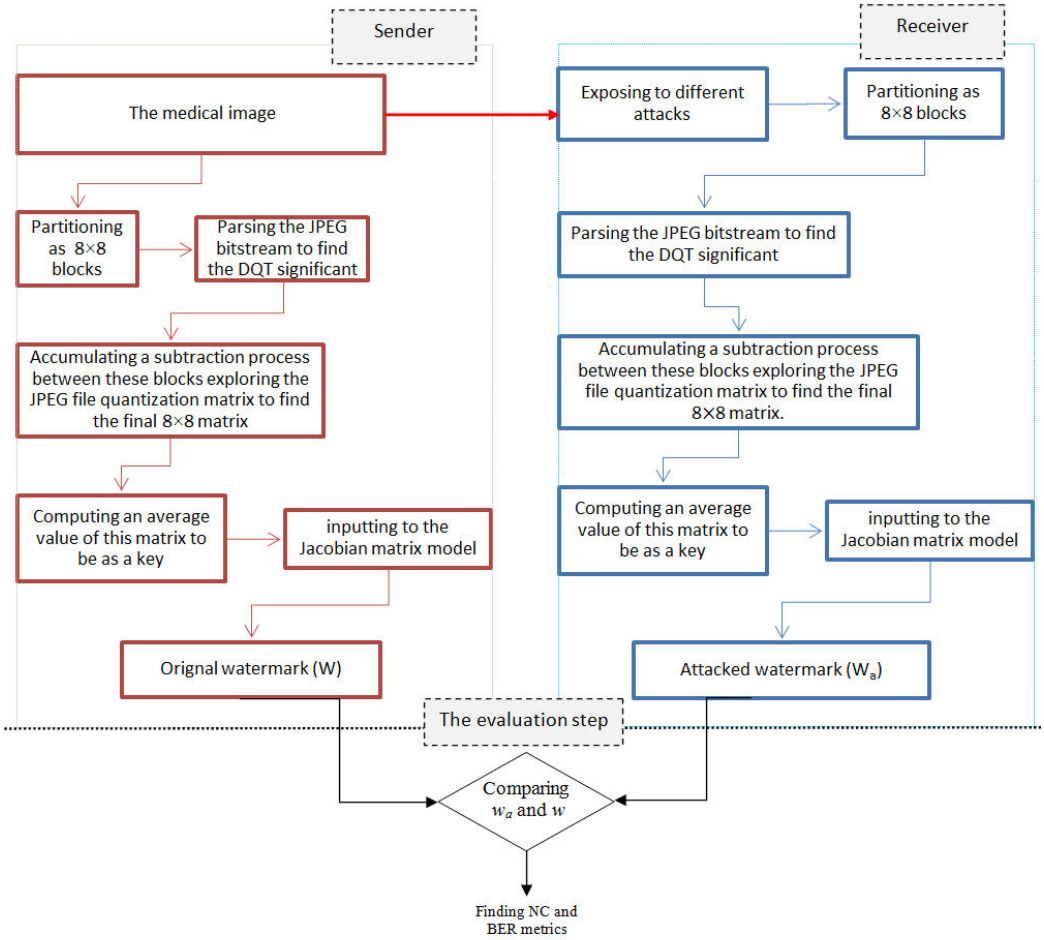


Figure 15: The framework of the suggested model.

4.3.1 *Extracting the quantization matrix from JPEG Bitstream*

In the first step, the proposed approach is initiated by parsing the JPEG file of the host image to extract the QM. The QM is one of the segments that represent the JPEG file for a given image. Each of these segments defines a specified chunk of JPEG file structure and starts by a specified flag [34]. The QM may differ from one image to another based on its nature. The 64 bytes QM starts from FF DB flags. Figure 16 shows the composed segments of the JPEG bitstream in terms of their flags and their value. The QM segment is the concerned part in our work. The extracted 8×8 QM is used as a fixed indicator to generate the watermark. Algorithm 1 illustrates the pseudo-code of this process.

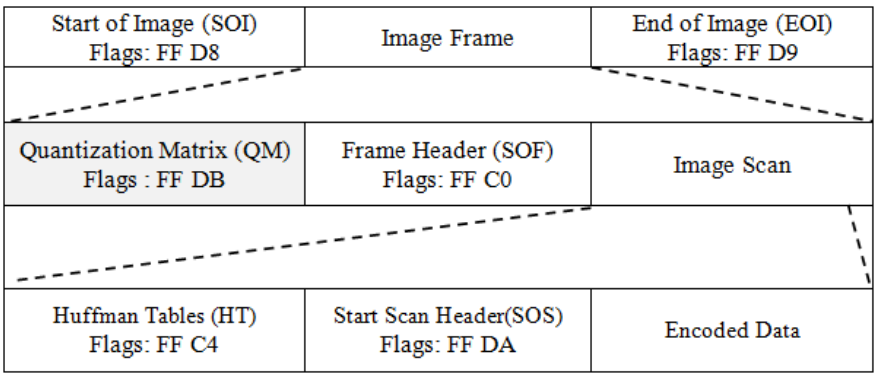


Figure 16: Syntax of JPEG file structure.

Algorithm 1 The pseudo-code of extraction QM in zero-watermarking approach for medical images based on Jacobian matrix.

1: **Input:** original image I
2: **begin**
3: open the JPEG bitstream file
4: parsing the JPEG bitstream file to find the Define Quantization Table (DQT) significant by marker *FFDB* in hexadecimal
5: save the 64 bytes of DQT segment into QM as 8×8 matrix in zig-zag order
6: close the JPEG file
7: **end**
8: **output:** An 8×8 QM

4.3.2 *Key (k) Extraction*

In the process of watermark generation, the original image is partitioned into 8×8 non-overlapped blocks. All blocks are considered as an input to accumulate subtraction process until outcome with a single 8×8 block. The subtraction process starts by subtracting the first 8×8 block of the original image and the 8×8 QM. The average value of the resulted 8×8 block is utilized as a key k, and will be an input to the Jacobian matrix model to generate a zero watermark. In practice, using the QM in the subtraction process avoids reaching a zero matrix. The computation of the average value k and the use of the Jacobian matrix model in the proposed approach are discussed in the system analysis section 4.7. Figure 17 below illustrates the watermark generation process based on k and its corresponding Jacobian model. In addition, algorithm 2 presents the pseudo-code of this process.

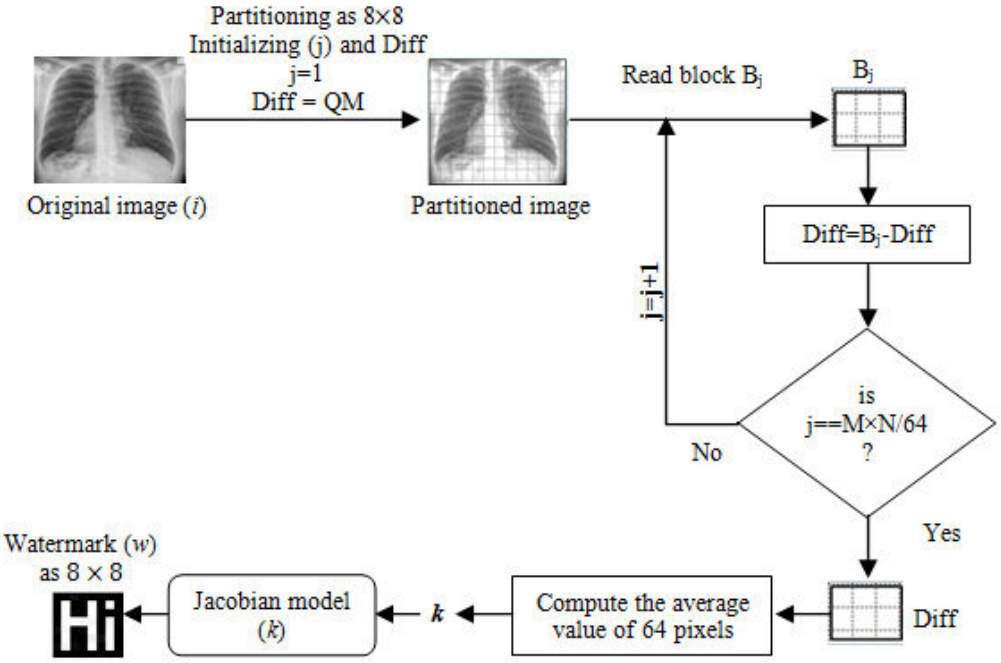


Figure 17: The watermark generation framework.

Algorithm 2 The pseudo-code of key (k) extraction in zero-watermarking approach for medical images based on Jacobian matrix.

Initialization: *Diff*=QM and *j=1*
Input: original image I in square size $M \times N$
begin
partitioning I into 8×8 blocks results with $M \times N/64$ blocks (B_j: $j=1,2,...,M \times N/64$)
while $j \neq M \times N/64$ **do**
    read B_j value
    $Diff=B_j\text{-}Diff$
    $j=j+1$
end while
k=average value of 64 pixels of resulting *Diff* matrix
end
output: key k

Based on the Jacobian matrix model illustrated in section 4.2, we suggest eight functions with eight parameters to generate an 8×8 matrix that can be exploited as a meaningful image (i.e. zero-watermark). These functions are stated below from y_1 until y_8. One of the parameters is equal to k, while the rests are equal to zeros. By applying the Jacobian functions, we can conclude that k is the most significant value, which is utilized in building a zero-watermark.

The proposed Jacobian matrix model consists of eight functions *f:* $R^8 \rightarrow R^8$ with these components:

$y_1 = x_1$

$y_2 = x_2 \times x_1 + x_5 \times x_1 + x_7 \times x_1$

$y_3 = x_2 \times x_1 + x_5 \times x_1$

$y_4 = x_2 \times x_1 + x_3 \times x_1 + x_4 \times x_1 + x_5 \times x_1 + x_7 \times x_1$

$y_5 = x_2 \times x_1 + x_5 \times x_1 + x_7 \times x_1$

$y_6 = x_2 \times x_1 + x_5 \times x_1 + x_7 \times x_1$

$y_7 = x_2 \times x_1 + x_5 \times x_1 + x_7 \times x_1$

$y_8 = x_6 \times x_8$

The Jacobian matrix J of f is a 8×8 matrix given by:

$$J_f(x_1,\ldots,x_8) = \begin{bmatrix} \frac{\partial y_1}{\partial x_1} & \frac{\partial y_1}{\partial x_2} & \frac{\partial y_1}{\partial x_3} & \frac{\partial y_1}{\partial x_4} & \frac{\partial y_1}{\partial x_5} & \frac{\partial y_1}{\partial x_6} & \frac{\partial y_1}{\partial x_7} & \frac{\partial y_1}{\partial x_8} \\ \frac{\partial y_2}{\partial x_1} & \frac{\partial y_2}{\partial x_2} & \frac{\partial y_2}{\partial x_3} & \frac{\partial y_2}{\partial x_4} & \frac{\partial y_2}{\partial x_5} & \frac{\partial y_2}{\partial x_6} & \frac{\partial y_2}{\partial x_7} & \frac{\partial y_2}{\partial x_8} \\ \frac{\partial y_3}{\partial x_1} & \frac{\partial y_3}{\partial x_2} & \frac{\partial y_3}{\partial x_3} & \frac{\partial y_3}{\partial x_4} & \frac{\partial y_3}{\partial x_5} & \frac{\partial y_3}{\partial x_6} & \frac{\partial y_3}{\partial x_7} & \frac{\partial y_3}{\partial x_8} \\ \frac{\partial y_4}{\partial x_1} & \frac{\partial y_4}{\partial x_2} & \frac{\partial y_4}{\partial x_3} & \frac{\partial y_4}{\partial x_4} & \frac{\partial y_4}{\partial x_5} & \frac{\partial y_4}{\partial x_6} & \frac{\partial y_4}{\partial x_7} & \frac{\partial y_4}{\partial x_8} \\ \frac{\partial y_5}{\partial x_1} & \frac{\partial y_5}{\partial x_2} & \frac{\partial y_5}{\partial x_3} & \frac{\partial y_5}{\partial x_4} & \frac{\partial y_5}{\partial x_5} & \frac{\partial y_5}{\partial x_6} & \frac{\partial y_5}{\partial x_7} & \frac{\partial y_5}{\partial x_8} \\ \frac{\partial y_6}{\partial x_1} & \frac{\partial y_6}{\partial x_2} & \frac{\partial y_6}{\partial x_3} & \frac{\partial y_6}{\partial x_4} & \frac{\partial y_6}{\partial x_5} & \frac{\partial y_6}{\partial x_6} & \frac{\partial y_6}{\partial x_7} & \frac{\partial y_6}{\partial x_8} \\ \frac{\partial y_7}{\partial x_1} & \frac{\partial y_7}{\partial x_2} & \frac{\partial y_7}{\partial x_3} & \frac{\partial y_7}{\partial x_4} & \frac{\partial y_7}{\partial x_5} & \frac{\partial y_7}{\partial x_6} & \frac{\partial y_7}{\partial x_7} & \frac{\partial y_7}{\partial x_8} \\ \frac{\partial y_8}{\partial x_1} & \frac{\partial y_8}{\partial x_2} & \frac{\partial y_8}{\partial x_3} & \frac{\partial y_8}{\partial x_4} & \frac{\partial y_8}{\partial x_5} & \frac{\partial y_8}{\partial x_6} & \frac{\partial y_8}{\partial x_7} & \frac{\partial y_8}{\partial x_8} \end{bmatrix}$$

As example: Let the computed k is equal to 255. This value is assigned to x_1 and the other parameters (x_2,x_3,x_4,x_5,x_6,x_7,x_8) are equal to zeros. The Jacobian matrix model with such inputs starts its calculations to obtain the following matrix:

$$J_f(x_1,\ldots,x_8) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 255 & 0 & 0 & 255 & 0 & 255 & 0 \\ 0 & 255 & 0 & 0 & 255 & 0 & 0 & 0 \\ 0 & 255 & 255 & 255 & 255 & 0 & 255 & 0 \\ 0 & 255 & 0 & 0 & 255 & 0 & 255 & 0 \\ 0 & 255 & 0 & 0 & 255 & 0 & 255 & 0 \\ 0 & 255 & 0 & 0 & 255 & 0 & 255 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

This 8×8 Jacobian matrix can be written as an image of size 8×8 to generate a robust zero-watermark as illustrated in figure 18. Algorithm 3 illustrates the pseudo-code of the zero-watermark generation.

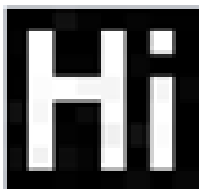


Figure 18: Watermark (w) as 8×8 block.

Algorithm 3 The pseudo-code of zero-watermark generation in zero-watermarking approach for medical images based on Jacobian matrix.

1: **Initialization:** x_1=k and $\{x_2,x_3,...,x_8\}$=0
2: **Input:** the extracted key (k), the seven zeros parameters
3: **begin**
4: apply the proposed Jacobian matrix $J_f(x_1...x_8)$ using the parameters of $\{x_1,x_2,...,x_8\}$
5: zero-watermark ← 8×8 Jacobian matrix (JM)
6: **output:** zero-watermark

4.3.3 *Sending Process*

Once the zero-watermark is generated, the sending process takes place by sending the original image and the extracted k to the receiver. In this stage, there is no need to send the generated zero-watermark, while the receiver can generate it by inputting the value k into the Jacobian matrix model. This reduces the amount of data sent on the network. Figure 19 illustrates the sending operation.

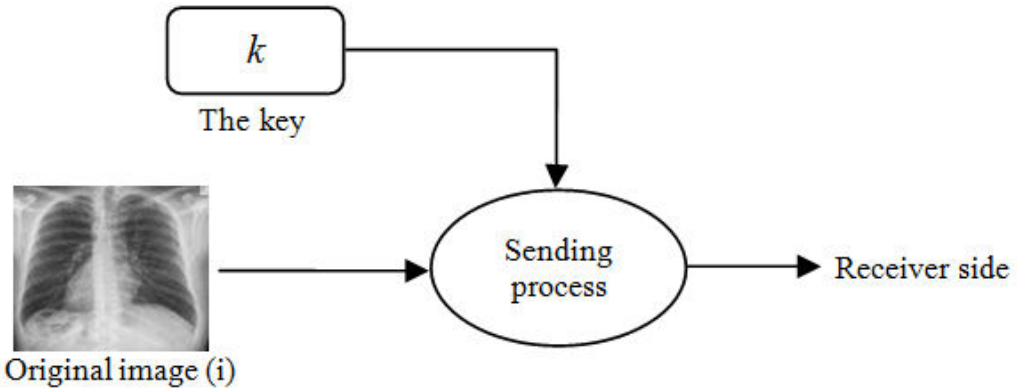


Figure 19: The sending operation.

4.3.4 *Receiving Process*

By considering that the sending process is achieved via a public network, the original image can be the target to different kind of attacks. The receiver has to extract the key k from the attacked image to input it to the Jacobian matrix model in order to extract the attacked watermark (w_a). As well, to reconstruct the original watermark (w), the receiver needs to use the received k. By comparing the extracted attacked watermark (w_a) with original one (w), the similarity and the error probability between w_a and w are measured. In addition, we can also measure the proposed approach robustness against different kind of attacks. Figure 20 presents the receiving task.

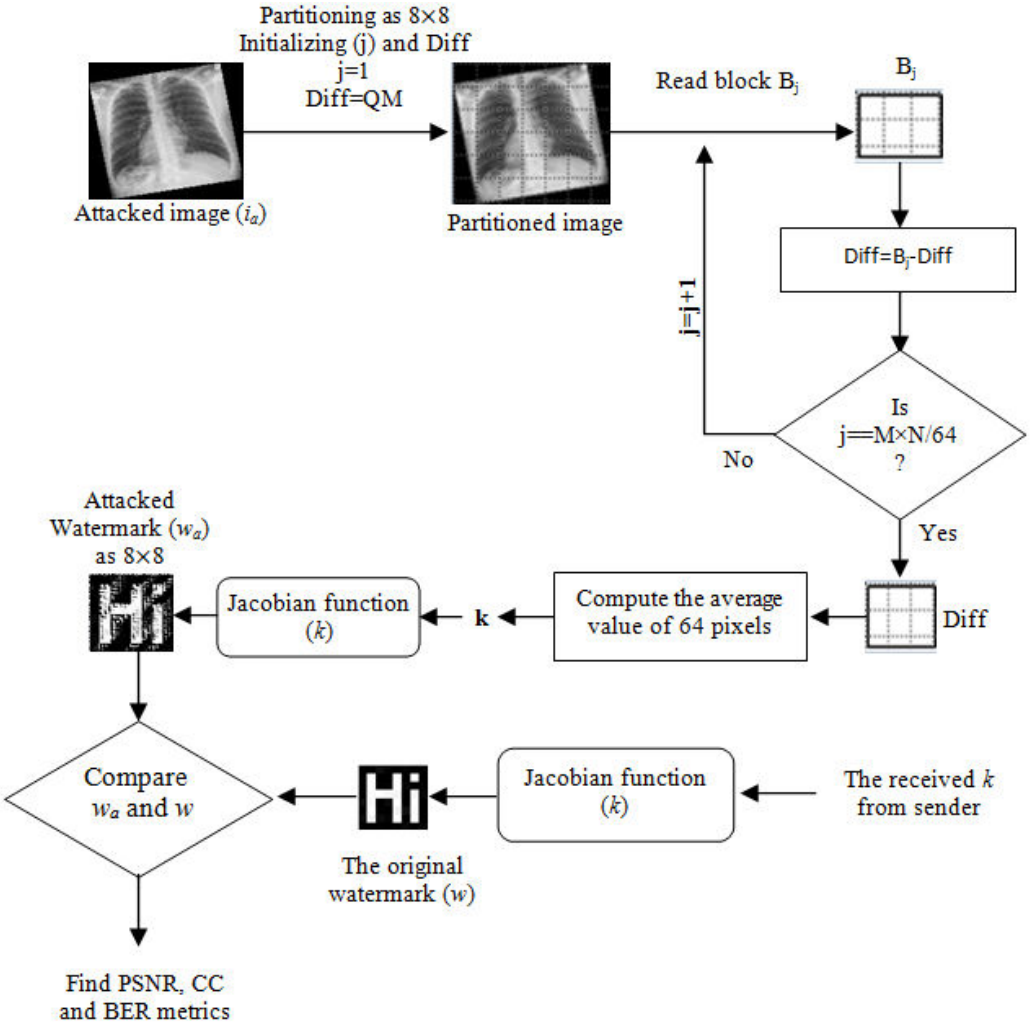


Figure 20: The receiving operation.

4.4 EXPERIMENT RESULTS

To evaluate the efficiency of the proposed approach, three parameters have been used to judge the efficiency of the watermarking approach. These parameters are NC, BER and the execution time. The efficiency of the proposed approach may be interpreted based on the ability to rebuild the original watermark from the attacked original image in terms of an acceptable NC and BER.

The experiments are conducted on medical gray-scale and natural gray-scale images of dimensions 512×512 pixels, where each pixel has a value between 0 and 255, expressed by 8-bits. The sample of medical gray-scale images are collected from radiology image database[1], and the sample of natural gray-scale images are collected from USC-SIPI database[2]. Figure 21 presents the sample of medical gray-scale images besides the computed key (k) and its generated watermark. As well, figure 22 presents the sample of natural gray-scale images besides the computed key (k) and its generated watermark.

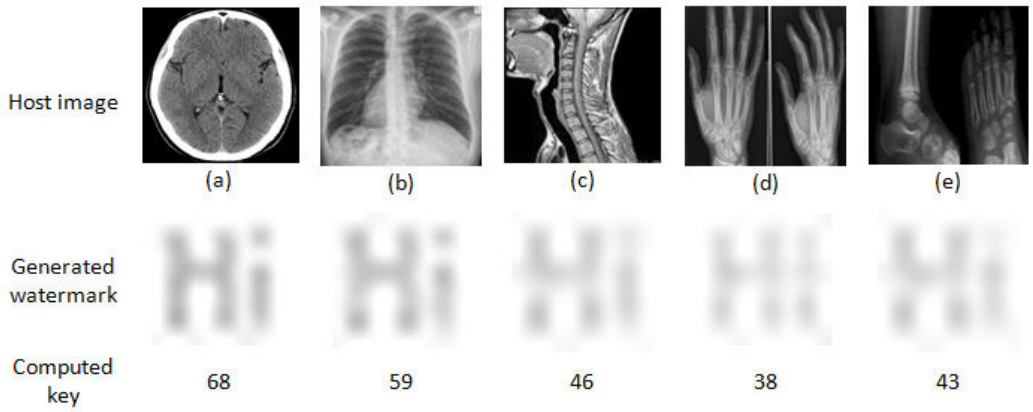


Figure 21: Medical gray-scale host images: (a) CT-head, (b) X-ray1, (c) MRI, (d) X-ray2, (e) X-ray3, corresponding generated watermark (w) and the key.

1 Radiology Image Database, https://lifeinthefastlane.com/table/radiology-database/
2 USC-SIPI database, http://sipi.usc.edu/database/

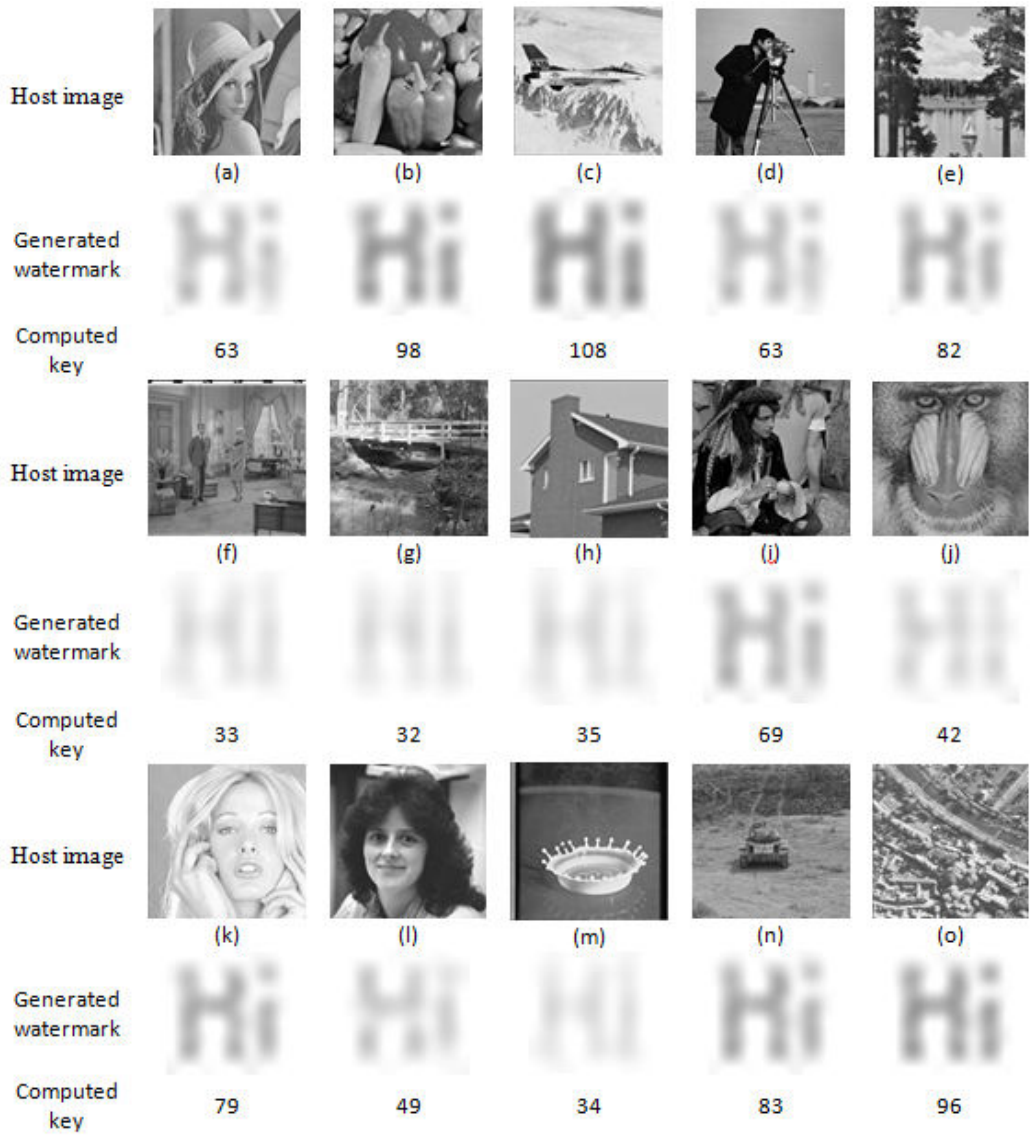


Figure 22: Natural gray-scale host images: (a) Lena, (b) Peppers, (c) Airplane, (d) Cameraman, (e) Sailboat, (f) Couple, (g) Stream, (h) Home, (i) Man, (j) Baboon, (k) Tiffany, (l) Women, (m) Splash, (n) Truck, (o) Aerial, corresponding generated watermark (w) and the key.

To evaluate the robustness of the proposed approach, the experiments are conducted with a particular focus on noise corruption, filtering, image compression and geometric correction. The ID, the name and the factor of the fourteen different attacks (i.e. a1-a14) are illustrated in table 15. StirMark Benchmark v.4 [80] and Matlab (v.R2016a) are used to apply these attacks on the watermarked image. The principles of the main attacks are illustrated in section 2.7.

Attack's id	Attack's name and factor
a1.	JPEG compression (quality factor (QF)=20)
a2.	Gaussian noise (variance=20,mean=0)
a3.	salt&pepper (noise density=0.01)
a4.	median filtering (3×3)
a5.	histogram equalization
a6.	rotation (counterclockwise 45°)
a7.	scaling (0.5) shrink image from 512×512 to 256×256
a8.	crop (25%) left up corner (black)
a9.	crop down (78×111) center (black)
a10.	crop (25%) surround (black)
a11.	affine transformation (2)
a12.	RML (10)
a13.	translation vertically (10)
a14.	LATESTRNDDIST (1)

Table 15: The ID, the name and the factor of the fourteen different attacks (a1-a14)

4.4.1 *Robustness results*

In this subsection, the robustness results in terms of BER and NC of the processed medical and natural gray-scale images are presented. The generated key and the extracted watermark from each attacked watermarked image are also presented.

A *Robustness results on medical gray-scale images*

The achieved robustness ratios of the proposed watermarking approach on medical gray-scale images against the attacks (a1-a14) are presented in figure 23 and figure 24. Figure 23 presents the robustness results against attacks (a1-a7), while figure 24 presents the robustness results against attacks (a8-a14).

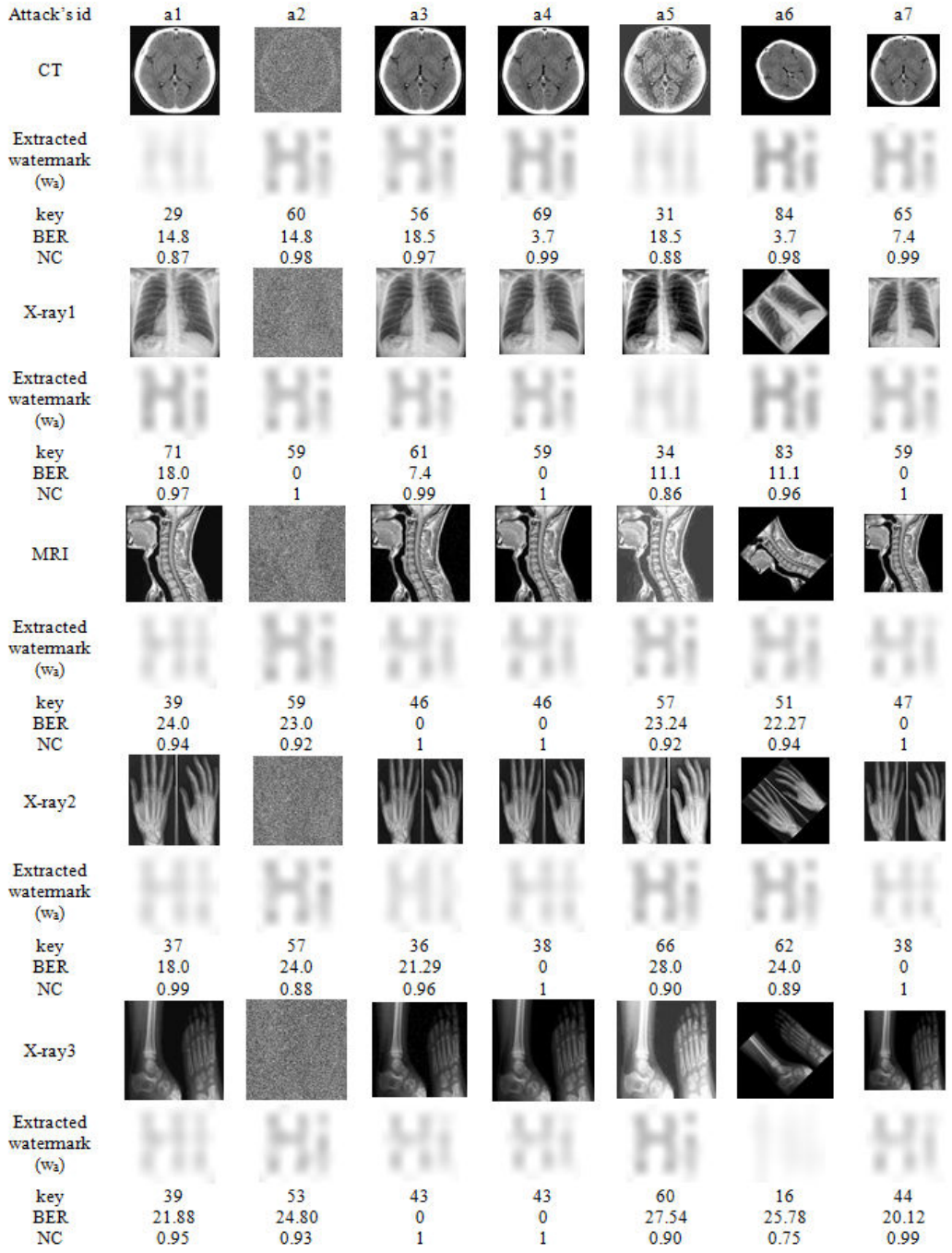


Figure 23: Robustness results of medical gray-scale images against attacks a1-a7.

The obtained results in figure 23 show that the proposed watermarking approach achieves good robustness against salt&pepper noise (a3), median filtering (a4) and scaling attacks (a7). The NC between the original watermark and extracted one against attacks (a3,a4,a7) ranges 0.96-1, and the BER ranges 0-21.3%. The best NC and BER ratios are presented in case of median filtering attack (a4), the NC ranges 0.99-1 and BER ranges 0-3.7%. As well, the results in figure 23 show that the proposed watermarking approach achieve moderate

robustness against compression (a1), Gaussian noise with high variance (a2), histogram equalization (a5) and rotation (a6) attacks. The NC between the original watermark and extracted one against attacks (a1,a2,a5,a6) ranges 0.75-1, and the BER ranges 3.7-28%. The worst NC and BER ratios are presented in case of histogram equalization (a5), the NC ranges 0.86-0.92 and BER ranges 11.1-28.0%. However, the robustness results in case of CT image are better than the robustness results in cases of x-ray and MRI images. The BER in case of CT image did not exceed 18.5%, and the NC ranges 0.87-0.99. In cases of x-ray and MRI images the BER reaches 28% and the NC ranges 0.75-1.

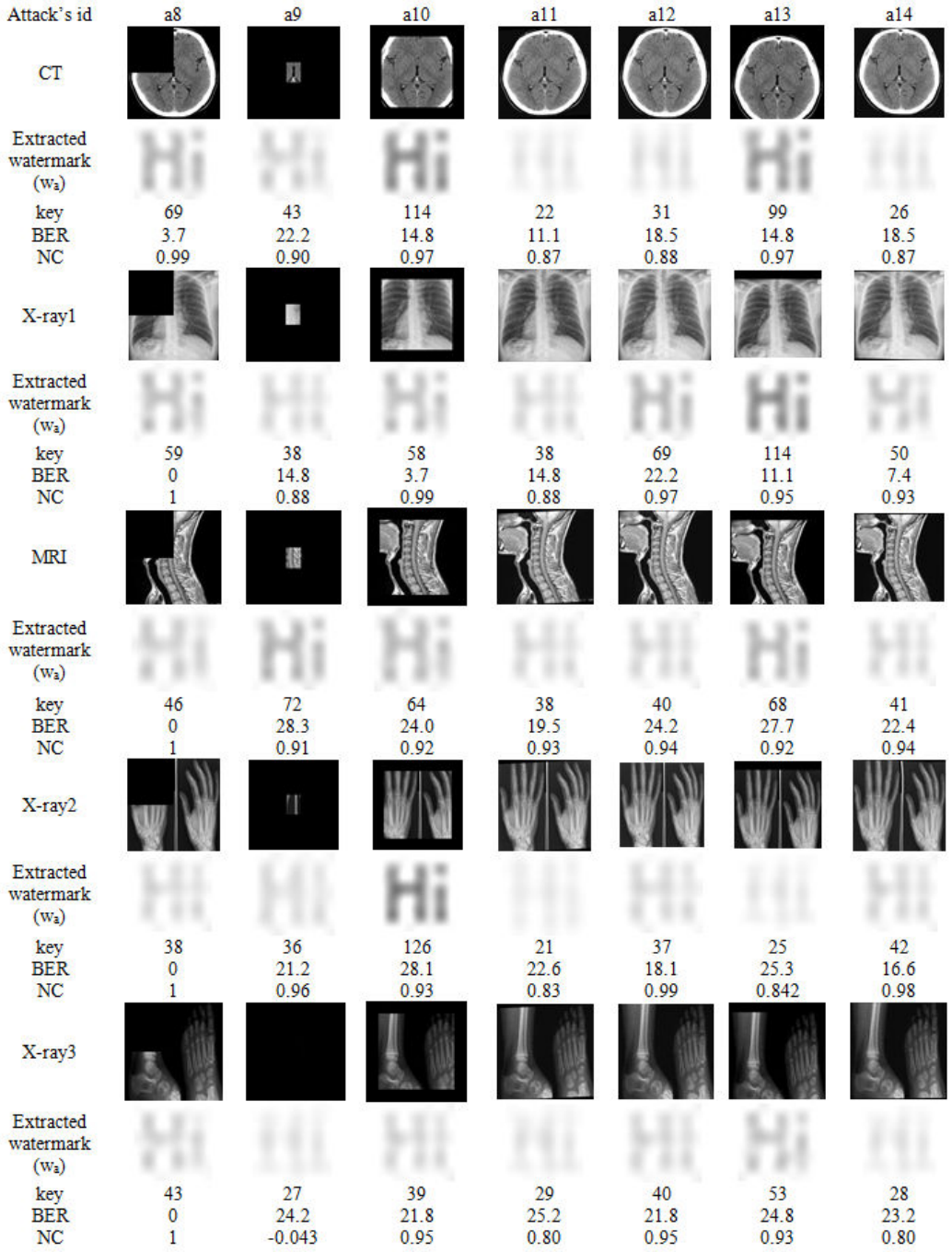


Figure 24: Robustness results of medical gray-scale images against attacks a8-a14.

The results in figure 24 show that the proposed watermarking approach achieves good robustness against cropping left corner (a8), cropping surrounding (a10) and LATESTRNDDIST attacks (a14). The NC between the original watermark and extracted watermark against attacks (a8, a10, a14) ranges 0.80-1 (for a14 with X-ray3), and the BER ranges 0-28.1%. The best NC and BER ratios are presented in case of cropping left corner (a8), the NC ranges 0.99-1 and BER ranges 0-3.7%. As well, the results in figure 24 show that the proposed watermarking ap-

proach achieve moderate robustness against cropping down (a9), Affine transformation (a11), RML (a12) and translation vertically (a13) attacks. The NC between the original watermark and extracted watermark against attacks (a9,a11,a12,a13) ranges -0.04-0.99, and the BER ranges 11.1-28.3%. The worst NC and BER ratios are presented in case of cropping down (a9), the NC ranges -0.04-0.96 and BER ranges 14.8-28.3%. However, the robustness results in cases of CT and x-ray1 images are better than the robustness results in cases of x-ray2, x-ray3 and MRI images against (a8-a14) attacks. The BER in case of CT and x-ray1 images did not exceed 22.2% and the NC ranges 0.87-1. In cases of x-ray2, x-ray3 and MRI images the BER reaches 28.3% and the NC ranges -0.04-1.

Accordingly, the mentioned robustness results of figure 23 and figure 24 show that the proposed watermarking approach is more robust against median filtering and cropping left corner than other kinds of attacks. The BER ranges 0-7.4 and the NC ranges 0.99-1. On the other hand, the proposed watermarking approach achieves less robustness against compression, histogram equalization, cropping down and affine transformation attacks. The BER ranges 11.1-28.3% and the NC ranges -0.04-0.99.

B *Robustness results on natural gray-scale images*

The achieved robustness ratios of the proposed approach on natural gray-scale images against the attacks (a1-a14) are presented in figures 25, 26, 27, 28, 29 and 30 also in terms of BER and NC. Figures 25, 26 and 27 present the robustness results of natural gray-scale images against attacks (a1-a7), while figures 28, 29 and 30 present the robustness results against attacks (a8-a14).

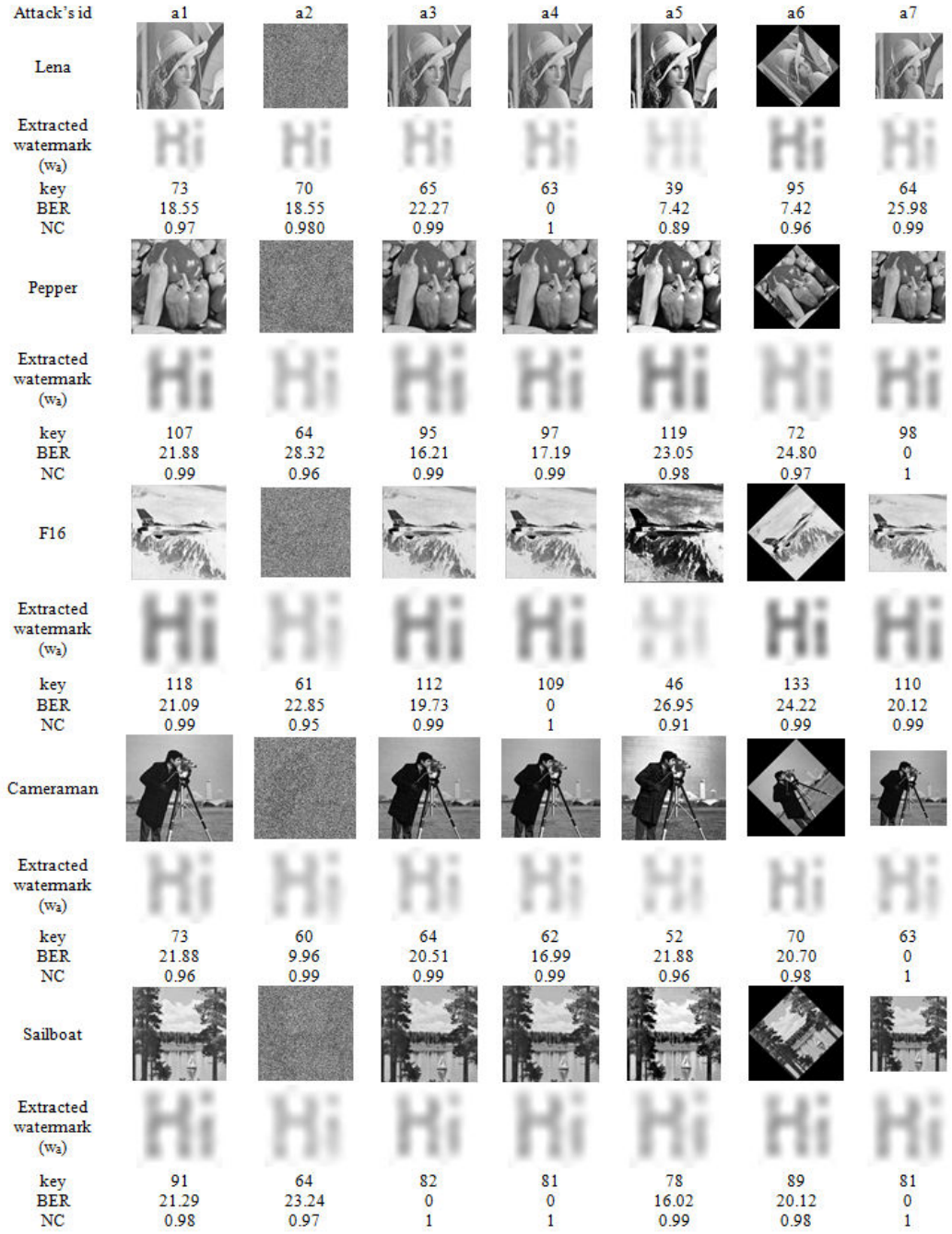


Figure 25: Robustness results of natural gray-scale images (a-e) against attacks a1-a7.

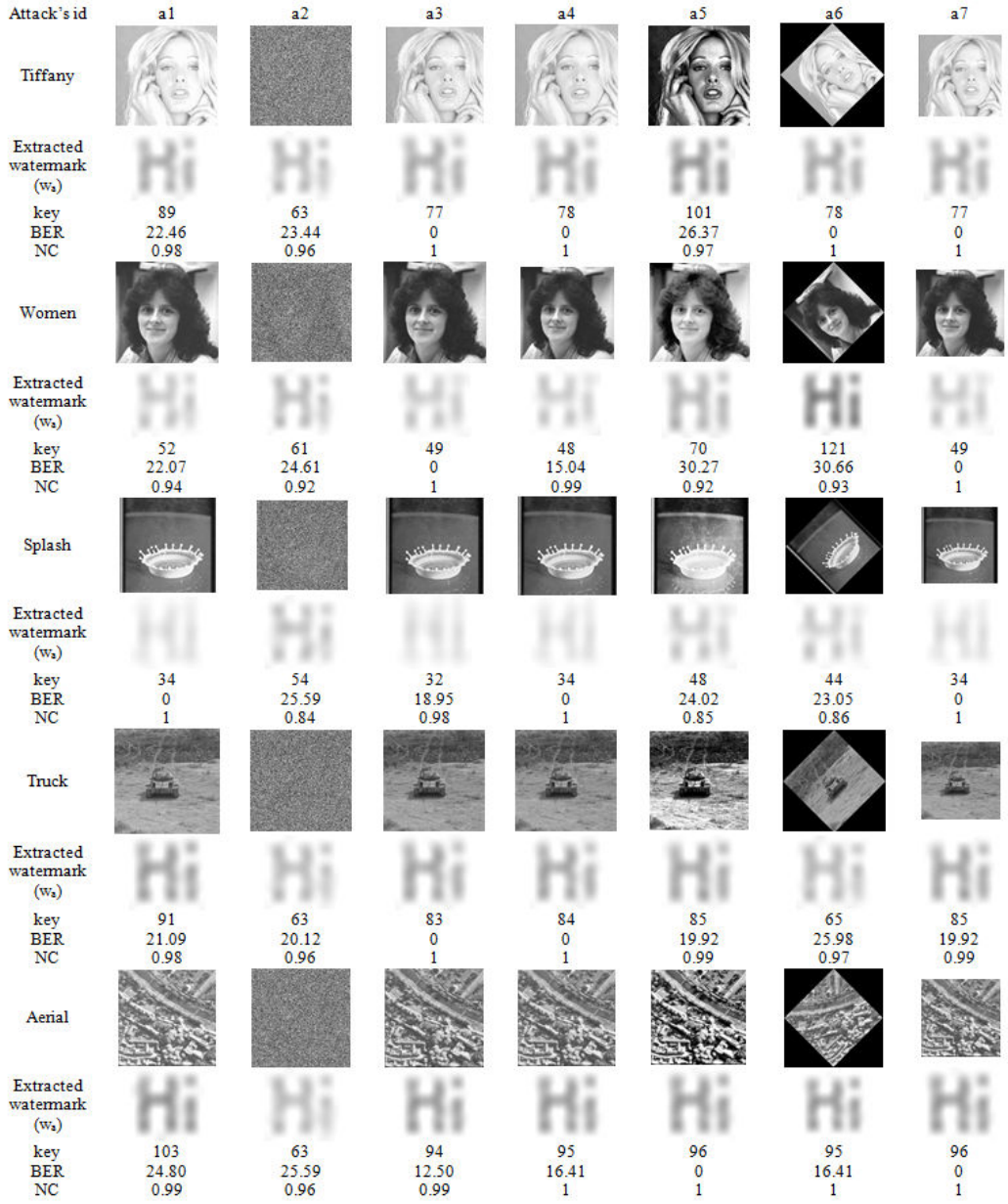


Figure 26: Robustness results of natural gray-scale images (f-j) against attacks a1-a7.

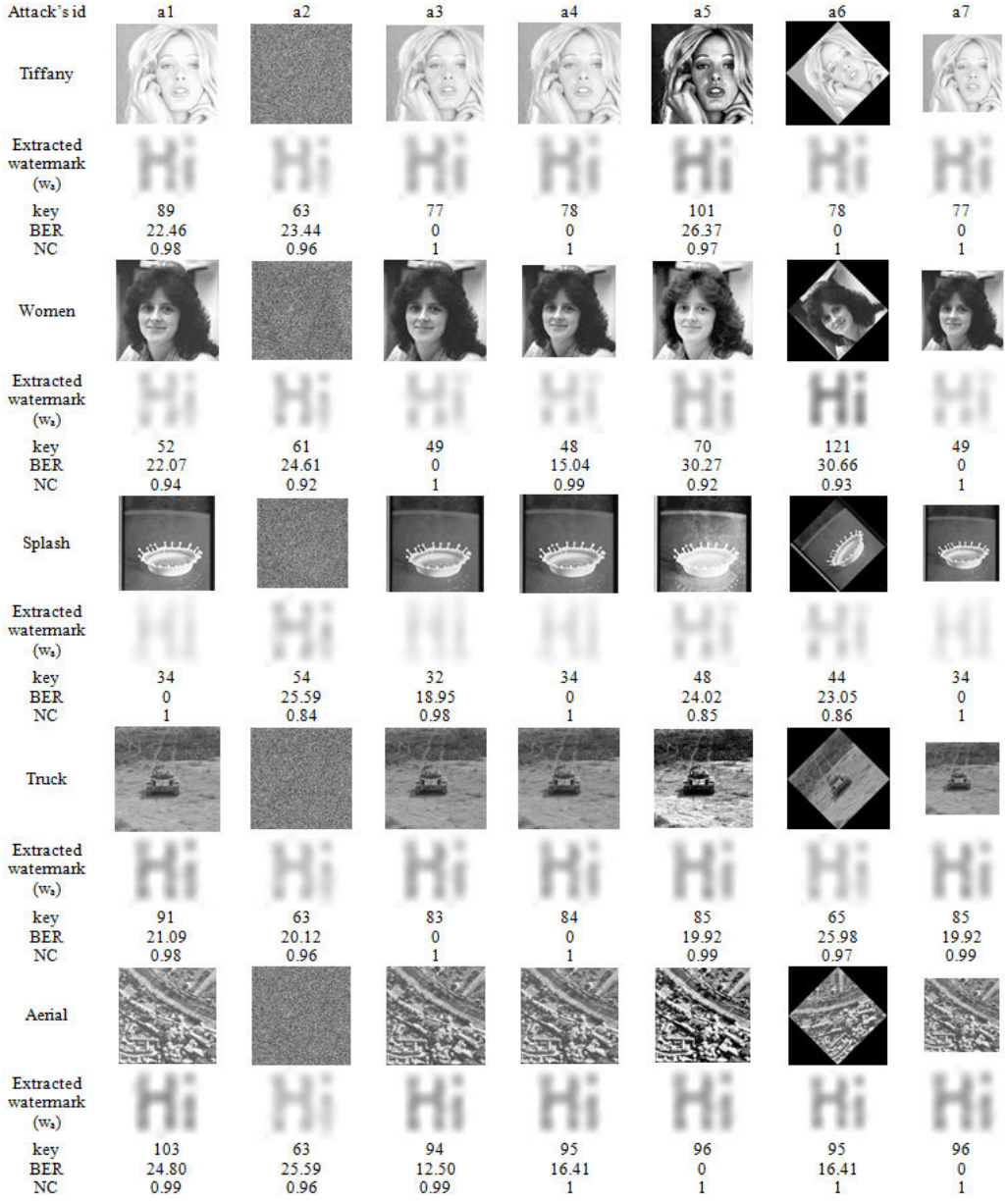


Figure 27: Robustness results of natural gray-scale images (k-o) against attacks a1-a7.

The results in figures 25, 26 and 27 show that the proposed watermarking approach achieves good robustness against salt&pepper noise (a3), median filtering (a4) and scaling attacks (a7). The NC between the original watermark and extracted watermark against attacks (a3,a4,a7) ranges 0.95-1 and the BER ranges 0-25.9%. The best NC and BER ratios are presented in case of median filtering attack (a4), the NC ranges 0.98-1 and BER ranges 0-18.9% respectively. On the other hand, the results in figures 25, 26 and 27 show that the proposed watermarking approach achieve moderate robustness against compression (a1), Gaussian noise with high variance (a2), histogram equalization (a5) and rotation (a6) attacks. The NC between the original watermark and extracted watermark

against attacks (a1,a2,a5,a6) ranges 0.83-1 and the BER ranges 0-30.6%. The worst NC and BER ratios are presented in case of Gaussian noise with high variance (a2), the NC ranges 0.84-0.98 and BER ranges 9.96-28.32%.

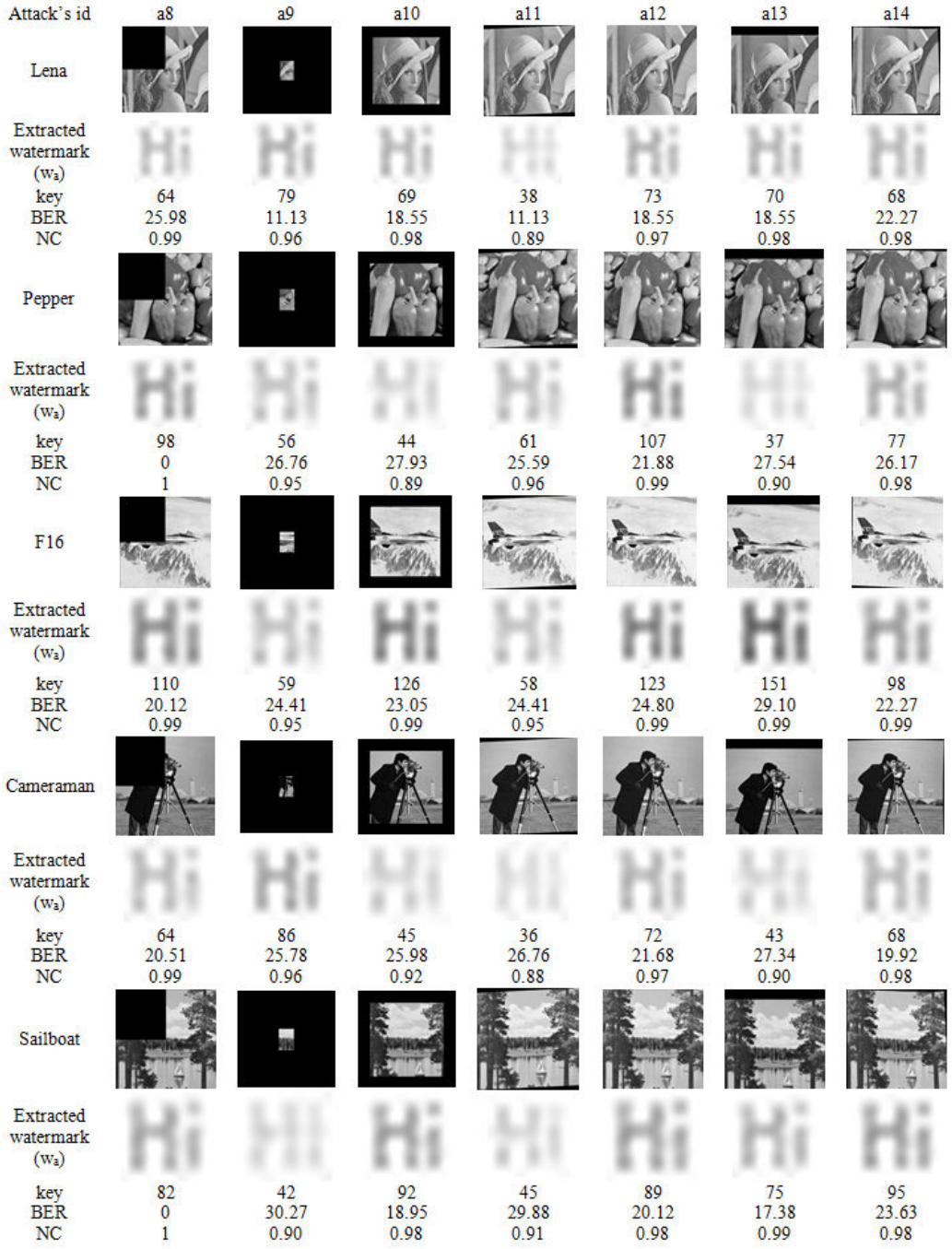


Figure 28: Robustness results of natural gray-scale images (a-e) against attacks a8-a14.

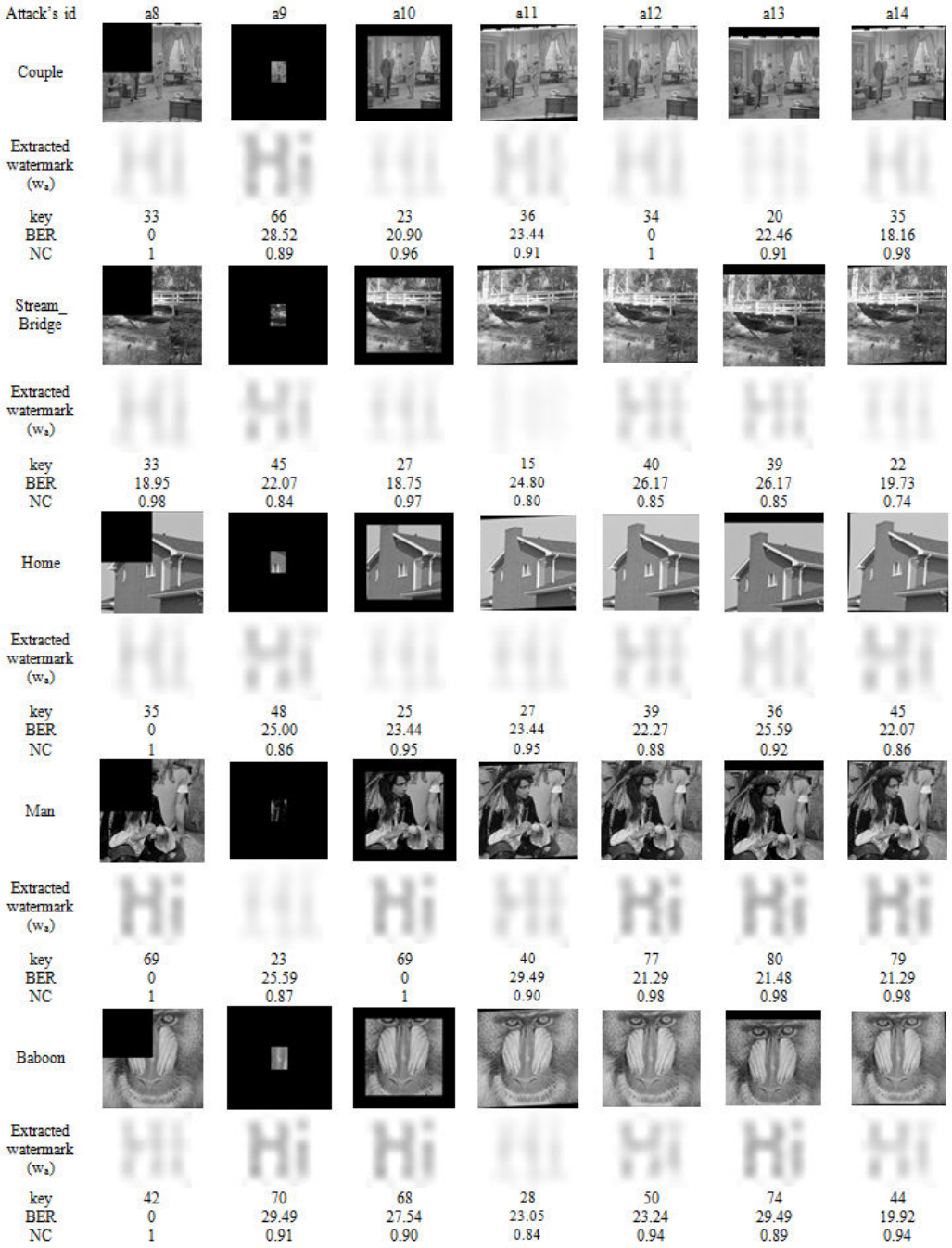


Figure 29: Robustness results of natural gray-scale images (f-j) against attacks a8-a14.

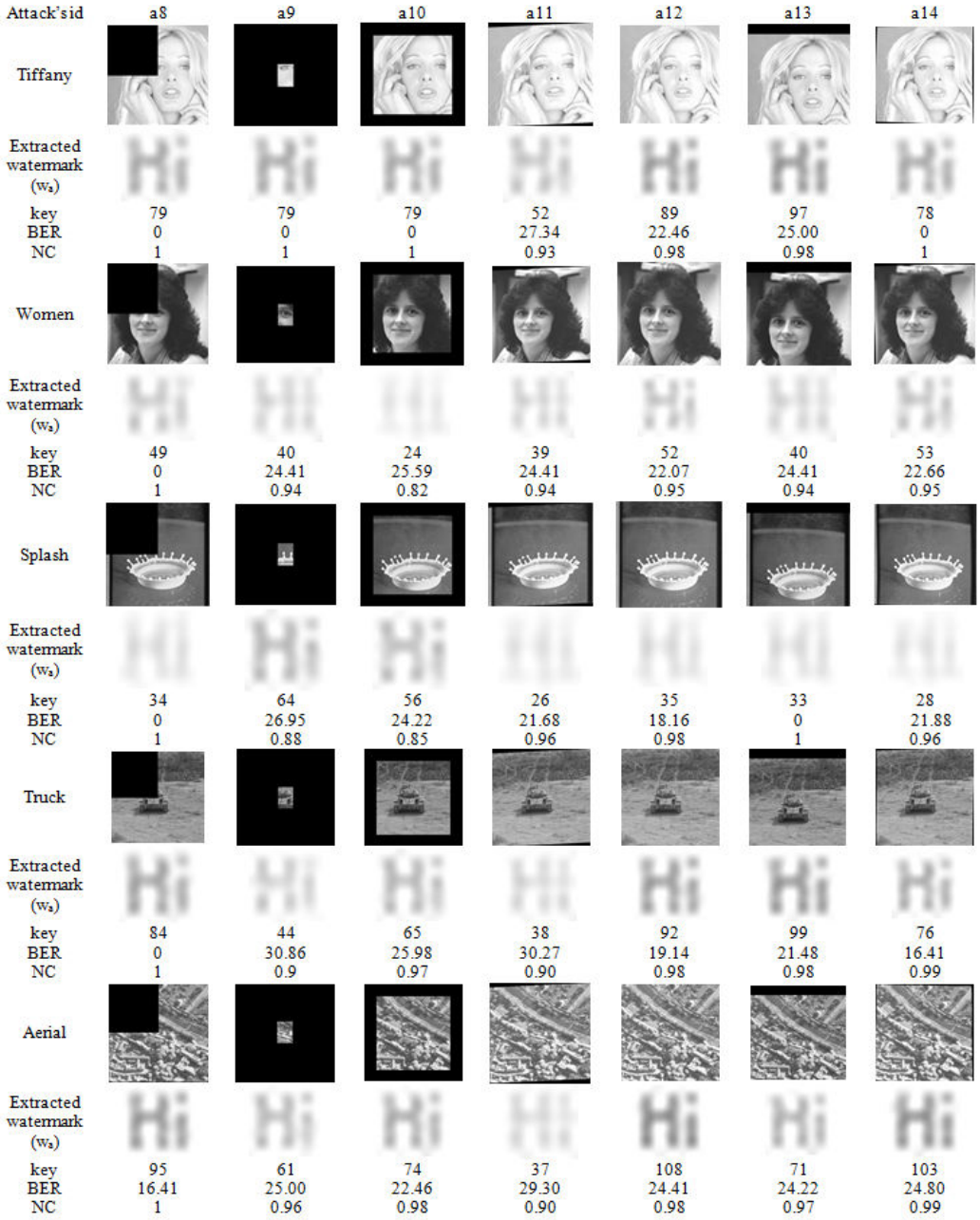


Figure 30: Robustness results of natural gray-scale images (k-o) against attacks a8-a14.

The results in figures 28, 29 and 30 show that the proposed approach achieves good robustness against cropping left corner (a8) and LATESTRNDDIST attacks (a14). The NC between the original watermark and extracted watermark against attacks (a8,a14) ranges 0.74-1 and the BER ranges 0-26.17%. The best NC and BER ratios are presented in case of cropping left corner (a8). The NC ranges 0.98-1 and BER ranges 0-25.98%. As well, the results in figures 28, 29 and 30 show that the proposed watermarking approach achieve moderate robustness against cropping down (a9), cropping surrounding (a10), Affine transformation (a11), RML (a12) and translation vertically (a13) attacks. The NC between the original

watermark and extracted watermark against attacks (a9,a10,a11,a12,a13) ranges 0.80-1 and the BER ranges 0-30.86%. The worst NC and BER ratios are presented in case of cropping down (a9), the NC ranges 0.84-1 and BER ranges 0-30.86%.

Accordingly, the mentioned robustness results of figures 25, 26, 27, 28, 29 and 30 show that the proposed watermarking approach is more robust against median filtering (a4), scaling (a7), cropping left corner (a8) and LATESTRNDDIST (a14) than other kinds of attacks. The BER ranges 0-26.17 (for a14 with Peppers image) and the NC ranges 0.74-1 (for a14 with Stream_Bridg image). On the other hand, the proposed watermarking approach achieves less robustness against compression, histogram equalization, cropping down, cropping surround and affine transformation attacks. The BER ranges 0-30.8% and the NC ranges 0.80-1.

4.4.2 *Execution Time*

In this subsection, the required execution time to generate the watermark and its extraction from each attacked medical or natural gray-scale image is presented. All executions were achieved on HP machine 3.4 GHz Intel(R)/core(TM) i7 CPU with 8.0 GB RAM.

A *Execution time on medical gray-scale images*

Table 16 presents the execution time in seconds to generate a zero-watermark from each host medical gray-scale image, and table 17 presents the execution time in seconds to extract a zero-watermark from each attacked medical gray-scale image.

Image name	Execution time/seconds
CT-head	2.79
Lungs	2.81
MRI	2.88
Hands	2.75
Legs	2.91

Table 16: The execution time in seconds to generate a zero-watermark from the host medical gray-scale images.

Image name	Execution time/seconds
CT-head	2.93
Lungs	2.84
MRI	2.97
Hands	2.78
Legs	2.81

Table 17: The execution time in seconds to extract a zero-watermark from the attacked medical gray-scale images.

The execution time results in tables 16 and 17 show that the execution time to generate the zero-watermark and to extract it from different attacked medical gray-scale images did not exceed 6 seconds.

B *Execution time on natural gray-scale images*

Table 18 presents the execution time in seconds to generate a zero-watermark from the host natural gray-scale images, and table 19 presents the execution time in seconds to extract a zero-watermark from the attacked natural gray-scale images.

Image name	Execution time/seconds	Image name	Execution time/seconds	Image name	Execution time/seconds
Lena	2.74	Couple	2.88	Tiffany	2.80
Peppers	2.95	Stream	2.99	Women	2.81
Airplane	2.93	Home	2.87	Splash	2.98
Cameraman	2.94	Man	2.96	Truck	2.90
Sailboat	2.90	Baboon	2.97	Aerial	2.73

Table 18: The execution time in seconds to generate a zero-watermark from the host natural gray-scale images.

Image name	Execution time/seconds	Image name	Execution time/seconds	Image name	Execution time/seconds
Lena	2.78	Couple	2.97	Tiffany	2.84
Peppers	2.96	Stream	2.77	Women	2.93
Airplane	2.90	Home	2.68	Splash	2.81
Cameraman	2.90	Man	2.89	Truck	2.82
Sailboat	2.79	Baboon	2.88	Aerial	2.72

Table 19: The execution time in seconds to generate a zero-watermark from the attacked natural gray-scale images.

The results in tables 18 and 19 show that the execution time to generate the zero-watermark and to extract it from attacked natural gray-scale images did not exceed 6 seconds.

The mentioned results in tables 16, 17, 18 and 19 prove the applicability of proposed zero-watermarking approach for real-time applications.

4.5 COMPUTATIONAL COMPLEXITY ANALYSIS

The proposed zero-watermarking approach is implemented with low computational complexity and execution time. The overall computational complexity is $O(M \times N)$. The low complexities in the computation and execution time present the proposed approach as practical for real time applications.

4.6 COMPARATIVE STUDY

This section presents comparative studies between the performance of the proposed zero-watermarking approach with other related watermarking approaches. The performance of the proposed approach and other related watermarking approaches is evaluated by considering many aspects either on medical or natural gray-scale images results. The robustness against different attacks, the domain based, the type of generated watermark, the computational complexity and the execution time are set of aspects that are considered in the evaluation process.

Table 20 presents NC value comparison between the proposed approach and the related approach in [108] for x-ray, MRI and CT medical gray-scale images under various geometric and non-geometric attacks.

	NC for Watermark Logo					
Test image	X-ray	MRI	CT	X-ray	MRI	CT
Attack	Thanki et al., 2017 [108]			Proposed approach		
JPEG compression (Q=90)	0.97	0.98	0.98	0.97	0.93	0.88
JPEG compression (Q=80)	0.93	0.74	0.96	0.98	0.94	0.88
JPEG compression (Q=70)	0.95	0.71	0.74	0.98	0.94	0.88
JPEG compression (Q=60)	0.76	0.59	0.79	0.98	0.94	0.88
JPEG compression (Q=50)	0.71	0.59	0.64	0.98	0.94	0.88
Speckle noise (variance=0.004)	0.87	0.95	0.94	1	0.99	0.99
Salt&Pepper noise (variance=0.005)	0.87	0.90	0.91	1	1	0.98
Gaussian noise (mean=1,variance=0.001)	0.93	0.81	0.86	0.99	0.91	0.89
Median filtering (2×2)	0.95	0.97	0.96	1	1	0.99
Average filtering (2×2)	0.87	0.85	0.88	1	1	0.99
Blurring	0.70	0.96	0.91	0.99	0.98	0.92
Sharpening	0.94	0.97	0.97	1	1	0.99
Histogram equalization	0.97	0.96	0.97	0.86	0.92	0.88
Flipping	0.87	0.73	0.89	0.95	1	1
Rotation(90°)	0.79	0.90	0.94	0.99	0.92	0.99
Cropping (20%)	0.97	0.97	0.96	0.99	0.92	0.97

Table 20: NC value comparison of proposed approach and related approach [108] for X-ray, MRI and CT medical gray-scale images under various attacks.

The mentioned NC results between the original watermark and the extracted ones under different attacks in table 20 show that the proposed watermarking approach achieves higher ratios than the related approach of [108] for X-ray, MRI and CT medical gray-scale images. The achieved ratio of NC against compression, adding noise, filtering, blurring, sharpening, flipping, rotation and cropping attacks ranges 0.88-1 in the proposed approach, while it ranges 0.59-0.97 in the related approach [108]. In case of JPEG compression (Q=90) and histogram equalization attacks, the related approach of [108] achieves higher NC than the proposed approach. The achieved ratio of NC against JPEG compression (Q=90) and histogram equalization ranges 0.96-0.98 in the related approach of [108], while it ranges 0.86-0.97 in the proposed approach.

However, the results in table 20 show that the proposed zero-watermarking approaches provides higher robustness for x-ray and MRI images than CT image. While, the related approach [108] provides higher robustness for x-ray and CT images than MRI image.

Table 21 presents NC value comparison between the proposed approach and other related approaches such in [96][77][106][108] for x-ray medical gray-scale image under various geometric and non-geometric attacks.

	NC for Watermark Logo				
Attack	Singh et al., 2015 [96]	Parah et al., 2017 [77]	Thakkar et al., 2017 [106]	Thanki et al., 2017 [108]	Proposed approach
JPEG compression (Q=90)	0.74	0.99	1	0.97	0.97
JPEG compression (Q=20)	0.72	0.96	0.68	<0.69	0.97
Sharpening	0.74	0.95	1	0.97	1
Median filtering (2×2)	0.67	0.94	1	0.96	1
Gaussian noise (μ=0, σ=0.01)	0.74	0.92	0.88	0.64	0.99
Salt&Pepper noise (μ=0.1)	0.71	×	1	0.75	0.93
Histogram equalization	0.74	0.98	1	0.97	0.86
Scaling (0.5)	×	0.78 [106]	0.91	×	1
Scaling (2)	0.74	1 [106]	1	1	1
Cropping 25% left up corner	×	0.67 [106]	0.71	×	1
Cropping 25% center	×	0.44 [106]	0.51	×	1

Table 21: NC value comparison of proposed approach with existing approaches [96][77][106][108] for X-ray medical image under various watermarking attacks.

The mentioned NC results for x-ray image under different attacks in table 21 show that the proposed approach achieves higher NC ratios against JPEG compression (Q=20), sharpening, median filtering (2×2) and Gaussian noise (μ=0, σ=0.01) comparing to other related approaches in [96][77][108]. The NC ratio ranges 0.97-1 in the proposed approach against JPEG compression (Q=20), sharpening, median filtering (2×2) and Gaussian noise (μ=0, σ=0.01), while it ranges 0.64-0.97 in the related approaches [96][77][108]. Additionally, the proposed approach achieves higher NC ratio against scaling (0.5), cropping 25% left up corner and cropping 25% center attacks than other related approaches in [77][106]. The NC in the proposed approach equals 1, while it ranges 0.44-0.91 in the related approaches [77][106]. In case of salt&pepper noise (μ=0.1) attack the proposed approach achieves higher NC ratios than the related approaches of [96][108], and in case of scaling (2) the proposed approach achieves similar NC value to the related approaches in [77][106][108].

In contrary, the related approaches in [77][106][108] achieved higher NC ratios against histogram equalization than the proposed approach. The difference in NC value between the related approaches in [77][106][108] and the proposed approach did not exceed 14%. As well, the related approaches of [77][106] achieved higher NC ratios against JPEG compression (Q=90) and histogram equalization than the proposed approach. The difference in NC value between them did not exceed 2%.

However, the related approach in [106] achieved higher robustness than the related approaches in [96][77][108] against most mentioned attacks. Furthermore, the proposed approach achieves interesting robustness results in terms of NC against most mentioned attacks over the other related approaches in [96][77][106][108].

To evaluate the performance of the proposed approach over other related watermarking approaches, table 22 presents a comparison between the proposed approach and other related approaches in [96][68][77][106][108] with various aspects. The domain based, the types of tested images, the type of generated watermark, the robustness against different attacks, the computational complexity and the execution time are set of aspects used in the comparison process.

approach	Singh et al., 2015 [96]	Mehto et al., 2016 [68]	Parah et al., 2017 [77]	Thakkar et al., 2017 [106]	Thanki et al., 2017 [108]	Proposed approach
Domain based	DWT	DCT and DWT	DCT	DWT and SVD	FDCuT and DCT	Spatial domain
Types of images tested	Medical gray-scale (US, MRI and CT)	Medical gray-scale (X-ray, MRI and CT)	Medical gray-scale (CT)	Medical gray-scale (X-ray, CT and mammography)	Medical gray-scale (X-ray, US, MRI and CT)	Medical gray-scale (X-ray, MRI and CT)
Type of watermarking	Robust	Fragile	Robust	Robust	Robust	Robust
Type of watermark	1-bit binary image (0 or 1)	8-bit Gray-scale image (0-255)	1-bit binary image (0 or 1)	1-bit binary image (0 or 1)	8-bit binary image (0 or 255)	8-bit Gray-scale image (0-255)
Maximum PSNR (dB)	37.75	45.0	48.0	46.9	55.06	Infinity
Maximum/ Average/ Range NC	0.75 as maximum	Reversible watermarking	0.44-1	0.51-1	0.94 in average	0.86-1
Maximum BER	5.5%	Reversible watermarking	19.8	26.3%	Not mentioned	18.5%
Execution time (second)	Not mentioned	Not mentioned	Not mentioned	1.24	29.95	5.96
Computational complexity	$O(M\times N)$	$O((M\times N)^2 log_2(M\times N))$	$O((M\times N)^2 log_2(M\times N))$	$O(M\times N)^2$	$O((M\times N)^2 log_2(M\times N))$	$O(M\times N)$

Table 22: Comparison of proposed approach with related approaches [96][68][77][106][108] with various features.

Table 22 shows several watermarking approaches that are proposed in the literature to achieve medical images authentication. The values of the evaluating aspects in table 22 show that all related approaches in [96][68][77][106][108] are designed in frequency domain, while the proposed approach is designed in spatial domain. As well as, the type of generated watermark in the related approaches in [96][77][106][108] was binary watermark, while it is a gray-scale

image in the proposed approach. In spite of these two properties and their effect on the robustness, the proposed approach provides better NC values than other related approaches in [96][77][106][108]. The NC in the proposed approach ranges 0.86-1, while it is ranged 0.44-1 in [96][77][106][108]. The BER in the proposed approach did not exceed 18.5% and it outperforms the BERs in the related approaches in [77][106]. It is worth to note that the mentioned values of NC and BER in this table are against attacks that are considered in table 21, and the approach of [68] introduced a reversible watermarking approach.

However, the BER in approach [96] outperforms the BER in the proposed approach due to the domain based and the difference in the type of generated or used watermark. The approach in [96] exploited the DWT coefficients to embed a binary watermark where each bit in the watermark has a value either 0 or 1, while the proposed approach based on spatial domain generates a gray-scale watermark where each bit has a value between 0 and 255. Thus, the probability to get erroneous bits after extracting gray-scale watermark from attacked image becomes higher than the probability to get erroneous bits after extracting a binary watermark from attacked image.

For the aspect of perceptual image quality in terms of PSNR, our proposed approach achieves an infinity dB because no data is added to the host image. The other related watermarking approaches require embedding watermark in the original image, which then causes noticeable image quality distortion.

In terms of computational complexity, the proposed approach has lower computational complexity comparing to [68][77][106][108] approaches. The computational complexity in the proposed approach is $O(M \times N)$, while it is an $O((M \times N)^2 log_2(M \times N))$ in [68][77][108] approaches and $O(M \times N)^2$ in [106]. However, the proposed approach and the approach in [96] has the same computational complexity. For the execution time complexity, the proposed approach is executed in less time comparing to [108] approach. The execution time in the proposed approach equals 5.96 seconds and in [108] was 29.95 seconds. However, the execution time of the related approach in [106] outperforms the execution time of the proposed approach, it was 1.24 second. The difference in the execution time between the mentioned approaches could be due to the machines used in the experiments execution. In most mentioned approaches, the specifications of the machines that are used in the testing are not available.

Table 23 presents NC value comparison between the proposed approach and the related zero-watermarking approach [86] for natural gray-scale images under various geometric and non-geometric attacks.

	NC for Watermark Logo							
Test image	Peppers	Lena	Baboon	Cameraman	Peppers	Lena	Baboon	Cameraman
Attack	Rani et al., 2015 [86]				Proposed approach			
Gaussian noise addition (5%)	0.97	0.98	0.96	0.95	0.99	0.99	0.95	0.99
Average filtering (7×7)	0.98	0.98	0.98	0.96	0.99	0.98	1	0.99
Median filtering (7×7)	0.98	0.98	0.98	0.97	0.99	0.98	1	1
Scaling (0.5)	0.99	0.99	0.99	0.99	1	0.99	0.95	1
Rotation (50°)	0.86	0.87	0.86	0.85	0.98	0.96	0.94	0.98
Cropping(50%)	1	1	1	1	0.99	0.98	1	0.92
Cropping (75%)	1	1	1	1	0.99	0.98	0.94	0.90
Histogram equalization	0.98	0.98	0.99	0.96	0.99	0.90	0.84	0.97
JPEG compression (Q=40)	0.99	0.99	0.99	0.99	0.99	0.97	0.94	0.97

Table 23: NC value comparison of proposed approach and existing zero-watermarking approach [86] for natural gray-scale images under various attacks.

The results in table 23 show that the proposed approach achieves higher NC ratios comparing to approach in [86] for the natural gray-scale images against Gaussian noise addition (5%), average filtering (7×7), median filtering (7×7), scaling (0.5) and rotation (50°). The NC in the proposed approach ranges 0.94-1, while it ranges 0.85-0.99 in the approach in [86]. In case of cropping(50%), cropping (75%), histogram equalization and JPEG compression (Q=40) NC ratios in the proposed approach and the related approach in [86] are convergent with slight overcome of the related approach of [86] by 10% in the worst case.

However, the results in table 23 show that the proposed zero-watermarking approach achieves good robustness for Peppers, Lena and Cameraman images over than Baboon image and in general the proposed approach and the related approach [86] show good robustness against the mentioned attacks.

To evaluate the performance of the proposed approach over other related zero-watermarking approaches, table 24 presents a comparison between our proposed approach and other related zero-watermarking approaches in [86][33][114][94][95][115] with various aspects. The domain based, the types of images tested, the type of generated watermark, the robustness against different attacks, the computational complexity and the execution time are set of aspects used in the evaluation process.

approach	Rani et al., 2015 [86]	Gao et al., 2015 [33]	Chun-peng et al., 2016 [114]	Shen et al., 2017 [94]	Singh et al., 2017 [95]	Wang et al., 2017 [115]	Proposed approach
Domain based	DWT and SVD	Bessel-Fourier transform	Pure quaternion numbers [6]	NURP	DWT and SVD	PCET	Spatial domain
Types of images tested	Natural gray-scale	Natural and medical gray-scale	Natural color	Natural gray-scale	Fundus color (medical)	Natural and medical gray-scale	Natural and medical gray-scale
Type of generated watermark	8-bit binary image (0 or 255)	8-bit binary image (0 or 255)	8-bit binary image (0 or 255)	8-bit binary image (0 or 255)	1-bit binary image (0 or 1)	8-bit binary image (0 or 255)	8-bit Gray-scale image (0-255)
Robust or fragile	Robust	Robust	Robust	Robust	Robust against non-geometric attacks	Robust	Robust
Robustness	NC ranged 0.50-1	BER<21.1% [114]	BER<12.4%	NC ranged 0.86-0.98 and BER<10.9%	NC ranged 0.69-1 and BER<7.3%	BER ranged 1.2-10.2%	NC ranged 0.86-1 and BER<18.5%
Computation complexity	$O(\min(M\times N^2, M^2\times N))$	$O(M^2\times N^2)$	$O(M\times N)$	$O(M\times N)$	$O((M\times N)^3 \log_2 M\times N)$	$O(M\times N\times \omega^2)$	$O(M\times N)$
Execution time (seconds)	90	4345.64 [114]	740.51	Not mentioned	3.5	21.84	5.96

Table 24: Comparison of proposed approach with related zero-watermarking approaches [86][33][114][94][95][115] with various features.

Table 24 shows several zero-watermarking approaches that are proposed in the literature to achieve medical and natural images authentication. All of the related approaches in [86][33][114][94][95][115] are designed in frequency domain, while the proposed zero-watermarking approach is designed in spatial domain. Moreover, the type of the generated watermark in the related approaches of [86][33][114][94][95][115] was a binary watermark, while its gray-scale watermark in the proposed approach. In spite of the proposed approach is designed in spatial domain and the generated watermark is gray-scale image, it still provides good robustness ratios comparing with other related approaches in terms of NC and BER. The NC in the proposed approach ranges 0.86-1, while it ranged 0.50-1, 0.86-0.98 and 0.69-1 in [86][94][95] respectively. The BER in the proposed approach did not exceed 18.5%, while it did not exceed 21.1%, 12.4%, 10.9%, 7.3 and 10.2% in [33][114][94][95][115] respectively. The BER in the related approaches in [114][94][95][115] outperforms the BER in the proposed approach due to the difference in the type of generated watermarks. In case of gray-scale watermark each pixel has by a value between 0 and 255, while in case of bi-

nary watermark each pixel has a value either 0 or 1. Then, the probability to get erroneous bits after extracting gray-scale watermark from attacked image becomes higher than the probability to get erroneous bits after extracting binary watermark from attacked image.

In terms of computational complexity, the proposed approach implements with low computational complexity comparing to [86][33][95][115] approaches. The computational complexity in the proposed approach is $O(M \times N)$, while it was $O(min(M \times N^2, M^2 \times N))$, $O(M^2 \times N^2)$, $O((M \times N)^3 \log_2 M \times N)$ *and* $O(M \times N \times \omega^2)$ in [86][33] [95][115] respectively. The computational complexity in [114][94] was similar to the complexity of the proposed approach. For the execution time, the proposed approach is executed in less time comparing to [86][33][114][115] approaches. However, the execution time of the approach in [95] outperforms the execution time of the proposed approach, it was 3.5 second. The difference in the execution time between the mentioned approaches could be due to difference of performance of the machines used in the experiments execution. In most mentioned approaches, the specifications of the machines that are used in the testing are not available.

4.7 SYSTEM ANALYSIS

This section introduces a discussion of the most important aspects that distinguish the proposed approach from the other addressed related approaches and explains the reasons for this improvement. The main aspects and reasons are discussed in the following.

4.7.1 *Selecting the Key* k

Some attacks such as cropping and translation have an effect on a specific part of the image rather than the whole image. Hence, in the proposed approach, selecting a specific value (such as the first pixel, the last pixel, or the center pixel) from the resulted block after accumulation subtraction process could not resist efficiently to the impact of attack on the overall image [117]. Thus, selecting the key k as an average value of the accumulated subtraction of all 8×8 blocks is more efficient to cover the impact of attacks.

4.7.2 *Using the Jacobian Matrix*

Several zero-watermarking approaches such as those proposed in [115][95][94][33][86] are based on a key value obtained by *xor-ing* the extracted feature from the host image and the pre-defined watermark. This key is sent to the receiver as well

to *xor* with the extracted feature from the attacked image to extract the attacked watermark. This technique involves several limitations including increasing the complexity, where the sender should send the watermark and the extracted feature to the receiver. As well they do not give a fair indication to the impact of the attack (i.e. variation in the pixel's value due to attacks). Jacobian matrix model helps to address these limitations by building a meaningful watermark image from the average value k, which gives a true indication to the impact of the attack. Moreover, the proposed approach presents less complexity since it uses pixel values to extract k rather than the frequency techniques.

4.7.3 *Security Requirement*

Many related approaches require securing the image features or the pre-defined watermark image before embedding process. This task aims to reduce the chance on detecting any information that could be used by the illegal user to remove or alter the watermark. The proposed approach does not need to send the generated watermark, but needs only to send the extracted k. Therefore, there is no need to any security strategy.

4.7.4 *Imperceptibility*

For any zero-watermarking approach, the host images are not subject to any degradation in term of visual quality because no embedding procedure takes place. Thus, the imperceptibility ratio in terms of PSNR equals infinity and the SSIM equals 1.

4.7.5 *Robustness*

The essential need of zero-watermarking system in Telemedicine by transmitting the medical images through an e-healthcare network has been realized through this work. The proposed zero-watermarking approach achieves the medical images authentication and robustness against different geometric and non-geometric attacks. The watermark is regenerated from the attacked image with high acceptable robustness rate. The NC is ranged 0.86-1 and the BER did not exceed 28.3% against various geometric and non-geometric attacks. These results ensure the efficiency of the proposed approach to achieve the authenticity of the transmitted medical images through an e-healthcare network. Furthermore, the proposed approach may help the researchers to develop a new approach to control access on patient data and relevant medical records in Telemedicine environments.

4.7.6 *Computational Complexity and Execution Time*

The proposed zero-watermarking approach is implemented with low computational complexity and execution time. The overall computational complexity is *O(M×N)* and the execution time of the proposed algorithm requires 6 seconds. The low complexities in the computation and execution time present the proposed approach as practical for real time applications.

4.8 CONCLUSION

An efficient and robust zero-watermarking of medical images approach is proposed. The proposed approach is characterized by building a meaningful watermark image by computing the average value of accumulated subtraction of all 8×8 blocks, and then exploiting it as a main parameter input to a proposed Jacobian matrix. The proposed approach sends the block average value to the receiver, rather than the generated watermark, which usually needed a security strategy. This design has many advantages including: giving a fair indication of the attack impact proportion on processed image; decreasing the complexity by exploiting the pixels values rather than frequency coefficients. The proposed approach is also tested on natural images to ensure its efficiency with different kinds of images. The experiments result through NC and BER metrics, proves that the proposed approach enhances the robustness against several scenarios of attacks. The NC ratio in average reaches 93%, and the probability to recover the watermark image is higher than 71%. Besides that, the proposed approach has been implemented with low computational complexity and execution time. It is implemented with overall computational complexity of *O(M×N)* and execution time equals 6 seconds. These results are very encouraging comparing to other related zero-watermarking approaches and ensure that the proposed approach would be highly practical for real time processes.

Chapter 5

IMAGE WATERMARKING APPROACH BASED ON ROUGH SET THEORY

Contents

5.1 INTRODUCTION

Establishing procedures to preserve digital images security and authentication are significant issues. Many sensitive applications require transmitting a huge amount of digital images in secure way such as medical and remote sensing imaging systems. Designing image security and authentication models require considering the major constraints including computational complexity and robustness against different attacks [35].

Managing these constraints requires an intensive work to deal with image characteristics including the texture/smooth nature, the relationships between the pixels or coefficients in transform spaces and the structure of image's surface/background. These characteristics, which have significant correlation with the Human Visual System (HVS), are vague and uncertain, since there is no precise meaning or real standard of these characteristics [93].

The fuzzy theory is a heuristic-based approach aiming to introduce efficient solutions based on a set of rules and fuzzy membership function. The fuzzy rules

deal with incomplete and inexact knowledge such as the concepts of bigger, taller or faster. Fuzzy set, fuzzy logic, and rough sets are the most important techniques in the CI, and they can be combined to give a definition for vagueness and imprecise knowledge in different fields [79][128][132]. Extracting hidden patterns from data, medical diagnosis, pattern recognition, image classification and intelligent dispatching are set of application whose design can be based on fuzzy sets, fuzzy logic and rough sets techniques.

The key features of rough set theory including the ability to characterize and deal with uncertainty and vague image data, as well as no need to any preliminary or additional information about data like probability in statistics or value of possibility, has encouraged us to investigate it uses for enhancement of watermarking.

This chapter is organized as follows. Background related to the principles of classical set and rough set is presented in section 5.2. Section 5.3 introduces watermarking approach in spatial domain based on HVS characteristics and rough set theory. The experiment results are presented in section 5.4 and the computational complexity analysis is presented in section 5.5. The comparative study is presented in section 5.6 and the system analysis is presented in section 5.7. This chapter ends with conclusion in section 5.8.

5.2 CLASSICAL SET AND ROUGH SET PRINCIPLES

The classical set is a primitive notion in mathematics and natural sciences. The set can be defined in such a way that all elements in the universal set are classified definitely into members or nonmembers based on predefined characteristic function. The characteristic function assigns either 0 or 1 for each element in the universe set.

Let U denote the universe set and u denote the general elements, then the characteristic function $F_S(u)$ maps all members in universal set U into set {0,1}. The mapping process classified the universe elements into crisp sets [130], where the principle of crisp set is defined in such a way that the boundary region of U is empty, this means that all universe set elements are classified definitely either as member or non-member.

The general syntax of characteristic function is mentioned below. $F_S(u):U\rightarrow\{0,1\}$ Mathematically, the classical sets can be denoted by one of the following expressions:

- List, denoted as: $S=\{x_1, x_2,..., x_n\}$
- Formula, denoted as: S={X | X satisfies a given property, for example (X is an even number)}

- Membership function, denoted as

$$F_S(u) = \begin{cases} 1 & \text{if u belongs to S} \\ 0 & \text{if u does not belong to S} \end{cases}$$

In contrast of crisp set principle, which deals with precise information and knowledge [130], the fuzzy set theory is a mathematical approach to solve the vagueness and uncertainty information about the problem's knowledge. The fuzzy set principle was introduced by Lotfi Zadeh [130] to define a set of elements that is formulated by employing a fuzzy membership function. Any set that is defined by membership function is defined as a fuzzy (imprecise) set and not as a crisp (precise) set [130].

For fuzzy sets, the membership function expresses the relationship between the value of an element and its degree of membership in a set. The membership function of a fuzzy set S is denoted by F_S, where F_S:U$\rightarrow$ [0,1]. If an element u in the universe set U is a member of the fuzzy set S, then it become member of S with a degree of membership given by F_S (U)$\rightarrow$ [0,1].

Figure 31 shows the difference between the crisp and fuzzy sets. The crisp set principle is presented by figure 31 –i, where each element of the set {A,B,C} has a crisp value by the characteristic function. While, the fuzzy set principle is presented in figure 31 –ii in such a way that element B is located on the boundary of crisp set with a partial membership.

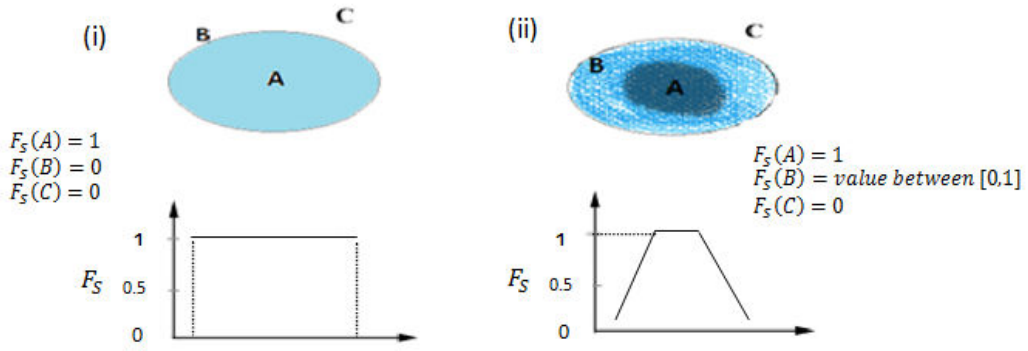


Figure 31: An example presents the difference between crisp and fuzzy sets

As well, the rough set that was proposed by Zdzislaw Pawlak [79] is used efficiently to provide a solution to uncertainty and vagueness knowledge problem. As introduced in [79], the vagueness problem in rough set can be formulated by employing the concept of boundary region of a set rather than partial membership function such used in fuzzy set theory [79]. If the boundary region of a set is empty, then it means that the set is crisp (precise), otherwise, the set is rough (imprecise). Non-empty boundary region of a set gives indication that our information and knowledge about the problem is vague and uncertain [79].

Table 25: An example of information system

Objects	a_1	a_2	a_3	a_4
x_1	yes	no	yes	no
x_2	yes	no	no	yes
x_3	no	yes	no	no
x_4	no	no	yes	yes
x_5	no	no	no	yes

To describe the rough set problem more precisely, suppose that we have an information system (IS), as presented in table 25. The IS is expressed by a finite set of objects (U) called (universe) described by a finite set of attributes (R). In the sample IS, U={x_1,x_2,x_3,x_4,x_5} and R={a_1,a_2,a_3,a_4}.

The representing of lack of knowledge about objects of U, can be defined through equivalence relation given by a subset of attributes P, P⊆R. Let x and y be arbitrary objects in U, and P an arbitrary non empty subset of R, P⊆R. Then, objects x and y are denoted to be indiscernible by P, if and only if x and y have the same vectors of attributes values on all elements in P [132]. The indiscernible relation can denoted as below.

$$\text{ind(P)}=\{(x,y)\in U^2 \mid \forall\, a\in P,\ a(x)=a(y)\}$$

The equivalence relation between x and y is an indiscernible relation by attributes of P, where $(x,y)\in \mathrm{ind}(P)$. The equivalence class of an object x with respect to P is denoted by $[x]_{\mathrm{ind}(P)}$ or $[x]_P$, where $x\in U$ [132][58]. Based on the *IS* in table 25, if P={a_1, a_3}, then objects x_3 and x_5 are indiscernible.

For a subset X⊆ U, X with respect to P can be characterized by upper and lower approximation sets such as the following:

- The upper approximation of a set X with respect to P is the set of all objects which can be possibly classified as X with respect to P (are possibly member of X in view of P).

$$\overline{AP}(X)=\{x\in U|[x]_{\mathrm{ind}(P)}\bigcap X\neq\phi\}$$

- The lower approximation of a set X with respect to P is the set of all objects, which can certainty be classified as X with respect to P (are certainly member of X with respect to P).

$$\underline{AP}(X)=\{x\in U|[x]_{\mathrm{ind}(P)}\subseteq X\}$$

- The boundary region of a set X with respect to P is the set of all objects, which cannot be classified with respect to P neither as certainly member of X nor as certainly non member of X with respect to P.

$$BN_P(X)=\overline{AP}(X)-\underline{AP}(X)$$

Based on these definitions, the set X is crisp, if the boundary region of X is empty; otherwise the set X is rough. The first case indicates that set X is *exact* with respect to P, whereas the second case indicates that set X is *inexact* with respect to P.

The information granules is another denotation to the equivalence classes of the indiscernibility relation generated by P. The granule represents the elementary portion of knowledge that can be recognized due to indiscernibility relation P. Then, approximation sets can also be described in terms of granules information [132].

- The upper approximation of set X ($\overline{AP}(X)$) is a union of all granules that have non-empty intersection with the set X.
- The lower approximation of a set X ($\underline{AP}(X)$) is a union of all granules that are completely included in the set X.
- The boundary region of a set X is the difference between the upper and lower approximation sets.

Figure 32 represents the upper and lower approximation sets and the boundary region with means to the information granule.

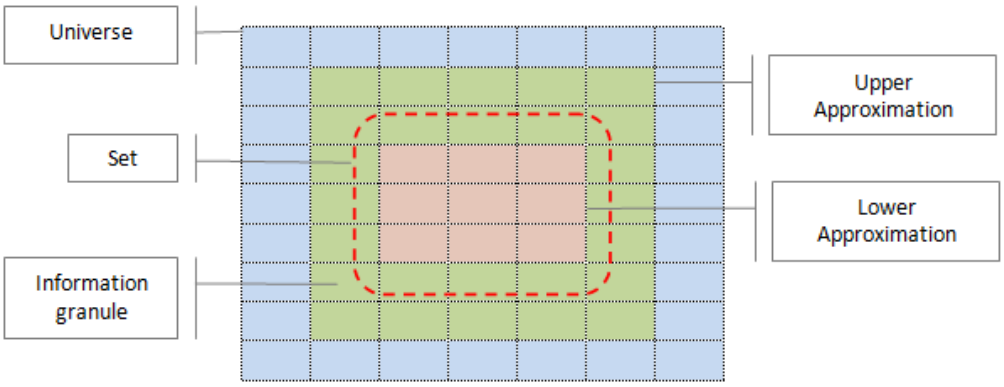


Figure 32: The elements of rough set theory in terms of approximation sets

The roughness metric is usually used to measure the amount of uncertainty of the extracted rough set [132]. For any information system (IS) involving set of objects (U) and set of attributes (R), and for any non-empty subset $X \subseteq U$ and attributes $P \subseteq R$, the roughness metric of set X with respect to P is denoted in equation 18.

$$R_P(X) = 1 - \frac{|\underline{AP}(X)|}{|\overline{AP}(X)|} \tag{18}$$

Where $X \neq \phi$, $|S|$ denoted the cardinality of the finite set S, and $R_P(X) \in [0,1]$.

5.3 WATERMARKING APPROACH IN SPATIAL DOMAIN BASED ON HVS CHARACTERISTICS AND ROUGH SET THEORY

A robust image watermarking approach based on HVS characteristics and rough set theory is proposed. The proposed approach deals with the vague and uncertainty definition of the textured regions of host image in aims to identify more appropriate regions for embedding watermark with reasonable imperceptibility and robustness ratios. The approach took into account two indiscernible HVS characteristics and processed them by rough set theory.

5.3.1 *Problem statement*

The proposed watermarking approach deals with two problems that are related to the sensitivity of color representations of the processed image for the human eyes and the indiscernible effects of DCT coefficients on the perceptual quality of the processed image. These problems in watermarking system have a close relationship with the principles of HVS in terms of robustness and imperceptibility. The color representation problem deals with the degree of sensitivity of each color space of the host image for the human eyes. Many studies confirmed that analyzing RGB image in means of HVS requires to convert it into another color spaces like *YCbCr*, which defined three components: luminance (Y), chrominance blue (Cb) and chrominance red (Cr) [53]. The luminance component means the gray-scale of the original RGB image, it expresses the most information in the image. The chrominance components refers to the color components and they express the details of host image. In means of HVS characteristics, the human eyes are more sensitive to the luminance component and are less sensitive to the *Cb* component. For designing watermarking system, hiding watermark in *Cb* component will be more appropriate in terms of imperceptibility and robustness, since the human eye will not be able to easily note the modification or change in the watermarked image. The difficulty here is deciding the amount of bits that can be embedded in the *Cb* component without degrade significantly the perceptual quality of watermarked image.

The DCT coefficients ambiguity deals with the DC and AC coefficients of the transformed image based on DCT. The literature mentions that the DC coefficient of each image's block expresses the most magnitude information of that block and to describe the nature of the block (smooth or texture) [47]. These perspectives can be analyzed in terms of HVS and for designing watermarking system. In terms of HVS, the changes in DC coefficients are more sensitive to the human eyes rather than changes in AC coefficients, which define the details of image's information. For designing watermarking system, it is proved

that embedding watermark bits in DC coefficients is more appropriate in terms of robustness than embedding them in AC coefficients [47][39]. The vague and uncertainty in this case can be described by the amount of bits that can be embedded in the DC coefficients by preserving the robustness and the perceptual quality of the watermarked image.

5.3.2 *System model*

In order to solve these two ambiguity problems, the proposed watermarking approach exploits the capability of rough set theory. Initially, the approach builds two information systems related to the nature of host images, which are based on the amount of image content. Then, rough set theory is applied to define the upper and lower approximation sets and subsequently to extract the rough set, which defines approximately most appropriate blocks to embed watermark in terms of robustness and imperceptibility.

5.3.3 *Initialization*

The proposed approach considers two types of color images: semi-textured and textured images to construct two information systems. Any color image, which is represented by RGB bitmap is converted to *YCbCr* components to display luminance component(Y), chrominance blue (Cb), and chrominance red (Cr) components. The approach is designed only by considering the *Cb* matrix, that is partitioned into non-overlapping 64×64 blocks. Based on rough set theory each one is a granule. The approach does the analysis of each 64×64 block to define two attributes: attribute (1) defines the average value of pixels in every block in *Cb* matrix, where each pixel's value is ranged between [0-255], attribute (2) represents the category value of DC coefficient for each block in *Cb* matrix. Indeed, each 64×64 block is partitioned into 8×8 non-overlapping sub-blocks, then the DC coefficient for each 8×8 sub-block is computed in spatial domain according to equation 7 (see subsection 2.6.2) [97]. The average value of all DC coefficients of all 8×8 sub-blocks is calculated and it mapped into a category value according to Huffman coding table presented in [104]. The categories of DC coefficients are ranged [0-11]. The structure of the system initialization is presented in figure 33.

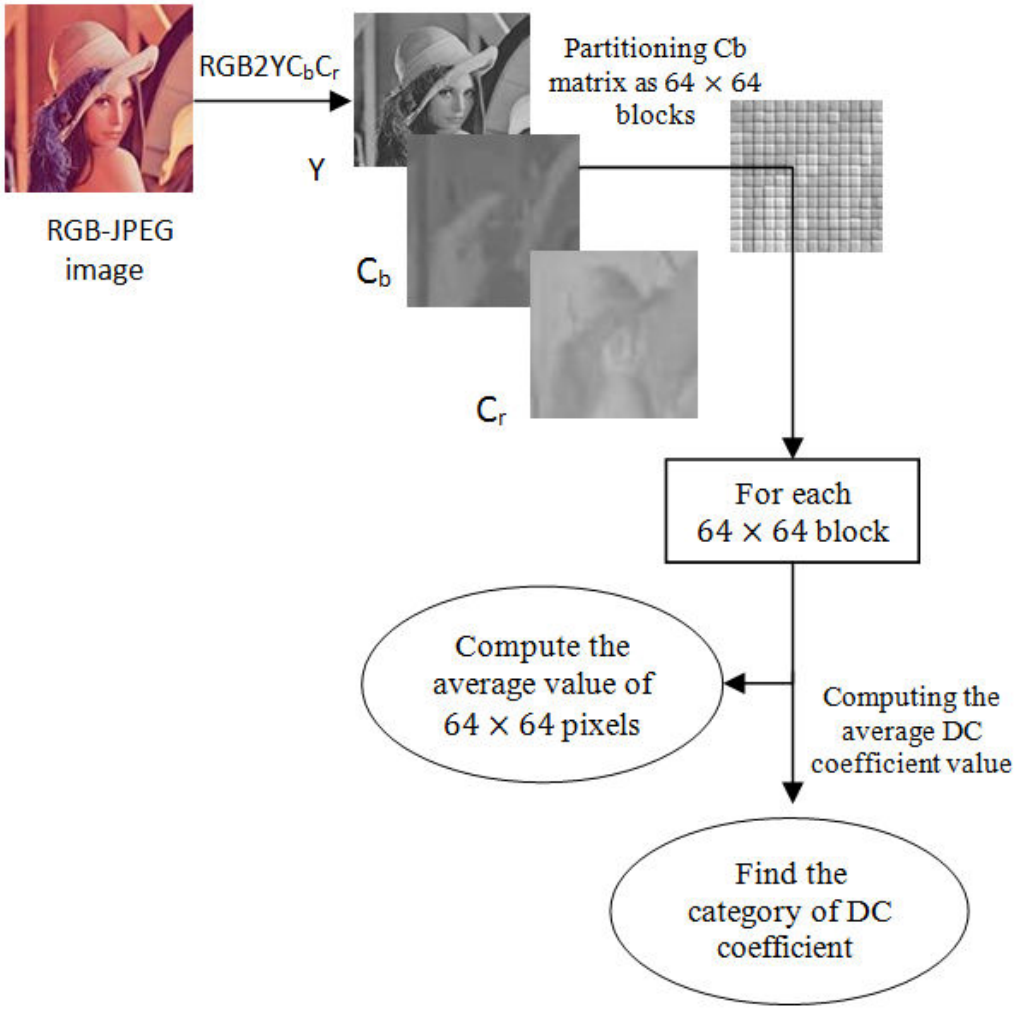


Figure 33: The structure of system initialization

5.3.4 *Construction of an Information System for Digital Images*

A *Construct an information system for both semi-textured and textured images*

The *Cb* matrix can be represented as an information system *I(U,R)* that involves a set of objects *U* and a set of attributes *R*. The proposed system defines two information systems, which are theoretically well-matched with the watermarking process, and are efficient in terms of robustness and imperceptibility of watermarked image.

Each one of these information systems consists of 12 objects, and three attributes. The attributes include the average value of 64×64 pixels corresponding to *Cb* attribute, the category of DC coefficient of the 64×64 processed block, and the decision attribute. Defining 12 objects in the information system is arbitrary, the average value of *Cb* pixels is ranged between [0-255], the category of encoded DC coefficient is ranged [0-11]. The decision attributes express the

possibility of the object to hold watermark efficiently (achieve good robustness against different image processing attacks and preserving a perceptual quality of watermarked image).

Table 26, illustrates the information system for semi-textured images. The decision of the information system is based on threshold T that corresponds to the class number. By demonstrating the information system in table 26, the decision for embedding watermark in semi-textured image blocks depends on $T \leqslant 5$. This can be explained theoretically by noting that all blocks in any semi-textured images are flat and most significant information content is characterized with low *Cb* values and low DC categories. Then, embedding watermark in these blocks will become more appropriate to preserve perceptual image quality and achieving high robustness. In case that some image blocks have DC category in [4-5], this means that these blocks have much information content but it would be significantly low. Therefore, increasing these information by embedding watermark bits will become noticeable by human eyes, and the watermark becomes fragile against attacks.

Table 26: Information system of semi-textured images

Class No.	Average value of Cb pixels	Category of DC coefficients	Decision
1	X$\leqslant$ 127	0	Yes
2	X>127	0	Yes
3	X$\leqslant$ 127	[1-3]	Yes
4	X>127	[1-3]	Yes
5	X$\leqslant$ 127	[4-5]	Yes
6	X>127	[4-5]	No
7	X$\leqslant$ 127	[6-7]	No
8	X>127	[6-7]	No
9	X$\leqslant$ 127	[8-9]	No
10	X>127	[8-9]	No
11	X$\leqslant$ 127	[10-11]	No
12	X>127	[10-11]	No

On the other hand, table 27 illustrates the information system for textured images. The decision depends on $T \geqslant 4$. This can be explained theoretically by noting that all blocks in any textured images are represented by high *Cb* values and high DC categories, where all blocks have significant information content. Embedding watermark through these blocks will become more appropriate to

preserve perceptual image quality and achieving high robustness. In case that some image blocks have DC category in [1-3], this means that these blocks have low information content. Therefore, increasing this information by embedding watermark bits will become noticeable by human eyes, and the watermark becomes fragile against attacks.

Table 27: Information system of textured images

Class No.	Average value of Cb pixels	Category of DC coefficients	Decision
1	X$\leqslant$ 127	0	No
2	X>127	0	No
3	X$\leqslant$ 127	[1-3]	No
4	X>127	[1-3]	Yes
5	X$\leqslant$ 127	[4-5]	Yes
6	X>127	[4-5]	Yes
7	X$\leqslant$ 127	[6-7]	Yes
8	X>127	[6-7]	Yes
9	X$\leqslant$ 127	[8-9]	Yes
10	X>127	[8-9]	Yes
11	X$\leqslant$ 127	[10-11]	Yes
12	X>127	[10-11]	Yes

5.3.5 *Rough Set Implementation*

From the information systems illustrated in table 26 and table 27, a unified information system that deals with any image regardless its nature can be built.

The unified information system is illustrated in table 28, where it expresses the ambiguity in the decision of watermarking process due to the indiscernibility in defining an appropriate ranges of *Cb* and DC category for each candidate block to embed watermark in term of the HVS.

Table 28: Unified information system for semi-textured and textured images

Class No.	Average value of Cb pixels	Category of DC coefficients	Decision
1	X⩽ 127	0	Yes
2	X⩽ 127	0	No
3	X>127	0	Yes
4	X>127	0	No
5	X⩽ 127	[1-3]	Yes
6	X⩽ 127	[1-3]	No
7	X>127	[1-3]	Yes
8	X>127	[1-3]	Yes
9	X⩽ 127	[4-5]	Yes
10	X⩽ 127	[4-5]	Yes
11	X>127	[4-5]	No
12	X>127	[4-5]	Yes
13	X⩽ 127	[6-7]	No
14	X⩽ 127	[6-7]	Yes
15	X>127	[6-7]	No
16	X>127	[6-7]	Yes
17	X⩽ 127	[8-9]	No
18	X⩽ 127	[8-9]	Yes
19	X>127	[8-9]	No
20	X>127	[8-9]	Yes
21	X⩽ 127	[10-11]	No
22	X⩽ 127	[10-11]	Yes
23	X>127	[10-11]	No
24	X>127	[10-11]	Yes

Based on table 28, the unified information system is expressed by the universe U={1,2,...,23,24} that described by subset P={average value of Cb pixels, category of DC coefficients}, then the set X={1,3,5,7,8,9,10,12,14,16,18,20,22,24} is the set of blocks with decision *yes*. By rough set theory, the upper approximation set ($\overline{AP}(X)$) and lower approximation set ($\underline{AP}(X)$) are extracted. Then, $\overline{AP}(X)$ and $\underline{AP}(X)$ are used to extract the boundary region (BN) set.
$(\overline{AP}(X))\rightarrow$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24\}.
$(\underline{AP}(X))\rightarrow$\{7,8,9,10\}.

(BN)→{1,2,3,4,5,6,11,12,13,14,15,16,17,18,19,20,21,22,23,24}.

The representation of upper, lower and boundary sets for a given problem, are described in figure 34.

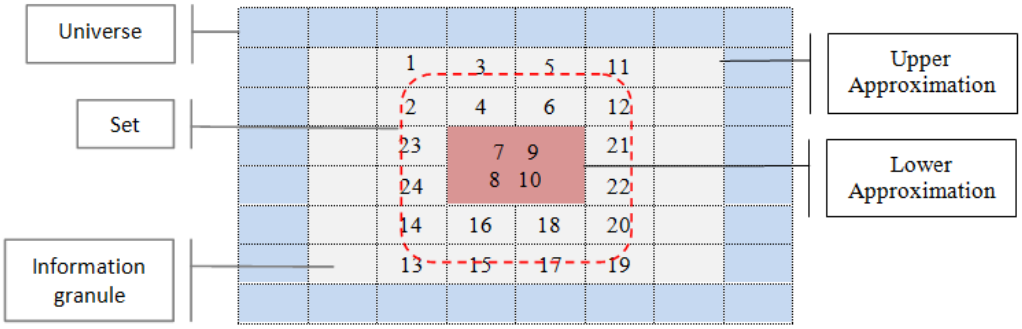


Figure 34: The representation of upper, lower and boundary sets for a given problem

The proposed approach concerns all of those blocks that are matching the condition for any boundary set element (BN). Based on the results of rough set theory, the selected image's blocks would be defined as the most appropriate blocks to embed watermark by taking into consideration the robustness and perceptual quality of embedded image.

5.3.6 *Embedding Process*

The proposed approach used the linear interpolation equation for embedding watermark in host image. This equation gives the ability to control the imperceptibility of watermarked image by using a proper interpolation factor t. The pseudo-code of the embedding process is illustrated by algorithm 4 and the structure of embedding process is presented in figure 35.

Algorithm 4 The pseudo-code of embedding watermark

Initialization: Converting the host image I from RGB bitmap into *YCbCr* bitmap
Input: The *Cb* matrix of host image I, the watermark image w and t=0.99
Partitioning *Cb* matrix into 64×64 blocks (B) where B={1,2,...,N}, N is the total number of 64×64 blocks
Each 64×64 block is partitioned into 8×8 non-overlapping sub-blocks, and the DC coefficient for each 8×8 sub-block is computed according to equation 7
Calcualting the average value of all DC coefficients of all 8×8 sub-blocks
for `i ← 1 to N` **do**
    $Cb_i \leftarrow$ *Avg value of Cb pixels of* B_i *block*
    $DC_i \leftarrow$ *Category of the average DC of* B_i *block*
    if Cb_i and DC_i are matched with the condition of any element in the boundary (BN) set **then**
        $B_i^* \leftarrow (1-t)\times w + t\times B_i$; $0<t<1$
    end if
end for
$Cb^* \leftarrow$ *combining all* B_i^*
$Iw_{YCb^*Cr} \leftarrow$ *combining (Y,Cb*,Cr)*
$Iw_{RGB} \leftarrow$ *converting* (Iw_{YCb^*Cr})

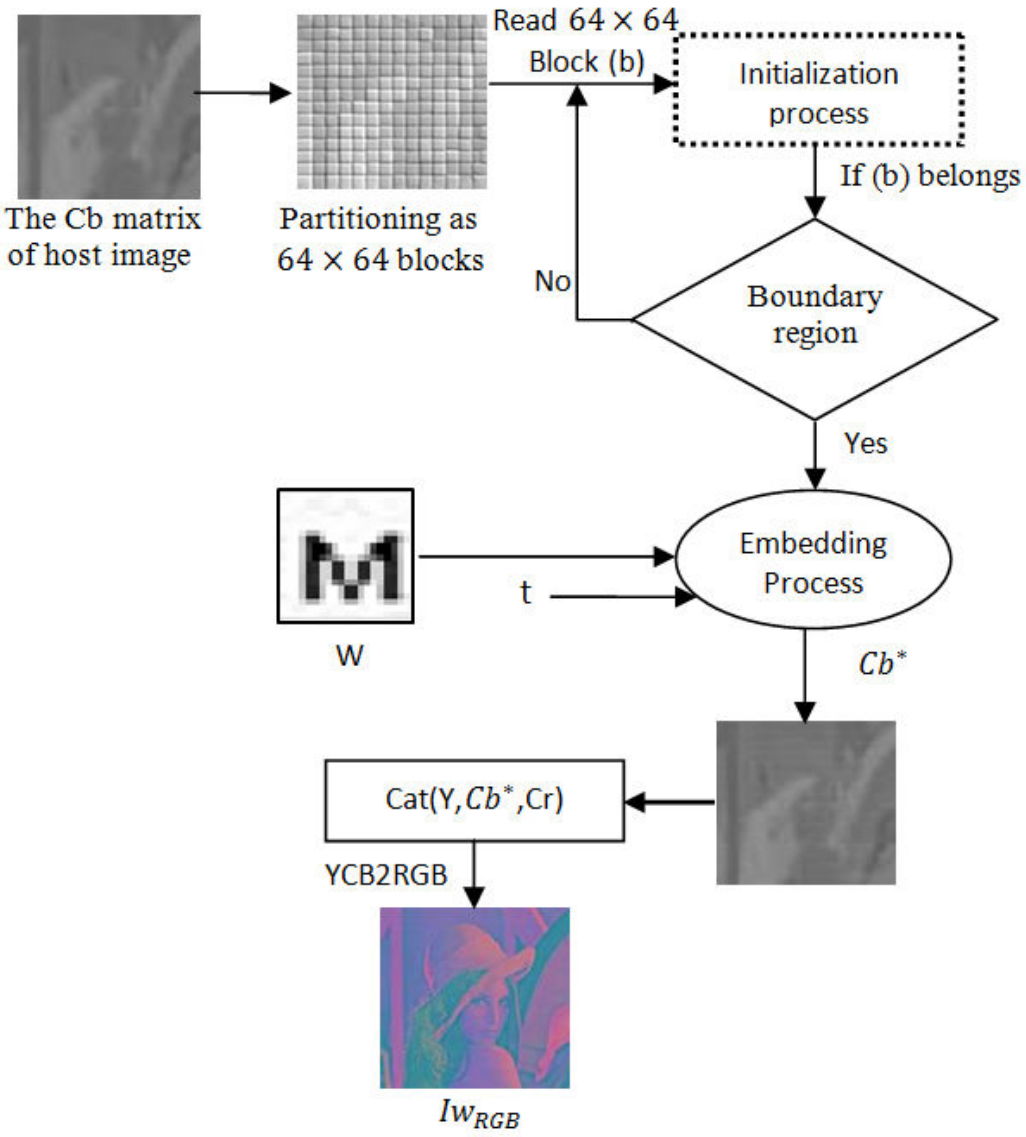


Figure 35: Watermark embedding process

5.3.7 *Extraction Process*

The proposed approach used the inverse linear interpolation equation to extract watermark from attacked watermarked image Iw^*_{RGB}, where the watermarked image Iw_{RGB} is usually exposed to different kinds of attacks. The pseudo-code of the watermark extraction is illustrated by algorithm 5 and the structure of watermark extraction is presented in figure 36.

Algorithm 5 The pseudo-code of extraction watermark

1: **Initialization:** Converting the attacked watermarked image Iw^*_{RGB} from RGB bitmap into *YCbCr* bitmap, the result is Iw^*_{YCbCr}
2: **Input:** The Iw^*_{Cb} matrix of attacked watermarked image Iw^*_{YCbCr}, the original watermark image w, the elements of the boundary (BN) set and t=0.99
3: Partitioning Iw^*_{Cb} matrix into 64×64 blocks (B*) where B={1,2,...,N}, N is the total number of 64×64 blocks
4: **for** `i ← 1 to N` **do**
5: **if** $B_i{}^*$ is one block of the boundary (BN) set **then**
6: $w_i \leftarrow (1/t)\times w - ((1-t)/t)\times B^*_i$; $0<t<1$
7: **end if**
8: **end for**
9: $w \leftarrow$ *set of all* w_i

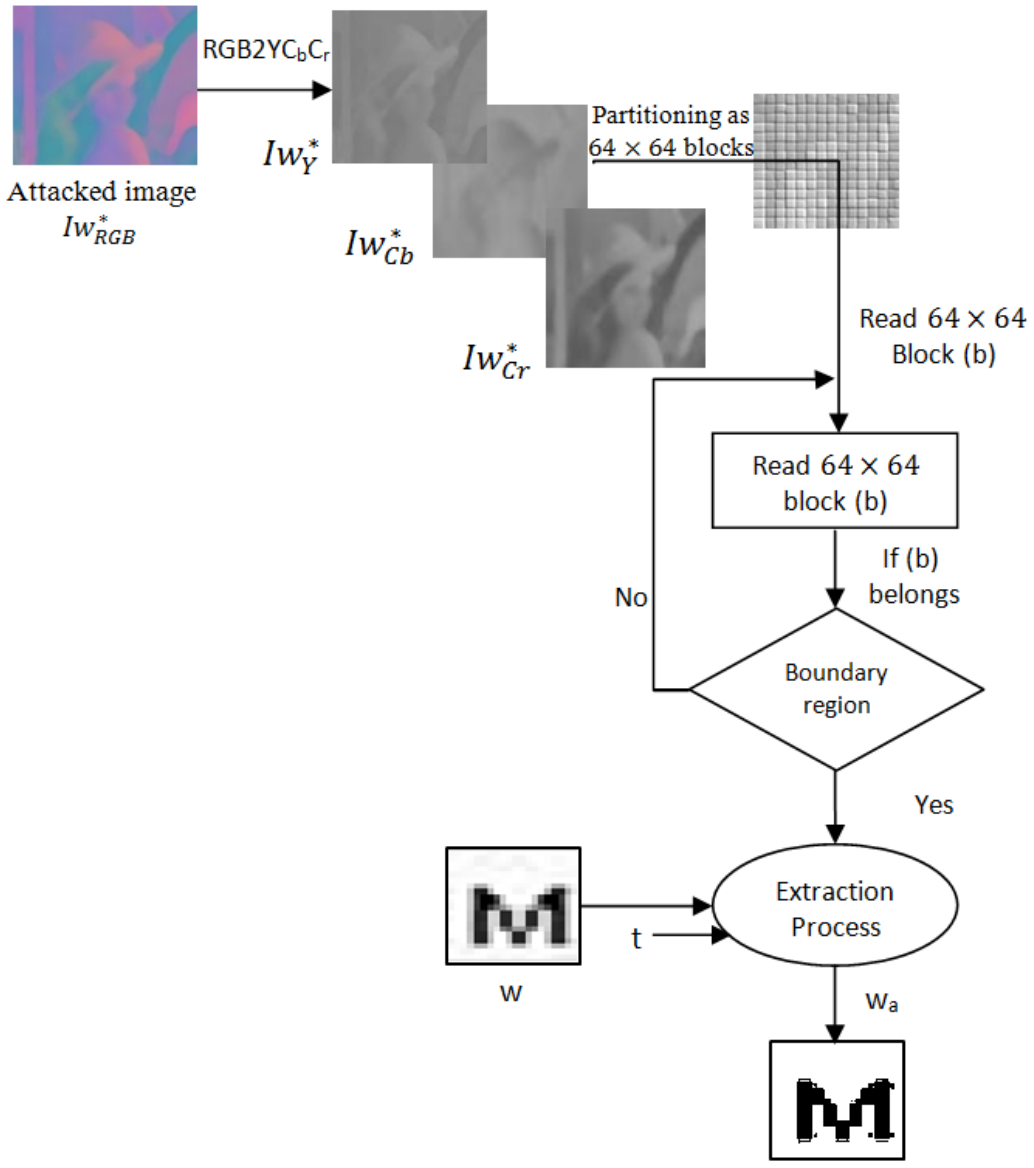


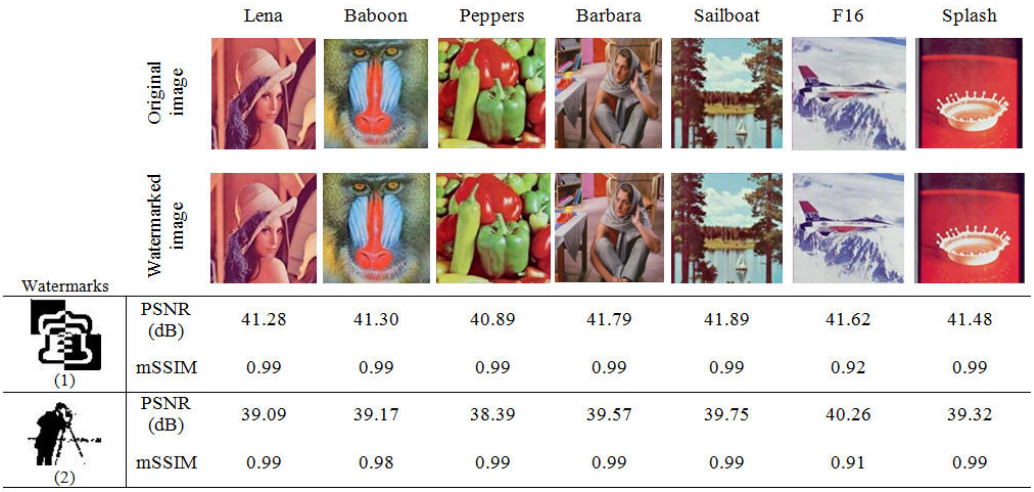
Figure 36: Watermark extraction process

5.4 EXPERIMENT RESULTS

This section presents the imperceptibility and the robustness results after testing the proposed approach on set of color images. The proposed approach is tested on natural color images sized 512×512 and using 64×64 gray-scale image as watermark.

5.4.1 *Watermark imperceptibility*

Figure 37 presents the imperceptibility results of the proposed approach on set of host color images that are collected from CVG-UGR database[1]. The PSNR and the MSSIM are computed for each original image with two watermarks.



Watermarks		Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
(1)	PSNR (dB)	41.28	41.30	40.89	41.79	41.89	41.62	41.48
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.92	0.99
(2)	PSNR (dB)	39.09	39.17	38.39	39.57	39.75	40.26	39.32
	mSSIM	0.99	0.98	0.99	0.99	0.99	0.91	0.99

Figure 37: The imperceptibility results on set of color images.

The results in figure 37 show that the proposed approach achieves a good imperceptibility. The PSNR ranges 39.1-41.9 dB, while the MSSIM reaches 0.99 in all tested images except in case of F16 image where MSSIM reaches 0.92. Visually, F16 image has high luminance masking and low chrominance values whereby distortion becomes more visible with any change in the chrominance spaces.

5.4.2 *Watermarking robustness*

To evaluate the robustness of the proposed approach, the experiments are conducted with a particular focus on noise corruption, filtering, image compression and geometric correction. The consequence of applying various attacks on color Lena image is illustrated in figure 38. All watermarked images are exposed to

1 CVG-UGR database, http://decsai.ugr.es/cvg/dbimagenes/

a variety of geometric and non-geometric attacks using StirMark Benchmark v.4 [80] and Matlab.

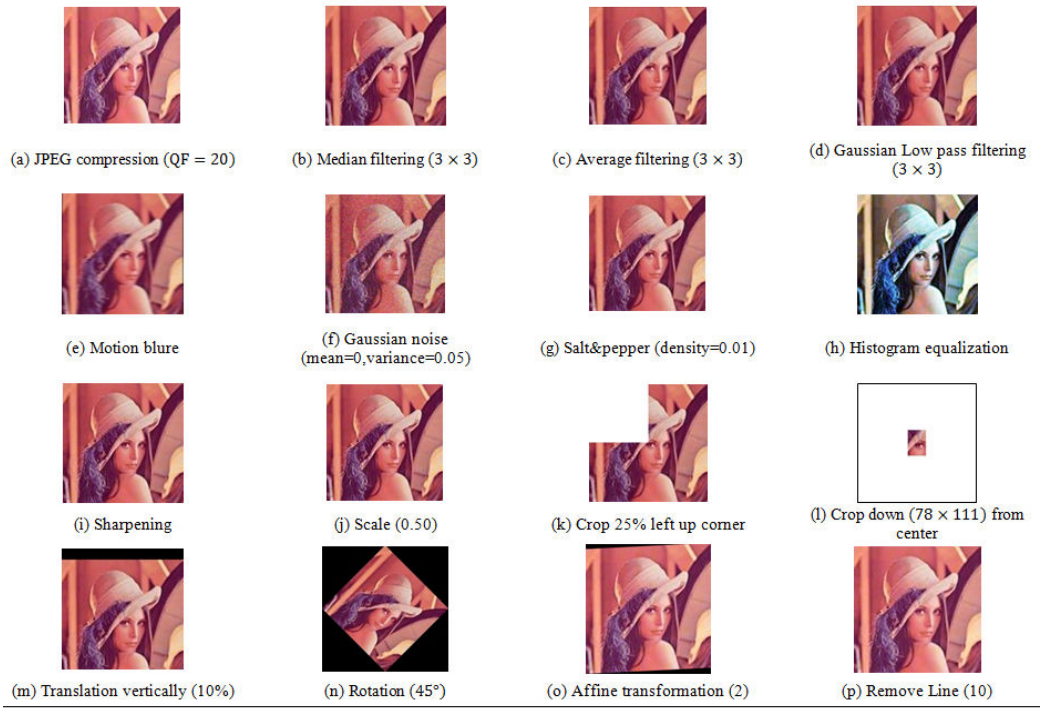


Figure 38: The consequences of applying different attacks on watermarked color Lena image.

Due to the large number of blocks that satisfy the boundary rough set, the experiments result is displayed in average as showed in table 29 and table 30. The BER and NC are calculated between the original watermark and the extracted watermark for each attacks scenario.

In all experiments using the two watermarks logos, the NC ranges 0.99-1. This means that the proposed approach is able to recover the embedded watermark from attacked watermarked image with high similarity. The original watermark and the extracted one are absolutely identical.

Table 29 shows BER results for host color images using watermark logo 1 under various attacks. As well, table 30 presents BER results for host color images using watermark logo 2 under various attacks.

	BER for Watermark Logo 1						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	6.84	6.84	6.80	6.86	6.85	11.41	6.84
Median filtering (3×3)	6.84	6.84	6.80	6.84	6.85	11.41	6.84
Average filtering (3×3)	6.84	6.84	6.80	6.84	6.85	11.41	6.84
Gaussian low pass filtering (3×3)	6.84	6.84	6.80	6.84	6.85	11.41	6.84
Motion Blure	6.84	6.84	6.79	6.84	6.85	11.41	6.84
Gaussian noise (mean=0,variance=0.05)	6.84	6.84	6.79	6.84	6.85	10.34	6.84
Salt&Pepper noise (noise density=0.01)	6.84	6.83	6.79	6.84	6.85	10.34	6.84
Histogram equalization	6.84	6.83	6.79	6.84	6.85	8.16	6.84
Sharpening	6.84	6.83	6.79	6.84	6.85	8.16	6.84
Scaling (0.5) 512×512 → 256×256	6.84	6.83	6.79	6.84	6.85	8.16	6.84
Cropping left up corner (25%)	6.84	6.83	6.79	6.84	6.85	8.16	6.84
Cropping down from center (78×111)	6.84	6.83	6.79	6.84	6.85	8.16	6.84
Translation vertically (10%)	6.84	6.83	6.79	6.84	6.85	8.16	6.84
Rotation(45°)	6.84	6.83	6.79	6.84	6.85	8.16	6.83
Affine transformation (2)	6.84	6.83	6.79	6.84	6.85	8.16	6.83
RML (10)	6.84	6.83	6.79	6.84	6.85	8.16	6.83

Table 29: BER results for natural color images using watermark logo 1 under various attacks.

The BER results in table 29 show the robustness of the proposed approach against various attacks when using watermark logo 1. The BER for all images did not exceed 7% except in case of F16 image, where it ranges 8.16-11.41%. The lower robustness in case of F16 image comparing with other images could be explained due to the large pixels values of F16 image. Visually the predominant color in F16 image is the white color, which has value equal or close to 255. Thus, the extraction process using interpolation technique leads to loss more watermark data when it is subtracted from high value of watermarked image.

	BER for Watermark Logo 2						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	3.80	3.80	3.79	3.80	3.82	6.39	3.80
Median filtering (3×3)	3.80	3.80	3.79	3.80	3.80	6.35	3.80
Average filtering (3×3)	3.80	3.80	3.79	3.80	3.80	6.35	3.80
Gaussian low pass filtering (3×3)	3.80	3.80	3.79	3.80	3.80	6.35	3.80
Motion Blure	3.80	3.80	3.79	3.80	3.80	6.35	3.80
Gaussian noise (mean=0,variance=0.05)	3.80	3.80	3.79	3.80	3.80	5.70	3.80
Salt&Pepper noise (noise density=0.01)	3.80	3.80	3.79	3.80	3.80	5.70	3.80
Histogram equalization	3.80	3.80	3.79	3.80	3.80	3.97	3.80
Sharpening	3.80	3.80	3.79	3.80	3.80	3.97	3.80
Scaling (0.5) 512×512 → 256×256	3.80	3.80	3.79	3.80	3.80	3.97	3.80
Cropping left up corner (25%)	3.80	3.80	3.79	3.80	3.80	3.97	3.80
Cropping down from center (78×111)	3.80	3.80	3.79	3.80	3.80	3.97	3.80
Translation vertically (10%)	3.80	3.80	3.79	3.80	3.80	3.97	3.79
Rotation (45°)	3.80	3.80	3.79	3.80	3.80	3.97	3.79
Affine transformation (2)	3.80	3.80	3.79	3.80	3.80	3.97	3.79
RML (10)	3.80	3.80	3.79	3.80	3.80	3.97	3.79

Table 30: BER results for natural color images using watermark logo 2 under various attacks.

As well as, the BER results in table 30 show the robustness of proposed approach against various attacks where using watermark logo 2. The BER for all images did not exceed 4% except in case of F16 image, where it ranges 3.97-6.39%. The lower robustness in case of F16 image comparing with other images is also explained due to the same reason as that mentioned in the previous paragraph.

The mentioned experiments result in terms of PSNR, mSSIM, BER and NC prove the efficiency of the proposed approach and its capability to deal with the color representation and DCT coefficients problems in terms of HVS. This gives a sense that the proposed rough set-based watermarking technique is very interesting to ensure high robustness and imperceptibility ratios.

5.4.3 *Embedding rate analysis*

In the proposed approach, the watermark of size 64×64 8-bits gray-scale image is embedded in many locations of the 512×512 24-bits color image. The minimum

embedding rate is obtained when only one location of blue color space is used for embedding watermark, while the maximum embedding rate is obtained when all locations of blue color space are used to embed watermark. The minimum number of location (of size 64×64) is 1, and the maximum number of locations (each of size 64×64) in blue color space is equal 64. Hence, the minimum embedding rate ER is equal (64×64×8)/512×512×3= 32768/786432= 0.04166 (BPP) while the maximum embedding rate ER is equal (64×64×8×64)/(512×512×3)= 2097152/786432= 2.66 (BPP).

5.4.4 *Execution time result*

In the experiments, HP machine 3.4 GHz Intel(R)/core(TM) i7 CPU with 8.0 GB RAM is used as the computing platform. The overall execution time on any host images and under various attacks using the proposed approach is equal 6.5 seconds. The extraction process requires a little bit more execution time than the embedding process due to writing many watermarks images on a specific file.

However, the proposed approach presents an efficient performance in terms of execution time.

5.5 COMPUTATIONAL COMPLEXITY ANALYSIS

The proposed approach is implemented through several tasks on color host image of size $M \times N$. These tasks including building the information systems, partitioning the host image, computing the average of *Cb* pixels of each partitioned block, computing the DC coefficient of each partitioned blocks and finally building the decision table based on rough set principle have the purpose to define the significant visual blocks concerned to be embedded.

The information systems in the proposed approach are built based on theoretical thresholds without machine processing. Computationally this task requires O(1). Afterward, the tasks of partitioning host image of size $M \times N$ into set of non-overlapping blocks and computing the average value of *Cb* pixels of each partitioned block each requires O(M×N) computationally. Computing the DC coefficient of each partitioned blocks requires O(M×N), while building the decision table based on rough set is achieved without any machine processing while its computationally requires O(1). For identifying the significant visual blocks in host image, the values of average *Cb* and DC coefficients are compared with the average *Cb* and DC coefficient in each decision table class. This task requires O(M×N×k) where *k* is the decision length table. Thus, the overall computational complexity (*T*) of the proposed approach equals O(M×N×k).

5.6 COMPARATIVE STUDY

This section presents a comparative study in term of performance between the proposed watermarking approach with other watermarking approaches. Various aspects are considered including: the imperceptibility and the robustness ratios against different attacks, the domain based, the embedding rate, the execution time, and the computational complexity.

According to these aspects, table 31 presents a general comparison between the proposed approach and some proposed color image watermarking approaches in [78][98][69][88][97][2][116][90][62].

Approach	Parah et al., 2016 [78]	Su et al., 2017 [98]	Moosazadeh et al., 2017 [69]	Roy et al., 2017 [88]	Su et al., 2017 [97]	Abraham et al., 2017 [2]	Wang et al., 2017 [116]	Saxena et al., 2018 [90]	Liu et al., 2018 [62]	Proposed
Domain based	DCT	Hessenberg transform	DCT	DCT	Spatial domain	Spatial domain	QWT and QDFT	DWT and SVD	DWT and SVD	Spatial domain
Embedding space(s)	Red, Green and Blue of RGB	Red, Green and Blue of RGB	Y of YCoCg	Green and Blue of RGB	Blue of RGB	Blue of RGB	low frequency of QDFT of RGB image	Singular Values of RGB	Blue of RGB	Cb of YCbCr
Type of watermarking	Robust	Robust	Robust	Robust	Robust	Fragile to geometric attacks	Fragile to local geometrical distortions	Robust	Robust	Robust
Type of watermark	1-bit binary image (0 or 1)	24-bit color image (0-255)	1-bit binary image (0 or 1)	1-bit binary image (0 or 1)	1-bit binary image (0 or 1)	1-bit binary image (0 or 1)	1-bit binary image (0 or 1)	24-bit color image (0-255)	8-bit gray-scale image (0-255)	8-bit gray-scale image (0-255)
Maximum PSNR (dB)	41.8	37.6	41.03	43.03	50.08	53.6	41.77	36.87	48.03	41.89
Maximum/ Average/ Range NC	Ranged 0.84-0.98	0.63-1	0.42-1	0.82-1	0.76-1	0.25-1	×	×	0.60-0.97	0.99
Maximum BER	16.7	×	12.8	26.0	×	75.0	43.7	×	×	11.4
Execution time (second)	×	0.88	×	×	5.99	×	×	×	×	6.5
Computational complexity	$O((M\times N)^2 log_2(M\times N))$	$O(M\times N)$	$O((M\times N)^2 log_2(M\times N))$	$O((M\times N)^2 log_2(M\times N))$	$O(M\times N)$	$O(M\times N)$	$O(M\times N)$	$O(min(M\times N^2, M^2\times N))$	$O(min(M\times N^2, M^2\times N))$	O(M×N×k)
Embedding rate (ER) (BPP)	0.0156	0.0312	0.0039	0.0078	0.0013	0.0052	0.0052	8	6.065	2.66

Table 31: Comparison the proposed approach with some color image watermarking approaches under various aspects.

Table 31 shows several watermarking approaches that are proposed in the literature for image authentication. From the domain based aspect, the proposed approaches in [78][98][69][88][116][90][62] have used the transformed coefficients for embedding watermark while the others have used the spatial domain. Since the HVS is less sensitive to any change in the blue color space, most of the proposed approaches based on this significance, embed the watermark in the blue space to maintain less noticeable image quality distortion. Some of the proposed approaches such in [78][98] have used all RGB spaces for embedding watermark to increase the embedding rate.

From the robustness point of view, most of the proposed approaches are robust against geometric and non-geometric attacks except the proposed approaches in [2][116], where they did not withstand to some kind of attacks.

Most watermarking approaches used 1-bit binary watermark to ensure image authentication, while the proposed approach uses 8-bit gray-scale logo as watermark comparing to other approaches in [98][90][62] in which use a 24-bit color logo as watermarks. The amount of embedded watermark bits into host image has a significant impact on the imperceptibility and robustness ratios. Inserting more watermark bits, gain more noticeable change on the host image, but could lead to good robustness against different attacks.

The proposed approach achieved an acceptable PSNR comparing to the other proposed approach; some of them achieved high PSNR than the proposed approach. Indeed, the proposed approaches in [97][2][62][88] achieved high PSNR than the proposed approach, the difference in PSNR is ranged 1-12%. In addition to the different representation of watermark image (1-bit or 8-bit), the approaches in [97][2] have embedded the watermark in the spatial domain by changing the LSBs, where the embedding process will impact less noticeable image quality distortion.

The proposed approach and the approach in [62] are similar by embedding 8-bit gray-scale watermark, while the approach in [62] has embedded the watermark in the LSBs of the singular values of DWT LL sub-band of the host image. This preserves less noticeable image quality distortion.

In term of robustness, the proposed approach achieved high NC and low BER ratios against various kind of attacks comparing with other proposed approaches. As well, the proposed approach and the approach in [90] achieved the maximum embedding rate comparing to the other approaches. The embedding rate in [90] reached 8 (BPP), while it reaches 2.66 (BPP) in the proposed approach.

From the execution time point of view, the proposed approach was executed in 6.5 seconds, while the proposed approaches in [98][97] are executed in 0.88 and 5.99, respectively. The difference in execution time between the proposed approach and the proposed approach in [98] is high, the announced execution time in [98] could represent the abstract time required for implementing em-

bedding and extraction procedures without consideration to the initialization or finalizing procedures.

For the computational complexity, the proposed approach is executed with lower computational complexity comparing to the proposed approaches in [78][69][88][90][62] but with high computational complexity comparing to the proposed approaches in [97][98][2][116] by k value. The approaches in [97][2] were designed in spatial domain and they did not implement any complicated function in their approaches, while the proposed approaches in [98][116] were based on low complexity transformation algorithms.

5.6.1 *Comparing the imperceptibility results*

Table 32 presents imperceptibility results comparison between the proposed approach and the some proposed approaches in [98][69][88][97][2][78][116][90][62] on color Lena image.

Approach	PSNR	SSIM
Su et al., 2017 [98]	36.4	0.94
Moosazadeh et al., 2017 [69]	40.3	×
Roy et al., 2017 [88]	42.2	×
Su et al., 2017 [97]	49.9	0.98
Abraham et al., 2017 [2]	47.6	0.97
Parah et al., 2016 [78]	41.2	×
Wang et al., 2017 [116]	40.4	×
Saxena et al., 2018 [90]	36.9	×
Liu et al., 2018 [62]	48.03	×
Proposed	41.3	0.99

Table 32: Imperceptibility results comparison in terms of PSNR and SSIM on color Lena image.

The results in table 32 show that the proposed approach achieves acceptable imperceptibility results in terms of PSNR and SSIM comparing to other proposed approaches. The PSNR in the proposed approach is higher than the achieved ones in the other proposed approaches in [98][69][78][116][90], while it is lower than the achieved PSNR in the proposed approaches in [88][97][2][62]. All of the proposed approaches in [88][97][2][62] have embedded the watermark in the LSBs, which get least noticeable image quality distortion.

For the SSIM results, the proposed approach achieved higher value comparing with other proposed approaches that used this metric. The SSIM reached 0.99 in the proposed approach, and was 0.94, 0.98 and 0.97 in [98][97][2], respectively.

5.6.2 *Comparing the robustness results*

Tables 33 and 34 present the robustness results comparison between the proposed approach and the other proposed approaches in [78][98][69][88][2][116] on color Lena image.

Attack	Parah et al., 2016 [78]	Moosazadeh et al., 2017 [69]	Roy et al., 2017 [88]	Abraham et al., 2017 [2]	Wang et al., 2017 [116]	Proposed
Median filtering (3×3)	9.95	0.19	0.44	×	2.05	3.8
Average filtering (3×3)	×	1.36	16.8	7.71	2.96	3.8
Gaussian filtering (3×3)	×	0	0	0.10	0.27	3.8
Histogram equalization	3.87	0	7.1	×	×	3.8
Sharpening	2.98	0	0	7.8	×	3.8
Gaussian noise (variance=0.001)	8.66	0.03	11.0	×	0.78	3.8
Salt&pepper noise (noise density=0.01)	15.6	2.53	6.7	3.9	0.37	3.8
Rotation (1°)	0.39	1.46	×	×	0	3.8
Rotation (5°)	2.12	×	3.9	×	0	3.8
Rotation (45°)	7.9	×	×	×	0.71	3.8
Cropping left up corner (25%)	3.5	8.3	13.9	25.0	×	3.8
Scaling (0.5) 512×512 → 256×256	7.25	0.68	0	5.18	43.7	3.8
JPEG (QF=30)	5.57	0	3.5	24.2	7.5	3.8

Table 33: BER results comparison between the proposed approach and some related approaches on color Lena image.

The BER results in table 33 show that the proposed approach achieved low BER against different attacks comparing to the other proposed approaches, especially against cropping, scaling and JPEG compression attacks. The BER in the proposed approach against cropping attack was 3.8%, while it reached 8.3% in [69], 13.9% in [88] and 25.0% in [2]. For scaling attack the achieved BER in the proposed approach was 3.8%, while it was 7.25 % in [78] and 43.7% in [116]. In case of JPEG compression attack, the achieved BER in the proposed approach was 3.8%, and was 5.57%, 24.2% and 7.5% in [78][2][116], respectively. For average filtering attack the proposed approach achieved lower BER than the proposed approaches in [2][88] and approximately the proposed approaches in [78][88] achieved the worst BER against median filtering, average filtering, histogram equalization, noise corruption and rotation attacks comparing with the other ap-

proaches. The proposed approach in [69] achieved the lowest BER against the most attacks except for cropping attack.

Attack	Parah et al., 2016 [78]	Moosazadeh et al., 2017 [69]	Roy et al., 2017 [88]	Abraham et al., 2017 [2]	Liu et al., 2018 [62]	Proposed
Median filtering (3×3)	0.94	0.99	0.99	×	0.95	0.99
Average filtering (3×3)	×	0.97	0.88	0.94	0.76	0.99
Gaussian filtering (3×3)	×	1	0.99	0.99	×	0.99
Histogram equalization	0.97	1	0.93	×	×	0.99
Sharpening	0.97	1	1	0.94	×	0.99
Gaussian noise (variance=0.001)	0.94	0.99	0.90	×	0.94	0.99
Salt&pepper noise (noise density=0.01)	0.86	0.95	0.95	0.97	0.92	0.99
Rotation (1°)	0.99	0.97	×	×	×	0.99
Rotation (5°)	0.98	×	0.97	×	×	0.99
Rotation (45°)	0.96	×	×	×	0.76	0.99
Cropping left up corner (25%)	0.99	0.84	0.86	0.75	×	0.99
Scaling (0.5) 512×512 → 256×256	0.97	0.98	0.99	0.96	×	0.99
JPEG (QF=30)	0.98	1	0.97	0.82	0.93	0.99

Table 34: NC results comparison between the proposed approach and other related approaches on color Lena image.

The NC results in table 34 show that the proposed approach achieved high NC against different attacks comparing with the other proposed approaches in [78][69][88][2][62], especially against cropping attack. In the proposed approach, the NC was 0.99 against all kind of attacks. In case of cropping attack, the NC in [69] was 0.84, in [88] was 0.86 and was 0.75 in [2]. Against JPEG attack, the proposed approach outperformed the other approaches and the approach in [2] had the lowest NC; the NC was 0.82. In case of average filtering and rotation (45°) attacks the approach in [62] achieved the lowest NC ratio comparing with the other proposed approaches, the NC was 0.76. As well, the proposed approach in [78] achieved the lowest NC comparing with the other proposed approaches against salt&peppers attack. It was 0.86. For other kinds of attacks all the approaches achieved convergent NC ratios. They ranged 0.90-1.

5.7 SYSTEM ANALYSIS

This section introduces a discussion of the most important aspects that distinguish the proposed approach from the other addressed approaches.

5.7.1 *Using rough set theory*

The correlations between image characteristics and the HVS are investigated in this chapter using rough set theory to introduce efficient image watermarking approach. Rough set theory is applied to examine the sensitivity of human eye to the color representations and to the brightness obtained from DC coefficient. It approximate the image blocks into upper and lower sets using two theoretical based thresholds which are related to the values of blue color and DC coefficient. This technique helps to identify the visual significant locations in host image for holding watermark. Inserting watermark in host image through these locations is more acceptable with less vulnerability to attacks and causing less noticeable visual distortion on watermarked image. In the proposed approach, all blocks in the boundary region are used as visual significant blocks for adding watermark data.

5.7.2 *Imperceptibility and robustness*

In the proposed approach, the spatial pixels of boundary region blocks are increased in a level that guarantees less visual distortion and withstands to various attacks. The interpolation factor (t) in linear interpolation equation that is presented in algorithm 4 is used to maintain the amount of bits that could be embedded in the host image without causing noticeable image quality distortion, while selecting the visual significant blocks using rough set has as good preserve robustness. The PSNR reached 41.89 dB and mSSIM reached 0.99, while the NC reached 0.99 and the maximum BER did not exceed 11.4 against various geometric and non-geometric attacks. These results ensure the efficiency of the proposed approach to reach authenticity.

5.7.3 *Computational complexity and execution time*

The proposed watermarking approach is implemented in moderate computational complexity and execution time. The overall computational complexity is $O(M \times N \times k)$ and the execution time of the proposed algorithm requires 6.5 seconds. The moderate computational complexity and execution time make the proposed approach practical for real time applications.

5.7.4 *Embedding rate*

The proposed watermarking approach embedded watermark of size 64×64 8-bits gray-scale image in many locations of 512×512 24-bits color image. The minimum embedding rate ER is obtained when one block of blue color space is used for embedding watermark, in this case the ER equal 0.04166 (BPP) while the maximum embedding rate ER is obtained when all block of the blue color spaces are used for embedding watermark. Hence the ER equal 2.66 (BPP). The range of embedding rate in the proposed algorithm exhibited excellent performance and help for a better resolution of tamper localization and for validating watermark robustness.

5.8 CONCLUSION

The rough set theory represents one of the important computational intelligence systems that has a significant role in extracting rough information from vague and uncertain knowledge. It is efficient to solve vague problems linked to image processing and intelligent support decision making. This chapter illustrated the capability of rough set theory to deal with some ambiguity problems in digital images. These problems are associated with image characteristics, and have a close relation with HVS principles in case of designing an efficient image authentication system. The approximation principle based on rough set theory has been utilized to extract rough information from the vague image characteristics to suggest an efficient watermarking approach in terms of perceptual quality of watermarked image, watermark robustness against different image processing attacks, embedding rate and computational complexity.

The PSNR reached 41.89 dB and mSSIM reached 0.99, while the NC reached 0.99 and the maximum BER did not exceed 11.4 against various attacks. The embedding rate ranged 0.041-2.66 (BPP), while the overall computational complexity is $O(M \times N \times k)$ and the execution time requires 6.5 seconds. These results ensure the efficiency of the proposed approach to achieve color images authenticity and to be practical for real time applications.

Chapter 6

IMAGE WATERMARKING APPROACHES BASED ON TEXTURE ANALYSIS

Contents

6.1 INTRODUCTION

Preserving high perceptual quality of the watermarked image and high robustness of the embedded watermark are the basic dilemmas in designing any watermarking system. Image characteristics such as texture, color, and brightness/-darkness can help to reach an efficient watermarking solution. The importance of these properties emerged from the principles of HVS. The human eye is highly sensitive to these characteristics. Analyzing these characteristics according to the HVS can be done with the help of different intelligent techniques. These techniques manipulate image characteristics to identify visual significant locations

or coefficients in host image for holding watermark. Inserting watermark in host image in these locations or coefficients would be acceptable with less vulnerability to attacks and causing less noticeable visual distortion on image.

In this chapter, five image watermarking approaches exploiting the correlation between texture characteristic and HVS are presented. These approaches use different intelligence and knowledge discovery methods for analyzing texture characteristics. The goal is to identify visual significant locations within host image to hold the watermark with high level of imperceptibility and robustness.

The Multi-Criteria Decision Making (MCDM), the Formal Concept Analysis (FCA), the Frequent Pattern Mining (FPM), and the Association Rule Mining (ARM) methods are used to analyze texture characteristic by offering many benefits to improve the performance of watermarking in terms of robustness and imperceptibility.

This chapter is organized as follows. The problem statement is presented in section 6.2. Texture analysis of digital images is addressed in section 6.3. Section 6.4 presents image watermarking approaches based on texture analysis using MCDM. Section 6.5 presents image watermarking approach based on texture analysis using FCA. Image watermarking approach based on texture analysis using FPM is presented in section 6.6 while image watermarking approach based on texture analysis using ARM is presented in section 6.7. A comparative study is presented in section 6.8, and the system analysis to evaluate the overall performance of the proposed approaches is presented in section 6.9. Finally, section 6.10 concludes this chapter.

6.2 PROBLEM STATEMENT

Texture property is one of the important spatial characteristics of host image that has high significant relation with HVS. Analyzing this property can help to identify visual significant (i.e. highly textured) blocks within host image to hold the watermark with least noticeable image quality distortion and high robustness. The various features that are often used to analyze the texture property are intangible and uncertain because there is no formal, mathematical definition of texture and there is no precise level for each feature to distinguish between textured and untextured block within host image.

For the design of watermarking systems, the principles of HVS confirm that embedding watermark in strongly textured locations leads to high imperceptibility and robustness. Indeed, modifications in highly textured blocks in host image due to embedding of watermark are less sensitive to the human eye [61].

Intelligent and knowledge discovery methods are used to solve the imprecision of the image characteristics and exploit them to achieve image authentication, through the identification of significant visual locations for embedding the

watermark. In this context, Multi-Criteria Decision Making (MCDM), Formal Concept Analysis (FCA), Frequent Pattern Mining (FPM) and Association Rule Mining (ARM) methods are used to identify highly significant visual locations in host image.

MCDM is an example of intelligent method, while FCA, FPM and ARM are examples of knowledge discovery methods.

6.3 TEXTURE ANALYSIS OF DIGITAL IMAGES

Two main approaches are used for analyzing texture of image: structural approach and statistical approach [66]. A structural approach builds a hierarchy structure of spatial pixels in order to find a set of repetitive texture elements called texel occurring in some regular or repeated pattern, while a statistical approach characterizes the texture through non-deterministic features that govern the distributions and relationships between the gray-scale intensities of an image based on one of the following techniques: first-order histogram measures, co-occurrence metrics, variograms, Fourier analysis, wavelets, fractal geometry and Markov random fields [66].

Histogram-based features such as DC, skewness, kurtosis, and entropy are used for texture analysis for a given image [66]. All of these features are calculated according to the values or the intensities of pixels of a given image. The analysis of the relationships between these features helps to define the strongly textured blocks to embed watermark and to enhance the robustness and imperceptibility ratios. To accomplish the analysis process, a transaction matrix is built by computing the values of the texture features and a Boolean matrix is built by identifying some thresholds that represent the texture level corresponding to each feature. The principle for each texture features, and the pseudo-codes that are used to compute the values of texture features and to build the transaction and Boolean matrices are described below.

6.3.1 *DC coefficient*

The 2D-DCT process transforms the pixels of an image block sized 8×8 into frequency domain coefficients. The result is 8×8 coefficients matrix consisting in one coefficient called DC and 63 coefficients called ACs. Figure 14 presents the location of DC coefficient and the locations of ACs coefficients in the resulted matrix. From the perspectives of texture analysis and HVS, the DC coefficient expresses the average information of the overall magnitude in the processed block and used as a fine property to define the energy [97]. A high-energy block is more textured than a low-energy one.

The DC coefficient of a given block of size $N \times N$ is directly obtained in spatial domain without needing 2D-DCT process (this point gives an advantage by decreasing the computational complexity). The value of DC coefficient in 8-bit depth image depends on the size of the processed block. For a 8×8 block, the DC coefficient ranges [-1024-1016] after shifting the pixels values by 128. The DC of $N \times N$ block is computed according to equation (7).

Algorithm 6 defines textured blocks based on the DC value. The average value of all DC coefficients of all blocks is selected as a threshold. The blocks having a DC value greater than a threshold are considered as textured where the others are considered as untextured. As well, algorithm 6 is used to set the DC values in the transaction matrix and to set the corresponding values in the Boolean matrix.

Algorithm 6 The pseudo-code of defining texture blocks based on DC value

input: host image I of size $M \times N$
partitioning I into $L \times L$, the result is B blocks: $B=\{B_1, B_2, ..., B_{M/L \times N/L}\}$
for each B_i: i=1:M/L×N/L **do**
    compute the DC value of B_i as DC_{B_i}
    store the value in the transaction matrix
end for
compute the average value of the DC values of all blocks as Avg_{DC}
for each B_i: i=1:M/L×N/L **do**
    if $DC_{B_i} \geqslant Avg_{DC}$ **then**
        the block B_i is textured (value set to 1 in Boolean matrix)
    else
        the block B_i is untextured (value set to 0 in Boolean matrix)
    end if
end for
output: set of textured blocks based on DC value analysis

6.3.2 *Skewness*

Skewness measures the degree of the distribution asymmetry of gray-level intensities around the mean. It is used to indicate if the block is dense toward the black or toward the white [22][127]. In the context of texture analysis, the skewness describes three cases of gray-level intensities histogram distribution [22].

1. Normal distribution: is a symmetrical distribution case, where the block is not dense toward neither the black nor the white. As illustrated in figure 39(a), the mean of gray-level intensities is equal to the median, and the skewness value is zero.

2. Negative distribution: the histogram distribution presents high gray-level intensities (the block is dense toward the white). In this case, the median of gray-level intensities is greater than the mean and the values of skewness are usually negative.

3. Positive distribution: the histogram distribution presents low gray-level intensities (the block is dense toward the black). In this case, the median of gray-level intensities is less than the mean and the values of skewness are usually positive.

   Based on the mentioned cases, the host image block is textured if it is dense towards the white (in case of negative distribution) or towards the black (in case of positive distribution). The case of normal distribution expresses no texture. The textured zone in cases of negatively and positively skewed can be defined as illustrated in figures 39(b) and 39(c), respectively.

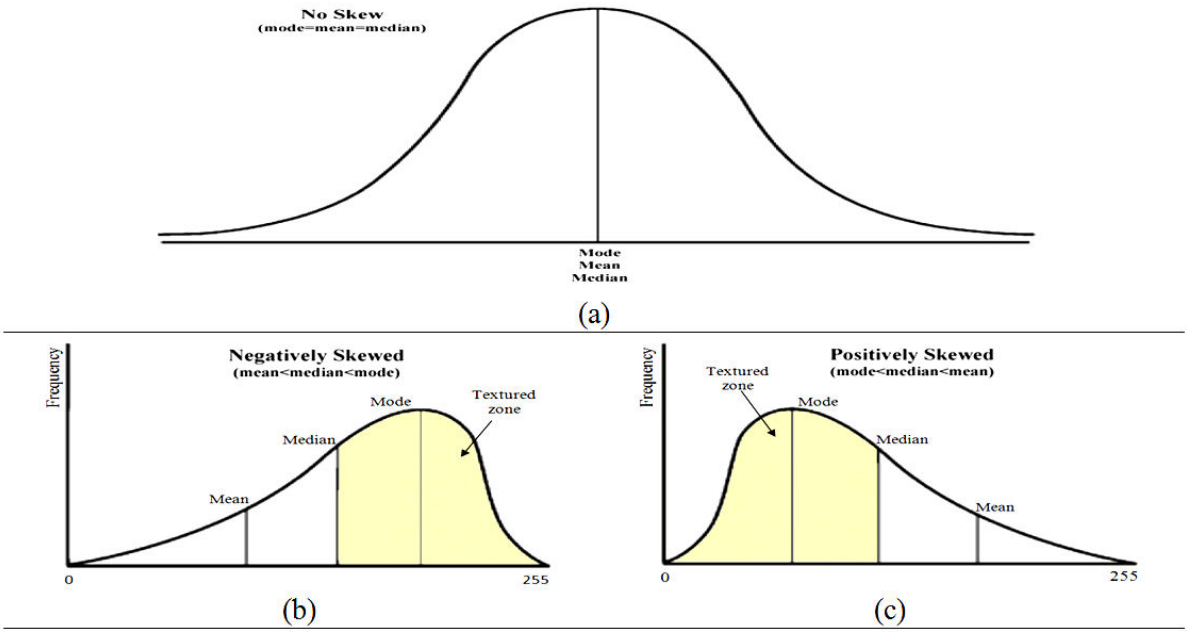


Figure 39: Diagram of (a) normal distribution, (b) negatively skewed distribution and (c) positively skewed distribution of gray-scale intensities.

The skewness feature of a given block of size $N \times N$ is obtained by computing the intensity-level of all pixels in that block *h(i)* (i=0,1,...,255) and computing the density of occurrence of the intensity levels *P(i)* (i=0,1,...,255). The skewness value is calculated using equation (19).

$$skewness = \sigma^{-3} \sum_{i=0}^{255} (i - \mu)^3 \times P(i) \tag{19}$$

where $P(i)=h(i)/(N\times N)$, $\mu=\sum_{i=0}^{255} i \times P(i)$ is the mean value of block pixels, and $\sigma=\sqrt{\sum_{i=0}^{255}(i-\mu)^2 P(i)}$ is the square root of the variance.

Algorithm 7 defines textured blocks based on skewness feature. The algorithm discriminates between textured and untextured blocks by defining two thresholds; the first one is the average skewness for all blocks that have positive skewness values called ($Avg_{positiveSkew}$), while the second one is the average skewness of all blocks that have negative skewness values called ($Avg_{negativeSkew}$). As well, algorithm 7 is used to set the skewness values in the transaction matrix and to set the corresponding values in the Boolean matrix.

Algorithm 7 The pseudo-code of defining texture blocks based on skewness value

1: **input:** host image I of size $M\times N$
2: partitioning I into $L\times L$, the result is B blocks: $B=\{B_1,B_2,...,B_{M/L\times N/L}\}$
3: **for** each B_i: i=1:M/L×N/L **do**
4: compute the skewness value of B_i as $skewness_{B_i}$ and store it in the transaction matrix
5: **end for**
6: compute the average value of all positive skewness values of all blocks as $Avg_{positiveSkew}$
7: compute the average value of all negative skewness values of all blocks as $Avg_{negativeSkew}$
8: **for** each B_i: i=1:M/L×N/L **do**
9: **if** ($skewness_{B_i}\geqslant 0$ and $skewness_{B_i}\geqslant Avg_{positiveSkew}$) or ($skewness_{B_i}<0$ and $skewness_{B_i}\geqslant Avg_{negativeSkew}$) **then**
10: the block B_i is textured (value set to 1 in Boolean matrix)
11: **else**
12: the block B_i is untextured (value set to 0 in Boolean matrix)
13: **end if**
14: **end for**
15: **output:** set of textured blocks based on skewness feature analysis

6.3.3 *Kurtosis*

It measures the flatness of gray-level intensities around the mean [22], and expresses the amount of image's information through two cases as follows.

1. If the distribution of gray-level intensities is peaky around the mean as illustrated in figure 40(a), then the kurtosis value of the processed block

is high and its surface follows the dense gray-scale value. In this case, the information content is significantly low and the block is untextured.

2. If the distribution of the gray-level intensities is flat around the mean as illustrated in figure 40(b), then the kurtosis value of the processed block is low and the block is textured [22].

Based on the analysis of case (1) and case (2), it is clear that the kurtosis value of host image zones is related to the nature of the host image. Low kurtosis value expresses the case of textured image, which has much information, while high kurtosis value expresses the case of untextured image, which has little information.

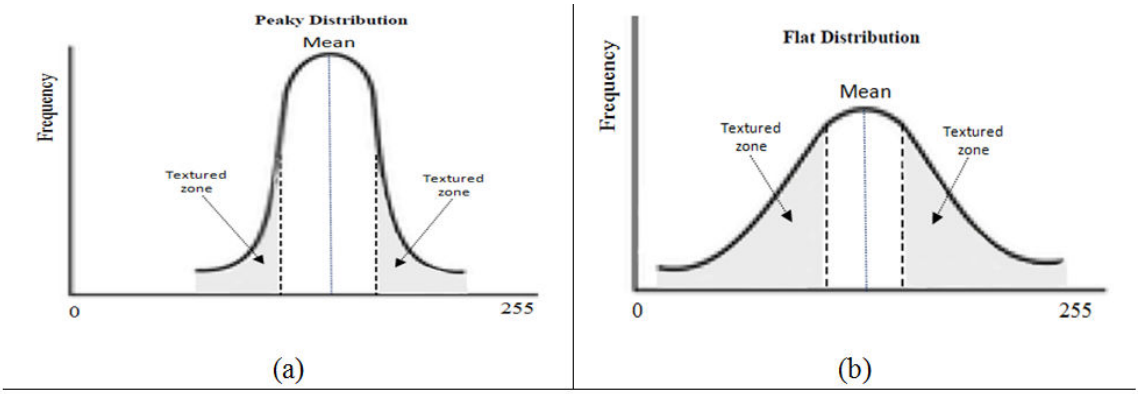


Figure 40: Diagram of (a) peaky distribution and (b) flat distribution in case of kurtosis property.

The kurtosis feature of a given block of size $N \times N$ is obtained using equation (20).

$$\text{kurtosis} = \sigma^{-4} \sum_{i=0}^{255} (i - \mu)^4 \times P(i) - 3 \tag{20}$$

Algorithm 8 defines textured blocks based on the kurtosis value. The average value of all kurtosis values of all blocks is selected as a threshold used to separate textured blocks from untextured ones. As well, algorithm 8 is used to set the kurtosis values in the transaction matrix and to set the corresponding values in the Boolean matrix.

Algorithm 8 The pseudo-code of defining texture blocks based on kurtosis value

1: **input:** host image I of size $M \times N$
2: partitioning I into $L \times L$, the result is B blocks: $B=\{B_1, B_2, ..., B_{M/L \times N/L}\}$
3: **for** each B_i: i=1:M/L×N/L **do**
4: compute the kurtosis value of B_i as $kurtosis_{B_i}$ and store it in the transaction matrix
5: **end for**
6: compute the average value of the kurtosis values of all blocks as $Avg_{kurtosis}$
7: **for** each B_i: i=1:M/L×N/L **do**
8: **if** ($kurtosis_{B_i} \leqslant Avg_{kurtosis}$ **then**
9: the block B_i is textured (value set to 1 in Boolean matrix)
10: **else**
11: the block B_i is untextured (value set to 0 in Boolean matrix)
12: **end if**
13: **end for**
14: **output:** set of textured blocks based on kurtosis feature analysis

6.3.4 *Entropy*

Entropy measures the uniformity/randomness of the distribution of gray-level intensities along the image. This property is considered as an indicator to the magnitude of image's information. High entropy value means that the gray-level intensities are distributed randomly along the image, and the image combines dispersant pixels' values. This case indicates that the image has much information and well textured.

Low entropy value means that the distribution of gray-level intensities is uniform along the image, and the image combines similar pixels' values. This case indicates that the image has little information and considered as less textured [112].

The entropy feature of a given block of size N×N is obtained using equation (21).

$$entropy = -\sum_{i=0}^{255} P(i) \log_2[P(i)] \tag{21}$$

Algorithm 9 defines textured blocks based on entropy property, using the average value of all entropies of all blocks as a threshold for discrimination between textured and untextured blocks. As well, algorithm 9 is used to set the entropy values in the transaction matrix and to set the corresponding values in the Boolean matrix.

Algorithm 9 The pseudo-code of defining texture blocks based on entropy value

input: host image I of size $M \times N$
partitioning I into $L \times L$, the result is B blocks: $B=\{B_1, B_2, ..., B_{M/L \times N/L}\}$
for each B_i: i=1:M/L×N/L **do**
    compute the entropy value of B_i as $entropy_{B_i}$ and store it in the transaction matrix
end for
compute the average value of the entopy values of all blocks as $Avg_{entropy}$
for each B_i: i=1:M/L×N/L **do**
    if ($entropy_{B_i} \geqslant Avg_{entropy}$ **then**
        the block B_i is textured (value set to 1 in Boolean matrix)
    else
        the block B_i is untextured (value set to 0 in Boolean matrix)
    end if
end for
output: set of textured blocks based on entropy feature analysis

6.4 IMAGE WATERMARKING APPROACHES BASED ON TEXTURE ANALYSIS USING MULTI-CRITERIA DECISION MAKING

This section presents how the texture problem can be analyzed using one of MCDM methods in order to identify highly textured blocks within host image to hold the watermark with high imperceptibility, high robustness, high embedding rate and low computational complexity. The problem of the textured regions identification in an image can be considered as a decision-making problem. A set of partitioned blocks of host image is a set of possible alternatives to be evaluated using a set of criteria (texture features) to select which of them are more appropriate to hold the watermark. The first order histogram features can be used as set of criteria to achieve the evaluation process. Hence, a decision matrix can be built and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) method can be applied to rank all alternatives and select the best alternative for embedding watermark. Two new image watermarking approaches based on texture analysis using TOPSIS method are presented.

We introduce a general overview of multi-criteria decision making problem in subsection 6.4.1; the main principles, the general steps of MCDM methods and specifically TOPSIS method. Then, two image watermarking approaches based on analyzing texture features using TOPSIS method are presented in subsection 6.4.2. The experiment results on set of gray-scale images in terms of imperceptibility, robustness, embedding rate and execution time are presented in subsection 6.4.3. Finally, the computational complexity is presented in subsection 6.4.4.

6.4.1 *Multi-Criteria Decision Making Problem*

A general overview of decision-making problem and the main steps for solving such type of problems using various MCDM methods are presented below. Among these methods, the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method that has been used in the proposed approach is presented in more depth.

A *General overview of decision-making problem*

Decision-making is the study of solving problems that are characterized as a choice among many alternatives to find the best one based on different criteria and decision-maker's preferences. Many problems in our life involve multiple objectives and criteria. These problems are related to the fields of engineering, industry, commercial, and human resource management.

MCDM is a branch of Operational Research field (OR) whose aim is to provide solutions for many complex decision-making problems. Some of these problems are related to high imprecise/uncertainty information and conflicting objectives. MCDM is divided into two categories: Multi-Objective Decision Making (MODM) and Multi-Attribute Decision Making (MADM). MODM relates to an infinite or numerous number of alternatives. It assumes a simultaneous evaluation with regard to a set of objectives that are optimized to a set of criteria in order to find the best alternative. In contrast, MADM is based on evaluation of a relative predetermined number of alternatives characterized by criteria. The evaluation process searches for how well the alternatives satisfy the objectives. Weighting the importance of selected criteria and assigning preference for alternatives are taken into account in MADM [21]. In this section, MCDM methods refer to MADM category. Any MCDM problem has three main elements:

1. Decision: is choosing one solution as the best among many conflicting solutions due to multiplicity of the criteria.

2. Alternatives: represent the different choices of solutions available to the decision-maker. The decision-maker evaluates these solutions based on some criteria.

3. Criteria: a set of attributes or guidelines used as basis for decision-making and for selecting the best solution. These attributes represent the different dimensions from which the solutions can be viewed. Since multi-criteria represent different dimensions of solutions, then they may conflict with each other. Two criteria conflict if the solution which is the best in one criterion is not the best with the other criterion.

B *General steps of* MCDM *methods*

There are many MCDM methods proposed in the literature to solve problems that are characterized as a choice among alternatives. All of these methods implement same steps to solve the decision-making problem [21]. These main steps of any MCDM method are illustrated in the following:

Step 1. Defining the problem, the alternatives and the criteria

This step involves the analysis of the decision-making problem to define the multiple conflicting criteria, different measurement among the criteria and the possible alternatives.

Step 2. Assigning criteria weights

Most of MCDM methods require that attributes be assigned weights of importance. Usually, these weights are normalized so that their sum equals 1. This step manages the priorities of the criteria by assigning them proper weights. These weights show the relative importance of the selected criteria. The weights of the

different criteria may be assigned by mutual consultation, pair wise comparison between criteria or by establishing a hierarchy of priorities using Analytical Hierarchy Process (AHP) [89].

Several normalized equations are used to normalize the values. Some of often used equations are presented in (22), (23) and (24).

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1,j=1}^{m,n} x_{ij}^2}}, i = 1, ..., m; j = 1, ..., n \tag{22}$$

$$r_{ij} = \frac{x_{ij} - min_j}{max_j - min_j}, i = 1, ..., m; j = 1, ..., n \tag{23}$$

$$r_{ij} = \frac{x_{ij}}{max_j}, i = 1, ..., m; j = 1, ..., n \tag{24}$$

where m is the number of alternatives, n is the number of criteria and x_{ij} is the score of alternative A_i when it is evaluated in terms of decision criterion C_j.

Step 3. Construction of the evaluation matrix

An MCDM problem can be expressed in a matrix format. A decision matrix A is an ($m \times n$) matrix in which the element x_{ij} indicates the score of alternative A_i when it is evaluated in terms of decision criterion C_j, *i=1,2,...,m and j=1,2,...,n*.
It is also assumed that the decision-maker has determined the weights of relative performance of the decision criteria (denoted as W_j, *for j=1,2,...,n*). This information is summarized in the following matrix.

$$A = \begin{array}{c} \text{Attributes/Criteria} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{12} & \cdots & x_{mn} \end{bmatrix} \end{array}$$

Step 4. Selecting the appropriate method

In this step, the decision-maker is responsible to select a proper MCDM method for selecting the preferred alternative. Based on the matrix illustrated in step 3, the MCDM method is used to determine the suitable alternative A^* with the highest degree of desirability with respect to all relevant criteria.

Step 5. Ranking the alternatives

In the final step, the set of alternatives are ranked and the first ranked alternative with the highest value based on user's preferences is selected as an optimal solution.

C *Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method*

TOPSIS method is a simple ranking method to solve the problems of large number of discrete alternatives [45]. It has the ability to allocate the scores to each alternative based on its geometric distance from the positive and negative ideal solutions. The closest alternative (the shortest geometric distance) to the positive ideal solution and the farthest (the longest geometric distance) to the negative ideal alternative is the best alternative among all alternatives.

TOPSIS method assumes that we have m alternatives and n attributes/criteria, as well as the score of each alternative with respect to each criterion. Let x_{ij} the score of alternative i with respect to criterion j and $X=(x_{ij})_{(m\times n)}$ the decision matrix. The TOPSIS method uses the following steps to find best alternative:

Step 1. Constructing the normalized decision matrix

This step transforms various dimensional attributes into non-dimensional attributes to allow comparisons across criteria. Different normalization methods are proposed in the literature to transform decision matrix $X=(x_{ij})_{(m\times n)}$ into a normalized matrix $R=(r_{ij})_{(m\times n)}$, where each attribute value in decision matrix is transformed into a value between [0-1] according to one of equations 22, 23 and 24.

Step 2. Constructing the weighted normalized decision matrix

The TOPSIS method assumes a weight value w_j for each criterion j, where $\sum_{j=1}^{n} w_j = 1$. Then, each column of the normalized decision matrix R is multiplied by its associated weight w_j. This step results in a new matrix V, where each element r_{ij} in matrix R is transformed using equation (25).

$$V_{ij} = w_j \times r_{ij}, i = 1, ..., m; j = 1, ..., n \tag{25}$$

Step 3. Determining the positive ideal and negative ideal solutions

In this step, two alternatives A^+ (the positive ideal alternative) and A^- (the negative ideal alternative) are defined. The choice of positive ideal solution is presented in equation (26) and the choice of negative ideal solution is presented in equation (27).

$$\begin{aligned} &A^+ = \{v_1^+, ..., v_n^+\}, \\ &v_j^+ = \begin{cases} max(v_{ij}), & \text{if } j \in J \\ min(v_{ij}), & \text{if } j \in J^- \end{cases} \\ &(i = 1, ..., m; j = 1, ..., n)\} \end{aligned} \tag{26}$$

$$
\begin{aligned}
&A^- = \{v_1^-, ..., v_n^-\},\\
&v_j^- = \begin{cases} \min(v_{ij}), & \text{if } j \in J \\ \max(v_{ij}), & \text{if } j \in J^- \end{cases} \\
&(i = 1, ..., m; j = 1, ..., n)\}
\end{aligned} \tag{27}
$$

where J is associated with benefit attribute, which offers an increasing utility with its higher values, and J^- is associated with cost criteria.

Step 4. Calculating the separation measures for each alternative

In this step, the separation measurement relative to the positive ideal alternative is performed by calculating the distance between each alternative in V and the positive ideal alternative A^+ using Euclidean distance as illustrated in equation (28).

$$
S_i^+ = \sqrt{\sum_{j=1}^{n} (v_j^+ - v_{ij})^2}, i = 1, ..., m; j = 1, ..., n \tag{28}
$$

Similarly, the separation measurement relative to the negative ideal alternative is performed by calculating the distance between each alternative in V and the negative ideal alternative A^- using Euclidean distance as illustrated in equation (29).

$$
S_i^- = \sqrt{\sum_{j=1}^{n} (v_j^- - v_{ij})^2}, i = 1, ..., m; j = 1, ..., n \tag{29}
$$

Step 5. Calculating the relative closeness to the ideal solution C_i^+

In this step, the closeness of A_i to the positive ideal solution A^+ is calculated using equation (30).

$$
C_i^+ = \frac{S_i^-}{S_i^+ + S_i^-}, i = 1, ..., m; 0 < C_i^+ < 1 \tag{30}
$$

In this case, C_i^+=1 if V_i=A^+ and C_i^+=0 if V_i=A^-. Afterward, a set of alternatives can be ranked in preference order according to the descending order of C_i^+. Then, the alternative with C_i^+ closest to 1 indicates the best alternative with highest performance.

6.4.2 *Proposed Approaches*

Two robust image watermarking approaches based on TOPSIS method are presented. The first approach is semi-blind and the second one is blind. These approaches use four image features/criteria (skewness, kurtosis, entropy, and

DC coefficient) to analyze the texture nature of each partitioned block (alternatives) in the host image. Then, the TOPSIS method is used to rank all partitioned blocks based on their texture magnitude. Afterward, the proposed approaches select 10% of highly textured blocks to embed the watermark. This procedure enhances the ability to prove the origins of host image even with geometric attacks (such cropping, rotation, affine transformation, and translation).

The two approaches share the texture analysis phase, but they differ in the implementation of embedding and extraction procedures. The texture analysis of an image is based mainly on TOPSIS method to identify the highly textured blocks, which are more appropriate for embedding watermark. Applying TOPSIS method for texture analysis phase is presented in next subsection and followed by the proposed embedding and extraction procedures.

The pseudo-code of the the proposed TOPSIS method based image watermarking approaches is presented in algorithm 10.

Algorithm 10 The pseudo-code of the proposed image watermarking approaches based on texture analysis using TOPSIS method

1: **preliminary:** defining the set $k=\{k_1,..., k_n\}$ as texture features (the criteria) and defining the weight vector (WV)
2: **input:** watermark image w sized $L\times L$, and host image I of size $M\times N$ (assuming M and N is multiple of L)
3: partitioning host image I into $L\times L$ blocks, results by m blocks, $m=M/L\times N/L$
4: **for** each feature k_j, j=1,...,n **do**
5: **for** each block(b_i), i=1,...,m **do**
6: define x_{ij} score of alternative b_i with respect to criterion k_j
7: **end for**
8: **end for**
9: constructing the decision matrix $X=(x_{ij})_{m\times n}$
10: applying TOPSIS method to rank all blocks based on closeness value (texture amount)
11: selecting top 10% of highest ranked blocks as preferable to hold the watermark
12: embedding watermark (I,w)
13: extracting watermark (I_{wa},w)

A *Applying TOPSIS Method for Texture Analysis*

In aims to solve the problem of detection of highly textured locations in host image, TOPSIS method is applied to evaluate all possible alternatives based on defined criteria and to rank them based on the closeness to ideal solution. This approach also provides a practical way to measure the importance and the effect of each of the used features on the results of texture analysis by using diverse

Weight Vectors (WVs). The texture analysis using TOPSIS method follows following steps.

Step 1. Initially, the gray-scale host image of size $M \times N$ (8-bit depth) is partitioned into a set of non-overlapping $L \times L$ blocks (alternatives) based on the size of watermark.

Step 2. The texture features including DC, skewness, kurtosis, and entropy are calculated for each partitioned block using the equations presented in (7) (see subsection 2.6.2), (19), (20) and (21) (see section 6.3).

Step 3. Building the decision matrix X, where the blocks $(b_1,...,b_{(M/L \times N/L)})$ of host image represent the set of alternatives and the texture features (DC, skewness, kurtosis, and entropy) represent the set of attributes (criteria). The entries of this matrix are the numerical values of intangible attributes of all alternatives. An example of decision matrix is illustrated as follows.

$$X = \begin{array}{c} \text{alternatives/criteria} \\ b_1 \\ b_2 \\ \vdots \\ b_{M/L \times N/L} \end{array} \begin{array}{c} \begin{array}{cccc} \text{DC} & \text{skewness} & \text{kurtosis} & \text{entropy} \end{array} \\ \begin{bmatrix} 271.3 & -1.86 & 3.18 & 4.81 \\ -45.69 & -0.12 & -0.60 & 4.80 \\ \vdots & \vdots & \vdots & \vdots \\ -131.2 & 1.36 & 4.61 & 6.2 \end{bmatrix} \end{array}$$

Step 4. Applying TOPSIS method on decision matrix to rank all blocks based on closeness to the ideal solution C_i^+. Through this step, the proposed approach uses equation (23) as a normalization method rather than equations (22) or (24). Because the numerical scales of DC, skewness and kurtosis features could be either negative or positive, and the goal of normalization step is to normalize all numerical values into positive values in range [0-1]. This in fact, allows a comparison of the given attributes.

On the other hand, the proposed approach suggests to assign multiple Weight Vectors (WVs) to evaluate the performance of the proposed approaches through different cases.

Five WVs are defined as follows: the first vector assigns same weight to all features, while each of the other vectors assigns high weight value to one of the used features, such as following:

- WV1 $=< 1/4, 1/4, 1/4, 1/4 >$ assigns the same weight values for all features.
- WV2 $=< 3/4, 1/12, 1/12, 1/12 >$ assigns high weight value for DC coefficient and others have same weight value.
- WV3 $=< 1/12, 3/4, 1/12, 1/12 >$ assigns high weight value for skewness feature and others have same weight value.
- WV4 $=< 1/12, 1/12, 3/4, 1/12 >$ assigns high weight value for kurtosis feature and others have same weight value.

- WV5 $=< 1/12, 1/12, 1/12, 3/4 >$ assigns high weight value for entropy feature and others have same weight value.

Analyzing the performance of the proposed approaches using different WVs makes it possible to measure the significance of each feature by comparing the obtained results through all cases. In addition, this suggestion introduces a way to define which WV is more preferable for texture analysis and may be recommended to other researchers.

Step 5. Selecting the top 10% of highest closeness blocks as the preferred blocks for embedding watermark with high imperceptibility and high robustness. Embedding watermark in many locations within host image gives more possibility to prove the origin of host image against geometric attacks.

As an example, figure 41 presents the locations of highly textured blocks corresponding to the WVs. The distribution of those blocks within host image increases the opportunity of the proposed approaches to prove the origin of image even after different attacks and especially after cropping attack.

Figure 41: Locations of highly textured blocks corresponding to different weight vectors.

Table 35 illustrates the index of top 10% of highly textured blocks that are more close to the ideal solution using five WVs. These blocks are arranged descending from the closest to the ideal solution towards the farthest from the ideal solution.

Table 35: Indexes of top 10% of highly textured blocks selected using five WVs.

WV no.	← goes to the closest block					
WV 1	26	24	11	10	1	19
WV 2	47	48	22	24	13	21
WV 3	5	26	18	11	3	10
WV 4	2	39	6	1	24	8
WV 5	36	30	43	54	51	38

Table 35 shows the set of blocks that are frequently selected with different WVs which can exactly define which block is frequently selected with most WVs. The blocks which have indexes {26,24,11,10,1} are frequently selected as highly textured blocks with five WVs, and the block which has index *24* is the most textured block among all other alternatives. Thus, the block which has index *24* is the highest textured block among all other blocks. As well, the weight vectors *WV1* and *WV3* worked well by identifying most or even all of frequently textured blocks mentioned above. This, in turn, gives a way to define the importance of each of the used criteria.

Figure 42 presents a partitioning of Lena image into *64×64* non-overlapping blocks, and figure 43 presents the nature of the blocks that are frequently selected in the proposed approach as the most textured.

Figure 42: Partitioning Lena image into non-overlapping 64×64 blocks.

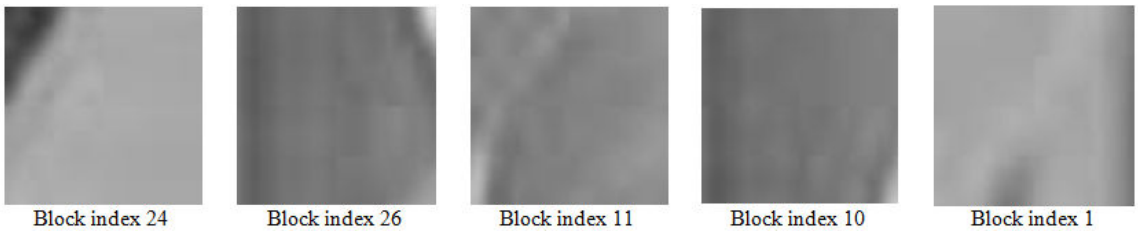


Figure 43: Texture nature of the selected frequent blocks in the proposed approach.

Based on visual nature analysis of the selected textured blocks in figure 43, the blocks are trend to either high brightness or high darkness. Visually, blocks 1 and 24 have high luminance masking while blocks 10, 11 and 26 have high contrast masking. Luminance masking whereby image distortions tend to be less visible in bright regions in the image, and contrast masking whereby distortions become less visible in highly significant activity or texture regions in the image.

B *Approach 1: Semi-blind image watermarking approach in spatial domain*

The first image watermarking approach starts by applying texture analysis phase to identify the top 10% of highly textured blocks for the watermark embedding process. Then, it uses the linear interpolation technique to achieve watermark embedding in the original image I and uses the inverse form of linear interpolation to extract the attacked watermark w_a from the attacked watermarked image I_{wa}. This approach is semi-blind watermarking since it requires the original watermark for the watermark extraction procedure.

The general framework of the first approach is illustrated in figure 44 and the embedding/extraction procedures are presented below.

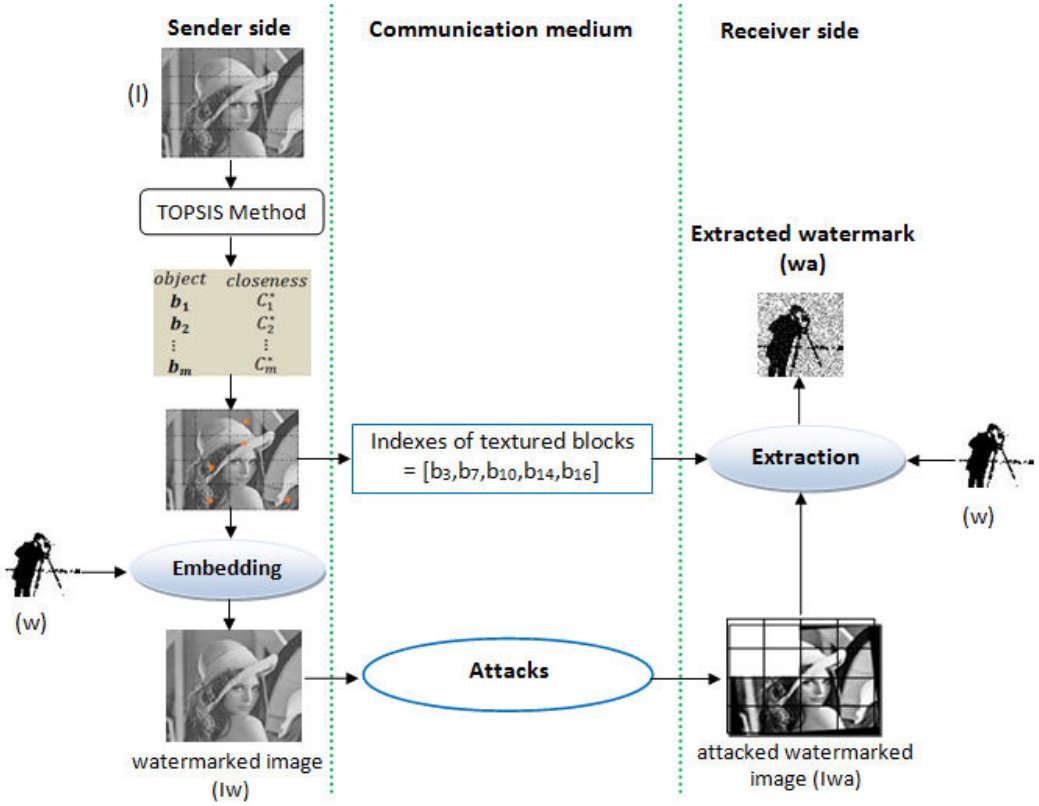


Figure 44: General framework of semi-blind image watermarking approach based on texture analysis using TOPSIS method.

Figure 44 shows that the original image I is partitioned into a set of non-overlapping blocks and the decision matrix is built and processed by TOPSIS method to identify the top 10% of highly textured blocks for embedding watermark. The embedding procedure takes place using linear interpolation and the given result is a watermarked image I_w. The I_w and the indexes of textured blocks are transmitted via communication medium to the receiver side. The receiver extracts the embedded watermark to verify the image origins. The extraction process using inverse form of linear interpolation takes place to extract the

attacked watermark. Measuring the similarity between the original watermark and the extracted one proves image authenticity.

- **Watermark embedding process**

  The watermark is embedded in the selected blocks using linear interpolation technique. This technique is useful because it provides the ability to manage a trade-off between imperceptibility and robustness by selecting proper interpolation factor. Equation (31) presents the linear interpolation technique, and algorithm 11 presents the pseudo-code of the watermark embedding process.

Algorithm 11 The pseudo-code of embedding watermark in semi-blind image watermarking approach based on texture analysis using TOPSIS method.

1: **input:** watermark image w sized $L \times L$, host image I of size $M \times N$ (assuming M and N is multiple of L), the selected textured blocks by TOPSIS method B, and interpolation factor t=0.99
2: partitioning I into $L \times L$, the result is n blocks_I
3: **for** $k \leftarrow 1$ to n **do**
4: **if** $\text{block}_I(k) \in$ the set of textured blocks B, $\text{block}_I(k) \in I$ **then**

$$\text{block}_{Iw}(k) \leftarrow (1 - t) \times w + t \times \text{block}_I(k) \tag{31}$$

5: **end if**
6: **end for**
7: **output:** watermarked image (I_w)

- **Watermark extraction process**

After the embedding process, the obtained watermarked image I_w will be sent to the receiver via public networks and it could be exposed to different kind of attacks. Therefore, the received image is an attacked watermarked image I_{wa} and the extraction process must be applied to prove the origin of image by extracting the set of attacked watermarks w_a from I_{wa}. The inverse form of linear interpolation, presented in equation (32), is applied and the pseudo-code of attacked watermark extraction process is illustrated in algorithm 12.

Algorithm 12 The pseudo-code of extraction watermark in semi-blind image watermarking approach based on texture analysis using TOPSIS method.

1: **input:** attacked watermarked image I_{wa} of size $M \times N$, original watermark image w of size $L \times L$, the selected textured blocks by TOPSIS method B, and interpolation factor t=0.99
2: partitioning I_{wa} into $L \times L$, the result is n blocks_{Iwa}
3: **for** k $\leftarrow$ 1 to n **do**
4: **if** $\text{block}_{Iwa}(k) \in$ the set of textured blocks B **then**

$$w_a \leftarrow \frac{1}{t} \times w - \frac{1-t}{t} \times \text{block}_{Iwa}(k) : t \in]0-1[\tag{32}$$

5: **end if**
6: **end for**
7: **output:** set of attacked watermarks (w_a)

C *Approach 2: Blind image watermarking in spatial domain*

The second image watermarking approach also starts by applying texture analysis phase to identify the top 10% of highly textured blocks for the watermark embedding process. Then, it uses the closeness value of each of the selected blocks to achieve embedding and extraction procedures. As well, it uses the maximum closeness value to define a public key (α) for a blind watermarking. The value of the public key (α) is calculated according to equation (33). The general framework of approach 2 is illustrated in figure 45 and the embedding and extraction procedures are presented below.

$$\alpha \leftarrow \frac{max(closeness)}{100} \times w \tag{33}$$

where w is the original watermark.

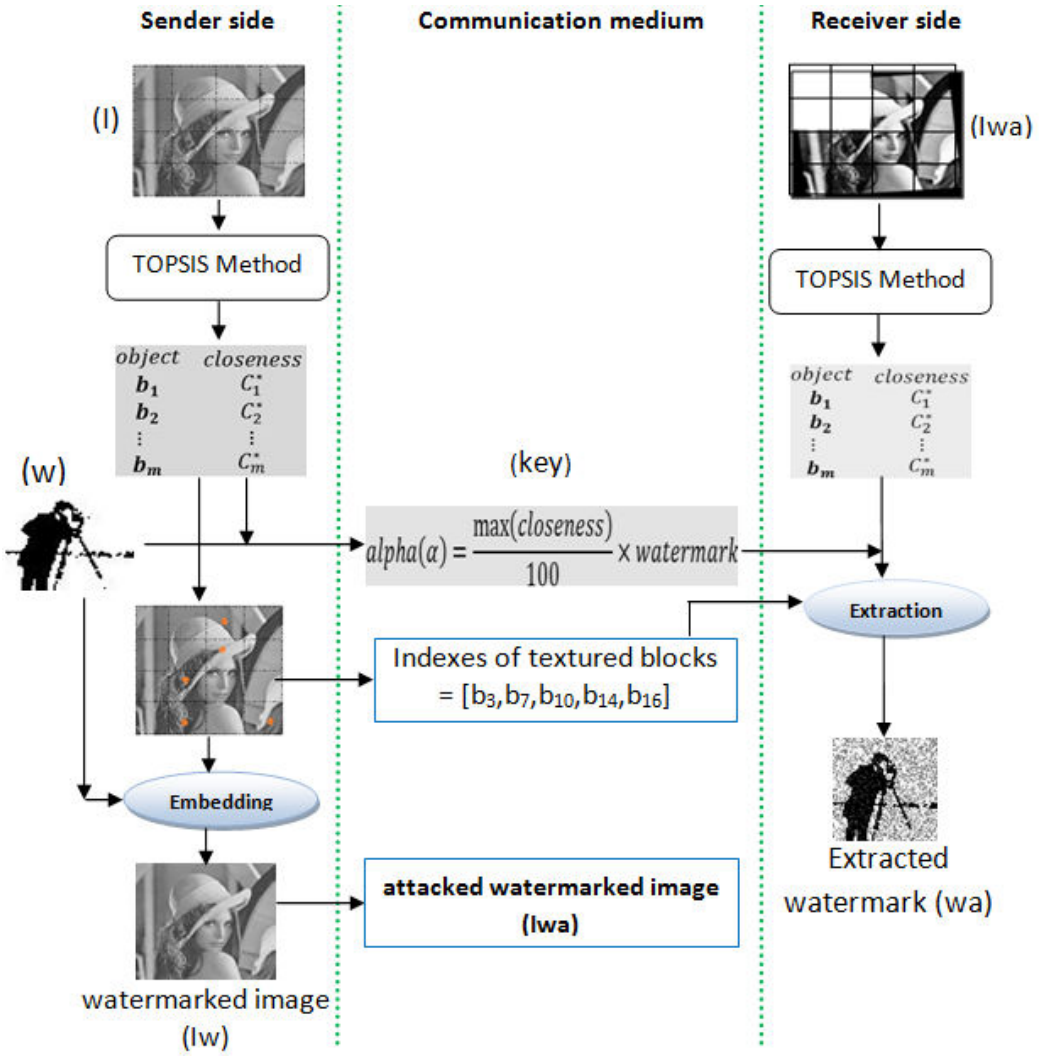


Figure 45: General framework of blind image watermarking approach based on texture analysis using TOPSIS method.

Figure 45 shows that the original image I is partitioned into set of non-overlapping blocks and the decision matrix is built and processed by TOPSIS method to identify the top 10% of highly textured blocks for embedding watermark. The maximum closeness and the original watermark are used to generate the public key (α) and then the embedding procedure takes place using closeness value of each of selected blocks and the original watermark. The result is the watermarked image I_w. I_w, α, and the indexes of textured blocks are transmitted via communication medium to the receiver to extract the embedded watermark.

- **Watermark embedding process**

A new embedding technique is proposed in this approach using the closeness coefficients of the selected textured blocks. Equation (34) presents the embedding equation, and algorithm 13 presents the pseudo-code of the watermark embedding process.

Algorithm 13 The pseudo-code of embedding watermark in blind image watermarking approach based on texture analysis using TOPSIS method.

1: **input:** watermark image w of size $L \times L$, host image I of size $M \times N$ (assuming M and N is multiple of L), the indexes of selected textured blocks B, and the closeness values of B
2: partitioning I into $L \times L$, the result is n blocks_I
3: **for** $s \leftarrow 1$ to n **do**
4: **if** $\text{block}_I(s) \in$ the set of textured blocks B **then**

$$\text{block}_{Iw}(s) \leftarrow \text{block}_I(s) + \frac{closeness(\text{block}_I(s))}{100} \times w \tag{34}$$

5: **end if**
6: **end for**
7: **output:** watermarked image (I_w)

- **Watermark extraction process**

Once watermark embedding is achived, the extraction equation in (35) is applied to extract the watermarks from the attacked watermarked image. Initially, the receiver runs the texture analysis phase to find the closeness values of the attacked textured blocks and the extraction process uses these closeness values and the public key alpha (α) to extract the attacked watermark. The pseudo-code of attacked watermarks extraction process is illustrated in algorithm 14.

Algorithm 14 The pseudo-code of extraction watermark in blind image watermarking approach based on texture analysis using TOPSIS method.

preliminary: defining the set $k=\{k_1,\ldots, k_n\}$ as texture features and defining the weight vector (WV)
input: attacked watermarked image I_{wa} of size $M\times N$, the indexes of selected textured blocks B, and alpha (α)
partitioning I_{wa} into $L\times L$ blocks, results are m $\text{blocks}_{I_{wa}}$, $m=M/L\times N/L$
for each feature k_t, t=1,...,n **do**
    for each $\text{block}_{I_{wa}}$(s), s=1,...,m **do**
        define $x_{s,t}$ score of alternative $block_{I_{wa}}(s)$ with respect to criterion k_t
    end for
end for
constructing the decision matrix $X=(x_{s,t})_{m\times n}$
applying TOPSIS method to find the closeness values of all partitioned blocks
for each $\text{block}_{I_{wa}}$(s), s=1,...,m **do**
    if $\text{block}_{I_{wa}}(s) \in$ the set of textured blocks B **then**

$$w_a \leftarrow \frac{100}{\text{closeness}(\text{block}_{I_{wa}}(s))} \times \alpha \tag{35}$$

    end if
end for
output: set of attacked watermarks (w_a)

As illustrated in equation (35), the extraction procedure is blind. Indeed, the receiver uses only the public key alpha (α) to extract the attacked watermarks without any knowledge about the original watermark or the original image. As well, the public key alpha (α) used in the extraction process is not fixed. For any host image, a different key is generated depending on the host image nature. This increases the robustness of the watermarking process against brute-force attacks.

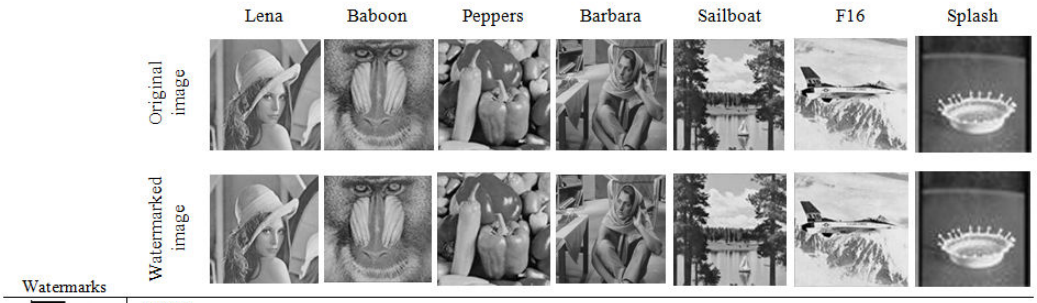
6.4.3 *Experiment Results*

This section presents the experiment results of the proposed approaches on set of gray-scale images sized 512×512 using 64×64 gray-scale image as watermark. The imperceptibility, robustness, embedding rate and execution time results are discussed in the following.

A *Watermark imperceptibility*

Figures 46 and 47 present the imperceptibility results of the proposed approaches 1 and 2 on set of host gray-scale images that are collected from CVG-UGR

database[1]. The PSNR and the MSSIM are computed for each original image with two used watermarks.



Watermarks		Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
(1)	PSNR (dB)	56.03	56.37	55.13	56.04	54.37	54.86	55.74
	mSSIM	0.98	0.99	0.99	0.99	0.99	0.99	0.98
(2)	PSNR (dB)	56.89	56.49	55.03	56.71	55.60	57.38	55.47
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.99

Figure 46: Imperceptibility results of semi-blind image watermarking approach based on texture analysis using TOPSIS method on set of gray-scale images.

The results in figure 46 show that the proposed approach 1 achieves a good level of imperceptibility. The PSNR ranges 54.37-57.38 dB, while the MSSIM ranges 0.98-0.99 in all tested images.

Watermarks		Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
(1)	PSNR (dB)	56.63	55.13	55.33	56.56	55.36	55.13	56.21
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.99
(2)	PSNR (dB)	54.95	53.80	53.88	54.89	53.97	53.86	54.75
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.99

Figure 47: Imperceptibility results of blind image watermarking approach based on texture analysis using TOPSIS method on set of gray-scale images.

The results in figure 47 show that the second proposed approach achieves a good level of imperceptibility. The PSNR ranges 53.80-56.63 dB, while the MSSIM reaches 0.99 in all tested images.

1 CVG-UGR database, http://decsai.ugr.es/cvg/dbimagenes/

B *Watermarking robustness*

To evaluate the robustness of the proposed approaches, experiments are conducted with a particular focus on noise corruption, filtering, image compression, and geometric correction. The consequence of applying various attacks on gray-scale Lena image is illustrated in figure 48. All watermarked images are exposed to a variety of geometric and non-geometric attacks using StirMark Benchmark v.4 [80] and Matlab (v.R2016a).

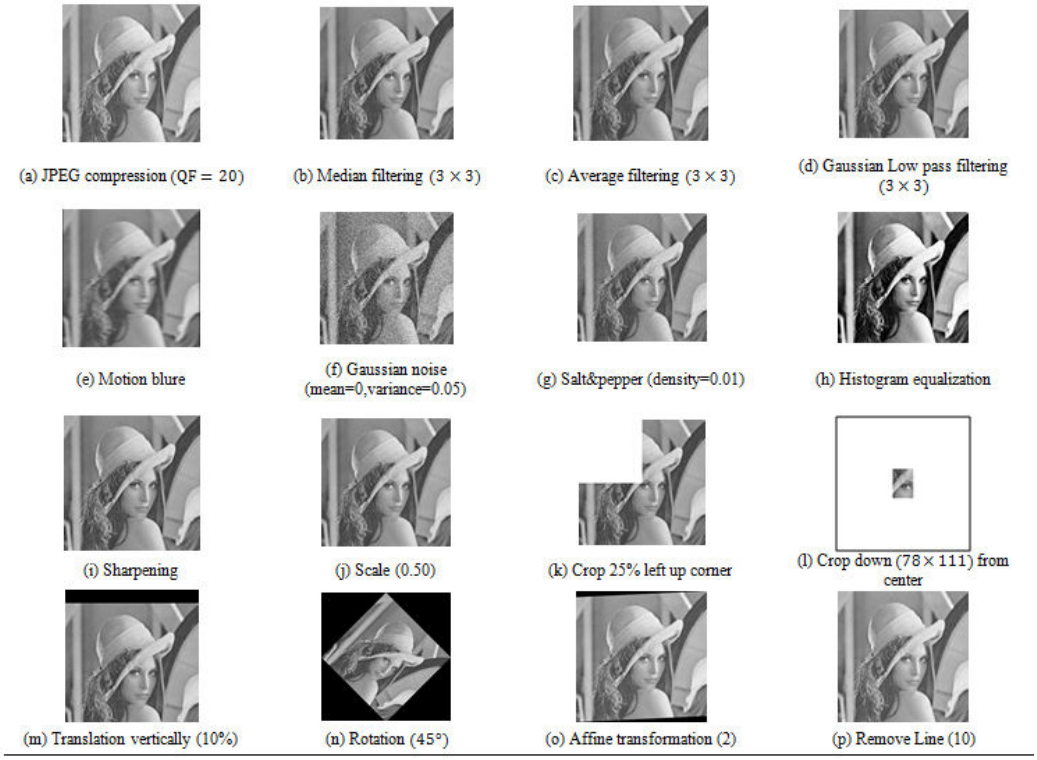


Figure 48: Some attacks on watermarked gray-scale Lena image.

In all experiments using the two watermarks logos, the NC ranges 0.99-1. This means that the proposed approaches are able to recover the embedded watermark from attacked watermarked image with high similarity. The original watermark and the extracted ones are visually absolutely identical.

Tables 36 and 37 show BER results after testing the first approach on the host images using watermarks logo 1 and logo 2, respectively. While, tables 38 and 39 show BER results after applying the second approach on the host images using watermarks logo 1 and logo 2, respectively.

	BER for Watermark Logo 1						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	5.5	7.4	7.2	6.9	6.9	6.8	7.8
Median filtering (3×3)	6.9	7.5	7.4	7.1	6.2	6.8	7.6
Average filtering (3×3)	6.9	7.5	7.4	7.1	6.3	6.8	7.6
Gaussian low pass filtering (3×3)	6.9	7.5	7.4	7.1	6.2	6.8	7.6
Motion Blure	6.9	7.5	7.4	7.1	6.7	6.8	7.6
Gaussian noise (mean=0,variance=0.05)	6.5	5.9	5.4	6.0	6.7	7.9	4.9
Salt&Pepper noise (noise density=0.01)	6.9	7.5	7.4	7.1	6.2	6.8	7.4
Histogram equalization	6.1	2.8	5.5	6.6	5.9	7.0	6.5
Sharpening	6.9	7.5	7.4	7.1	6.1	6.8	7.6
Scaling (0.5) 512×512 → 256×256	6.9	7.5	7.4	7.1	6.3	6.8	7.6
Cropping left up corner (25%)	7.1	7.5	7.4	7.3	6.2	6.8	7.6
Cropping down from center (78×111)	12.2	12.2	9.9	9.1	12.2	12.2	9.5
Translation vertically (10%)	1.4	7.2	7.0	6.8	1.5	1.4	7.5
Rotation(45°)	0	0	0	0	0	0	0
Affine transformation (2)	4.0	4.8	7.1	6.9	4.4	5.4	7.8
RML (10)	5.6	7.1	7.2	6.9	6.9	6.9	7.8

Table 36: BER results of semi-blind image watermarking approach based on texture analysis using TOPSIS method on set of natural gray-scale images using watermark logo 1 under various attacks.

In table 36, the BER for all images did not exceed 8% except in case of cropping down (78×111) attack, where the BER ranges 9.1-12.2%. The lower robustness in case of cropping down attack for all images is explained due to loss of large amount of pixels by cropping. The first approach achieves zero BER against rotation attack for all images, this indicates that some blocks where not affected by the rotation attack. As well as, the first approach introduces lower BER against translation vertically attack in case of Lena, Sailboat, and F16 images. The BER did not exceed 1.5%.

	BER for Watermark Logo 2						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	3.8	4.0	3.9	3.7	3.8	3.8	4.0
Median filtering (3×3)	3.8	4.1	4.1	3.1	3.6	3.8	3.9
Average filtering (3×3)	3.8	4.1	4.1	3.3	3.7	3.8	3.9
Gaussian low pass filtering (3×3)	3.8	4.1	4.1	3.2	3.7	3.8	3.9
Motion Blure	3.8	4.1	4.1	3.8	3.7	3.7	4.0
Gaussian noise (mean=0,variance=0.05)	3.4	3.1	2.7	3.1	3.7	4.2	2.4
Salt&Pepper noise (noise density=0.01)	3.8	4.1	4.1	3.1	3.6	3.7	3.8
Histogram equalization	3.7	1.2	2.6	2.6	3.5	3.6	3.1
Sharpening	3.8	4.1	4.1	3.0	3.5	3.7	3.9
Scaling (0.5) 512×512 → 256×256	3.8	4.1	4.1	3.2	3.7	3.7	3.9
Cropping left up corner (25%)	3.8	4.1	4.1	3.4	3.6	3.7	3.9
Cropping down from center (78×111)	6.6	6.6	5.7	5.5	6.6	6.6	4.3
Translation vertically (10%)	0.7	3.9	3.3	3.6	0.6	0.6	4.1
Rotation(45°)	0	0	0	0	0	0	0
Affine transformation (2)	3.1	2.3	3.8	3.7	2.2	3.1	4.0
RML (10)	3.8	3.8	3.8	3.7	3.7	3.7	4.0

Table 37: BER results of semi-blind image watermarking approach based on texture analysis using TOPSIS method on set of natural gray-scale images using watermark logo 2 under various attacks.

In table 37, the BER for all images did not exceed 5% except in case of cropping down (78×111) attack, the BER reaches 6.6%. Similarly to the first approach, the second approach achieves zero BER against rotation attack for all images and introduces lower BER against translation vertically attack in case of Lena, Sailboat, and F16 images. The BER did not exceed 0.7%.

	BER for Watermark Logo 1						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	0	0	0	0	0	0	0
Median filtering (3×3)	0	0	0	0	0	1.08	0
Average filtering (3×3)	0	0.19	0	0	0.13	0.20	0.02
Gaussian low pass filtering (3×3)	0	0	0	0	0.19	0.57	0.006
Motion Blure	0	1.38	0	0	0	0	0
Gaussian noise (mean=0,variance=0.05)	0	1.80	0	0	0	0	0.10
Salt&Pepper noise (noise density=0.01)	0	0.027	0.11	0	0.048	0.13	0
Histogram equalization	0	1.83	0	0	0	1.37	0
Sharpening	0	0	0	0	0	0	0
Scaling (0.5) 512×512 → 256×256	0	0	0	0	0	0	0
Cropping left up corner (25%)	0.006	2.03	1.36	1.80	0.01	0.02	0.57
Cropping down from center (78×111)	2.3	2.6	2.31	2.26	2.1	2.2	2.10
Translation vertically (10%)	0.115	1.38	0	0	1.8	0.20	0.10
Rotation(45°)	0.024	2.09	1.38	0.73	0.73	1.69	0.26
Affine transformation (2)	0	2.14	0	0	0	0.19	0.02
RML (10)	0	0	0	0	0	0	0

Table 38: BER results of blind image watermarking approach based on texture analysis using TOPSIS method on set of natural gray-scale images using watermark logo 1 under various attacks.

In table 38, the BER for all images are close to zero and did not exceed 3% against all attacks. The second approach achieves zero BER against JPEG compression, filtering, adding noise, sharpening, scaling, and RML attacks.

	BER for Watermark Logo 2						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	0	0	0	0	0	0.003	0
Median filtering (3×3)	0	0	0	0	0	0.62	0
Average filtering (3×3)	0	0.05	0	0	0.07	0.09	0.003
Gaussian low pass filtering (3×3)	0	0.003	0	0	0.07	0.20	0.003
Motion Blure	0	0.80	0	0	0	0	0
Gaussian noise (mean=0,variance=0.05)	0	1.19	0	0	0	0	0.051
Salt&Pepper noise (noise density=0.01)	0	0.25	0.12	0	0.25	0.33	0
Histogram equalization	0	1.1	0	0	0	0.83	0
Sharpening	0	0.01	0	0	0	0	0
Scaling (0.5) 512×512 → 256×256	0	0	0	0	0	0	0
Cropping left up corner (25%)	0	1.3	0.81	1.17	0.003	0.003	0.14
Cropping down from center (78×111)	66.3	66.3	1.57	1.51	66.3	66.3	1.42
Translation vertically (10%)	0.052	0.81	0.003	0	1.17	0.12	0.09
Rotation(45°)	0.003	1.41	0.81	0.33	0.33	1.1	0.12
Affine transformation (2)	0	1.44	0	0	0	0.08	0.003
RML (10)	0	0	0	0.01	0	0	0

Table 39: BER results of blind image watermarking approach based on texture analysis using TOPSIS method on set of natural gray-scale images using watermark logo 2 under various attacks.

As well as, the BER results in table 39 show that the BER for all images did not exceed 2% against all attacks. The BER results of second approach using watermark logo 2 are more interesting than the BER results of second approach using watermark logo 1. Logo 2 has less information than logo 1 and it is recovered from attacked images with less error rate.

From the mentioned BER results in tables 36, 37, 38, and 39 it could be concluded that the second approach achieves higher robustness than the first approach. The extraction procedure in the second approach is more efficient to recover the watermark from attacked watermarked images than the first approach. This result is based on the closeness value of textured blocks in the attacked watermarked image, which is ranged between 0-1, and on the key (α). Through experiments, the closeness values of textured blocks have not significantly changed over the original closeness. This could be explained due to less effect of different attacks on highly textured blocks.

In the first approach, the extraction procedure depends on the pixels values of the textured blocks in the attacked watermarked image. From experiments, the pixels values of these blocks have significantly changed even with a slight attack.

c *Embedding rate*

In the proposed approach, the watermark of size 64×64 8-bits gray-scale image is embedded in many locations of 512×512 8-bits gray-scale image. The minimum embedding rate is obtained when only one location is used for embedding watermark, while the maximum embedding rate is obtained when all locations are used for embedding watermark. The minimum number of location (of size 64×64) is 1, and the maximum number of locations (each of size 64×64) is equal 64.

In the proposed approaches, 10% (approximately 6 blocks) of all partitioned blocks are embedded with watermark. Hence, the minimum embedding rate ER is equal $((64\times64\times8)/(512\times512))\times6 = 32768/262144\times6 = 0.75$ (BPP). While, the maximum embedding rate ER is equal $((64\times64\times8\times64)/(512\times512)) = 2097152/262144 = 8$ (BPP).

d *Execution time*

In the experiments, HP machine 3.4 GHz Intel(R)/core(TM) i7 CPU with 8.0 GB RAM is used as a computing platform. The overall execution time on any host images and under various attacks using the first approach is equal to 8 seconds and using the second approach is equal to 10 seconds. The extraction process requires a little bit more execution time than the embedding process due to writing many watermarks images on a specific file.

6.4.4 *Computational complexity*

The efficiency of using TOPSIS method in designing image watermarking is measured from the computational complexity.

In TOPSIS method, the size of decision matrix is $M\times N$. The complexity value resulting from the calculation of score values normalization and weighting is $O(M\times N)$. The complexity of calculation of positive and negative ideal solutions is $O(M\times N)$, and the complexity of calculation of geometric distance to ideal solutions is $O(Mlog(N))$. The algorithmic complexity of calculation of the closeness values is $O(M)$ and that of the ranking of results is $O(Mlog(M))$. Therefore, the total time complexity of the proposed approach is $O(M\times N)$.

6.5 IMAGE WATERMARKING APPROACH BASED ON TEXTURE ANALYSIS USING FORMAL CONCEPT ANALYSIS

In this section, an image watermarking approach based on texture analysis using Formal Concept Analysis (FCA) method is presented. FCA is used to find a meaningful knowledge that helps to embed watermark efficiently, to obtain high imperceptibility and robustness. The formal concepts resulting from the application of the FCA method are exploited to extract highly textured blocks in the targeted image that are convenient with HVS and more preferable to embed the watermark with least image quality distortion and high robustness.

This section starts by presenting the principle of FCA method in subsection 6.5.1 and then the proposed image watermarking approach based on texture analysis using FCA is presented in subsection 6.5.2. The experiment results on set of gray-scale images in terms of imperceptibility, robustness, embedding rate and execution time are introduced in subsection 6.5.3. Finally, the computational complexity is presented in subsection 6.5.4.

6.5.1 *Principle of Formal Concept Analysis*

FCA is a technique used to investigate and analyze image characteristics, in order to find meaningful and comprehensive knowledge [81]. It was developed in the field of data mining, knowledge representation, and knowledge discovery in databases [5].

FCA manipulates a data matrix, which combines set of objects and set of attributes, to find the set of all objects that share a common subset of attributes and the set of all attributes that are shared by one of the objects.

FCA theory relies on different notions. The basic notion in FCA is a formal context defined as a triple $\beta=(G,M,I)$, where G is a set of formal objects, M is a set of formal attributes, and I is a binary relation called incidence such as $I \subseteq G \times M$. The notation gIm stands for $(g,m) \in I$, which is read as: the object g has the attribute m [81].

A pair (X,Y) is a Formal Concept (FC) of (G,M,I) if and only if: $X \subseteq G$ (X is a subset of objects of G), $Y \subseteq M$ (Y is a subset of attributes of M), $X'=Y$ (X' is the set of attributes in M such that all objects in X have all attributes in X'), and $X=Y'$ (Y' is the set of objects in G such that all attributes in Y fall under all objects in Y'). X and Y are respectively called the Extent and the Intent of the FC.

6.5.2 *Proposed Approach*

The proposed approach proposes a semi-blind image watermarking based on texture analysis using FCA method. The FCA is used to deduce the texture features of targeted image (based on DC, skewness, kurtosis, and entropy), and then to discover a meaningful knowledge that helps to identify highly textured blocks for embedding the watermark. The principle of embedding watermark in highly textured regions is correlated with HVS principles, where the attacker eye becomes less sensitive to any change in highly textured regions rather than smooth regions [127]. This, in fact, may lead to preserve perceptual image quality and to achieve high robustness. The pseudo-code of the proposed approach is presented in algorithm 15.

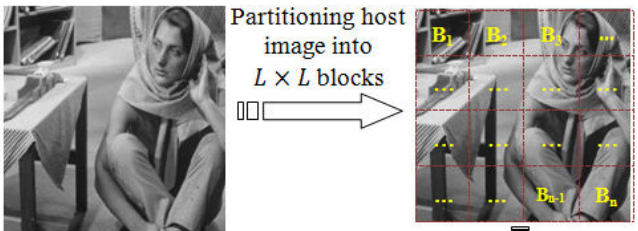
Algorithm 15 The pseudo-code of image watermarking approach based on texture analysis using FCA method

1: **preliminary:** defining the set x={x_1, x_2,..., x_n} as texture features
2: **input:** watermark image w sized $L\times L$ and host image I sized $M\times N$ (assuming M and N is multiple of L)
3: partitioning host image I into $L\times L$ blocks, results by T blocks, T=M/L×N/L and computing the corresponding features, where T={T_1,T_2,...,$T_{(M/L\times N/L)}$}, is the set of transaction matrix and each transaction T_i={x_1,x_2,...,x_n} is a set of items x:$T_i \subseteq x$
4: building the transactions matrix and Boolean matrix
5: applying FCA to extract the set of formal concepts
6: computing the frequency of each object in formal concepts, as well as computing the mean and the median of all frequencies to assign maximum one as a threshold (T)
7: identifying a set of highly textured blocks based on (T)
8: embedding watermark (I,w)
9: extracting watermark (I_{wa},w)

According to algorithm 15, the proposed approach operates mainly through six phases that are illustrated in the following subsections.

A *Building the transactions and Boolean matrices*

In this phase, the targeted image is partitioned into $L\times L$ non-overlapping blocks and the values of the texture features for every block are computed using the equations presented in (7), (19), (20), and (21) to build the transactions matrix. Subsequently, the transactions matrix is transformed into a Boolean matrix based on the thresholds that are presented in algorithms 6, 7, 8, and 9. Figure 49 presents the structure of this step.



(Transactions Matrix)

Transaction ID	itemsets			
	DC	skewness	kurtosis	entropy
B_1	6275.0	0.295	-2.99	7.34
B_2	3661.9	1.491	-2.96	6.15
B_3	7983.5	-0.93	3.02	6.71
...	...	...	...	...
$B_n, n = \frac{M \times N}{L \times L}$	4756.5	0.486	-2.98	6.77

Thresholds

$\mathbf{Avg_{DC}}$= 7540.2, $\mathbf{Avg_{entropy}}$= 6.58, $\mathbf{Avg_{kurtosis}}$= 2.58

$\mathbf{Avg_{negativeSkewness}}$= -2.184, $\mathbf{Avg_{positiveSkewness}}$=1.149

(Boolean Matrix)

Transaction ID	itemsets			
	DC	skewness	kurtosis	entropy
B_1	0	0	1	1
B_2	0	1	1	0
B_3	1	1	0	1
...	...	...	...	...
$B_n, n = \frac{M \times N}{L \times L}$	0	0	1	1

Figure 49: Structure of transactions and Boolean matrices.

B *Applying* FCA *to extract the formal concepts*

In this phase, FCA processes the Boolean matrix to extract the set of formal concepts. The resulting formal concepts present the relationships between the objects (blocks) and the attributes (texture features). As example, figure 50 shows a structure of formal concepts for a given Boolean matrix in (a), which consists of eight objects and four attributes. (b) presents the concept lattice for 6 formal concepts. Table 40 presents the 6 formal concepts that combines set of objects as Extent and set of attributes as Intent.

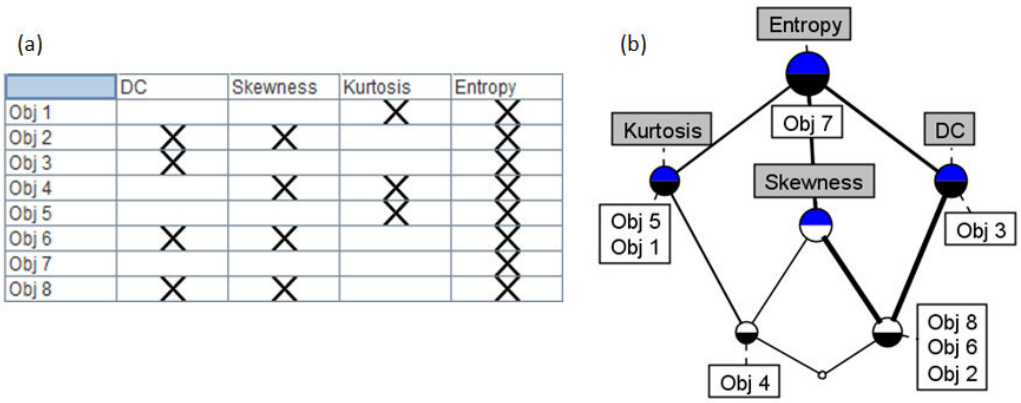


Figure 50: Structure of formal concepts.

Formal Concept no.	Extent	Intent
1	$\{obj_4\}$	{Skewness, Kurtosis, Entropy }
2	$\{obj_2, obj_6, obj_8\}$	{DC, Skewness, Entropy}
3	$\{obj_1, obj_4, obj_5\}$	{Kurtosis, Entropy }
4	$\{obj_2, obj_4, obj_6, obj_8\}$	{Skewness, Entropy }
5	$\{obj_2, obj_3, obj_6, obj_8\}$	{DC, Entropy}
6	$\{obj_1, obj_2, obj_3, obj_4, obj_5, obj_6, obj_7, obj_8\}$	{Entropy }

Table 40: Six formal concepts of a given Boolean matrix in figure 50 (a).

c *Computing the frequency of each object in the formal concepts and identifying a set of highly textured blocks based on threshold (T)*

The frequency of each object through all formal concepts is computed, then the average and the median values of these frequencies are computed. The maximum between the average and median defines the threshold (T).

Any object (block) whose frequency is greater than the threshold (T) is considered highly textured. An object whose frequency is high in all formal concepts has a high ratio of attributes falling under it. Table 41 presents this step.

Object no.	Frequency
Obj_1	2
Obj_2	4
Obj_3	2
Obj_4	4
Obj_5	2
Obj_6	4
Obj_7	1
Obj_8	4
Average of frequencies	3.83
Median of frequencies	3
Threshold (T)	3.83

Table 41: Frequency of each object in the formal concepts and the identified threshold.

D *Watermark Embedding Process*

All blocks identified as highly textured are considered in the embedding process. This process is achieved by applying the linear interpolation technique presented in equation (31) (see subsection 6.4.2). Algorithm 16 illustrates the watermark embedding process.

Algorithm 16 The pseudo-code of embedding watermark in image watermarking approach based on texture analysis using FCA

1: **Input:** watermark image w sized $L \times L$, host image I of size $M \times N$ (assuming M and N is multiple of L), the selected textured blocks by FCA method B, and interpolation factor t=0.99
2: partitioning I into $L \times L$, the result is n blocks_I
3: **for** k $\leftarrow$ 1 to n **do**
4: **if** $\text{block}_I(k) \in$ the set of textured blocks B, $\text{block}_I(k) \in I$ **then**
5: applying equation (31)
6: **end if**
7: **end for**
8: **output:** watermarked image (I_w)

E *Watermark extraction process*

The resulting watermarked image I_w, which holds the watermark data, is subject to channel errors and attacks due to the transmission across a public network. The extraction process in the receiver side is achieved to verify the authenticity of transmitted images. Algorithm 17 presents the watermark extraction process

using the inverse form of linear interpolation technique presented in equation (32) (see subsection 6.4.2). It uses the same interpolation factor t as that used in the embedding process.

Algorithm 17 The pseudo-code of extraction of watermark in image watermarking approach based on texture analysis using FCA

1: **input:** attacked watermarked image I_{wa} of size $M \times N$, watermark image w of size $L \times L$, the selected textured blocks by FCA method B, and interpolation factor t=0.99
2: partitioning I_{wa} into $L \times L$, the result is n blocks_{Iwa}
3: **for** k $\leftarrow$ 1 to n **do**
4: **if** block_{Iwa}(k) $\in$ the set of textured blocks B **then**
5: applying equation (32)
6: **end if**
7: **end for**
8: **output:** set of attacked watermarks (w_a)

6.5.3 *Experiment Results*

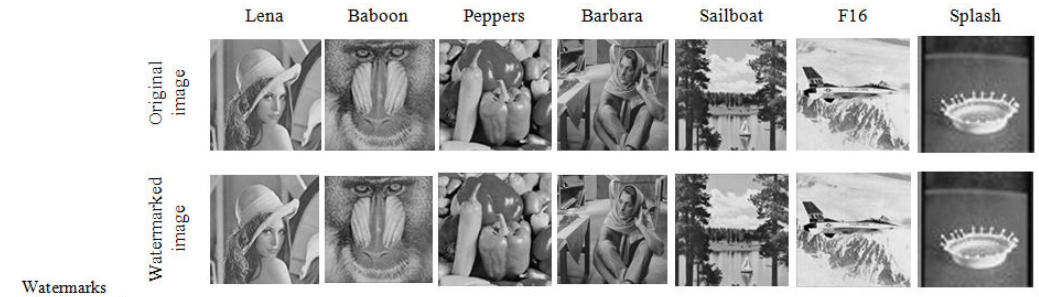
This section presents the experiment results of the proposed approach on set of natural gray-scale images of size 512×512 and using 64×64 gray-scale image as watermark.

Initially, the targeted image is partitioned into 64×64 non-overlapping blocks, and the texture features for each block are analyzed to build the Boolean matrix. The Boolean matrix is used as input of Concept Explorer (ConExp) tool v1.3 [129], which provides basic functionality needed to extract the set of formal concepts. The high frequency objects (blocks), which frequently appear with most formal concepts, express the most textured blocks within the targeted image. These textured blocks are used as input in the watermark embedding process. The performance of the proposed watermarking approach is evaluated in terms of imperceptibility, robustness, embedding rate and execution time.

A *Watermark imperceptibility*

Figure 51 presents the imperceptibility results of the proposed approach on set of host gray-scale images that are collected from CVG-UGR database[2]. The PSNR and the MSSIM are computed for each original image by considering its watermarking with two watermarks.

2 CVG-UGR database, http://decsai.ugr.es/cvg/dbimagenes/



Watermarks		Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
 (1)	PSNR (dB)	49.20	49.24	48.68	48.73	47.76	48.04	48.26
	mSSIM	0.97	0.99	0.98	0.99	0.98	0.97	0.94
 (2)	PSNR (dB)	49.74	49.46	48.52	48.22	47.82	49.80	47.98
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.97

Figure 51: Imperceptibility results of semi-blind image watermarking approach based on texture analysis using FCA method on set of gray-scale images.

The results in figure 51 show that the proposed approach achieves a good level of imperceptibility. The PSNR ranges 47.7-49.8 dB, while the MSSIM ranges 0.94-0.99 in all tested images.

B *Watermarking robustness*

To evaluate the robustness of the proposed approach, the experiments are conducted with a particular focus on noise corruption, filtering, image compression and geometric correction. All watermarked images are exposed to a variety of geometric and non-geometric attacks using StirMark Benchmark v.4 [80] and Matlab (v.R2016a).

In all experiments and using the two watermarks logos, the NC ranges 0.99-1. This means that the proposed approach is able to recover the embedded watermark from attacked watermarked image with high similarity.

Table 42 shows BER results for host gray-scale images using watermark logo 1 and under various attacks. As well, table 43 presents BER results for host gray-scale images using watermark logo 2 under also various attacks.

	BER for Watermark Logo 1						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	6.8	7.1	3.6	5.3	4.9	6.1	2.3
Median filtering (3×3)	6.8	6.9	3.1	4.5	3.0	6.0	0.5
Average filtering (3×3)	6.8	7.0	3.1	4.6	3.0	6.1	0.5
Gaussian low pass filtering (3×3)	6.8	6.9	3.1	4.6	3.0	6.1	0.5
Motion Blure	6.8	7.2	3.3	5.1	3.4	6.1	0.5
Gaussian noise (mean=0,variance=0.05)	5.6	5.3	4.1	4.5	3.9	6.5	2.7
Salt&Pepper noise (noise density=0.01)	6.8	6.8	3.1	4.4	3.1	6.0	0.6
Histogram equalization	2.3	2.1	1.9	3.2	2.2	2.2	0
Sharpening	6.8	6.8	3.1	4.3	2.9	5.9	0.5
Scaling (0.5) 512×512 → 256×256	6.8	6.9	3.1	4.6	3.0	6.0	0.5
Cropping left up corner (25%)	6.8	7.2	3.1	4.8	3.0	6.0	0.5
Cropping down from center (78×111)	9.2	9.5	9.3	8.3	8.5	9.1	9.5
Translation vertically (10%)	1.5	1.6	1.5	1.5	1.1	1.4	0.02
Rotation(45°)	0	0	0	0	0	0	0
Affine transformation (2)	5.0	4.9	2.7	3.9	4.6	4.4	2.4
RML (10)	6.8	7.0	3.5	5.5	4.9	6.0	2.5

Table 42: BER results of semi-blind image watermarking approach based on texture analysis using FCA method on set of natural gray-scale images using watermark logo 1 under various attacks.

In table 42, the BER for all images did not exceed 9.5%. The lowest BER is obtained against histogram equalization, translation vertically (10%), and rotation(45°) attacks; the BER did not exceed 3.2%. In case of cropping down (78×111) attack the proposed approach achieves the lowest robustness comparing with other attacks; the BER reaches 9.5%.

	BER for Watermark Logo 2						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	3.8	3.8	1.7	2.9	2.4	1.4	2.2
Median filtering (3×3)	3.8	3.5	1.5	1.9	1.4	2.7	0.02
Average filtering (3×3)	3.8	3.6	1.5	1.9	1.4	2.7	0.03
Gaussian low pass filtering (3×3)	3.8	3.5	1.5	1.9	1.4	2.7	0.03
Motion Blure	3.8	3.7	1.5	2.2	1.5	2.8	0.03
Gaussian noise (mean=0,variance=0.05)	2.7	2.7	1.9	2.1	1.9	3.0	1.5
Salt&Pepper noise (noise density=0.01)	3.7	3.5	1.5	1.8	1.4	2.7	0.34
Histogram equalization	0.12	1.1	1.1	0.8	0.9	0.7	0
Sharpening	3.7	3.5	1.5	1.6	1.4	2.7	0.02
Scaling (0.5) 512×512 → 256×256	3.8	3.5	1.5	1.9	1.4	2.7	0.03
Cropping left up corner (25%)	3.8	3.9	1.5	1.8	1.4	2.7	0.02
Cropping down from center (78×111)	4.3	4.3	5.6	4.2	3.2	4.1	4.3
Translation vertically (10%)	0.67	0.8	0.7	0.8	0.5	0.68	0.01
Rotation(45°)	0	0	0	0	0	0	0
Affine transformation (2)	2.9	2.8	1.8	1.8	2.5	1.2	2.1
RML (10)	3.79	3.8	1.7	1.7	2.4	1.3	2.2

Table 43: BER results of semi-blind image watermarking approach based on texture analysis using FCA method on set of natural gray-scale images using watermark logo 2 under various attacks.

As well, the BER results in table 43 show that the BER for all images did not exceed 6%. Similarly to the BER results in table 42, the proposed approach achieves higher robustness against histogram equalization, translation vertically (10%), and rotation(45°) attacks. The proposed approach achieves the lowest robustness against cropping down (78×111) attack.

However, the BER results in table 43 are lower than the BER results in table 42. This is due to the difference in data amount between logo 1 and logo 2.

c *Embedding rate*

In the proposed approach, the watermark of size 64×64 8-bits gray-scale image is embedded in many locations of 512×512 8-bits gray-scale image. The minimum embedding rate is obtained when only one location is used for embedding watermark, while the maximum embedding rate is obtained when all locations are used for embedding watermark image. The minimum number of location (of

size 64×64) is 1, and the maximum number of locations (each of size 64×64) is equal to 64.

Through experiments on the proposed approach, at least 30% (approximately 19 blocks) of all partitioned blocks are included in the embedding watermark process. Hence, the embedding rate ER is equal ((64×64 × 8 × 19)/(512×512))= 622592/262144= 2.375 (BPP). While, the maximum embedding rate ER is equal ((64×64 × 8 × 64)/(512×512))= 2097152/262144= 8 (BPP).

D *Execution time*

In the experiments, HP machine 3.4 GHz Intel(R)/core(TM) i7 CPU with 8.0 GB RAM is used as computing platform. The overall execution time on any host images under various attacks using the proposed approach is equal to 15 seconds. The extraction process requires a little bit more execution time than the embedding process due to writing of many watermarks images on a specific file.

6.5.4 *Computational complexity*

The efficiency of using FCA method in designing image watermarking is measured from the computational complexity.

In FCA method, the size of host image is $M \times N$. The complexity of partitioning the host image is $O(M \times N)$ and the complexity value resulting from the calculation of transaction and Boolean matrices is $O(M \times d)$, where d is the number of features. The complexity of applying FCA to extract the formal concepts is $O(M \times d \times 2^k)$, where $k=min(M,d)$ and 2^k is the maximum number of formal concepts of a given Boolean matrix. The complexity of calculation of the frequency of each object is $O(M \times 2^k)$. Therefore, the total time complexity of the proposed approach is $O((M \times N) \times d \times 2^k)$.

6.6 IMAGE WATERMARKING APPROACH BASED ON TEXTURE ANALYSIS AND USING FREQUENT PATTERN MINING

This section explore the use of Frequent Pattern Mining (FPM) method to achieve the image authentication based on texture analysis. The proposed approach exploits some texture features to extract the maximum frequent patterns in the image's data, that satisfy the minimum support. The maximal relevant patterns are exploited to infer knowledge about textured blocks and smooth blocks within the host image. The textured blocks are convenient with HVS and more preferable to embed the watermark with high imperceptibility and robustness.

This section starts by introducing the principles of frequent pattern mining and Apriori algorithm in subsections 6.6.1 and 6.6.2, respectively. Then, the proposed semi-blind image watermarking approach based on texture analysis using FPM is presented in subsection 6.6.3. The experiment results on set of gray-scale images in terms of imperceptibility, robustness, embedding rate and execution time are introduced in subsection 6.6.4. This chapter ends by the presentation of the computational complexity in subsection 6.6.5.

6.6.1 *Principle of Frequent Patterns Mining*

Frequent pattern mining is one of the most important search issues in computational and algorithmic development. It deals with finding the maximal relevant items that are frequently occurring together within a transaction database. One of the popular examples that uses the frequent pattern mining is the basket data analysis, where the mining method is normally used to analyze the regularities of shopping behavior of the customers and then to find sets of relevant products that are often purchased together. The extracted frequent patterns may then be expressed as an association rule, which has a valuable role to improve the arrangement of products in the shelves, and helps decision makers in advantageous actions regarding shelf stoking or any recommendations to add other products [4].

Different frameworks for frequent pattern mining problem have been proposed such as constraint-based mining, where an item-set must satisfy a set of the user-defined constraints [85], redundancy-aware top-k mining, where top-k patterns with similar or redundant patterns are excluded [125], and the support-based framework [109]. The most common framework is the support-based framework, where an item-set is considered frequently if satisfying the minimum support [4]. With note that the support of item-set is defined as a fraction of how frequently the item-set appears over all transaction.

Basic notions of frequent item set mining are denoted below:

- Let $I=\{i_1,i_2,...,i_n\}$, represent a set of items, where the items depend on the processed application. In the image-mining, the items may represent set of features, regions or other attributes of the image. Any subset $i \in I$, is called an item-set.
- Let $T=\{t_1,t_2,...,t_n\}$, be a transaction database. $\forall\, t_x: 1 \leqslant x \leqslant n$, $t_x \subseteq I$.

A pattern P is defined as frequent pattern, if it satisfies the minimum support. Many techniques are developed in literature to solve the support based frequent pattern mining such as Apriori, Eclat, and FP-growth algorithms [4]. Each of these techniques has some advantages over the others. Regardless this issue, the proposed approach is based on the Apriori algorithm, because it is practical with large transactions and it is easy to implement [57]. The proposed approach is also based on support parameter to extract the maximal pattern via the Apriori algorithm. Using support parameter in the proposed approach is an arbitrary choice, but many literatures proved that using the support parameter was a good indicator of how frequently pattern appears in the transaction database, and it was useful to prune irrelevant patterns [4].

6.6.2 *Principle of Apriori Algorithm*

Apriori algorithm is one of the well-known algorithms for mining frequent item-sets in a database, where the most relevant frequent pattern is used to generate association rules. It is a simple search method that requires less computation time than sequential analysis to mine frequent itemsets [63]; it does not require any additional parameter except the minimum support [24].

Apriori algorithm deals with a digital image as a database that consists of a set of objects (the partitioned image's blocks) and a set of items (image's attributes). It passes over the database's objects to find the most relevant sets of attributes based on predefined user's preferences (minimum support). The support of an item-set denotes the frequency of transactions that contain this item-set along all transactions. An item-set is considered frequently if it is satisfying the minimum support [4].

Let us have a set of items $I=\{i_1,...,i_n\}$, a transactions matrix $T=\{T_1,...,T_n\}$ and each transaction T_i is a set of items I, where $T_i=\{i_1,...,i_k\}$ and $T_i \subseteq I$. Then, the function $(T,S)=\{p \subseteq I \mid support(p) \geqslant S\}$ denotes those items whose support is greater than or equal to the minimum support (S) are only turned to be frequent [4].

In general, Apriori algorithm is presented as a join-based algorithm [4], and it is run in three phases [4]:

1. creates the k-candidate sets using k-itemset.
2. pruning irrelevant k-candidate sets to generate large k-itemsets using the minimum support, where the large k-itemsets is initially represented as k-frequent pattern.
3. using the join operator to generate (k+1) candidates from the frequent k-patterns.

Apriori algorithm is terminated when the set of frequent k-pattern in a given iteration is empty [4]. The pseudo-code of Apriori algorithm is illustrated in algorithm 18.

Algorithm 18 The pseudo-code of Apriori algorithm.

input: Boolean matrix and minimum support ratio
generate the candidate item-sets denoted by C_1
prune irrelevant C_1 using minimum support ratio
generate the frequent item-sets denoted by f_1
k=2
while $f_{k-1} \neq \emptyset$ **do**
    generate C_k-candidate item-sets by using joins on f_{k-1}
    prune irrelevant C_k using minimum support ratio
    generate f_{k+1} frequent item-sets
    k= k+1.
end while
output: f_{k-1}

Figure 52 presents the mining process on a simple transaction matrix, which consists of four transactions $\{T_1,T_2,T_3,T_4\}$ and five items $\{1,2,3,4,5\}$, using Apriori algorithm.

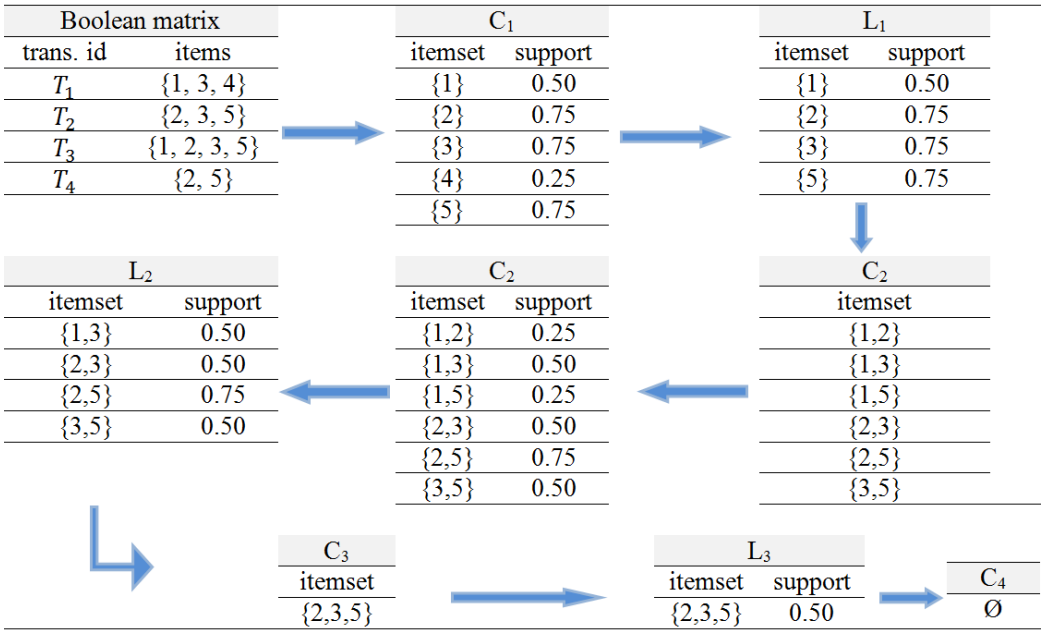


Figure 52: Apriori algorithm working.

The transaction matrix in figure 52 is mined using Apriori algorithm to find the frequent pattern, where the user's preference in terms of minimum support equals 50%.

The Apriori algorithm combines two recursive steps; finding the candidates (C) and the frequent itemset (L). For each step i, the potential candidates used to build C_i are the set of all itemsets of size (i). The final candidates of C_i(i>1) are obtained after pruning using L_{i-1}. Therefore, each item in the database is a candidate in the set C_1. Then, any candidate in C_1 that satisfies the minimum support is frequent candidate in L_1.

Level 2 potential candidates for C_2 are {{1,2}, {1,3}, {1,4}, {1,5}, {2,3}, {2,4}, {2,5}, {3,4}, {3,5}, {4,5}}. As mentioned previously, these candidates are pruned using L_1, which leads to the following values for C_2. These steps are recursively executed until the set of candidate is empty, then eventually the most frequent pattern is the itemset that appears in last L.

6.6.3 *Proposed Approach*

The proposed approach proposes an image watermarking based on texture analysis using FPM method. The FPM method is used to deduce the relationships between texture features of host image, and then to extract the maximal frequent pattern among all frequent patterns. The maximal frequent pattern is a meaningful knowledge that helps to identify highly textured blocks considered for embedding the watermark with high imperceptibility and robustness. The pseudo-code of the proposed approach is illustrated in algorithm 19.

Algorithm 19 The pseudo-code of image watermarking approach based on texture analysis using FPM method

1: **preliminary:** defining the set x={x_1, x_2,..., x_n} as texture features
2: **input:** watermark image w sized $L\times L$, host image I sized $M\times N$ (assuming M and N are multiple of L), and minimum support=10%
3: partitioning host image I into $L\times L$ blocks, results by T blocks, T=M/L×N/L and computing the corresponding features, where T={T_1,T_2,...,$T_{(M/L\times N/L)}$}, is the set of transaction matrix and each transaction T_i is a set of items of x: $T_i \subseteq x$
4: building the transactions matrix and the Boolean matrix
5: applying Apriori algorithm (Boolean matrix and min support ratio) to extract the maximal frequent patterns, which satisfy the minimum support ratio
6: identifying set of blocks matching maximal frequent pattern
7: embedding watermark (I,w)
8: extracting watermark (I_{wa},w)

According to algorithm 19, the proposed approach operates mainly through four phases that are detailed in the following subsections. In the proposed approach, 10% has been chosen as the minimum support ratio. This choice is based on two arguments: (i) several examples in the literature show the effectiveness of this ratio with most databases [49][54]. (ii) by experiments, 10% is approximately the best choice to obtain a reasonable set of frequent patterns and to prevent the producing of large candidate sets via Apriori algorithm.

A *Building the transactions and Boolean matrices*

Initially, the host image is partitioned into $L\times L$ non-overlapping blocks and the values of the texture features for every block are computed using the equations presented in (7) (see subsection 2.6.2), (19), (20) and (21) (see section 6.3) to build the transactions matrix. Subsequently, the transactions matrix is transformed into a Boolean matrix based on the thresholds that are presented in algorithms 6, 7, 8 and 9 (see section 6.3). Figure 49 presents the structure of this phase.

B *Applying Apriori algorithm to extract the maximal frequent pattern*

Once the Boolean database is constructed, the Apriori algorithm is applied to extract the maximal pattern. Normally, the maximal pattern among all patterns has a certain user-defined minimum support, where this leads to define the most robust blocks from all blocks to be concerned in embedding watermark. The algorithm combines many steps that are illustrated in the following.

To simulate these steps, suppose that the proposed approach is tested on images of size 512×512 and partitioned into 64×64 non-overlapping blocks. Then,

there are totally 64 transactions in the transactions matrix. As well, suppose that the texture features are occurring in the Boolean matrix as follows: the DC feature occurs 52 times, the skewness feature occurs 41 times, the kurtosis feature occurs 37 times, and the entropy feature occurs 49 times.

- **Step 1:** Finding the item-sets

  Counts the number of features that are used in mining frequent patterns. In the proposed approach, the number of items is 4 (DC, skewness, kurtosis, and entropy).

- **Step 2:** 1^{st} level candidates

  This step based on the Boolean matrix consists to computes how many times each item is appearing through all transactions. The 1^{st} level candidate (C_1) is illustrated in table 44.

Itemset	Count	Support=Count/number of transactions
{DC}	52	81.25%
{skewness}	41	64.0%
{kurtosis}	37	57.8%
{entropy}	49	76.5%

Table 44: 1^{st} level candidates (C_1) with minimum support of 10%.

- **Step 3:** 1^{st} level frequent pattern

  Extract all candidate's itemset that satisfy the minimum support using algorithm 20, and the selected patterns are illustrated in table 45.

Algorithm 20 The pseudo-code of 1^{st} level frequent pattern

```
input: 1st level candidates (C1)
for each item-set ⊆ C1 do
    if the count in C1/number of transactions ⩾ minimum support then
        add it to the 1st level frequent pattern (L1)
        prune it
    end if
end for
output: 1st level frequent pattern (L1)
```

item-set (L_1)
{DC}
{skewness}
{kurtosis}
{entropy}

Table 45: 1^{st} level frequent patterns (L_1).

- **Step 4:** Build the 2^{nd} level candidates (C_2)

  C_2 is the set of itemsets of size 2 pruned using L_1. It is shown in table 46.

- **Step 5:** Compute the support of 2^{nd} level candidates

  Computes how many times each item-set in C_2 is appearing through all transactions. Suppose the count values in table 46 are those obtained for the (C_2) level candidates. Then, the support values are those given in the last column.

C_2	Count	Support=Count/number of transactions
{DC, skewness}	31	48.4%
{DC, kurtosis}	20	31.25%
{DC, entropy}	24	37.5%
{skewness, kurtosis}	6	9.3%
{skewness, entropy}	16	25.0%
{kurtosis, entropy}	27	42.1%

Table 46: 2^{nd} level candidates and corresponding count and support values.

- **Step 6:** 2^{nd} level frequent patterns (L_2)

  Extract all candidate's itemset in C_2 satisfying the minimum support. The selected patterns are shown in table 47. The candidate {skewness, kurtosis} has been pruned, because it does not satisfy the minimum support.

Item-sets (L_2)
{DC, skewness}
{DC, kurtosis}
{DC, entropy}
{skewness, entropy}
{kurtosis, entropy}

Table 47: 2^{nd} level frequent patterns.

- **Step 7:** 3^{rd} level frequent patterns (L_3)

  Applying a process similar to that of the 2^{nd} level candidates leads to the 3^{rd} level candidates and corresponding support as illustrated in table 48, as well as to the 3^{rd} level frequent patterns shown in table 49.

C_3	Count	Support=Count/number of transactions
{DC,skewness,kurtosis}	6	9.3%
{DC,skewness,entropy}	18	28.1%
{DC,kurtosis,entropy}	6	9.3%
{skewness,kurtosis,entropy}	4	6.25%

Table 48: 3^{rd} level candidates and corresponding count and support values.

Item-sets(L_3)
{DC, skewness, entropy}

Table 49: 3^{rd} level frequent pattern.

- **Step 8:** 4^{th} level frequent patterns (L_4)

  The potential candidates of level 4 are a single set {DC, skewness, entropy, kurtosis}, but this candidate is pruned using L_3. So, after pruning, $C_4 = \emptyset$.

- **Step 9:** Extract the maximal frequent pattern

  Since C_4 is empty, the resulting maximal frequent pattern that satisfying the minimum support are those obtained in at level 3 (the itemset {DC, skewness, entropy}). By returning to the Boolean matrix, those blocks which are matching with the maximal pattern, are identified to be concerned in embedding watermark. These blocks are supposed to be the suitable blocks to embed the

watermark with least image quality distortion and robustness against different attacks.

C *Embedding Process*

This phase involves the embedding process of watermark w in the robust blocks that satisfy the maximal frequent pattern, as explained in algorithm 21. A linear interpolation technique (equation 31) (see subsection 6.4.2) is applied to obtain the watermarked image. Once the watermarked image I_w is obtained, it is sent to the receiver via a public network.

Algorithm 21 The pseudo-code of watermark embedding in semi-blind image watermarking approach based on texture analysis using FPM method.

1: **Input:** host image I, watermark image w of size $L \times L$, selected textured blocks by FPM method B, and interpolation factor t=0.99
2: partitioning I into $L \times L$, the result is n blocks_I
3: **for** k $\leftarrow$ 1 to n **do**
4: **if** block_I(k) $\in$ the set of textured blocks B, block_I(k) $\in I$ **then**
5: applying equation (31)
6: **end if**
7: **end for**
8: **output:** watermarked image (I_w)

D *Extraction Process*

The resulting watermarked image I_w, which holds the watermark data, is subject to channel errors and attacks due to the transmission across a public network. The extraction process at the receiver side is achieved to verify the authenticity of transmitted images. Algorithm 22 presents the watermark extraction process using the inverse form of linear interpolation technique (equation 32) (see subsection 6.4.2). It uses the same interpolation factor t as used in the embedding process.

Algorithm 22 The pseudo-code of watermark extraction in semi-blind image watermarking approach based on texture analysis using FPM method.

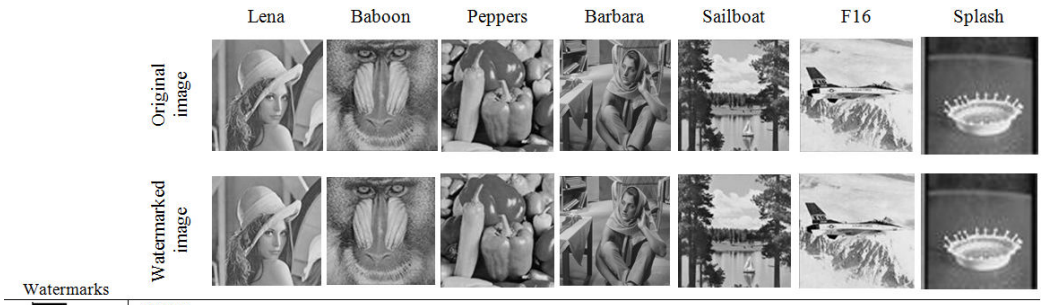
1: **input:** attacked watermarked image I_{wa} of size $M \times N$, original watermark image w of size $L \times L$, selected textured blocks by FPM mining method B, and interpolation factor t=0.99
2: partitioning I_{wa} into $L \times L$, the result is n blocks_{Iwa}
3: **for** k $\leftarrow$ 1 to n **do**
4: **if** block_{Iwa}(k) $\in$ the set of textured blocks B **then**
5: applying equation (32)
6: **end if**
7: **end for**
8: **output:** set of attacked watermarks (w_a)

6.6.4 *Experiment Results*

This section presents the experiment results of the proposed approach on a set of gray-scale images sized 512×512 using 64×64 gray-scale image as watermark. The imperceptibility, robustness, embedding rate and execution time results are presented in the following.

A *Watermark imperceptibility*

Figure 53 presents the imperceptibility results of the proposed approach on a set of host gray-scale images that are collected from CVG-UGR database[3]. The PSNR and the MSSIM are computed for each original image with two watermarks.



Watermarks		Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
(1)	PSNR (dB)	50.03	50.37	49.64	49.48	48.70	48.50	49.18
	mSSIM	0.98	0.99	0.99	0.99	0.98	0.97	0.95
(2)	PSNR (dB)	50.53	50.70	49.38	48.91	48.73	50.24	49.03
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.97

Figure 53: Imperceptibility results of semi-blind image watermarking approach based on texture analysis using FPM method on set of gray-scale images.

3 CVG-UGR database, http://decsai.ugr.es/cvg/dbimagenes/

The results in figure 53 show that the proposed approach achieves a good level of imperceptibility. The PSNR ranges 48.5-50.7 dB, while the MSSIM ranges 0.95-0.99 in all tested images. The results of imperceptibility using the two watermarks are convergent for all host images.

B *Watermarking robustness*

To evaluate the robustness of the proposed approach, the experiments are conducted with a particular focus on noise corruption, filtering, image compression and geometric correction. All watermarked images are exposed to a variety of geometric, and non-geometric attacks using StirMark Benchmark v.4 [80] and Matlab (v.R2016a).

In all experiments using the two watermarks logos, the NC ranges 0.99-1. This means that the proposed approach is able to recover the embedded watermark from attacked watermarked image with high similarity.

Table 50 shows BER results for host gray-scale images using watermark logo 1 and under various attacks. As well, table 51 presents BER results for host gray-scale images using watermark logo 2 also under various attacks.

	BER for Watermark Logo 1						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	6.8	7.1	3.6	5.3	4.9	6.1	4.3
Median filtering (3×3)	6.8	6.9	3.1	4.5	3.0	6.0	2.4
Average filtering (3×3)	6.8	7.0	3.1	4.6	3.0	6.1	2.3
Gaussian low pass filtering (3×3)	6.8	6.9	3.1	4.6	3.0	6.1	2.3
Motion Blure	6.8	7.2	3.3	5.1	3.4	6.1	2.2
Gaussian noise (mean=0,variance=0.05)	5.7	5.4	4.1	4.5	3.9	6.5	3.4
Salt&Pepper noise (noise density=0.01)	6.8	6.8	3.1	4.4	3.1	6.0	2.5
Histogram equalization	2.9	2.5	1.9	3.2	2.2	2.2	1.2
Sharpening	6.8	6.8	3.1	4.3	2.9	5.9	2.4
Scaling (0.5) 512×512 → 256×256	6.8	6.9	3.1	4.6	3.0	6.0	2.4
Cropping left up corner (25%)	6.8	7.2	3.1	4.8	3.0	6.0	2.4
Cropping down from center (78×111)	9.2	9.9	9.3	8.3	8.5	9.1	9.5
Translation vertically (10%)	1.5	1.6	1.5	1.5	1.1	1.4	0.41
Rotation(45°)	0	0	0	0	0	0	0
Affine transformation (2)	5.0	4.9	2.7	4.5	4.6	4.4	3.8
RML (10)	6.8	7.0	3.5	5.5	4.9	6.1	4.5

Table 50: BER results of semi-blind image watermarking approach based on texture analysis using FPM method on set of natural gray-scale images using watermark logo 1 under various attacks.

In table 50 the BER for all images did not exceed 9.9%. The lowest BER is achieved against histogram equalization, translation vertically (10%), and rotation(45°) attacks; the BER did not exceed 2.9%. In case of cropping down (78×111) attack, the proposed approach achieves the lowest robustness comparing with other attacks; the BER reaches 9.9%.

	BER for Watermark Logo 2						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	3.8	3.8	1.7	2.9	2.9	2.8	2.4
Median filtering (3×3)	3.8	3.5	1.5	1.9	1.7	2.7	1.9
Average filtering (3×3)	3.8	3.6	1.5	1.9	1.7	2.7	1.9
Gaussian low pass filtering (3×3)	3.8	3.5	1.5	1.9	1.7	2.7	1.9
Motion Blure	3.8	3.7	1.5	2.2	1.9	2.8	2.1
Gaussian noise (mean=0,variance=0.05)	2.7	2.7	1.9	2.1	2.03	3.0	2.2
Salt&Pepper noise (noise density=0.01)	3.8	3.5	1.5	1.8	1.8	2.7	1.9
Histogram equalization	0.12	1.1	1.1	0.83	1.3	0.78	0.38
Sharpening	3.7	3.5	1.5	1.6	1.7	2.7	1.9
Scaling (0.5) 512×512 → 256×256	3.8	3.5	1.5	1.9	1.8	2.7	1.9
Cropping left up corner (25%)	3.8	3.9	1.5	1.8	1.7	2.7	2.1
Cropping down from center (78×111)	5.7	4.3	5.6	4.2	3.2	4.1	4.3
Translation vertically (10%)	0.67	0.79	0.81	0.78	0.49	0.68	0.12
Rotation(45°)	0	0	0	0	0	0	0
Affine transformation (2)	2.9	2.8	1.8	2.1	2.7	2.3	2.1
RML (10)	3.7	3.8	1.7	2.9	2.8	2.7	2.3

Table 51: BER results of semi-blind image watermarking approach based on texture analysis using FPM method on set of natural gray-scale images using watermark logo 2 under various attacks.

As well, in table 51, the BER for all images did not exceed 6%. Similarly to the BER results in table 50, the proposed approach achieves higher robustness against histogram equalization, translation vertically (10%), and rotation (45°) attacks; the BER did not exceed 1.1%. While, the proposed approach achieves the lowest robustness against cropping down (78×111) attack comparing with other attacks; the BER reaches 5.7%.

However, the BER results in table 51 are lower than the BER results in table 50. This is due to the difference in data amount between logo 1 and logo 2.

c *Embedding rate*

In the proposed approach, the watermark of size 64×64 8-bits gray-scale image is embedded in many locations in 512×512 8-bits gray-scale image. The minimum embedding rate is obtained when only one location is used for embedding watermark, while the maximum embedding rate is obtained when all locations

are used for embedding watermark image. The minimum number of location (of size 64×64) is 1, and the maximum number of locations (each of size 64×64) is equal 64.

In the proposed approach and based on the minimum support ratio, at minimum 10% (approximately 6 blocks) of all partitioned blocks are included in the minimum embedding watermark process. Hence, the embedding rate ER is equal $((64\times64\times8)/(512\times512))\times6 = 32768/262144\times6 = 0.75$ (BPP). While, the maximum embedding rate ER is equal $((64\times64\times8\times64)/(512\times512)) = 2097152/262144 = 8$ (BPP).

D *Execution time*

In the experiments, HP machine 3.4 GHz Intel(R)/core(TM) i7 CPU with 8.0 GB RAM is used as a computing platform. The overall execution time on any host images and under various attacks using the proposed approach is equal to 8 seconds. The extraction process requires a little bit more execution time than the embedding process due to writing many watermarks images on a specific file.

6.6.5 *Computational complexity*

The efficiency of using FPM method in designing image watermarking is measured from the computational complexity.

In the proposed approach, the size of host image is $M\times N$. The complexity value resulting from the calculation of transaction and Boolean matrices is $O(M\times N)$. The complexity of Apriori algorithm calculation is $O((M\times N)\times d^2)$, where d is the number of features [41]. Therefore, the total time complexity of the proposed approach is $O((M\times N)\times d^2)$.

6.7 IMAGE WATERMARKING APPROACH BASED ON TEXTURE ANALYSIS USING ASSOCIATION RULE MINING

This section presents a blind image watermarking approach based on texture analysis using Association Rule Mining (ARM) method. The principle is to identify the strongly textured locations in the host image to insert watermark. Indeed, texture is correlated to HVS. It can be considered in designing a watermarking approach to enhance the imperceptibility and the robustness. In the proposed solution, four gray-scale histogram based-image features (DC, skewness, kurtosis, and entropy) are chosen as input data to design association rules. Subsequently, Apriori algorithm is applied to mine the relationships between the selected features. The higher significant relationships between the selected features are used to identify the strongly textured blocks for embedding watermark. Two strong parameters (lift and confidence) calculated using association rule mining are used to design a blind watermarking.

This section starts by presenting the principles of image mining and association rules in subsection 6.7.1. Then, the mining process metrics are presented in subsection 6.7.2. The proposed blind image watermarking approach based on texture analysis using ARM is presented in subsection 6.7.3. The experiment results on set of gray-scale images in terms of imperceptibility, robustness, embedding rate and execution time are introduced in subsection 6.7.4. Finally, the computational complexity is presented in subsection 6.7.5 .

6.7.1 *Image mining and association rules*

Automated image acquisition and storage technology have led to tremendous amount of images stored in databases. Image mining is an interdisciplinary field that draws its basic principles from concepts in databases, statistics, soft computing, and machine learning. Image mining aims to discover nontrivial and useful information from large collections of images that helps to understand certain characteristics of a specific image. The obtained information describes implicit image data relationships and significant patterns of image. The basic components in image mining are identifying the frequent patterns and generating association rules from the low-level image information. These components in fact require many preprocessing steps including feature extraction, object identifying and applying one of image mining algorithms.

The association rules is a well-known data mining technique that aims to discover implicit knowledge and hidden relations between data items in large databases. It is an important data-mining model studied extensively by the database and data mining researchers community. Primarily, the association

rules were used in the marketing field to discover set of hidden frequent patterns of products that are purchased together by customers. The extracted hidden patterns support the decision-makers to enhance the marketing process through useful actions for shelf stocking and recommendations to add other products [102].

Association rule is very interesting and useful to users in different applications such object tracking, remote sensing images, and medical treatments [99].

Mining association rules can be used to improve the watermarking process by extracting useful information from the host image. This information could be a strong relationship between specific image features that enhances the robustness and the imperceptibility ratios. Typically, mining association rules initiates by partitioning the image into a set of non-overlapping blocks, defining some features and applying one of the mining algorithms such Eclat, Apriori, and FP-growth [24].

The general syntax of association rules can be defined formally as follows:

- Let $I=\{i_1,i_2,\ldots,i_l,\ldots,i_m\}$, $1\leqslant l\leqslant m$, a set of items that defines the features of the processed database.
- Let $T=\{t_1,t_2,\ldots,t_j,\ldots,t_n\}$, $1\leqslant j\leqslant n$, a transaction matrix for a specific system, $t_j\subseteq I$.
- Let X,Y be independent item-sets from I. The rule is an implication in the form $X\rightarrow Y$, where $X\subseteq I$, $Y\subseteq I$, $X\cap Y=\emptyset$. Then, the association rule of form $X\rightarrow Y$ implies that any transaction within the transaction matrix containing the itemset X must also contain itemset Y.

6.7.2 *Mining process metrics*

Many descriptive and statistical metrics are often used to evaluate the effectiveness and usefulness of the candidates association rules for different applications. These metrics are categorized into descriptive and statistical metrics. Three descriptive metrics including support, confidence, and lift are usually used to extract the frequent data patterns and then to filter or sort the association rules [38].

Using association rules for mining frequent itemsets generated with algorithm such as Apriori, is based mainly on three quality metrics: support, confidence and lift. These metrics reflect the user's preferences and determine the strength of relationships between the elements of an itemset in database. These metrics are described below.

1. Support metric

The support of the association rule ($X \rightarrow Y$) denotes the frequency of transactions that contain both X and Y itemsets. Its value ranges between 0-1. High support ratio means that the association rule ($X \rightarrow Y$) occurs frequently in the database and involves a great part of database's transactions. The support ratio is computed according to equation (36).

$$support(X \rightarrow Y) = \frac{N_{(X \cup Y)}}{N} \tag{36}$$

Where N is the number of transactions, and $N_{(X \cup Y)}$ is the number of transactions covering both X and Y.

2. Confidence metric

   The confidence of the association rule ($X \rightarrow Y$) denotes how often each item in Y appears in the transactions that contain item/s X, its value ranges between 0-1. High confidence ratio means that the rule is more useful to the user. The confidence ratio is computed according to equation (37).

$$confidence(X \rightarrow Y) = \frac{support(X \cup Y)}{support(X)} = \frac{N_{(X \cup Y)}}{N_X} \tag{37}$$

   Where N_X is the number of transactions covering X.

3. Lift metric

   The lift of the association rule ($X \rightarrow Y$) denotes the importance of the rule, and checks the randomness of selecting the rule. The lift value is ranged between zero and positive infinity. High lift value presents high significance of the rule, and high correlation between X and Y itemsets. The lift ratio is computed according to equation (38).

$$lift(X \rightarrow Y) = \frac{confidence(X \rightarrow Y)}{support(Y)} = \frac{N_{(X \cup Y)} \times N}{N_X \times N_Y} \tag{38}$$

   Where N_Y is the number of transactions covering Y.

   The resulted lift value, which expresses the importance of association rule, can be presented through three cases [11][103]:

   Case 1. lift ($X \rightarrow Y$)>1 indicates that itemsets X and Y appear more often together; this means that the occurrences of X have a positive effect on the occurrences of Y, and it expresses a high correlation between items X and Y.

   Case 2. lift ($X \rightarrow Y$)<1 indicates that the itemsets X and Y appear less often together; this means that the occurrences of X have a negative effect on the occurrences of Y, and it expresses negative correlation between items X and Y.

Case 3. lift (X→Y) ≈ 1 indicates that itemsets X and Y are independent; this means that the occurrences of X has almost no effect on the occurrences of Y, and it expresses a no correlation between items X and Y.

6.7.3 *Proposed approach*

The proposed approach introduces image watermarking approach based on texture analysis using association rules mining method. Four gray-scale histogram based-image features (DC, skewness, kurtosis, and entropy) are chosen as input data for designing association rules. The Apriori algorithm is used to mine the association rules between the selected features. The highly significant association rules between the selected features are used to identify the strongly textured blocks for embedding watermark. The general structure of the proposed approach is illustrated in figure 54.

The proposed approach initiates by partitioning the host image into set of non-overlapping blocks, then the values of the four features in each block are calculated using the equations presented in (7), (19), (20), and (21) to construct a transactions matrix. In the transactions matrix, the blocks are the objects and the four features are the attributes. The transactions matrix is then transformed into a Boolean matrix based on the thresholds that are presented in algorithms 6, 7, 8, and 9. Apriori algorithm manipulates the resulting Boolean matrix based on a predefined minimum support to extract the most frequent patterns of the attributes over all objects. Then, the set of non-trivial subsets of frequent patterns are extracted and given in the form of association rules. The association rules, which describe the relationships between the features of frequent patterns, are mined using the lift and confidence values.

The proposed approach exploits the most relevant association rules based on support, confidence, and lift criteria to provide an authentication based watermarking.

When only one rule has the maximum confidence value, it is chosen as the most relevant association rule. If several rules have the maximum confidence value and only one has the maximum lift and confidence values, it is chosen as the most relevant one. When several rules have the maximum lift and confidence values, those among them with the maximum support value are considered as the most relevant rules. The most relevant association rules characterize strongly textured blocks in the host image. These textured blocks are more suitable to hold the watermark in terms of imperceptibility and robustness.

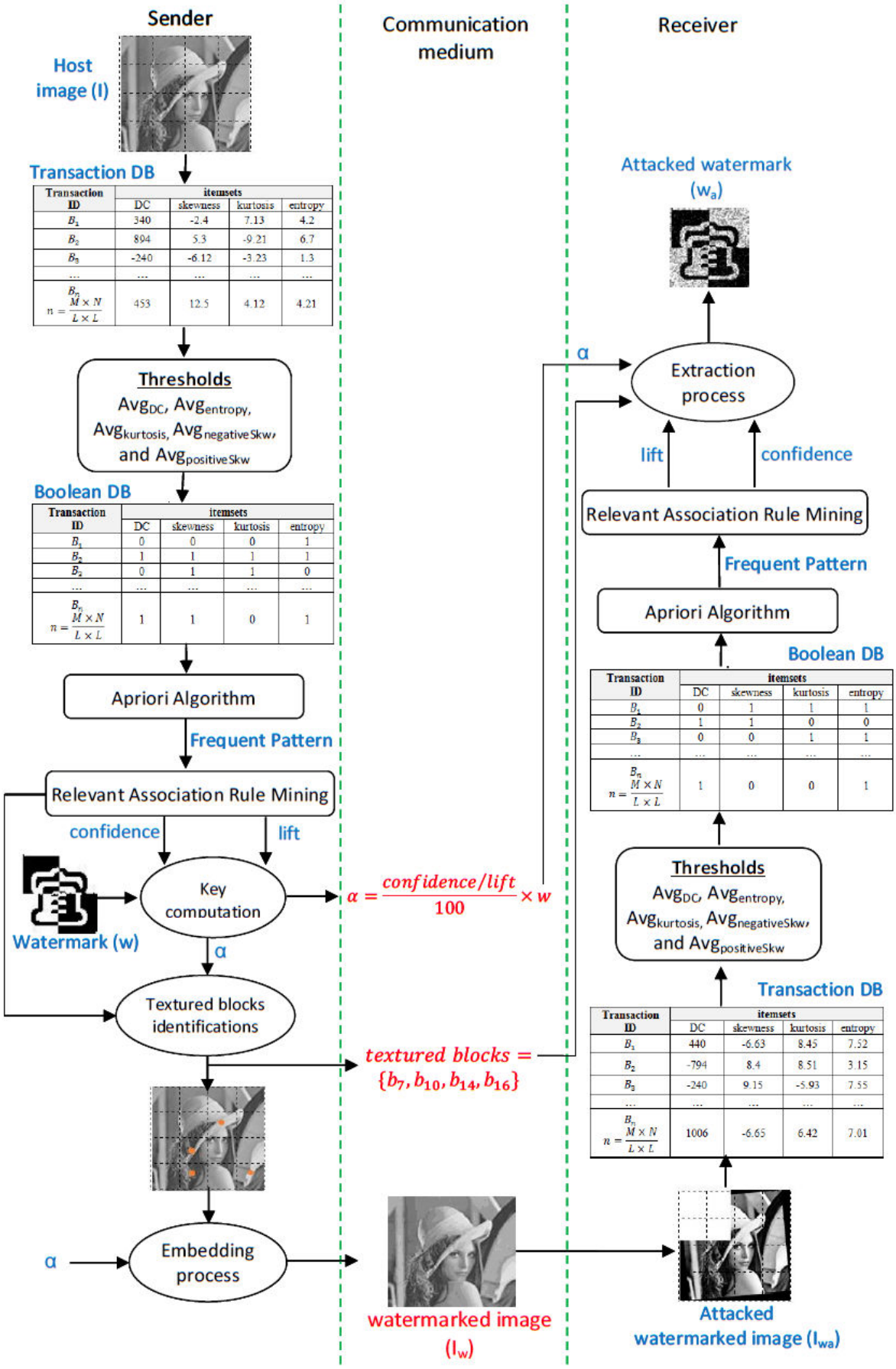


Figure 54: Structure of the proposed approach.

As illustrated in figure 54, the proposed approach implements mainly four phases:

1. Computing the values of texture features and building the Boolean matrix
2. Applying Apriori algorithm to mine association rules
3. Watermark embedding process
4. Watermark extraction process

These phases are presented in following subsections.

A *Computing the values of texture features and building the Boolean matrix*

In this step, the host image is partitioned into $L \times L$ non-overlapping blocks and the values of the texture features for every block are computed using the equations presented in (7), (19), (20), and (21) to build the transactions matrix. Subsequently, the transactions matrix is transformed into a Boolean matrix based on the thresholds that are presented in algorithms 6, 7, 8, and 9. Figure 49 presents the structure of this phase.

B *Applying Apriori algorithm to mine association rules*

The pseudo-code of this phase is given in algorithm 23. In this phase, Apriori algorithm explores the extracted Boolean matrix to generate all frequent itemsets z for which $N_z/N \geqslant$ minimum support (N_z is the number of transactions covering itemset z and N is the total number of transactions in the transactions matrix) and $|z| \geqslant 2$, since the goal is to interpret association rules. Then, for each frequent itemset z consider all ways in which z can be partitioned into two non-empty subsets X and Y-X such that ($X \rightarrow Y$-X). Each frequent itemset z can produce up to 2^k-2 association rules, where k is the number of attributes in each frequent itemset.

The set of candidates association rules (candidatesARs) can be pruned based on anti-monotone property of confidence of rules generated from the same itemset [99]. The anti-monotone property mentioned that if X' is a subset of X, then the confidence of ($X' \rightarrow Y$-X') cannot have higher confidence than ($X \rightarrow Y$-X).

This property ensures that the lowest confidence rule extracted from a frequent itemset contains only one item on its left-hand side and the highest confidence rule extracted from a frequent itemset contains only one item on its right-hand side.

The proposed approach concludes in finding the most relevant association rule. It starts by selecting all rules that have one item on the right hand side as initialARs, and subsequently selects as results the rules that have the maximum

confidence or the maximum lift when several rules have the maximum confidence value; or the maximum support when several rules have the maximum confidence value and the maximum lift value. The most relevant association rule is used to define strongly textured blocks.

In the proposed approach, 10% has been chosen as the minimum support ratio. The arguments of this choice have been presented in subsection 6.6.3.

Algorithm 23 The pseudo-code of the association rule mining process

Preliminary: Defining the itemset x={x_1,...,x_n} as texture features
Input: Boolean matrix and minimum support ratio
apply the Apriori algorithm (Boolean matrix, minimum support) to extract the frequent itemsets *Z*
if *Z* is empty **then**
    select another minimum support less than the predefined one
    redo step 3
end if
generate the association rules (ARs) from the non-trivial subset of frequent pattern/s
    candidatesARs ← non-trivial subset of frequent pattern/s
from candidatesARs select all rules that have one item on the right hand side as initialARs
    initialARs ⊆ candidatesARs
for each item x_i in x **do**
    find in initialARs the rule that has the maximum confidence among those having
item x_i on the right hand side
end for
sortedRules ← sort rules by confidence value in descending order tempARs ← rules from sorted rules with maximum confidence value interestingAR ← tempARs
if two rules or more have the same confidence value **then**
    from tempARs, select all association rules that have liftvalue>1
    tempARs ← {R ∈ tempARs | lift(R)>1}
    if tempARs is empty **then**
        tempARs ← {R ∈ tempARs | lift(R)=1}
    end if
    if tempARs is empty **then**
        tempARs ← interestingAR
    end if
    if tempARs has only one rule **then**
        interestingAR ← tempARs
    else
        interestingAR ← {R | R ∈ tempARs and *R* has maximum lift value}
        if interestingAR has two or more rules **then**
            interestingAR ← {R | R ∈ interestingAR and *R* has maximum support}
        end if
    end if
end if
output: the most relevant association rule (interestingAR)

c *Embedding Process*

All blocks that satisfy the most relevant association rule are among the most textured blocks, and are consequently more suitable for embedding watermark from imperceptibility and robustness points of views. A new embedding tech-

nique is proposed. It uses confidence and lift values of the relevant association rule (AR_i), which is extracted from the host image. Initially, the public key alpha (α) is computed according to equation (39).

$$\alpha = \frac{confidence(AR_i)/lift(AR_i)}{100} \times watermark \tag{39}$$

This key is used in the embedding procedure. It can be used efficiently in the extraction procedure to extract the watermark from attacked image without needing neither the original image nor the original watermark. The watermarked image is calculated by adding the value of public key (α) to the pixels values of the host image. Algorithm (24) presents the pseudo-code of the watermark-embedding phase.

Algorithm 24 The pseudo-code of embedding watermark in image watermarking approach based on texture analysis using ARM

Input: host image I of size $M \times N$, public key (α) of size $L \times L$, and set of textured blocks selected by ARM method B
partitioning I into $L \times L$, the result is n $blocks_I$
for k ← 1 to n **do**
    if $block_I(k) \in$ the set of textured blocks B, $block_I(k) \in I$ **then**
        $block_{Iw}(k) \leftarrow block_I(k) + \alpha$
    else
        $block_{Iw}(k) \leftarrow block_I(k)$
    end if
end for
output: watermarked image (I_w)

D *Extraction Process*

The watermarked image I_w, which holds the watermark, is subject to channel errors and attacks due to the transmission across public networks. The extraction procedure is achieved to verify the authenticity of the transmitted image. Initially, the most relevant association rule of the attacked watermarked image is extracted, and then the confidence and the lift values of the relevant rule are used to extract the attacked watermark as illustrated in algorithm (25).

Algorithm 25 The pseudo-code of extraction watermark in image watermarking approach based on texture analysis using ARM

1: **input:** attacked watermarked image I_{wa} of size $M \times N$, public key (α) of size $L \times L$, and set of textured blocks by ARM method B
2: partitioning I_{wa} into $L \times L$, the result is n blocks_{Iwa}
3: **for** k $\leftarrow$ 1 to n **do**
4: **if** $\text{block}_{Iwa}(k) \in$ the set of textured blocks B **then**
5: $w_a(\text{block}_{iwa}) \leftarrow \frac{\text{lift}_{iwa} \times 100}{\text{confidence}_{iwa}} \times \alpha - \frac{\text{confidence}_{iwa}}{\text{lift}_{iwa} \times 100 - \text{confidence}_{iwa}} \times \text{block}_{iwa}$
6: **end if**
7: **end for**
8: **output:** set of attacked watermarks (w_a)

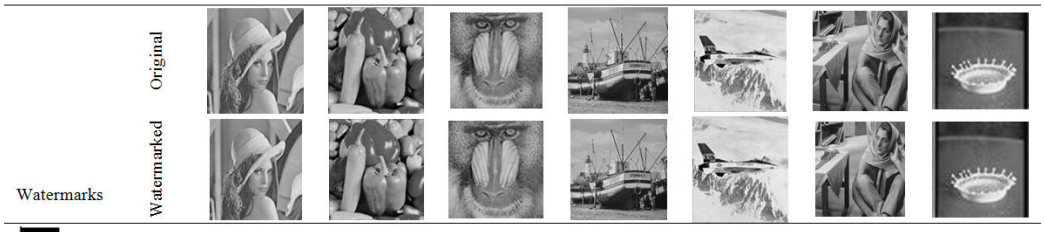
The proposed extraction process is blind. Indeed, the receiver uses only the public key alpha (α) to extract the attacked watermark without any knowledge about the original watermark or the original image.

6.7.4 *Experiment Results*

The proposed approach is analyzed for its performance against image processing attacks. These attacks are geometric, non-geometric, and hybrid attacks. The performance of the proposed approach in terms of imperceptibility, robustness, embedding rate, execution time, and computational complexity are presented in the following subsections.

A *Watermark imperceptibility*

Figure 55 presents the imperceptibility results of the proposed approach on set of host gray-scale images that are collected from CVG-UGR database[4]. The PSNR and the MSSIM are computed for each original image with two watermarks.



(1)	PSNR (dB)	50.38	49.85	49.92	49.89	48.72	50.2	49.11
	mSSIM	1	0.99	0.99	1	0.99	0.99	0.97
(2)	PSNR (dB)	49.17	48.68	48.6	48.67	47.48	50.0	47.86
	mSSIM	0.99	0.99	0.99	0.99	0.99	0.99	0.98

Figure 55: Imperceptibility results of semi-blind image watermarking approach based on texture analysis using ARM method on set of gray-scale images.

4 CVG-UGR database, http://decsai.ugr.es/cvg/dbimagenes/

The results in figure 55 show that the proposed approach achieves a good level of imperceptibility. The PSNR ranges 47.48-50.38 dB, while the MSSIM ranges 0.97-1 in all tested images. The results of imperceptibility using the two watermarks are convergent for all host images.

B *Watermarking robustness*

To evaluate the robustness of the proposed approach, the experiments are conducted with a particular focus on noise corruption, filtering, image compression, and geometric correction. All watermarked images are exposed to these attacks using StirMark Benchmark v.4 [80] and Matlab (v.R2016a).

In all experiments using the two watermarks logos, the NC ranges 0.99-1, except in case of crop down (78×111) attack where the NC ranges 0.83-0.95. This kind of attack has high impact on watermarked image, it leads to loss of much image data and this generates different confidence and lift values in comparison to the original values.

However, these ratios ensures the ability of the proposed approach to recover the embedded watermark from attacked watermarked image with high similarity. The original watermark and the extracted one are absolutely identical against different attacks.

Table 52 shows BER results for host gray-scale images using watermark logo 1 under various attacks. As well, table 53 presents BER results for host gray-scale images using watermark logo 2 under various attacks.

	BER for Watermark Logo 1						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	7.3	7.0	4.8	4.4	3.3	6.3	2.0
Median filtering (3×3)	7.2	3.5	3.8	4.4	3.2	6.2	0.18
Average filtering (3×3)	7.4	2.9	3.8	2.5	2.5	6.6	1.4
Gaussian low pass filtering (3×3)	7.4	2.9	3.8	3.4	2.5	6.6	1.1
Motion Blure	7.1	3.1	3.1	4.7	2.8	6.3	0.02
Gaussian noise (mean=0,variance=0.05)	4.2	3.4	4.1	4.8	3.7	5.8	5.0
Salt&Pepper noise (noise density=0.01)	7.1	6.1	4.0	4.3	6.2	5.1	4.4
Histogram equalization	3.1	3.2	3.4	2.1	2.9	3.1	2.3
Sharpening	6.2	3.5	3.9	4.1	2.6	5.5	0.18
Scaling (0.5) 512×512 → 256×256	6.5	4.8	3.9	2.3	2.6	6.0	0.06
Cropping left up corner (25%)	4.8	7.4	4.9	5.3	5.4	5.6	3.9
Cropping down from center (78×111)	10.9	9.4	8.8	10.2	10.3	8.9	9.4
Translation vertically (10%)	4.3	1.8	1.4	2.5	2.8	3.6	1.7
Rotation(45°)	2.3	1.1	2.3	2.2	0.13	1.0	4.0
Affine transformation (2)	5.2	5.9	4.1	2.7	2.7	5.7	1.3
RML (10)	7.3	6.5	5.1	3.3	3.4	5.2	2.0

Table 52: BER results of blind image watermarking approach based on texture analysis using ARM method on set of natural gray-scale images using watermark logo 1 under various attacks.

In table 52 the BER for all images did not exceed 7.4% except in case of cropping down (78×111) attack where the BER ranges 8.8-10.9%. The lowest BERis achieved against histogram equalization, translation vertically (10%), and rotation(45°) attacks; the BER did not exceed 4.3%. In case of cropping down (78×111) attack the proposed approach achieves the lowest robustness comparing to other attacks, due to the same reason as explained previously.

	BER for Watermark Logo 2						
Attack	Lena	Baboon	Peppers	Barbara	Sailboat	F16	Splash
JPEG compression (QF=20)	3.8	2.2	2.9	1.6	1.5	2.9	1.7
Median filtering (3×3)	3.5	1.6	2.8	1.3	0.33	2.7	0
Average filtering (3×3)	4.0	1.4	2.8	0.44	0.98	3.0	0.78
Gaussian low pass filtering (3×3)	3.8	1.3	2.8	0.61	0.98	3.0	0.52
Motion Blure	3.4	1.7	2.1	1.6	1.4	2.6	0.003
Gaussian noise (mean=0,variance=0.05)	2.2	2.3	2.4	2.6	1.7	2.8	2.6
Salt&Pepper noise (noise density=0.01)	3.7	3.0	2.9	1.5	2.7	2.2	2.1
Histogram equalization	0.98	1.8	2.2	0.20	0.48	1.8	1.4
Sharpening	2.4	1.6	2.8	1.9	0.36	1.9	0
Scaling (0.5) 512×512 → 256×256	2.4	2.3	2.8	0.50	0.31	2.0	0.003
Cropping left up corner (25%)	1.5	4.0	2.9	2.1	2.0	2.9	2.1
Cropping down from center (78×111)	5.3	4.6	4.4	4.9	4.9	4.7	4.6
Translation vertically (10%)	1.9	0.8	1.0	1.8	1.6	1.9	0.91
Rotation(45°)	1.5	0.62	1.5	1.3	0.07	0.62	2.0
Affine transformation (2)	2.4	3.4	2.7	0.48	1.4	3.2	0.53
RML (10)	3.8	3.0	2.9	1.1	1.5	1.7	1.6

Table 53: BER results of blind image watermarking approach based on texture analysis using ARM method on set of natural gray-scale images using watermark logo 2 under various attacks.

In table 53 the BER for all images did not exceed 4.0% except in case of cropping down (78×111) attack the BER ranges 4.4-5.3%. The lowest BER is achieved against histogram equalization, translation vertically (10%), and rotation(45°) attacks; the BER did not exceed 1.9%. In case of cropping down (78×111) attack the proposed approach achieves the lowest robustness comparing to other attacks.

However, the BER results in table 53 are lower than the BER results in table 52. This is due to the difference in data amount between logo 1 and logo 2.

C *Embedding rate analysis*

In the proposed approach, the watermark of size 64×64 8-bits gray-scale image is embedded in many locations of 512×512 8-bits gray-scale image. The minimum embedding rate is obtained when only one location is used for embedding watermark, while the maximum embedding rate is obtained when all locations are used for embedding watermark. The minimum number of location (of size

64×64) is 1, and the maximum number of locations (each of size 64×64) is equal 64.

In the proposed approach and based on the minimum support ratio, a minimum of 10% (approximately 6 blocks) of all partitioned blocks are included in the embedding watermark process. Hence, the minimum embedding rate ER is equal $((64\times64\times8)/(512\times512))\times6 = 32768/262144\times6 = 0.75$ (BPP). While, the maximum embedding rate ER is equal $((64\times64\times8\times64)/(512\times512)) = 2097152/262144 = 8$ (BPP).

D *Execution time result*

In the experiments, HP machine 3.4 GHz Intel(R)/core(TM) i7 CPU with 8.0 GB RAM is used as computing platform. The overall execution time on any host image under various attacks using the proposed approach is equal to 10 seconds. The extraction process requires a little bit more execution time than the embedding process due to writing many watermarks images on a specific file.

6.7.5 *Computational complexity*

The efficiency of using ARM method in designing image watermarking is measured from the computational complexity.

In the proposed approach, the size of host image is $M\times N$ and the complexity value resulting from the calculation of transaction and Boolean matrices is $O(M\times N)$. The complexity of Apriori algorithm calculation is $O((M\times N)\times d^2)$, where d is the number of features. The complexity of association rules generation is $O(2^d)$. Therefore, the total time complexity of the proposed approach is $O((M\times N)\times d^2)$.

6.8 COMPARATIVE STUDY

This section presents a comparative study between the performance of MCDM, FCA, FPM, and ARM based approaches and other related watermarking approaches proposed in [58][1][75][48][39][47][42][59]. All of these approaches are based on HVS characteristics and use different intelligent or knowledge discovery techniques. As well, all of these approaches are tested on set of natural gray-scale images.

Four tables synthesize a comparative study between these approaches; table 54 presents a summary description of each of the proposed approaches. The image characteristics that are correlated to the HVS and analyzed using one of the intelligent or knowledge discovery technique are also presented. Table 55 presents a comparative study between these approaches according to various aspects including: the domain based, the type of watermark, the maximum imperceptibility ratio, the maximum robustness ratio, the computational complexity, and the embedding rate. Table 56 shows an imperceptibility comparison between these approaches in case of gray-scale Lena image and in terms of PSNR. Lastly, tables 57 and 58 present a robustness comparison between these approaches in terms of BER and NC against different attacks.

Approach	Intelligent or knowledge discovery technique used	Image characteristics correlated to HVS	Benefits of using intelligent or knowledge discovery technique(s)
Kumar et al., 2017 [58]	Rough set theory	The properties of singular values and DWT bands	Rough set approximated one DWT band into upper and lower sets. The upper and lower sets are used as weight factors in embedding process to improve image quality. Watermark is also embedded in the singular values to improve the imperceptibility and robustness rates
Abdelhakim et al., 2017 [1]	Artificial Bee Colony (ABC)	The texture property obtained from the difference value between the DCT coefficients of adjacent blocks	Optimizing two embedding parameters led to obtain maximum level of robustness and lower level of image distortion
Papakostas et al., 2016 [75]	FIS and GA	Orthogonal moments of the spatial pixels of image that represent the fine image information	FIS generated the quantization factors of orthogonal moment to control the embedding strength of the watermark, while the GA optimized these factors to find the maximum number of bits that can be added to the image without causing visual distortion
Jagadeesh et al., 2016 [48]	FIS and BPANN	The texture and brightness properties obtained from DCT coefficients	FIS constructed a basis for selecting the high textured and high luminance blocks for holding watermark. BPANN optimized weight factor of embedding process to improve the robustness and imperceptibility rates
Han et al., 2016 [39]	GA	The singular values represent the luminance	Optimizing the values of embedding parameters improved the robustness and the imperceptibility rates
Jagadeesh et al., 2015 [47]	FIS	HVS characteristics including the luminance, texture, edge, and frequency sensitivities	FIS helped to identify approximately the best weighing factors that are used in the embedding watermark procedure to improve the imperceptibility and robustness rates
Hsu et al., 2015 [42]	BPANN	The correlation between the DCT coefficients of adjacent blocks expresses the texture	BPANN explored the correlation between the DCT coefficients to increase the value of one DCT coefficient according to the other to improve the imperceptibility and robustness rates
Lai et al., 2011 [59]	GA	The singular values represent the luminance	Optimizing the values of embedding parameters improved the robustness and the imperceptibility rates
MCDM based approaches (6.4.2)	MCDM	The sensitivity of human eye to the texture property (brightness, darkness, image surface and background)	TOPSIS examined the relationships between the texture features to identify the significant visual locations for watermark embedding with high imperceptibility and robustness rates
FCA based approach (6.5.2)	FCA	The sensitivity of human eye to the texture property (brightness, darkness, image surface and background)	FCA helped to identify significant visual blocks for embedding watermark with high imperceptibility and robustness rates
FPM based approach (6.6.3)	FPM	The sensitivity of human eye to the texture property (brightness, darkness, image surface and background)	FPM process identified highly correlated features that defined visual significant locations in host image for embedding watermark with low image distortion and high robustness
ARM based approach (6.7.3)	ARM	The sensitivity of human eye to the texture property (brightness, darkness, image surface and background)	ARM process identified highly significant association rule between the texture features to define visual significant locations in host image for embedding watermark with low image distortion and high robustness

Table 54: A summary description of several image watermarking approaches.

The summary in table 54 shows that various image characteristics are analyzed using different intelligent and knowledge discovery techniques to achieve image authentication based watermarking. Texture, luminance, edge sensitivity,

brightness and darkness are set of the main image characteristics that are analyzed in the proposed approaches. These characteristics are hidden knowledge in any given image and can be carried either in pixels or frequency coefficients.

The DCT coefficients carry many characteristics that are in relationship with the HVS, due to the high correlation between DCT coefficients of adjacent blocks. The DC coefficient for any image block expresses the brightness and the darkness characteristics of that region, while the difference value between the DCT coefficients of adjacent blocks expresses texture characteristic. These properties are exploited in [1][48][42] to design efficient image watermarking approaches. Increasing the value of a DCT coefficient according to the others enhances the imperceptibility but may not enhance the robustness. As well, adjusting slightly the values of high DC coefficients which correspond to the significant visual locations will not cause noticeable visual distortion of the image. Also, embedding watermark in these locations enhances robustness against different attacks.

SVD provides many properties correlated to HVS. Singular values, which are obtained from SVD process, stand for the luminance of the image while variance measures the relative contrast and smoothness of the intensity in the image. If a small data is added to an image, large variation of its singular values does not occur [59]. This property is exploited in [58][39][59] to design efficient image watermarking approaches.

Some parameters of the multi-resolution decomposition of the image using DWT are correlated to the HVS. DWT provides a proper spatial localization and decomposes an image into horizontal, vertical, and diagonal dimensions representing low and high frequencies. The energy distribution is concentrated in low frequencies, while the high frequencies cover the missing details. Since the human eye is more sensitive to the low frequency coefficients, then distributing the watermark on high frequency coefficients causes less visual distortion in image. This property is exploited in [58].

As well, the pixels carry many hidden knowledge; the texture is one of them. Many spatial features, which are correlated to HVS, are used to measure the texture of any image. MCDM, FCA, FPM, and ARM are knowledge discovery techniques used to examine the relationships between a set of spatial features to define highly textured regions of the host image for embedding watermark. Inserting watermark in visual significant regions in host image leads to high imperceptibility and robustness ratios.

Different intelligent techniques (such as ABC, GA, FIS, and BPANN) are used in the approaches proposed in [1][75][48][39][47][42][59] to optimize some embedding parameters to improve the imperceptibility and robustness ratios. Selecting highly visual significant locations or coefficients for embedding watermark or optimizing the embedding parameters leads to design an efficient image watermarking approaches in terms of imperceptibility and robustness.

Approach	Domain based	Type of watermark	Maximum PSNR (dB)	Maximum/ Average/ Range NC	Maximum BER	Computational complexity	Embedding rate (ER) (BPP)
Kumar et al., 2017 [58]	DWT and SVD	8-bits gray-scale image (0-255)	69.5	0.87	13%	$O(min(M\times N^2, M^2\times N))$	0.015
Abdelhakim et al., 2017 [1]	DCT	1-bit binary image (0 or 1)	47.1	×	50%	$O((M\times N)^2 log_2(M\times N))$	0.004
Papakostas et al., 2016 [75]	Orthogonal moments	binary message (0 or 1)	40.0	×	30%	$O((M\times N)\times p)$	0.008
Jagadeesh et al., 2016 [48]	DCT	1-bit binary image (0 or 1)	48.5	0.73-1	×	$O((M\times N)^2 log_2(M\times N))$	0.0039
Han et al., 2016 [39]	DCT and SVD	1-bit binary image (0 or 1)	46.0	0.83-0.93	×	$O((M\times N)^2 log_2(M\times N))$	0.8
Jagadeesh et al., 2015 [47]	DCT	1-bit binary image (0 or 1)	42.3	0.64-1	×	$O((M\times N)^2 log_2(M\times N))$	0.015
Hsu et al., 2015 [42]	DCT	1-bit binary image (0 or 1)	40.1	×	15.3%	$O((M\times N)^2 log_2(M\times N))$	0.015
Lai et al., 2011 [59]	SVD	8-bits gray-scale image (0-255)	47.5	0.99	×	$O(min(M\times N^2, M^2\times N))$	0.5
MCDM based approach 1 in (6.4.2)	Spatial domain	8-bits gray-scale image (0-255)	56.8	0.99	6.6	$O(M\times N)$	0.75
MCDM based approach 2 in (6.4.2)	Spatial domain	8-bits gray-scale image (0-255)	56.6	0.99	1.6	$O(M\times N)$	0.75
FCA based approach in (6.5.2)	Spatial domain	8-bits gray-scale image (0-255)	49.7	0.99	5.6	$O((M\times \mathrm{N})\times \mathrm{d}\times 2^{\mathrm{k}})$	2.37
FPM based approach in (6.6.3)	Spatial domain	8-bits gray-scale image (0-255)	50.7	0.99	5.7	$O((M\times \mathrm{N})\times \mathrm{d}^2)$	0.75
ARM based approach in (6.7.3)	Spatial domain	8-bits gray-scale image (0-255)	50.3	0.83-0.99	5.3	$O((M\times \mathrm{N})\times \mathrm{d}^2)$	0.75

Table 55: Comparison of MCDM, FCA, FPM, and ARM based approaches with other gray-scale image watermarking approaches in terms of various aspects.

Table 55 shows several watermarking approaches that are proposed to achieve gray-scale image authentication. From the domain based aspect, the proposed approaches in [58][1][75][48][39][47][42][59] have used the transformed coefficients for embedding watermark while the other approaches have used the spatial domain.

The proposed approaches in [1][75][48][39][47][42] have used 1-bit binary watermark to ensure the authenticity of the transmitted images, while the other approaches have used 8-bits gray-scale image as watermark. This aspect have impact on the the embedding rate; embedding a gray-scale watermark usually achieves higher embedding rate than embedding a binary watermark. However, the amount of embedded watermark bits into host image has a significant impact on the imperceptibility and robustness ratios. Inserting more watermark bits, lead to more noticeable change on the host image, but could lead to good robustness against different attacks.

All of the proposed approaches achieved an acceptable PSNR. The PSNR ratios of the proposed approaches in this chapter outperform the obtained PSNR in other approaches. The proposed approach in [58] achieved the maximum PSNR comparing with all other approaches, it embedded the singular values of watermark in the singular values of one band of DWT; this preserves less noticeable image quality distortion. The MCDM based approaches showed higher PSNR comparing with FCA, FPM, and ARM based approaches. This leads to say that TOPSIS method works efficiently to examine the relationships between texture features and results by identifying more significant visual locations for embedding watermark than using FCA, FPM, and ARM methods. However, the achieved PSNR in MCDM based approaches outperforms the obtained PSNR in FCA, FPM, and ARM based approaches by 6%.

From the watermarking robustness aspect, most of the proposed approaches are robust against geometric and non-geometric attacks, except the proposed approaches in [1][75]. They did not withstand some geometric attacks.

For the computational complexity, our proposed approaches are executed with lower computational complexity comparing with the proposed approaches in [58][1][48][39][47][42][59]. The proposed approach in [75] achieved lower computational complexity than FCA, FPM, and ARM based approaches, but with a constant value. The lowest computational complexity is achieved in MCDM based approaches, where computational complexity is $O(M \times N)$.

For the embedding rate aspect, MCDM, FCA, FPM, and ARM based approaches present higher embedding rate comparing to other proposed approaches except approach [39]; the ER equals 0.8 (BPP). The FCA based approach achieves the highest ER, because 30% of the partitioned blocks are selected for embedding watermark. The ER in [58][1][75][48][47][42] approaches did not exceed 0.015 (BPP).

6.8.1 *Comparing the imperceptibility results*

Table 56 presents imperceptibility results comparison between the proposed approaches and approaches in [58][1][75][48][39][47][42][59] on gray-scale Lena image.

Approach	PSNR
Kumar et al., 2017 [58]	52.69
Abdelhakim et al., 2017 [1]	46.89
Papakostas et al., 2016 [75]	40.0
Jagadeesh et al., 2016 [48]	47.0
Han et al., 2016 [39]	42.52
Jagadeesh et al., 2015 [47]	42.32
Hsu et al., 2015 [42]	40.50
Lai et al., 2011 [59]	47.5
MCDM based approach 1	56.8
MCDM based approach 2	56.6
FCA based approach	49.7
FPM based approach	50.5
ARM based approach	50.38

Table 56: Imperceptibility results comparison in terms of PSNR on gray-scale Lena image.

In table 56 the PSNR in MCDM, FCA, FPM and ARM based approaches is higher than the PSNR in [1][75][48][39][47][42][59]. The proposed approach in [58] achieved higher PSNR than FCA, FPM, and ARM based approaches by 2%, but it achieved lower PSNR comparing with MCDM based approaches by 4%.

The proposed approach in [58] have embedded the singular values of watermark in the singular values of one DWT band, which then get least noticeable image quality distortion.

6.8.2 *Comparing the robustness results*

Tables 57 present the BER results comparison between the proposed approaches and approaches in [58][1][42] on gray-scale Lena image.

Attack	Kumar et al., 2017 [58]	Abdelhakim et al., 2017 [1]	Hsu et al., 2015 [42]	MCDM based approach 1	MCDM based approach 2	FCA based approach	FPM based approach	ARM based approach
JPEG (QF=60)	6.0	2.0	0	3.8	0	3.8	3.8	3.8
Median filtering (3×3)	10.0	8.0	4.0	3.8	0.6	3.8	3.8	3.5
Average filtering (3×3)	6.0	6.0	×	3.8	0.05	3.8	3.8	4.0
Histogram equalization	×	2.0	4.5	3.7	1.2	1.1	1.3	2.2
Motion blur	11.0	×	×	3.8	0.8	3.8	3.8	3.4
Gaussian noise (variance=0.1)	13.0	×	9.25	3.18	1.1	3.0	3.0	2.8
Salt&pepper noise (noise density=0.01)	×	10.0	16.5	3.8	0.3	3.7	3.8	3.7
Rotation (10°)	11.0	×	×	0	0	0	0	2.0
Rotation (45°)	11.0	42.0	8.01	0	1.4	0	0	1.5
Cropping left up corner (25%)	×	1.0	12.6	3.8	1.3	3.9	3.8	4.0
Scaling (0.5) 512×512→256×256	×	1.0	2.10	3.8	0	3.8	3.8	2.4

Table 57: BER results comparison between MCDM, FCA, FPM, and ARM based approaches and other related approaches on gray-scale Lena image.

The BER results in table 57 show that the proposed approaches achieved lower BER against different attacks comparing with the other proposed approaches, especially against rotation, additive noise, filtering and blurring attacks. The BER in the proposed approaches against rotation attack did not exceed 2.0%, while it exceeded 8.0% in [58][42] and reached 42.0% in [1].

For additive noise, filtering blurring and histogram equalization attacks the BER in MCDM, FCA, FPM and ARM based approaches ranges 0.05-4%, while it ranged 2.0-16.5% in [58][1][42].

Against JPEG (QF=60) the proposed approaches in [1][42] achieved lower BER than FCA, FPM, and ARM based approaches. However, MCDM based approach 2 the BER equals zero. As well, MCDM, FCA, FPM, and ARM based approaches achieve lower BER than the proposed approach in [58] by 2.2%.

For the cropping left up corner (25%) attack the MCDM, FCA, FPM, and ARM based approaches achieve lower BER than the proposed approach in [42], but the proposed approach in [1] achieved lower BER than all other proposed approaches.

In case of scaling (0.5) attack the proposed approaches in [1][42] achieved lower BER than MCDM approach 1, FCA, FPM, and ARM based approaches by 2%, but the MCDM based approach 2 achieves zero BER.

However, the MCDM based approach 2 achieves the highest robustness against the mentioned attacks comparing with all other proposed approaches.

Tables 58 present the NC results comparison between the proposed approaches and the other proposed approaches in [58][48][47][59] on gray-scale Lena image.

Attack	Kumar et al., 2017 [58]	Jagadeesh et al., 2016 [48]	Jagadeesh et al., 2015 [47]	Lai et al., 2011 [59]	MCDM based approach 1	MCDM based approach 2	FCA based approach	FPM based approach	ARM based approach
JPEG (QF=60)	0.80	×	0.89	0.99	0.99	0.99	0.99	0.99	0.99
Median filtering (3×3)	0.80	0.93	0.78	×	0.99	0.99	0.99	0.99	0.99
Average filtering (3×3)	0.90	×	×	0.98	0.99	0.99	0.99	0.99	0.99
Histogram equalization	×	0.98	0.98	0.99	0.99	0.99	0.99	0.99	0.99
Motion blur	0.90	1	0.90	×	0.99	0.99	0.99	0.99	0.99
Gaussian noise (variance=0.1)	0.70	×	×	0.97	0.99	0.99	0.99	0.99	0.99
Salt&pepper noise (noise density=0.01)	×	0.96	0.65	×	0.99	0.99	0.99	0.99	0.99
Rotation (10°)	0.75	0.94	0.75	0.99	0.99	0.99	0.99	0.99	0.99
Rotation (45°)	0.74	×	×	×	0.99	0.99	0.99	0.99	0.99
Cropping left up corner (25%)	×	0.88	0.64	0.99	0.99	0.99	0.99	0.99	0.99
Scaling (0.5) 512×512→256×256	×	1	1	×	0.99	0.99	0.99	0.99	0.99

Table 58: NC results comparison between MCDM, FCA, FPM, and ARM based approaches and other related approaches on gray-scale Lena image.

The NC results in table 58 show that MCDM, FCA, FPM, and ARM based approaches achieve higher NC against different attacks comparing with the other proposed approaches in [58][48][47][59].

The NC ratios against cropping, rotation, salt&pepper noise, blurring, filtering, and JPEG compression attacks in MCDM, FCA, FPM, and ARM based approaches are more attractive comparing with [58][48][47][59] approaches. For the scaling (0.5) attack the proposed approach in [48][47] achieved higher NC than other proposed approach; the NC equals 1. For histogram equalization attack the achieved NC ratios are convergent in all proposed approaches; the NC ranged 0.98-0.99. The NC ratios in MCDM, FCA, FPM, and ARM based approaches are convergent to the NC ratios in the approach proposed in [59]; the NC ranged 0.97-0.99.

However, MCDM, FCA, FPM, and ARM based approaches and the approach proposed in [59] achieved higher NC ratios comparing with the proposed approaches in [58][48][47].

6.9 SYSTEM ANALYSIS

This section introduces a discussion about some important points to validate the performance of MCDM, FCA, FPM, and ARM based solutions for the enhancement of watermarking. These points include: the performance of MCDM, FCA, FPM and ARM methods in the proposed watermarking approaches, the security of key (α) in MCDM and ARM based approaches, and finally the note of for false positive detection.

A *Performance of* MCDM, FCA, FPM, *and* ARM *methods in the proposed watermarking approaches*

There are several advantages of using the MCDM, FCA, FPM, and ARM methods in building image watermarking approaches. The main advantage of TOPSIS method is ranking all blocks in a preference order using the resulted closeness values to the highest texture level. The highest ranked blocks are referenced as the significant textured blocks that are selected in embedding watermark with high imperceptibility and high robustness rates. In the context of texture analysis, TOPSIS method using different WVs makes it possible to measure the significance of each texture feature by comparing the obtained results through all cases of WVs. In addition, this suggestion introduces a way to define which WV is more preferable for texture analysis process and may be recommended to other researchers. The last benefit of TOPSIS method is that it makes it possible to generate a strong key (α), which allow blind watermarking. The calculation of this key is based on the closeness values of textured blocks, and these values are not significantly changed even when the watermarked image is exposed to different attacks. This benefit ensures the efficiency of the MCDM based approach 2 to recover the watermark.

FCA introduces an advantage by examining the relationships between the image features and image blocks. FCA manipulates the features and the image blocks to find the set of all blocks that share a common subset of features and the set of all features that are shared by one of the blocks. The result of this manipulation is set of formal concepts that give an indication about the set of blocks that satisfy the maximum number of texture features. These blocks are considered as the most visual significant blocks and are used for embedding watermark. By the experiments, FCA method achieved high embedding rate by identifying approximately 30% of partitioned blocks as textured blocks for watermark embedding.

The advantage of using FPM method is finding the most relevant features that frequently occur together within the host image. The highly correlated features compose a frequent pattern, which is a meaningful knowledge giving an indication about the set of blocks that satisfy the highly correlated texture features.

All blocks that satisfy this pattern are considered as the strongly textured blocks and are used for embedding watermark. The resulted frequent patterns after applying FPM are used as itemsets to generate the association rules, which help to realize a blind watermarking.

ARM method has some advantages over the FPM in building image watermarking approach. Actually, the relevant association rules result after a second level of mining process. Indeed, the first mining level involves extracting the most frequent patterns of features in terms of support ratio. The second mining level involves finding the relevant association rules that are built from the most frequent patterns in terms of confidence and lift ratios. The main advantage of extracting the relationships between the selected features using association rules mining is that it enhances the robustness, due to the accuracy in defining the strongly textured blocks. Another benefit of ARM is that it makes it possible to generate two secret parameters (lift and confidence), which allow blind watermarking.

High imperceptibility, high robustness, low execution time, low computational complexity, and high embedding rate results of MCDM, FCA, FPM, and ARM based image watermarking approaches ensures the efficiency and the benefits of these approaches over other proposed approaches in the literature.

B *Security of the key (α)*

In both blind image watermarking approaches using MCDM and ARM, the public key (α) is used in the extraction process as a reference to the original watermark. The key (α) is a matrix of 64×64 entries and it is not fixed; for any host image a different key is generated.

The value of each entry can be integer or float number between 0-255. When the entries of the key (α) are integer numbers, then the probability of determining one right number is $1/256$. Thus, the probability to extract right watermark of $64\times64=4096$ entries is equal $(\frac{1}{256}^{4096})=(7.06^{-9865})$. The probability is very low, because it is close to zero.

When the entries of the key (α) are float numbers, guessing the values of the key (α) becomes more hard. Thus, the probability of extracting right watermark is also close to zero.

C *False positive test*

To evaluate the security requirements of MCDM and ARM based approaches, false positive problem is tackled. A false positive is the fact of extracting the watermark from non-watermarked image, which has not actually belonged to the authorized owner. A false positive detection in any watermarking system is disturbing equally as any malfunctions that cause system failure. As well, this

problem encourages malicious owner in claiming other unauthorized image by generating his watermark easily. This problem should be avoided.

Let us consider three non-watermarked images and suppose that the attacker has three watermarks as illustrated in figure 56. The proposed extraction processes are applied on each non-watermarked image to extract the watermark. Any experiment starts by applying the embedding process using the host image and the watermark of the authorized owner, then the extraction process starts by using the non-watermarked image and the attacker's watermark. The false positive detection is occurring, if an extracted watermark is visually similar to the owner's watermark.

Figure 56 shows the NC results between the attacker's watermark and the extracted one in each non-watermarked image in blind image watermarking approach using MCDM method and blind image watermarking approach using ARM method.

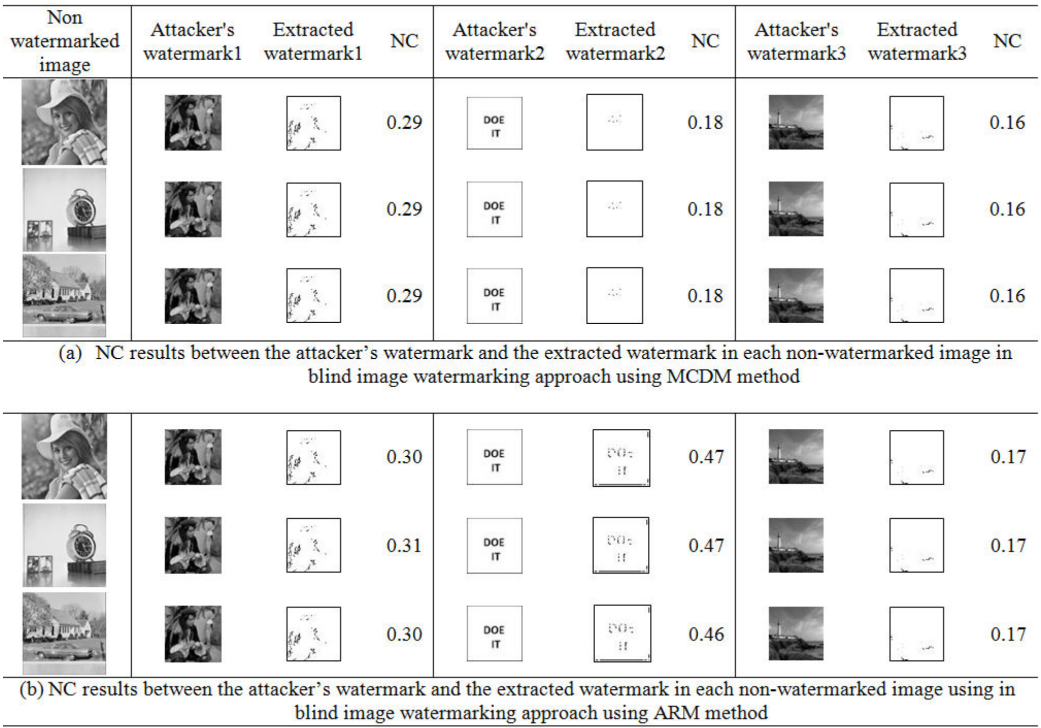


Figure 56: Sample false positive test results for the proposed approaches.

The similarity results in figure 56 prove that the proposed approaches meet the security requirements, where the value of NC did not exceed 0.60. The false positive has been tested on 100 gray-scale images available on CVG-UGR database[5], and the rate of false positive was zero. According to [107] the false positive arises if the NC value between the extracted watermark and the owner's watermark exceeds 0.60. Additionally, any proposed watermarking system can meet the security requirements if the false positive rate is less than 10^{-6} [20].

5 CVG-UGR database, http://decsai.ugr.es/cvg/dbimagenes/

6.10 CONCLUSION

This chapter introduces five image watermarking approaches based on texture analysis using knowledge discovery techniques. These five approaches exploit the correlation between texture characteristics and HVS to identify visual significant locations in host image to hold the watermark with high level of imperceptibility and robustness.

The Multi-Criteria Decision Making (MCDM), the Formal Concept Analysis (FCA), the Frequent Pattern Mining (FPM), and the Association Rule Mining (ARM) approaches are used to analyze texture characteristics by examining the relationships between set of texture features offering many advantages.

MCDM method worked to rank all blocks in a preference order using the resulted closeness values to the highest texture level. The highest ranked blocks are referenced as the significant textured blocks and are selected for embedding watermark. As well as, MCDM method makes it possible to measure the significance of each texture feature by comparing the obtained results through all cases of WVs. In addition, MCDM method makes it possible to generate a strong key (α), which allows blind watermarking.

FCA method worked to examine the relationships between the image features and image blocks. It manipulates texture features and the image blocks to find the set of all blocks that share a common subset of features and the set of all features that are shared by one of the blocks. The result of this manipulation is a set of visual significant blocks that are used for embedding watermark. FPM method finds the most relevant features that frequently occur together within a host image. The highly correlated features compose a frequent pattern. All blocks that satisfy this pattern are considered as the strongly textured blocks and are used for embedding watermark.

ARM method worked as a second mining level over FPM. It involves finding the relevant association rules that are built from the most frequent patterns in terms of confidence and lift ratios. The advantage of extracting the relationships between the selected features using association rules mining is that it enhances the robustness, due to the accuracy in defining the strongly textured blocks. Additionally, ARM method makes it possible to generate two secret parameters (lift and confidence), which allow blind watermarking.

The experiment results showed a higher performance of the proposed approaches over other related image watermarking approaches proposed in the literature in terms of imperceptibility, robustness, execution time, computational complexity, and embedding rate.

The security of the public key used in the embedding and the extraction steps in some of the proposed approaches has been analyzed against brute-force attack. The analysis showed high resistance of this key against brute-force attack.

Additionally, false positive problem has been addressed to evaluate the security requirements of the proposed blind approaches. The tests have shown that the proposed solutions satisfy the security requirements as far as false positive is concerned.

Part III

CONCLUSION

Chapter 7

CONCLUSION

Contents

The work presented in this thesis contributed to preserve images authentication based watermarking with high imperceptibility, high robustness and low computational complexity in spatial domain. It was done with two main ideas. The first one is that extracting a robust feature of host image allows designing zero-watermarking approach. The second one is that analyzing various image characteristics that are correlated to HVS helps to identify some hidden knowledge that could be used to identify the most relevant visual locations for embedding watermark. Indeed, embedding watermark in such locations of host image using spatial domain has beneficial impact on imperceptibility, robustness and computational complexity rates.

In this thesis, we studied the JPEG file structure and the images characteristics. We extracted a robust feature from the JPEG image and we used it to generate a verification watermark in zero-watermarking approach. We also investigated the use of image characteristics related to HVS in order to propose watermarking solutions providing more robustness and imperceptibility than existing ones, and meeting timing constraints of real-time applications. Color representations, texture nature and structure of image's surface/background are set of image characteristics correlated to the HVS. The color, the texture and the structure of image's surface/background characteristics have many different dimensions and there is no standard method for their representation. Hence, several intangible image features (color, texture,...) played an important role in describing (regions of interest) in an image based on these characteristics. Then, solving the intangibility of these characteristics and identifying the significance of each of the used image features are two concerned issues.

7.1 CONTRIBUTION SUMMARY

The work in this thesis contributed in two ranges of image watermarking by taking into account the imperceptibility, the robustness and the computational complexity: zero-image watermarking and spatial domain based image watermarking.

7.1.1 *Zero-watermarking approach for medical images based on Jacobian matrix*

Chapter 4 presented a zero-watermarking algorithm to assure the authenticity of the transmitted medical images through an e-healthcare network. The process consists in partitioning the targeted image into 8×8 non-overlapping blocks, accumulating a subtraction process between these blocks, and exploring the JPEG file quantization matrix to obtain the final 8×8 matrix. An average value of this matrix is computed to be an input to the Jacobian matrix in order to construct a meaningful watermark. In order to decrease the complexity of the process, our model does not need to encrypt the watermark image. The average value is only sent to the receiver. The importance of the proposed approach comes from many features of zero-watermarking including: (i) the fact that the zero watermarking algorithm does not make any modification in the original image and keeps the same size of the original image. (ii) the conflicting requirements in the conventional cryptographic techniques and frequency/spatial digital watermarking (i.e imperceptibility, robustness and embedding rate) are not taken into consideration in the zero-watermarking design. (iii) building a watermark in a zero-watermarking approach is based on extracting the key features from the targeted image; this does not provide any information that the attacker can use to affect the watermark. (iv) the medical images are not subject to any degradation in term of visual quality and this also helps to avoid any risk of misdiagnosis.

The main advantages of the proposed approach are presented as follows:

- The Jacobian matrix helped to build a meaningful watermark image from the average value, which gave a true indication to the impact of the attack.
- The proposed model presented less complexity since it used pixel values to extract the key rather than the frequency techniques.
- Many related works require securing image features or the predefined watermark image to use in the extraction process. This task aims to reduce the chance on detecting any information that could be used by the illegal user to remove or alter the watermark. The proposed model did not need to send the generated watermark, it needs only to send the extracted key. Therefore, there is no need to any security strategy.

On the other hand, the proposed approach has one limitation, where the obtained robustness is low.

7.1.2 *Spatial domain based image watermarking*

We employ our understanding to address the intangibility problems of color, texture and structure of image's surface/background, which help to design efficient image watermarking. The solution proposed in this range is the result of work that leads to the following contributions.

A *Color representations based image watermarking in spatial domain*

Chapter 5 presented an image watermarking approach exploiting the correlation between color representations and HVS. The approach dealt with two problems: the sensitivity of color representations of processed image to the human eyes and the indiscernible effects of DCT coefficients on the perceptual quality of the processed image.

These problems in case of watermarking system have a close relationship with the principles of HVS in terms of robustness and imperceptibility. The color representation problem deals with the degree of sensitivity of each color space of host image to the human eyes. In means of HVS principles, the human eyes are more sensitive to the red and green colors and are less sensitive to the blue color. For designing watermarking system, hiding watermark in blue space will be more appropriate in terms of imperceptibility and robustness, since the human will not be able easily to detect the modification or change in the embedded image. But, the difficulty is for deciding the amount of bits that can be embedded in the blue space without extreme deficiency in perceptual quality of the original image. The DCT coefficients ambiguity deals with the DC and AC coefficients of the transformed image by DCT. The literature mentions that the DC coefficient of each image's block expresses the most magnitude information of that block and is used as good measure to describe the nature of the block (smooth or texture). These perspectives can be analyzed in terms of HVS and for designing watermarking system. In terms of HVS, any change in DC coefficients are more sensitive to the human eyes rather than changes in AC coefficients, which define the details of image's information. For designing watermarking system, the literature proved that embedding watermark bits in DC coefficients is more appropriate in terms of robustness than embedding them in AC coefficients. The vague and uncertainty in this case can be described by the amount of bits that can be embedded in the DC coefficients with preservation of the robustness and perceptual quality of the original image.

In order to solve these two ambiguity problems, the proposed watermarking system exploits the capability of rough sets theory. Initially, the model built two

information systems related to the nature of original images, which are based on the amount of image's content. Then, rough sets theory is applied to define the upper and lower approximation sets and subsequently to extract the rough set, which defines most appropriate blocks to embed watermark in terms of robustness and imperceptibility.

The main advantages of the proposed approach are presented as follows:

- The capability of rough sets theory used efficiently to extract hidden pattern that help to build a color image watermarking approach with high imperceptibility, high robustness and low complexity.
- The locations chosen for watermark embedding are not fixed (i.e. new choice for every image) and the embedding is done in many blocks; this enhances withstand of watermark to geometric attacks.
- Embedding watermark is done in spatial domain rather than in frequency domain, which guarantees low computational complexity.

The proposed approach has one main limitation: it preserved authentication for color images only; it can not offer authentication for gray-scale.

B *Texture analysis based image watermarking in spatial domain*

Chapter 6 presented five image watermarking approaches exploiting the correlation between texture characteristics and HVS.

The texture is a complex visual pattern consisting of mutually related pixels that give an information about the color, brightness, darkness and image surface and background. All of these characteristics are correlated to the HVS and can be represented by calculating some statistical features like entropy, skewness, and kurtosis. Examining the relationships between these features helped to define highly textured regions in host image, which are more suitable for embedding watermark. Inserting watermark in visual significant regions in host image leads to high imperceptibility and robustness against various attacks [39][61].

Intelligent and knowledge discovery methods are used to solve the imprecision of the texture property and exploit them to achieve image authentication, through the identification of significant visual locations for embedding watermark. In this context, Multi-Criteria Decision Making (MCDM), Formal Concept Analysis (FCA), Frequent Pattern Mining (FPM), and Association Rule Mining (ARM) methods are used to identify highly significant visual locations in host image.

Section 6.4 presented how the texture problem can be analyzed using one of MCDM methods in order to identify highly textured blocks within host image to embed watermark with high imperceptibility, high robustness, high embedding rate and low computational complexity. The problem of the textured regions identification in an image is considered as a decision-making problem. A set of

partitioned blocks of host image is a set of possible alternatives to be evaluated using a set of criteria (texture features) to select which of them are more appropriate to hold the watermark. The first order histogram features is used as set of criteria to achieve the evaluation process. Hence, a decision matrix is built and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) method is applied to rank all alternatives and select the best alternative for embedding watermark.

Section 6.5 presented an image watermarking approach based on texture analysis using Formal Concept Analysis (FCA) method. FCA is used to find a meaningful knowledge that helps to embed watermark efficiently, to obtain high imperceptibility and robustness. The formal concepts resulting from the application of the FCA method are exploited to extract highly textured blocks in the targeted image that are convenient with HVS and more preferable to embed watermark with least image quality distortion and high robustness.

Section 6.6 presented an image watermarking approach based on texture analysis using Frequent Pattern Mining (FPM) method. The proposed approach exploited some texture features to extract the maximum frequent patterns in the image data, which satisfy the minimum support. The maximal relevant patterns are exploited to infer knowledge about textured blocks and smooth blocks within host image. The textured blocks are convenient with HVS and more preferable to embed watermark with high imperceptibility and robustness.

Section 6.7 presented a blind image watermarking approach based on texture analysis using Association Rule Mining (ARM) method. The principle is to identify the strongly textured locations in host image to insert watermark. In the proposed solution, four gray-scale histogram based-image features (DC, skewness, kurtosis and entropy) are chosen as input data to design association rules. Subsequently, Apriori algorithm is applied to mine the relationships between the selected features. The higher significant relationships between the selected features are used to identify the strongly textured blocks for embedding watermark. Two calculated strong parameters (lift and confidence) using association rule mining are used to design a blind watermarking.

The main advantages of the proposed approaches are presented as follows:

- The proposed approaches introduced a solution for the uncertainty problem of texture analysis by dealing with intangible features, which in turns helped to identify visual significant regions in host image for embedding watermark with high imperceptibility and robustness ratios.
- The proposed approaches embed watermark in many blocks; the watermark data may spread on 20% of image size. This enhanced withstand of watermark against geometric attacks.

- The proposed approaches embed watermark in spatial domain rather than in frequency domain, which guaranteed low computational complexity.
- TOPSIS method provides a practical way to measure the importance and the effect of each of the used features on the results of texture analysis by using diverse weight vectors.
- TOPSIS method helped to generate a strong parameter for a blind watermarking.
- The relevant association rule improved the way of selecting more suitable blocks for inserting watermark from the point of view of texture, rather than using only the extracted frequent pattern. (applying association rule represented the second level of mining after applying the frequent patterns).
- The relevant association rule gave a way to define a strong parameter for a blind watermarking.
- The relevant association rule gave a way to define two parameters (the confidence and the lift), which can be used in the embedding and the extraction procedures in order to make a balance between imperceptibility and robustness of watermark. The values of these parameters are not much affected with attacks.

7.2 FUTURE WORK

The work presented in this thesis has addressed issues regarding preserve images authentication based watermarking with high imperceptibility, high robustness and low computational complexity. Our plan is to utilize the knowledge and experience learned to address the identified limitations of our work in these subjects.

Regarding the work presented in chapter 4, our next objective is to employ the two parameters (the confidence and the lift) of relevant association rule to generate the verification watermark. The idea is to decrease the negative impact of used key in generating watermark on the robustness ratio. Indeed, the generated watermark from Jacobian matrix is sensitive to the value of extracted key from the host image.

In addition, in chapter 5 fuzzy equivalence relation and investigating information holding in preference order are two major issues that need to be analyzed from the perspective of rough sets theory. The fuzziness in rough set and multicriteria sorting based on rough sets theory are open issues that deal directly with the ambiguity and uncertainty in image knowledge. In case of watermarking system design, these issues could be analyzed to find other possibilities to minimize the effect of image ambiguity and uncertainty on the perceptual image quality and the robustness against different attacks.

For future directions related to the work presented in chapter 6, one proposal is to investigate other intelligent or knowledge discovery methods for solving the problem of texture property in order to evaluate the possible benefits in the watermarking process. Another perspective is the implementation of the proposed approaches through real experiments on wireless networks.

Part IV

RÉSUMÉ EN FRANÇAIS

RÉSUMÉ EN FRANÇAIS

Le travail présenté dans cette thèse contribue à l'authentification de l'image. L'idée de base est d'assurer l'authentification par le tatouage de l'image avec un haut degré d'imperceptibilité et de robustesse et un faible niveau de complexité computationnelle. L'authentification de l'image digitale comprend deux aspects principaux : la preuve de l'origine de l'image et son identification. Le processus de tatouage associe aux données de l'image hôte une marque qui doit être protégée de telle sorte qu'un attaquant ne puisse pas modifier, enlever ou remplacer la marque de tatouage de l'image hôte. Le tatouage peut être appliqué soit dans le domaine spatial sur les pixels de l'image, soit dans le domaine fréquentiel sur les coefficients de sa transformation (la Transformée en Cosinus Discrète - DCT, la Transformée Discrète en Ondelettes - DWT ou la Décomposition en Valeurs Singulières - SVD).

Pour tout processus de tatouage, l'imperceptibilité et la robustesse font partie des propriétés les plus importantes. A cause des ressources limitées dans certains systèmes, la complexité computationnelle est aussi un paramètre très important du tatouage.

Le tatouage-zéro ne modifie pas l'image originale (i.e. la qualité perceptuelle de l'image originale ne se dégrade pas) et sa la complexité computationnelle est faible. En analysant les caractéristiques spatiales de l'image et en extrayant quelques informations cachées corrélées avec le Système Visuel Humain (HVS) nous avons réussi à identifier des zones les plus adaptées pour l'insertion de la marque. L'insertion de la marque dans de telles zones de l'image hôte a un impact positif sur l'imperceptibilité, la robustesse et la complexité computationnelle.

La couleur, la texture et la nature de l'avant plan et de l'arrière-plan font partie des caractéristiques structurelles les plus importantes de l'image en corrélation avec le système visuel humain (HVS). Elles peuvent être analysées par des techniques de découverte de la connaissance à faible complexité computationnelle relevant du domaine de l'intelligence artificielle.

Cette thèse aborde trois problèmes.

1. Le premier problème est de construire un système de tatouage robuste avec une complexité computationnelle faible dans le domaine spatial. En effet, les travaux existants sur le tatouage prennent en compte surtout l'imperceptibilité et la robustesse et se préoccupent beaucoup moins de la complexité computationnelle qui est d'une importance capitale pour les applications à contraintes temporelles.

2. Le deuxième problème abordé est celui posé par l'imprécision de la notion de texture en tant que propriété de l'image, dans le cadre du tatouage de l'image. Les approches utilisées pour la caractérisation de la texture sont les approches statistiques, les approches structurelles et la transformée en ondelettes. Nous avons proposé des solutions pour la résolution de l'imprécision susmentionnée en nous basant sur des approches statistiques de caractérisation de la texture et sur des approches de l'intelligence artificielle.

3. Le troisième problème abordé est la mesure de l'importance de l'effet de chaque caractéristique de la texture pour le processus de tatouage. En effet, cette mesure permet une meilleure identification des paramètres à privilégier pour la sélection des zones de l'image qui sont les plus adaptées pour l'insertion de la marque. Dans cette perspective, nous avons proposé une approche basée sur la méthode de décision multicritère pour l'identification des paramètres les plus significatifs pour la caractérisation de la texture.

Nous présentons ci-après nos propositions en réponse aux problèmes susmentionnés.

Pour le problème 1, nous proposons une approche de tatouage zéro et six approches de tatouages dans le domaine spatial. Le tatouage zéro a été utilisé pour vérifier que l'authenticité de l'image est maintenue au cours de sa transmission. Sa complexité computationnelle est basse. Les autres approches sont basées sur l'analyse de la texture. Elles ont toutes un degré d'imperceptibilité élevé, une grande robustesse et une faible complexité computationnelle. Le système de tatouage zéro a été testé sur des images médicales et sur des images en niveaux de gris. Les autres systèmes ont été évalués pour des images RGB et des images en niveaux de gris.

Pour aborder le problème 2, nous utilisons des techniques de l'intelligence artificielle, de la découverte des connaissances et de fouille de données pour résoudre le problème lié à l'imprécision de la texture en tant que propriété de l'image. Ensuite nous exploitons les approches de modélisation de la texture pour identifier les zones les plus significatives visuellement, susceptibles de recevoir la marque de tatouage.

Les techniques susmentionnées nous permettent d'analyser les relations entre les caractéristiques primaires de la texture et, ensuite, de définir avec plus de précision, les blocs de pixels les plus appropriés pour recevoir la marque de tatouage. L'insertion de la marque de tatouage dans ces blocs permet d'améliorer les taux d'imperceptibilité et de robustesse.

Pour réaliser le processus d'analyse, les techniques utilisent une matrice construite à partir des valeurs des paramètres caractéristiques de la texture et une matrice booléenne construite à partir de cette dernière en utilisant des seuils permettant, pour chacun des paramètres de texture, de classer chaque zone de l'image en zone texturée ou non texturée.

Pour aborder le problème 3, nous avons choisi la méthode des vecteurs poids (Weighting Vectors – WV) consistant à faire varier les poids des différents paramètres caractéristiques de l'image et d'analyser leur impact sur la décision relative à la nature texturée ou non des images.

La thèse est organisée comme suit.

Le Chapitre 1 présente les fondements du traitement de l'image numérique.

Le Chapitre 2 présente les motivations, les exigences, le cadre et la classification des systèmes de tatouage de l'image. Les différentes techniques de tatouage, les principes des différentes attaques des systèmes de tatouage de l'image et les métriques utilisées dans l'évaluation d'un système de tatouage sont aussi présentés dans ce chapitre.

Le Chapitre 3 passe en revue plusieurs approches de tatouage existantes dans la littérature de spécialité qui ont comme principal objectif l'authentification et l'identification. Les contributions de cette thèse sont présentées dans les chapitres 4, 5 et 6.

Le Chapitre 4 propose une approche de tatouage zéro qui a comme objectif l'authentification des images médicales transmises à travers des réseaux privés ou publics. L'approche est basée sur une caractéristique robuste extraite de l'image hôte.

Le Chapitre 5 propose une approche de tatouage robuste basée sur les caractéristiques du système visuel humain et la théorie des ensembles approximatifs (rough sets) pour l'authentification des images RGB.

Le Chapitre 6 présente cinq approches de tatouage basées chacune sur la corrélation entre les caractéristiques de la texture et le système visuel humain. L'objectif est l'authentification des images en niveaux de gris. Ces approches utilisent certains modèles de fouille de données, de la découverte des connaissances et de l'intelligence artificielle pour l'analyse de la texture.

Le Chapitre 7 contient les conclusions et présente quelques directions pour les recherches futures.

Le sommaire par chapitre est présenté ci-après.

Chapitre 1 : Les fondements de l'analyse de l'image numérique

Le traitement de l'image pour son stockage, sa transmission et sa représentation pour une perception autonome par la machine est essentiel. L'analyse de l'image comprend plusieurs étapes structurées en trois niveaux : le niveau du traitement de base, le traitement de niveau intermédiaire et le traitement de haut niveau (la vision machine). Chaque niveau fournit un ensemble de tâches en relation chacune avec les propriétés élémentaires de l'image et ses représentations.

En même temps, chaque niveau fournit un ensemble de connaissances fondamentales sur l'image. Le niveau de base contient les tâches d'acquisition, de représentation, de compression et d'amélioration de l'image. Le niveau intermédiaire contient les tâches de reconnaissance des formes, de segmentation et de classification de l'image. Le niveau supérieur contient les tâches destinées à la compréhension de l'image et à la sémantique de l'image assistée par la machine.

La compréhension de tous ces niveaux nécessite la compréhension des concepts fondamentaux de l'image numérique, de ses formes de représentation, de ses modèles et leurs caractéristiques et des approches du traitement de l'image. Le codage de l'image (compression-décompression), l'amélioration de l'image, la restauration, la classification, la segmentation, les corrections géométriques et le tatouage de l'image représentent des fonctions liées aux tâches du traitement de l'image.

Ce chapitre introduit une discussion sur ces aspects. Dans la section 1.2, la notion fondamentale d'image numérique (digitale) est présentée. La section 1.3 contient différentes représentations de l'image numérique. Les principales caractéristiques de l'image numérique sont exposées dans la section 1.4. La section 1.5 présente des méthodes d'intelligence artificielle et de découverte de connaissances qui peuvent être utilisées pour résoudre certains problèmes soulevés par l'analyse de l'image. La section 1.6 présente quelques outils de traitement d'image et la section 1.7 les conclusions du chapitre.

Chapitre 2: Le tatouage de l'image numérique

Trois grandes familles de solutions ont été développées pour la protection des données numériques : la cryptographie, la stéganographie et le tatouage. La cryptographie est la plus connue et étudiée. Il s'agit de transformer les données initiales D en d'autres données Dc de telle sorte que seul l'utilisateur autorisé puisse obtenir D à partir de Dc. La stéganographie et le tatouage sont deux méthodes basées sur des techniques qui cachent certaines données.

La stéganographie cache les données importantes appelées « marque » dans un signal transporteur de telle sorte que personne, à l'exception du destinataire autorisé, ne connaisse l'existence de cette information (l'existence de la marque). Dans le tatouage, la marque peut être visible et l'information de transport est importante.

Les techniques basées sur la dissimulation de l'information comprennent la tâche de cacher la marque w dans les données originales D (le résultat est représenté par les données tatouées Dw) de telle sorte qu'un attaquant ne puisse ni enlever, ni modifier, ni remplacer la marque dans les données tatouées. Elles permettent de résoudre deux grands problèmes : la protection des données multimédia contre les attaques malencontreuses et leur protection contre une utilisation non désirée.

Par rapport aux autres techniques de protection, le tatouage présente des atouts du point de vue de l'amélioration de l'authentification des données, de l'intégrité des données et de la protection des droits d'auteurs. Dans le tatouage, les données initiales sont visibles et lisibles pour tout utilisateur, tandis que l'information secrète est n'est lisible et modifiable que par les utilisateurs autorisés.

La cryptographie ne peut pas aider le possesseur du contenu des données à contrôler comment un utilisateur légitime manipule les données après le décryptage. Le tatouage permet quant à lui de protéger les données même après le décryptage.

Ce chapitre introduit une discussion sur les objectifs du tatouage de l'image en section 2.2 et sur les exigences des systèmes de tatouage en section 2.3. La section 2.4 présente le cadre de base du tatouage et la section 2.5 la classification des systèmes de tatouage. La section 2.6 présente quelques systèmes de tatouage. La section 2.7 introduit les principes des différentes attaques sur les systèmes de tatouage. La section 2.8 présente les métriques d'évaluation du tatouage et la section 2.9 présente la plateforme Stirmark permettant de tester la robustesse des approches de tatouage d'image. Le chapitre se termine par des conclusions en section 2.10.

Chapitre 3 : Etat de l'art

Dans ce chapitre sont présentées et analysées plusieurs approches de tatouage proposées par différents auteurs. Elles sont regroupées en quatre catégories : les approches de tatouage zéro présentées en section 3.2 ; les approches de tatouage d'images médicales abordées en sous-section 3.3.1 ; les approches de tatouage d'images basées sur le Système Visuel Humain (HVS) présentées en sous-section 3.3.2 et les approches de tatouage reposant sur l'utilisation de techniques d'intelligence artificielle abordées en sous-section 3.3.3.

Pour chaque catégorie, une synthèse des approches a été effectuée en relevant les aspects suivants pour chacune d'entre elles : le type de l'image testée, l'objectif de l'approche, le domaine de représentation de l'image (spatial ou fréquentiel), le taux de robustesse, le taux de perte d'information, la complexité computationnelle.

En ce qui concerne la complexité computationnelle, nous avons considéré la limite supérieure du temps d'exécution (i.e. le pire temps d'exécution). La performance de chaque approche est testée sur des images hôtes I de dimension M×N, où M est la hauteur de l'image et N est la largeur de l'image.

La plupart des approches de zéro tatouage proposées dans la littérature sont basées sur l'extraction de quelques caractéristiques robustes pour construire le tatouage zéro à partir de coefficients de transformation. Chaque approche de zéro tatouage proposée extrait des caractéristiques robustes de SVD, DCT, de la transformée Bessel-Fourier ou PCET (Polar Complex Exponential Transform). Mais le calcul des coefficients dans ces cas conduit à une complexité computationnelle élevée par rapport au calcul réalisé par les approches basées sur DWT, QEMs (Quaternion Exponent Moments) ou NURP (Non-Uniform Rectangular Partition).

En plus, la plupart des approches de zéro tatouage proposées nécessitent quelques techniques de cryptage pour sécuriser la zéro-marque engendrée, ce qui consomme plus de temps d'exécution. Le taux de robustesse de ces approches contre différentes attaques est acceptable.

Le tableau 3 présente l'ensemble des caractéristiques robustes utilisées dans la construction des approches de tatouage zéro. Le tableau 4 présente les spécifications de plusieurs approches de tatouage zéro. Le tableau 5 fournit la complexité computationnelle et le temps d'exécution de ces approches.

Dans le cas des approches de tatouage basées sur l'intelligence artificielle et sur le Système Visuel Humain, la plupart des caractéristiques de l'image utilisées pour identifier les zones visuelles ou les coefficients susceptibles de recevoir la marque de tatouage sont obtenues en utilisant le domaine fréquentiel. Ce choix a un impact négatif sur la complexité computationnelle et sur le temps d'exécution.

Parmi les approches existantes qui analysent les caractéristiques de l'image pour identifier les zones les plus significatives visuellement pour l'insertion de la marque, peu sont basées sur le domaine spatial qui réduit considérablement la complexité. Ces approches font le choix du domaine fréquentiel en se basant sur le fait que le tatouage dans le domaine spatial soit en général plus fragile face aux attaques géométriques et qu'il conduise en général à une dégradation plus importante de la qualité visuelle de l'image.

Toutefois, les problèmes pointés par ces approches quant au domaine spatial peuvent être résolus en trouvant une solution à certains problèmes d'incertitude liés aux pixels tels que celui relatif à l'insertion de la marque dans une plage importante de valeurs de pixels et celui relatif à l'effet de l'insertion des bits de la marque sur la corrélation des pixels adjacents. L'analyse des relations entre les pixels de l'image et le Système Visuel Humain est très importante pour la construction d'un système de tatouage efficace dans le domaine spatial. Un autre facteur aussi important est d'attribuer des degrés d'importance appropriés aux différentes caractéristiques utilisées pour identifier les zones de l'image hôte les plus significatives pour l'insertion de la marque.

Différentes techniques d'intelligence artificielle ou connexes peuvent permettre de résoudre partiellement ce problème. En fait, elles peuvent être utilisées pour améliorer les approches de tatouages par (i) l'identification des meilleures zones ou des meilleurs coefficients parmi plusieurs alternatives pour l'insertion de la marque et (ii) l'obtention d'un facteur optimal de contrôle de la quantité des bits qui peuvent être insérés dans les différentes zones ou coefficients de l'image hôte sans sa dégradation et avec une robustesse élevée contre les attaques.

Le tableau 6 présente les caractéristiques de l'image corrélées avec le Système Visuel Humain et leur impact sur la performance des approches de tatouage des images médicales. Le tableau 7 présente les spécifications de plusieurs approches de tatouage d'images médicales. Le tableau 8 présente la complexité computationnelle et le temps d'exécution de plusieurs approches de tatouage d'images médicales. Le tableau 9 présente les caractéristiques de l'image liées au Système Visuel Humain et leur impact sur la performance d'un certain nombre d'approches de tatouage. Le tableau 10 présente les spécifications de quelques approches de tatouage basées sur le Système Visuel Humain. Le tableau 11 présente la complexité computationnelle et le temps d'exécution de quelques approches de tatouage basées sur le Système Visuel Humain. Le tableau 12 présente les caractéristiques liées au Système Visuel Humain et leur impact sur la performance de quelques approches de tatouage basées sur l'intelligence artificielle (IA) et le Système Visuel Humain (HVS). Le tableau 13 présente les spécifications de plusieurs approches basées IA et HVS. Le tableau 14 présente la complexité computationnelle et le temps d'exécution de ces approches. Les conclusions de ce chapitre sont présentées en section 3.4.

Chapitre 4 : Une approche de tatouage zéro pour les images médicales basée sur la matrice Jacobienne

Le chapitre 4 présente une nouvelle approche de tatouage qui assure l'authenticité des images transmises via des réseaux médicaux. Le système consiste en trois étapes : (i) la partition de l'image à tatouer en blocs de taille 8×8 qui ne se chevauchent pas, (ii) un processus cumulant les résultats de soustractions entre ces blocs et (iii) l'exploitation de la matrice JPEG de quantification (compression) pour obtenir la matrice finale de dimension 8×8. Une valeur moyenne de la matrice finale obtenue est calculée ensuite et cette valeur représente la donnée d'entrée pour la matrice jacobienne pour la construction de la marque.

De cette manière, on obtient une marque qui a un sens. Le schéma illustrant le fonctionnement de ce modèle est présenté dans la figure 15 et le principe de la matrice jacobienne est présenté en section 4.2.

Pour diminuer la complexité computationnelle, notre modèle ne crypte pas la marque de tatouage. Seule la valeur moyenne est transmise au destinataire. Cette approche tient ses principaux atouts de plusieurs caractéristiques du tatouage zéro : (i) le tatouage zéro ne doit pas modifier l'image originale et doit conserver sa taille. (ii) les exigences conflictuelles classiques entre la cryptographie et le tatouage (i.e. l'imperceptibilité, la robustesse et le taux d'insertion) ne sont pas prises en compte par le tatouage zéro. (iii) la construction de la marque dans le tatouage zéro est basée sur l'extraction des caractéristiques clé de l'image hôte, ce qui fait qu'aucune information n'est fournie au pirate en cas d'attaque. (iv) l'image médicale n'est soumise à aucune dégradation visuelle, ce qui aide le médecin à établir le bon diagnostic.

Des expérimentations ont été effectuées et les valeurs obtenues suite à l'application des métriques NC et BER sur les résultats expérimentaux montrent que l'approche proposée améliore la robustesse contre plusieurs attaques. Le taux de NC obtenu est de 93% et la probabilité de récupérer l'image de marque initiale est de 71%. En plus, cette approche a été implémentée avec une complexité computationnelle réduite et un temps d'exécution réduit. La complexité totale est de $O(M \times N)$ et le temps d'exécution de 6 secondes.

Ces résultats sont très encourageants en comparaison à ceux obtenus avec d'autres approches de tatouage zéro. Ils montrent que l'approche proposée peut répondre convenablement aux besoins des applications à contrainte temporelle. Le tableau 24 présente la comparaison entre cette approche et d'autres approches de tatouage zéro.

Les principaux avantages de l'approche de tatouage zéro proposée sont les suivants:

- La matrice jacobienne aide à construire une image de tatouage significative à partir de la valeur moyenne, ce qui donne une vraie indication de l'impact de l'attaque.

- Le modèle a une complexité computationnelle et un temps d'exécution réduits à cause de l'utilisation des valeurs des pixels et non de techniques fréquentielles.

- Plusieurs travaux de tatouage zéro imposent la protection des caractéristiques de l'image ou de l'image tatouée prédéfinie utilisées dans le processus d'extraction. Cette tâche est nécessaire pour réduire les chances de détection de l'information qui peut être utilisée illégalement. Quant à notre approche, elle ne nécessite pas la transmission de la marque générée au destinataire, mais uniquement l'envoi de la clé d'extraction. Il n'y a donc pas besoin de stratégie de protection de caractéristiques de l'image puisque la marque générée n'est pas transmise.

La limite du modèle proposé est sa faible robustesse.

Chapitre 5 : Une approche de tatouage dans le domaine spatial, basée sur les représentations des couleurs

Le chapitre 5 présente une approche de tatouage qui utilise la corrélation entre la représentation couleur et le HVS. L'approche vise principalement la résolution de deux problèmes à savoir la sensibilité de la représentation couleur de l'image à tatouer à l'œil humain et les effets de l'indiscernabilité des coefficients DCT sur la qualité perceptuelle de l'image traitée.

Ces deux problèmes, dans le cas d'un système de tatouage, ont une relation étroite avec les principes du HVS en terme de robustesse et d'imperceptibilité. Le problème de la représentation couleur est d'analyser le degré de sensibilité à l'œil humain de chaque espace de couleur de l'image hôte. En termes des principes du HVS, l'œil humain est plus sensible aux couleurs rouge et verte et moins sensible au bleu. Pour les systèmes de tatouage, cacher la marque de tatouage dans la composante bleue de l'image est plus approprié en termes d'imperceptibilité et de robustesse. Le but est de rendre invisible à l'œil les modifications apportées dans l'image par l'insertion de la marque. La difficulté est de décider de la quantité de bits qui peut être insérée dans l'espace du bleu sans trop détériorer la qualité perceptuelle de l'image originale.

L'ambiguïté dite « des coefficients DCT » est liée aux coefficients DC et AC obtenus suite à la transformée en DCT de l'image. Les études menées jusqu'ici montrent que le coefficient DC d'un bloc exprime la quantité d'information de ce bloc et ce coefficient est utilisé comme une bonne mesure pour la description de la nature de la texture du bloc (lisse ou texturé). Ces considérations peuvent être analysées du point de vue de l'impact sur le Système Visuel Humain dans le cadre de la réalisation d'un système de tatouage.

En ce qui concerne le HVS, les changements dans les coefficients DC sont plus perceptibles à l'œil humain que les changements dans les coefficients AC, ces derniers définissant des détails de l'information. Pour les systèmes de tatouage, les travaux existants montrent que l'insertion de la marque de tatouage dans les coefficients DC est plus appropriée en termes de robustesse que l'insertion dans les coefficients AC.

Le flou et l'incertitude dans ce cas peut être mesuré par la quantité de bits qui peuvent être insérés dans les coefficients DC avec une conservation de la robustesse et de la qualité perceptuelle de l'image originale.

Pour résoudre les deux problèmes susmentionnés, le système de tatouage que nous proposons exploite la puissance de la théorie des ensembles approximatifs (rough sets). Les notions de base de la théorie des ensembles approximatifs (rough sets) sont présentées en section 5.2 de ce chapitre.

Le fonctionnement de l'approche proposée est le suivant. En début, le modèle construit deux systèmes d'information liés à la nature de l'image originale et

basés sur le contenu de cette image. Ensuite, la théorie des ensembles approximatifs est utilisée pour définir l'approximation supérieure et l'approximation inférieure de l'image pour extraire des caractéristiques de l'image permettant la mise en œuvre d'une approche de tatouage efficace en termes de qualité perceptuelle de l'image tatouée, de robustesse contre différentes attaques, de taux d'insertion et de complexité computationnelle.

Le PSNR obtenu avec l'approche proposée atteint 41.89 dB, le mSSIM atteint 0.99, le NC atteint 0.99 et le BER obtenu suite à différentes attaques ne dépasse pas 11.4. Le taux d'insertion est compris entre 0.041 et 2.66 bpp. La complexité computationnelle de l'approche est $O(M \times N \times k)$ et le temps d'exécution de 6.5 secondes.

Ces résultats prouvent l'efficacité du système proposé pour l'authentification des images couleur dans les applications à contraintes temporelles. Le tableau 31 présente la comparaison entre notre approche et quelques approches de tatouage d'images couleurs sous plusieurs aspects. Le tableau 32 présente la comparaison des résultats de mesures d'imperceptibilité en terme de PSNR et de mSSIM entre notre approche et d'autres approches sur l'image Lena en couleur. Le tableau 33 présente la comparaison des valeurs des BER entre notre approche et d'autres approches sur l'image Lena en couleur.

Le tableau 34 présente la comparaison de la métrique NC entre notre approche et d'autres approches en utilisant l'image Lena en couleur.

Les avantages de l'approche présentée sont:

- La puissance de la théorie des ensembles approximatifs dans l'extraction des motifs cachés de l'image pour construire un système de tatouage de l'image couleur avec une haute imperceptibilité, une grande robustesse et une complexité computationnelle réduite.

- Les blocs de l'image choisis pour l'insertion de la marque ne sont pas fixes (le choix est variable en fonction de l'image).

- L'insertion se fait dans plusieurs blocs, ce qui donne une plus grande robustesse.

- Le tatouage de l'image est réalisé dans le domaine spatial, ce qui donne une complexité computationnelle réduite.

La limitation de cette approche est qu'elle ne s'applique qu'aux images couleurs.

La texture est une propriété importante de l'image représentée dans le domaine spatial ayant une relation significative avec le HVS. En analysant cette propriété, nous pouvons identifier des blocs significatifs visuellement dans l'image hôte susceptibles de recevoir la marque de tatouage avec moins de distorsions de la qualité visuelle et avec une grande robustesse. Les différentes caractéristiques qui sont habituellement utilisées pour analyser la texture ne permettent pas à elles seules d'affirmer si un bloc est texturé ou non texturé, parce qu'il n'existe pas une définition formelle précise de la texture. Il est difficile de préciser pour chaque caractéristique de la texture un niveau qui distingue les blocs texturés des blocs non-texturés de l'image hôte.

Pour la réalisation des systèmes de tatouage, le principe du HVS confirme que l'insertion de la marque dans les zones les plus texturées permet d'assurer une haute imperceptibilité et une haute robustesse. En effet, si la marque est insérée dans les blocs les plus texturés de l'image hôte, la modification provoquée par l'insertion de la marque est moins perceptible par l'œil humain qu'en cas d'insertion dans un bloc peu texturé. Les approches de découverte de connaissances et de l'intelligence artificielle peuvent être utilisées pour résoudre l'imprécision dans la définition des caractéristiques de l'image et les exploiter pour aboutir à un tatouage qui assure une bonne authentification de l'image.

La texture est un motif visuel complexe consistant en des pixels mutuellement liés qui donnent de l'information sur la couleur, la luminosité/obscurité, la surface de l'image et l'arrière plan de l'image. Toutes ces caractéristiques sont corrélées avec le HVS et peuvent être représentées en calculant certains paramètres statistiques de l'image tels que le coefficient DC, l'entropie, l'asymétrie de la fonction de distribution des pixels et l'aplatissement de cette fonction. L'étude de ces paramètres et des relations entre eux a aidé dans l'identification des zones les plus texturées de l'image hôte.

La méthode de décision multicritère (MCDM), l'analyse des concepts formels (FCA), l'analyse des motifs fréquents (Frequent Pattern Mining - FPM) et les règles d'association (Association Rules Mining-ARM) ont été utilisées pour l'analyse des paramètres de texture, dans le but d'améliorer les processus de tatouage.

L'approche MCDM réalise une classification de tous les blocs de pixels suivant le niveau de texture. Dans notre cas, la méthode TOPSIS associée à cette approche est utilisée pour la classification. A partir des valeurs obtenues pour chacune des caractéristiques de texture, elle définit un maximum idéal de texture et un minimum idéal de texture puis calcule la distance entre les différentes données à classer (vecteur donnant pour chaque bloc les valeurs des paramètres de texture) et le maximum idéal, ainsi que la distance entre ces données et le

minimum idéal, puis en déduit un coefficient de proximité par rapport au maximum idéal. Plus un bloc a un coefficient de proximité (du maximum idéal) élevé, plus il est considéré texturé. Les blocs les plus hauts dans cette hiérarchie sont significatifs pour recevoir la marque de tatouage.

La méthode MCDM peut aussi mesurer le degré d'importance de chaque caractéristique de la texture par rapport aux autres en comparant les résultats obtenus pour un certain nombre de jeux de données, en faisant varier le vecteur des poids (WV) qui affecte à chaque caractéristique un poids donné. Elle peut également être utilisée pour générer une clé (α) permettant le tatouage aveugle.

L'analyse des concepts formels est utilisée pour examiner la relation entre les caractéristiques de l'image et les blocs de pixels de l'image. Elle est utilisée pour trouver les blocs qui partagent un sous-ensemble commun de caractéristiques et pour trouver toutes les caractéristiques commune d'un ensemble quelconque de blocs. Le but est d'obtenir un ensemble de blocs significatifs visuellement qui sera, à son tour, utilisé pour l'insertion de la marque.

La méthode FPM détermine les caractéristiques les plus importantes qui apparaissent plus fréquemment (au dessus d'un seuil de fréquence fixé) ensemble dans l'image hôte. Ces caractéristiques forment un sous-modèle fréquent. Tous les blocs qui satisfont ce sous-modèle sont considérés comme fortement texturés et sont utilisés pour l'insertion de la marque.

La méthode ARM agit comme un niveau secondaire de FPM. Elle consiste à trouver les règles d'association les plus pertinentes construites à partir des sous-modèles les plus fréquents, en s'appuyant sur les mesures communément utilisées dans le domaine des règles d'associations, à savoir l'indice de support, l'indice de confiance et l'indice « lift ». L'avantage de l'extraction des relations entre les caractéristiques sélectionnées par les règles d'associations est l'amélioration de la robustesse grâce à une meilleure précision de la définition des blocs fortement texturés. En plus, la méthode ARM permet de générer deux paramètres secrets (l'indice de support et l'indice « lift ») qui permettent la mise en place d'un tatouage aveugle.

Le chapitre 6 introduit cinq approches de tatouage basées sur l'analyse de la texture par des techniques de l'intelligence artificielle.

La problématique de ce chapitre est présentée dans la section 6.2. Les notions d'analyse de la texture sont présentées dans la section 6.3. La section 6.4 montre comment le problème de la texture peut être analysé par l'approche MCDM de telle sorte que l'on obtienne les blocs les plus texturés de l'image hôte susceptibles de recevoir la marque avec une grande imperceptibilité, une grande robustesse, un grand taux d'insertion et une complexité computationnelle réduite. Le problème de l'identification des régions les plus texturées de l'image hôte est traité comme un problème de décision multicritères. Une partition en blocs de l'image hôte représente un ensemble d'alternatives à évaluer en utilisant

un ensemble de critères qui sont les caractéristiques de la texture. On construit une matrice de décision avec ces éléments et la méthode TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) est appliquée pour hiérarchiser toutes les alternatives et sélectionner la meilleure pour l'insertion de la marque.

Nous présentons deux approches de tatouage basées sur TOPSIS. La première est semi aveugle et la deuxième est aveugle. Les tests avec les métriques PSNR, mSSIM, NC et BER montrent que les approches proposées améliorent l'imperceptibilité et la robustesse. Le PSNR a atteint 56.8 dB et le mSSIM 0.99, tandis que le NC a atteint de 0.99 et la probabilité de restauration de l'image tatouée est supérieure à 93.4%. Le taux d'insertion est compris entre 0.75 et 8 (bpp). La complexité computationnelle globale est de $O(M \times N)$ et le temps d'exécution pour la première approche est de 8 secondes et pour la deuxième de 10 secondes.

La section 6.5 présente un modèle de tatouage basé sur l'analyse de la texture en utilisant l'analyse des concepts formels (FCA). La FCA est utilisée pour trouver une connaissance significative qui aide à une insertion efficace de la marque de tatouage. L'efficacité se mesure en termes d'imperceptibilité et de robustesse. Les concepts formels au sens de la FCA sont exploités pour extraire les blocs texturés en accord avec le HVS et susceptibles de recevoir la marque avec une faible dégradation de l'image originale et une grande robustesse.

Pour cette approche, les résultats obtenus au niveau des métriques PSNR, mSSIM, NC et BER montrent que l'approche améliore elle aussi l'imperceptibilité et la robustesse du processus. Le PSNR est compris entre 47.7 et 49.8 dB, la mSSIM entre 0.94 et 0.99, la NC atteint 0.99 et la probabilité de restauration de la marque originale est supérieure à 94.4%. Le taux d'insertion est compris entre 2.375 et 8 (bpp). La complexité computationnelle globale est de $O(M \times N \times d \times 2^k)$ et le temps d'exécution de 15 secondes.

La section 6.6 présente une approche de tatouage basée sur l'analyse de la texture en utilisant la méthode de la fouille des modèles fréquents (Frequent Pattern Mining - FPM). L'approche utilise quelques caractéristiques de l'image pour extraire les motifs les plus fréquents qui satisfont le support minimum. Les motifs les plus pertinents sont utilisés pour inférer de l'information sur les blocs texturés et les blocs lisses de l'image hôte. Les blocs texturés sont utilisés pour l'insertion de la marque.

Les résultats obtenus prouvent une amélioration de l'imperceptibilité et de la robustesse. Le PSNR est compris entre 48.5 et 50.7 dB et le mSSIM entre 0.95 et 0.99. Le NC atteint 0.99 et la probabilité de restauration de la marque est supérieure à 94.3%. Le taux d'insertion est compris entre 0.75 et 8 (bpp), la complexité computationnelle est de $O((M \times N) \times d^2)$ et le temps d'exécution de 8 secondes.

Dans la section 6.7, est présentée une approche de tatouage basée sur l'analyse de la texture utilisant les règles d'association (Association Rule Mining - ARM). Il s'agit toujours de l'identification des blocs les plus texturées de l'image hôte pour l'insertion de la marque de tatouage. Dans la solution proposée, les caractéristiques de la texture (DC, asymétrie, aplatissement et entropie) sont choisies comme données d'entrée pour construire les règles d'association. Ensuite, on applique l'algorithme Apriori pour fouiller les relations entre ces caractéristiques. La relation la plus significative entre les caractéristiques sélectionnées est utilisée pour identifier les blocs les plus texturés dans lesquels sera insérée la marque de tatouage. Deux paramètres appartenant au modèle des règles d'association, l'indice « lift » et l'indice de confiance sont utilisés pour construire un système de tatouage aveugle.

Les résultats des expérimentations ont montré que le PSNR est compris entre 47.48 et 50.38 dB, le mSSIM entre 0,97 et 1, le NC entre 0.83 et 0.99 et que la probabilité de restauration de la marque est supérieure à 94,7%. Le taux d'insertion est compris entre 0.75 et 8 (bpp), la complexité computationnelle est de $O((M \times N) \times d^2)$ et le temps d'exécution de 10 secondes.

Les résultats des approches présentées au chapitre 6 montrent qu'elles sont meilleures que d'autres présentées dans la littérature de spécialité en ce qui concerne l'imperceptibilité, la robustesse le temps d'exécution, la complexité computationnelle et le taux d'insertion.

Le tableau 54 présente une description sommaire comparative de plusieurs approches de tatouage.

La comparaison des approches basées sur MCDM, FCA, FPM et ARM avec d'autres approches de tatouage pour les images à plusieurs niveaux de gris est présentée dans le tableau 55.

Le tableau 56 présente les résultats comparatifs sur l'imperceptibilité en termes de PSNR sur l'image Lena en niveaux de gris.

Le tableau 57 présente les résultats de la métrique BER par comparaison entre nos approches MCDM, FCA, FMP, et ARM et d'autres approches sur l'image Lena en niveau de gris.

Finalement, le tableau 58 présente les résultats de la métrique NC par comparaison entre nos approches MCDM, FCA, FMP et ARM et d'autres approches sur l'image Lena en niveau de gris.

Nous avons testé aussi la sécurité de la clé publique utilisée dans les étapes d'insertion et d'extraction de certaines des approches que nous avons proposées et sa résistance contre l'attaque force brute. Les résultats montrent une résistance élevée de cette clé. Le problème des faux positifs a également été étudié pour évaluer si les solutions proposées satisfont les exigences de sécurité en matière de faux positifs. Les tests ont montré que les solutions proposées satisfont bien ces exigences.

La figure 56 présente quelques exemples de résultats de tests de faux positifs sur les approches proposées.

Les conclusions du chapitre se trouvent en section 6.10.

Les principaux avantages des approches proposées dans ce chapitre sont les suivants:

- Les approches proposées donnent une solution au problème d'imprécision de la texture, et permettent d'identifier les régions significatives dans l'image hôte pour l'insertion de la marque avec une imperceptibilité et une robustesse élevées.

- Les approches proposées insèrent la marque dans plusieurs blocs; la marque s'étend sur 20% de l'image hôte. Cela améliore la tenue de la marque contre les attaques géométriques.

- Les approches proposées insèrent la marque en utilisant le domaine spatial ce qui garantit une complexité computationnelle faible.

- La méthode TOPSIS fournit une solution pratique pour la mesure de l'importance de chaque caractéristique de la texture par l'utilisation de vecteurs poids.

- La méthode TOPSIS aide à générer un paramètre important pour le tatouage aveugle.

- L'application de la méthode de « règle d'association la plus significative » offre plusieurs avantages: Elle produit une meilleure sélection des blocs pour l'insertion de la marque après l'extraction des motifs les plus fréquents (l'application des règles d'association représente le deuxième niveau de fouille après l'application de la méthode de recherche des motifs les plus fréquents).

  Elle permet de définir un paramètre pour le tatouage aveugle. Elle permet de définir deux paramètres (l'indice « lift » et l'indice de confiance) qui peuvent être utilisés pour l'insertion et l'extraction avec comme objectif d'établir un équilibre entre l'imperceptibilité et la robustesse de la marque. Les valeurs de ces paramètres sont peu modifiées par les attaques.

Chapitre 7 : Conclusion et travaux futurs

Le travail présenté dans cette thèse contribue à assurer l'authentification de l'image en utilisant le tatouage dans le domaine spatial avec une haute imperceptibilité, une haute robustesse et une faible complexité computationnelle. Il a été réalisé suivant deux idées principales. La première idée est que l'extraction d'une caractéristique robuste de l'image hôte permet un tatouage zéro. La deuxième idée est que l'analyse des caractéristiques de l'image en corrélation avec le système visuel humain (HSV) permet d'identifier certaines connaissances cachées qui peuvent être utilisées pour l'identification des régions visuelles pertinentes pour l'insertion de la marque. L'insertion de la marque dans ces régions a un impact positif sur l'imperceptibilité, la robustesse et la complexité computationnelle.

Dans cette thèse, nous avons étudié la structure du fichier JPEG en rapport avec les caractéristiques de l'image. Nous avons extrait une caractéristique robuste de l'image JPEG et nous l'avons utilisée pour générer une marque de vérification dans le tatouage zéro. Nous avons aussi procédé à une étude des caractéristiques de l'image liées au Système Visuel Humain (HVS) pour construire des solutions de tatouage qui donnent plus de robustesse et d'imperceptibilité que les solutions existantes et qui prennent en compte les contraintes de temps indispensables au bon fonctionnement de certaines applications. La représentation couleur, la texture, la structure de la surface/arrière plan de l'image sont un ensemble de caractéristiques liées au HVS. Il n'y a pas de représentation standard précise de ces caractéristiques. Pourtant, elles jouent un rôle important dans la description des régions d'intérêt de l'image utilisées dans différentes applications. Par conséquent, la résolution de l'imprécision de ces caractéristiques et l'identification de l'importance de chacune d'entre elles, sont deux problèmes requérant une attention particulière.

Nous avons proposé plusieurs approches de tatouage basées sur l'analyse de caractéristiques visuelles de l'image et sur des techniques d'intelligence artificielles ou connexes. Ces dernières fournissent des moyens permettant de répondre aux deux problèmes susmentionnés.

Les solutions proposées ont été analysées du point de vue de l'imperceptibilité, de la robustesse et de la performance temporelle et les résultats d'analyses ont montré qu'elles apportent des améliorations significatives par rapport aux approches existantes.

Travail futur

Le travail présenté dans cette thèse a abordé des problèmes portant sur l'authentification de l'image basée sur le tatouage avec une haute imperceptibilité, une grande robustesse et une faible complexité computationnelle. Nous envisageons de pour-

suivre ces travaux par l'étude de solutions permettant de s'affranchir de certaines limitations rencontrées.

En ce qui concerne le travail présenté au chapitre 4, notre objectif suivant est d'utiliser deux paramètres (l'indice de « lift » et l'indice de confiance) de la règle d'association la plus pertinente pour générer la marque de vérification. L'idée est de diminuer l'impact négatif de la clé utilisée dans la construction de la marque afin d'obtenir une meilleure robustesse. En effet, la marque générée à partir de la matrice jacobienne dépend de la valeur de la clé extraite de l'image hôte.

Nous envisageons également l'étude de deux problèmes majeurs en relation avec les aspects abordés au chapitre 5. Il s'agit de: La prise en compte des relations d'équivalences floues et, L'étude de la relation d'ordre de préférence de l'information.

Ces 2 problèmes seront étudiés dans le cadre de la théorie des ensembles flous (fuzzy) et des ensembles approximatifs (rough sets). Le flou dans les ensembles approximatifs et le classement multicritère basé sur la théorie des ensembles approximatifs sont des problèmes ouverts qui sont en relation directe avec les problématiques relatives à modélisation de l'ambiguïté et de l'incertitude des données et paramètres caractéristiques de l'image. Dans le cadre de la conception des systèmes de tatouage, ces problèmes peuvent être étudiés afin de trouver d'autres moyens permettant de réduire significativement l'effet de l'ambiguïté et de l'incertitude sur la qualité perceptuelle de l'image et sur la robustesse contre différentes attaques.

Pour ce qui est des directions de recherche futures liées au chapitre 6, nous envisageons d'étudier d'autres méthodes et modèles de l'intelligence artificielle et de découverte de la connaissance pour l'analyse de la texture dans le but d'évaluer leurs éventuels bénéfices pour l'amélioration globale du processus de tatouage.

Une autre perspective est l'implémentation et l'expérimentation des approches proposées sur des réseaux sans fils.

BIBLIOGRAPHY

[1] Assem Mahmoud Abdelhakim, Hassan Ibrahim Saleh, and Amin Mohamed Nassar. A quality guaranteed robust image watermarking optimization with Artificial Bee Colony. *Expert Systems With Applications*, 72: 317–326, 2017.

[2] Jobin Abraham and Varghese Paul. An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University-Computer and Information Sciences*, pages 95–105, 2017.

[3] Radhakrishna Achanta, Francisco Estrada, Patricia Wils, , and Sabine Susstrunk. *Salient Region Detection and Segmentation*, volume 5008. Springer, Berlin, Heidelberg, 2008.

[4] Charu C. Aggarwal and Jiawei Han. *Frequent Pattern Mining*. Springer International Publishing, 2014.

[5] Faris Alqadah and Raj Bhatnagar. Similarity measures in formal concept analysis. *Annals of Mathematics and Artificial Intelligence*, 61(3):245–256, 2011.

[6] Jesus Angulo. Geometric algebra colour image representations and derived total orderings for morphological operators-part i: Colour quaternions. *Journal of Visual Communication and Image Representation*, 21(1):33–48, 2010.

[7] Veysel Aslantas. An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282: 769–777, 2009.

[8] Juan Pablo Balarini and Sergio Nesmachnow. A c++ implementation of otsu's image segmentation method. *Image Processing On Line*, 6:155–164, 2016.

[9] Valentina Balas, Janos Fodor, Annamária Várkonyi-Kóczy, Joszef Dombi, and Lakhmi Jain. *Soft computing applications*, volume 195. Springer, Berlin, Heidelberg, 2013.

[10] Herbert Bay, Tinne Tuytelaars, and Luc Van Gool. Surf: Speeded up robust features. *Computer Vision and Image Understanding*, 110(3):346–359, 2008.

[11] Riadh Ben-Messaoud, Omar Boussaid, and Sabine Loudcher Rabaseda. Mining association rules in OLAP cubes. In *Proceedings of Innovations in Information Technology*, pages 1–5. IEEE, 2006.

[12] Tobias Blickle and Lothar Thiele. A comparison of selection schemes used in genetic algorithms. Technical report, Computer Engineering and Communication Networks Lab, 1995.

[13] Dalel Bouslimi and Gouenou Coatrieux. A crypto-watermarking system for ensuring reliability control and traceability of medical images. *Signal Processing: Image Communication*, 47:160–169, 2016.

[14] ITU-R Recommendation BT-601-5. Studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios. Technical report, International Telecommunication Union (ITU), 1994.

[15] Emmanuel Candes, Laurent Demanet, David Donoho, and Lexing Ying. Fast discrete curvelet transforms. *Multiscale Modeling & Simulation*, 5(3): 861–899, 2006.

[16] Narasimham Challa and Jayaram Pradhan. Performance analysis of public key cryptographic systems RSA and NTRU. *International Journal of Computer Science and Network Security*, 7(8):87–96, 2007.

[17] Shiv Chandrasekaran, Ming Gu, Jianlin Xia, and Jiang Zhu. *A Fast QR Algorithm for Companion Matrices*, volume 179. Springer, Birkhäuser Basel, 2007.

[18] Brian Chen and Gregory W Wornel. Dither modulation: a new approach to digital watermarking and information embedding. In *Proceedings of Security and Watermarking of Multimedia Contents*, volume 3657, pages 342–353. SPIE, 1999.

[19] Tzung-Her Chen, Gwoboa Horng, and Wei-Bin Lee. A publicly verifiable copyright-proving scheme resistant to malicious attacks. *IEEE Transactions on Industrial Electronics*, 52(1):327–334, 2005.

[20] I.J. Cox, M.L. Miller, and J.A. Bloom. Watermarking applications and their properties. In *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC)*, pages 6–10. IEEE, 2000.

[21] San Cristobal and Jose Ramon. *Multi Criteria Analysis in the Renewable Energy Industry*. Springer-Verlag London, 2012.

[22] Apurba Das. *Image enhancement in spatial domain*. Springer, Cham, 2015.

[23] Satchidananda Dehuri, Susmita Ghosh, and Cho Sung-Bae. *Integration of Swarm Intelligence and Artificial Neural Network*. World Scientific, 2011.

[24] Youcef Djenouri and Marco Comuzzi. Combining apriori heuristic and bio-inspired algorithms for solving the frequent itemsets mining problem. *Information Sciences*, 420:1–15, 2017.

[25] Jiangtao Dong and Jingbing Li. A robust zero-watermarking algorithm for encrypted medical images in the dwt-dft encrypted domain. In *In: Chen YW., Tanaka S., Howlett R., Jain L. (eds) Innovation in Medicine and Healthcare (InMed). Smart Innovation, Systems and Technologies*, volume 60, pages 197–208. Springer, 2016.

[26] Paulo Drews, Rodrigo de Bem, and Alexandre de Melo. Analyzing and exploring feature detectors in images. In *In Proceedings of the 9th International Conference on Industrial Informatics*, pages 305–310. IEEE, 2011.

[27] Alaa Eleyan and Hasan Demirel. Co-occurrence matrix and its statistical features as a new approach for face recognition. *Turkish Journal of Electrical Engineering and Computer Sciences*, 19(1):97–107, 2011.

[28] Tarek Elgamal and Mohamed Hefeeda. Analysis of PCA algorithms in distributed environments. Technical report, Qatar Computing Research Institute, 2015.

[29] Ephzibah E.P. Time complexity analysis of genetic- fuzzy system for disease diagnosis. *Advanced Computing: An International Journal*, 2(4):23–31, 2011.

[30] Chun-Sung Ferng and Hsuan-Tien Lin. Multi-label classification with error-correcting codes. *Journal of Machine Learning Research*, 20:1–15, 2011.

[31] G. David Forney and Alexander Vardy. Generalized minimum-distance decoding of euclidean-space codes and lattices. *IEEE TRANSACTIONS ON INFORMATION THEORY*, 42(6):1992–2026, 1996.

[32] Guangyong Gao. Composite chaos-based lossless image authentication and tamper localization. *Pattern Recognition*, 63(3):947–964, 2013.

[33] Guangyong Gao and Guoping Jiang. Bessel-fourier moment-based robust image zero-watermarking. *Multimedia Tools and Applications*, 74(3):841–858, 2015.

[34] Musab Ghadi, Lamri Laouamer, Laurent Nana, and Anca Pascu. JPEG bitstream based integrity with lightweight complexity of medical image in wmsns environment. In *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems*, pages 53–58. ACM, 2015.

[35] Musab Ghadi, Lamri Laouamer, and Tarek Moulahi. Securing data exchange in wireless multimedia sensor networks: perspectives and challenges. *Multimedia Tools and Applications*, 75(6):3425–3451, 2016.

[36] Henry G.R. Gouk. *Accelerating Convolutional Neural Network Systems*. PhD thesis, University of Waikato, 2014.

[37] Serge Guillaume and Brigitte Charnomordic. Learning interpretable fuzzy inference systems with FisPro. *Information Sciences*, 181(20):4409–4427, 2011.

[38] Michael Hahsler and Chelluboina Sudheer. Visualizing association rules: Introduction to the R-extension package arulesViz. Technical report, Southern Methodist University, 2015.

[39] Jialing Han, Xiaohui Zhao, and Chunyan Qiu. A digital image watermarking method based on host image analysis and genetic algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 7(1):37–45, 2016.

[40] Aboul-Ella Hassanien, Ajith Abraham, Janusz Kacprzyk, and James Peters. *Computational intelligence in multimedia processing: foundation and trends*, volume 96. Springer, Berlin, Heidelberg, 2008.

[41] Markus Hegland. The apriori algorithm–a tutorial. *Mathematics and Computation in Imaging Science and Information Processing*, 11:209–262, 2005.

[42] Ling-Yuan Hsu and Hwai-Tsu Hu. Blind image watermarking via exploitation of inter-block prediction and visibility threshold in DCT domain. *Journal of Visual Communication and Image Representation*, 32:130–143, 2015.

[43] Ling-Yuan Hsu and Hwai-Tsu Hu. Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. *Journal of Visual Communication and Image Representation*, 46:33–47, 2017.

[44] Hwai-Tsu Hu and Ling-Yuan Hsu. A mixed modulation scheme for blind image watermarking. *International Journal of Electronics and Communications (AEÜ)*, 70:172–178, 2016.

[45] Ching-Lai Hwang and Kwangsun Yoon. *Multi attribute Decision Making: Methods and Applications A State-of-the-Art Survey*. Springer-Verlag Berlin Heidelberg, 1981.

[46] The igraph core team. Igraph reference manual for using the igraph C library. http://igraph.org/c/doc/igraph-Random.html, 2015. Online; accessed 19 February 2018.

[47] B. Jagadeesh, P. Rajesh Kumar, and P. Chenna Reddy. Fuzzy inference system based robust digital image watermarking technique using discrete cosine transform. *Procedia Computer Science*, 46:1618–1625, 2015.

[48] B. Jagadeesh, P. Rajesh Kumar, and P. Chenna Reddy. Robust digital image watermarking based on fuzzy inference system and back propagation neural networks using DCT. *Soft Computing*, 20(9):3679–3686, 2016.

[49] Viktor Jovanoski and Nada Lavrač. *Classification Rule Learning with APRIORI-C*, volume 2258. Springer, Berlin, Heidelberg, 2001.

[50] Rezvan Karimi, Fakhri Yousefi, Mehrorang Ghaedi, and Kheibar Dashtian. Back propagation artificial neural network and central composite design modeling of operational parameter impact for sunset yellow and azur (II) adsorption onto MWCNT and MWCNT-Pd-NPs: Isotherm and kinetic study. *Chemometrics and Intelligent Laboratory Systems*, 159:127–137, 2016.

[51] Christof Kauba and Andreas Uhl. Robustness evaluation of hand vein recognition systems. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–5, 2015.

[52] Mehdi Khalili. Dct-arnold chaotic based watermarking using jpeg-ycbcr. *Optik-International Journal for Light and Electron Optics*, 126:4367–4371, 2015.

[53] Mehdi Khalili. DCT-Arnold chaotic based watermarking using JPEG-YCbCr. *Optik-International Journal for Light and Electron Optics*, 126(23):4367–4371, 2015.

[54] Flip Korn, Alexandros Labrinidis, Yannis Kotidis, and Christos Faloutsos. Ratio rules:a new paradigm for fast, quantifiable data mining. In *Proceedings of the 24^{th} International Conference on Very Large Data Bases*, pages 1–12. Morgan Kaufmann Publishers Inc., 1998.

[55] Aleksey Koval, Y.Frank Shih, and Verkhovsky S.Boris. A pseudo-random pixel rearrangement algorithm based on gaussian integers for image watermarking. *Journal of Information Hiding and Multimedia Signal Processing*, 2(1):60–70, 2011.

[56] Robert Krauthgamer, Joseph Naor, Roy Schwartz, and Kunal Talwar. Non-uniform graph partitioning. In *In Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 1229–1243. ACM, 2014.

[57] B.Santhosh Kumar and K.V. Rukmani. Implementation of web usage mining using APRIORI and FP growth algorithms. *International Journal of Advanced Networking and Applications*, 1(6):400–404, 2010.

[58] Shishir Kumar, Neha Jain, and Steven Fernandes. Rough set based effective technique of image watermarking. *Journal of Computational Science*, 19:121–137, 2017.

[59] Chih-Chin Lai. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing*, 21(4): 522–527, 2011.

[60] Chih-Chin Lai. An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, 284(4):938–944, 2011.

[61] Guo Lihua and Zhang Yuanjian. Robust watermark using the auxiliary information. In *Proceedings of the International Conference on Communications, Circuits and Systems*, volume 1, pages 6–10. IEEE, 2006.

[62] Yang Liu, Shanyu Tang, Ran Liu, Liping Zhang, and Zhao Ma. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems With Applications*, 97:95–105, 2018.

[63] Fabrizio Maria Maggi, Claudio Di Ciccio, Chiara Di Francescomarino, and Taavi Kala. Parallel algorithms for the automated discovery of declarative process models. *Information Sciences*, 74(2):136–152, 2018.

[64] Aditi Majumder and Sandy Irani. Contrast enhancement of images using human contrast sensitivity. In *Proceedings of the 3rd symposium on Applied perception in graphics and visualization*, pages 69–76. ACM, 2006.

[65] N.J.Z. Mamat and J.K. Daniel. Statistical analyses on time complexity and rank consistency between singular value decomposition and the duality approach in ahp: A case study of faculty member selection. *Mathematical and Computer Modelling*, 46(7-8):1099–1106, 2007.

[66] Andrzej Materka and Michal Strzelecki. Texture analysis methods-a review. Technical report, Technical university of Lodz, institute of electronics, COST B11 Report, Brussels, 1998.

[67] Makoto Matsumoto and Takuji Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation*, 8(1):3–30, 1998.

[68] Amit Mehto and Neelesh Mehra. Adaptive lossless medical image watermarking algorithm based on dct & dwt. *Procedia Computer Science*, 78: 88–94, 2016.

[69] Mohammad Moosazadeh and Gholamhossein Ekbatanifard. An improved robust image watermarking method using DCT and YCoCg-R color space. *International Journal for Light and Electron Optics (Optik)*, 140:975–988, 2017.

[70] Benjamin Muller, Martin Holters, and Udo Zolzer. Low complexity soft-input soft-output hamming decoder. In *Proceedings of the 50th FITCE Congress -"ICT: Bridging an Ever Shifting Digital Divide" (FITCE)*, pages 1–5. IEEE, 2011.

[71] Moni Naory and Moti Yungz. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing (STOC)*, pages 33–43. ACM, 1989.

[72] Athanasios Nikolaidis and Ioannis Pitas. Asymptotically optimal detection for additive watermarking in the DCT and DWT domains. *IEEE TRANSACTIONS ON IMAGE PROCESSING*, 12(5):363–571, 2003.

[73] Chao-Yang Pang and Ben-Qiong Hu. Quantum discrete fourier transform with classical output for signal processing. *Quantum Physics*, pages 1–11, 2007.

[74] Chao-Yang Pang, Zheng-Wei Zhou, and Guang-Can Guo. Quantum discrete cosine transform for image compression. *Quantum Physics*, pages 1–30, 2006.

[75] G. A. Papakostas, E. D. Tsougenis, and D. E. Koulouriotis. Fuzzy knowledge-based adaptive image watermarking by the method of moments. *Complex & Intelligent Systems*, 2(3):205–220, 2016.

[76] G.A. Papakostas, Y.S. Boutalis, D.A. Karras, and B.G. Mertzios. Fast numerically stable computation of orthogonal Fourier-Mellin moments. *IET Computer Vision*, 1(1):11–16, 2007.

[77] A.Shabir Parah, A.Javaid Sheikh, Farhana Ahad, A.Nazir Loan, and Bhat M.G. Information hiding in medical images: a robust medical image watermarking system for e-healthcare. *Multimedia Tools and Applications*, 76 (8):10599–10633, 2017.

[78] Shabir A. Parah, Javaid A. Sheikh, Nazir A. Loan, and Ghulam M. Bhat. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digital Signal Processing*, 53:11–24, 2016.

[79] Zdzisław Pawlak. Rough sets. *International Journal of Computer and Information Sciences*, 11(5):341–356, 1982.

[80] Fabien Petitcolas, Ross Anderson, , and Markus Kuhn. Attacks on copyright marking systems. In *David Aucsmith, Ed., Second workshop on information hiding*, volume 1525, pages 218–238. Springer, 1998.

[81] Jonas Poelmans, Paul Elzinga, Stijn Viaene, and Guido Dedene. *Formal concept analysis in knowledge discovery: a survey*, volume 6208. Springer, Berlin, Heidelberg, 2010.

[82] Asaad F. Qasim, Farid Meziane, and Rob Aspin. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, 27:45–60, 2018.

[83] Min Qi, Bing-Zhao Li, and Huafei Sun. Image watermarking via fractional polar harmonic transforms. *Journal of Electronic Imaging*, 24(1):13004–13015, 2015.

[84] Chuan Qin, Zhihong He, Heng Yao, Fang Cao, and Liping Gao. Visible watermark removal scheme based on reversible data hiding and image inpainting. *Signal Processing: Image Communication*, 60:160–172, 2018.

[85] Luc De Raedt and Albrecht Zimmermann. Constraint-based pattern set mining. In *Proceedings of the 7$^{\text{th}}$ SIAM International Conference on Data Mining*, pages 237–248. SIAM, 2007.

[86] Asha Rani, Amandeep Bhullar, Deepak Dangwal, and Sanjeev Kumar. A zero-watermarking scheme using discrete wavelet transform. In *4$^{\text{th}}$ International Conference on Eco-friendly Computing and Communication Systems (ICECCS), Procedia Computer Science*, volume 70, pages 603–609. Elsevier, 2015.

[87] Mohamad Rostamim, Abbas Shahba, Saeid Saryazdi, and Hossein Nezamabadi-pour. A novel parallel image encryption with chaotic windows based on logistic map. *Computers and Electrical Engineering*, 62:384–400, 2017.

[88] Soumitra Roy and Arup Kumar Pal. A blind DCT based color watermarking algorithm for embedding multiple watermarks. *International Journal of Electronics and Communications (AEÜ)*, 72:149–161, 2017.

[89] R. W. Saaty. The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, 9(3–5):161–176, 1987.

[90] Nitin Saxena, K.K. Mishra, and Ashish Tripathi. *DWT-SVD-Based Color Image Watermarking Using Dynamic-PSO*, volume 554. Springer, Singapore, 2018.

[91] Bino Sebastian V, A. Unnikrishnan, and Kannan Balakrishnan. Grey level co-occurrence matrices: Generalisation and some new features. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, 2(2):151–157, 2012.

[92] Priya Selvam, Santhi Balachandran, Swaminathan Pitchai Iyer, and Rajamohan Jayabal. Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. *Optik-International Journal for Light and Electron Optics*, 145:655–671, 2017.

[93] Debashis Sen and Sankar Pal. Generalized rough sets, entropy, and image ambiguity measures. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 39(1):117–128, 2009.

[94] Zhangle Shen and kintak U. A novel image zero-watermarking scheme based on non-uniform rectangular. In *International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, pages 78–82. IEEE, 2017.

[95] Abhilasha Singh and Malay Dutta. A robust zero-watermarking scheme for tele-ophthalmological applications. *Journal of King Saud University-Computer and Information Sciences*, pages 1–14, 2017.

[96] Amit Singh, Basant Kumar, Mayank Dave, and Anand Mohan. Multiple watermarking on medical images using selective discrete wavelet transform coefficients. *Journal of Medical Imaging and Health Informatics*, 5(3): 607–614, 2015.

[97] Qingtang Su and Beijing Chen. Robust color image watermarking technique in the spatial domain. *Soft Computing*, 22(1):91–106, 2017.

[98] Qingtang Su and Beijing Chen. A novel blind color image watermarking using upper Hessenberg matrix. *International Journal of Electronics and Communications (AEÜ)*, 78:64–71, 2017.

[99] Ramadass Sudhir. A survey on image mining techniques: Theory and applications. *International Journal of Computer Engineering and Intelligent Systems*, 2(6):44–52, 2011.

[100] Kin Tak, Zesheng Tang, and Dongxu Qi. A non-uniform rectangular partition coding of digital image and its application. In *International Conference on Information and Automation (ICIA)*, pages 995–999. IEEE, 2009.

[101] U Kin Tak, Zesheng Tang, and Dongxu Qi. A non-uniform rectangular partition coding of digital image and its application. In *In Proceedings of International Conference on Information and Automation*, pages 995–999. ACM, 2009,.

[102] Pang-Ning Tan, Michael Steinbach, Anuj Karpatne, and Vipin Kumar. *Introduction to Data Mining*. Pearson Inc, USA, 2005.

[103] David Taniar. *Data Mining and Knowledge Discovery Technologies*. IGI Global, 2008.

[104] International Telegraph and Telephone Consultative Committee. Information technology-digital compression and coding of continuous-tone still images–requirements and guidelines. Technical report, International Telecommunication Union, 1993.

[105] Rasha Thabit and Bee Ee Khoo. A new robust lossless data hiding scheme and its application to color medical images. *Digital Signal Processing*, 38: 77–94, 2015.

[106] Falgun Thakkar and Vinay Srivastava. A blind medical image watermarking: Dwt-svd based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, 76(3):3669–3697, 2017.

[107] Rohit Thanki, Surekha Borra, Vedvyas Dwivedi, and Komal Borisagar. An efficient medical image watermarking scheme based on FDCuT–DCT. *Engineering Science and Technology, an International Journal*, 20(4):1366–1379, 2017.

[108] Rohit Thanki, Surekha Borra, Vedvyas Dwivedi, and Komal Borisagar. An efficient medical image watermarking scheme based on fdcut–dct. *Engineering Science and Technology, an International Journal*, 20:1366–1379, 2017.

[109] Yongxin Tong, Lei Chen, Yurong Cheng, and Philip S. Yu. Mining frequent itemsets over uncertain databases. In *Proceedings of the 38$^{\text{th}}$ International Conference on Very Large Data Bases*, volume 5, pages 1650–1661. ACM, 2012.

[110] Joseph D. Touch. Performance analysis of md5. In *International Conference on Applications, technologies, architectures, and protocols for computer communication (SIGCOMM)*, pages 77–86. ACM, 1995.

[111] Min-Jen Tsai. A visible watermarking algorithm based on the content and contrast aware (COCOA) technique. *Journal of Visual Communication and Image Representation*, 20:323–338, 2009.

[112] Scott E Umbaugh. *Digital image processing and analysis: human and computer vision applications with CIVP tools*. CRC Press, 2010.

[113] Alarcon-Aquino Vicente, Oleg Starostenko, Roberto Rosas-Romero, J Rodriguez-Asomoza, Otto Joel Paz-Luna, K Vazquez-Muñoz, and Leticia Flores-Pulido. Mammographic image analysis for breast cancer detection using complex wavelet transforms and morphological operators. In *Proceedings of the International Conference on Signal Processing and Multimedia Applications*, pages 79–85, 2009.

[114] Chun-peng Wang, Xing-yuan Wang, Xia Zhi-qiu, Zhang Chuan, and Chen Xing-jun. Geometrically resilient color image zero-watermarking algorithm based on quaternion exponent moments. *J. Vis. Commun. Image R.*, 41:247–259, 2016.

[115] Chun-peng Wang, Xing-yuan Wang, Xing-jun Chen, and Chuan Zhang. Robust zero-watermarking algorithm based on polar complex exponential

transform and logistic mapping. *Multimedia Tools and Applications*, 76(24): 26355–26376, 2017.

[116] Chunpeng Wang, Xingyuan Wang, Chuan Zhang, and Zhiqiu Xia. Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution. *Signal Processing*, 134:197–208, 2017.

[117] Feng-Hsing Wang, Jeng-Shyang Pan, and Lakhmi Jain. *Spatial-based watermarking schemes and pixel selection*, volume 232. Springer, Berlin, Heidelberg, 2009.

[118] Xiang-Yang Wang, Zhi-Fang Wu, Liang Chen, Hong-Liang Zheng, and Hong-Ying Yang. Pixel classification based color image segmentation using quaternion exponent moments. *Neural Networks*, 74:1–13, 2016.

[119] Xingyuan Wang and Chuanming Liu. A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimedia Tools and Applications*, 76(5):6229–6245, 2017.

[120] Zhou Wang, Alan C. Bovik, and Hamid R. Sheikh. *Structural Similarity Based Image Quality Assessment*. CRC Press, USA, 2005.

[121] Zhang Wenyin and Frank Y. Shih. Semi-fragile spatial watermarking based on local binary pattern operators. *Optics Communications*, 284:3904–3912, 2011.

[122] Yi-Leh Wu, Divyakant Agrawal, and Amr El Abbadi. A comparison of dft and dwt based similarity search in time-series databases. In *Proceedings of the ninth international conference on Information and knowledge management*, pages 488–495. ACM, 2000.

[123] Bin Xiao, Jian-Feng Ma, and Xuan Wang. Image analysis by bessel–fourier moments. *Pattern Recognition*, 43(8):2620–2629, 2010.

[124] Wang Xiaohong and Zhao Rongchun. A new method for image normalization. In *International Symposium on Intelligent Multimedia, Video and Speech Processing (ISIMP)*, pages 356–359. IEEE, 2001.

[125] Dong Xin, Hong Cheng, Xifeng Yan, and Jiawei Han. Extracting redundancy aware top-K patterns. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 444–453. ACM, 2006.

[126] Jing-Hao Xue and D. Michael Titterington. T-test, f-tests and otsu's methods for image thresholding. *IEEE Transactions on Image Processing*, 20(8): 2392–2396, 2011.

[127] Hengfu Yang and Jianping Yin. A secure removable visible watermarking for BTC compressed images. *Multimedia Tools and Applications*, 74(6):1725–1739, 2015.

[128] Y.Y. Yao. A comparative study of fuzzy sets and rough sets. *Information Sciences*, 109:227–242, 1998.

[129] Serhiy A. Yevtushenko. System of data analysis "concept explorer". In *Proceedings of the 7th national conference on Artificial Intelligence*, pages 127–134, 2000.

[130] Lotfi A Zadeh, George J Klir, and Bo Yuan. *Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems*. World Scientific Publishing, 1996.

[131] Khalil Zebbiche, Fouad Khelifi, and Khaled Loukhaoukha. Robust additive watermarking in the DTCWT domain based on perceptual masking. *Multimedia Tools and Applications*, pages 1–24, 2018.

[132] Qinghua Zhang, Qin Xie, and Guoyin Wang. A survey on rough set theory and its applications. *CAAI Transactions on Intelligence Technology*, 1(4):323–333, 2016.

[133] Yanping Zhang, Juan Jiang, Yongliang Zha, Heng Zhang, and Shu Zhao. Research on embedding capacity and efficiency of information hiding based on digital images. *International Journal of Intelligence Science*, 3(2): 77–85, 2013.

[134] Yubo Zhang, Hongbo Bi, Baoquan Zhu, and Bo Dong. An improved ica-based digital watermarking. *International Journal on Advances in Information Sciences and Service Sciences*, 4:167–174, 2012.

[135] Yaxun Zhou and Wei Jin. A novel image zero-watermarking scheme based on DWT-SVD. In *International Conference on Multimedia Technology*, pages 2873–2876. IEEE, 2011.

[136] Guibin Zhu, Bin Lei, Peng Quan, and Jiu Zhi Ye. Quasi-affine transform over limited integer grids and its application. In *Proceedings of the Third International Symposium on Information Science and Engineering*, pages 184–187. IEEE, 2010.

[137] Hegui Zhu, Xiangde Zhang, Hai Yu, Cheng Zhao, and Zhiliang Zhu. A novel image encryption scheme using the composite discrete chaotic system. *Entropy*, 18(276):1–27, 2016.

UNIVERSITE BRETAGNE LOIRE / MATHSTIC

UBO
Université de Bretagne Occidentale

Titre : Approches de tatouage pour l'authentification de l'image dans des applications à contraintes temporelles

Mots clés : tatouage de l'image, authentification, caractéristiques visuelles, techniques intelligentes, contraintes temporelles

Résumé : Dans de nombreuses applications dont celles du domaine médical et de l'embarqué, l'authentification des images nécessite de prendre en compte les contraintes temporelles, le taux d'insertion, la qualité visuelle et la robustesse contre différentes attaques. Le tatouage a été proposé comme approche complémentaire à la cryptographie pour l'amélioration de la sécurité des images. Il peut être effectué soit dans le domaine spatial sur les pixels de l'image, soit dans le domaine fréquentiel sur les coefficients de sa transformée. Dans cette thèse, le but est de proposer des approches de tatouage permettant d'assurer un niveau élevé d'imperceptibilité et de robustesse, tout en maintenant un niveau de complexité répondant aux exigences d'applications soumises à des contraintes temporelles. La démarche adoptée a consisté, d'une part, à s'appuyer sur les bénéfices du zéro-tatouage (zero-watermarking) qui ne change pas la qualité perceptuelle de l'image et qui a une faible complexité computationnelle, et d'autre part, à analyser les caractéristiques visuelles de l'image afin de détecter les zones les plus adaptées pour insérer la marque avec un bon niveau d'imperceptibilité et une bonne robustesse. Une approche de zéro-tatouage a ainsi été proposée dans cette thèse, ainsi que plusieurs approches de tatouage basées sur l'analyse de caractéristiques visuelles de l'image et sur des techniques d'intelligence artificielles ou connexes. Les solutions proposées ont été analysées du point de vue de l'imperceptibilité, de la robustesse et de la performance temporelle et les résultats d'analyses ont montré qu'elles apportent des améliorations significatives par rapport aux approches existantes.

Title : Watermarking approaches for images authentication in applications with time constraints

Keywords : Image watermarking, authentication, visual characteristics, intelligent techniques, time constraints

Abstract: In numerous applications such as those of medical and embedded domains, images authentication requires taking into account time constraints, embedding rate, perceptual quality and robustness against various attacks. Watermarking has been proposed as a complementary approach to cryptography, for improving the security of digital images. Watermarking can be applied either in the spatial domain on the pixels of the image, or in the frequency domain on the coefficient of its transform. In this thesis, the goal is to propose image watermarking approaches that make it possible to ensure high level of imperceptibility and robustness while maintaining a level of computational complexity fitting the requirements of time-constrained applications. The method adopted in this thesis has consisted, on the one hand, to rely on the benefit of zero-watermarking that does not degrade the perceptual quality of image data and has low computational complexity, and on the other hand, to analyze visual characteristics of digital image (characteristics that are correlated to the Human Visual System - HVS) in order to identify the locations the most adapted for embedding the watermark with good level of imperceptibility and robustness. A zero-watermarking has therefore been proposed in this thesis, as well as several watermarking approaches based on the analysis of visual characteristics of image and on artificial intelligence or related techniques. The proposed solutions have been analyzed with respect to imperceptibility, robustness and temporal performance and the results have shown significant improvements in comparison to existing approaches.