Développement d'une technique robuste du tatouage des images aux attaques print-cam

Khadija Gourrame

Université d'Orléans

École doctorale Mathématiques, Informatique, Physique Théorique et Ingénierie des Systèmes (MIPTIS)
Laboratoire PRISME
Pôle IRAuS, Axe Image et Vision

Université Ibn Zohr

Faculté des Sciences d'Agadir
Centre des Etudes Doctorales IBN ZOHR
Laboratoire IRF-SIC

THÈSE EN COTUTELLE INTERNATIONALE présentée par

Khadija GOURRAME

Soutenue le **21 décembre 2019 à l'Université Ibn Zohr**

Pour obtenir le grade de **Docteur de l'Université d'Orléans et de l'Université Ibn Zohr**

Discipline / Spécialité : **Sciences et technologies industrielles Mathématiques Informatique**

DEVELOPMENT OF ROBUST IMAGE WATERMARKING TECHNIQUE UNDER PRINT-CAM ATTACKS

THÈSE dirigée par :

DOUZI Hassan	Professeur, Université Ibn Zohr
HARBA Rachid	Professeur, Université d'Orléans

RAPPORTEURS :

BOUDRAA Abdel	Professeur, Ecole Navale de Brest
AMEUR El Bachir	Professeur Habilité, Université Ibn Tofail

EXAMINATEUR (président du jury) :

MAMMAS Driss	Professeur, Université Ibn Zohr

Acknowledgements

At first, I would like to express my deepest gratitude to my supervisors Dr.Hassan Douzi professor at University of Ibn Zohr in Morocco, and Dr.Rachid Harba professor at Orléans University in France for creating this opportunity to study exiting and fascinating research field in image processing. I am very thankful for their continued support from the beginning and valuable guidance throughout the research work to improve the quality of this thesis. As well, for the research collaboration they made possible.

I would like to express my sincere appreciation to the jury members starting with jury president Dr. Driss Mammass professor at University of Ibn Zohr in Morocco. I would like to deeply thank Dr. Boudraa Abdel professor at Brest Naval institution in France and Dr.Youssef Es-Saadi professor at University of Ibn Zohr in Morcco for accepting reviewing this work and for their valuable time dedicated to read this thesis report..

My gratitude also has to be expressed to Dr. Frederic Ros HDR associate researcher at Orléans University in France, Dr. Mohamed El Hajji professor at Regional center of professional education and training in Morocco, Dr. Rabia Riad associate professor at University of Ibn Zohr in Morocco for their continuous encouragement, support, great help, patience, valuable discussions, dedicated time, excellent suggestions and constructive advices during the progress of my PhD research.

I would like to thank my friends and colleagues in IRF-SIC lab in Morocco and in PRISME lab in France for their support and fruitful discussions and feedback on different aspects of my PhD journey. I would like also to thank all my friends who helped and guided me until I completed my research.

Finally, unlimited thanks go to my source of strength and faith, my mother for her unconditional love, everlasting support and persistent encouragement. To my sisters Nezha and Assia for their enormous love, support and understanding throughout different journeys in my life.

Résumé

Le tatouage d'images numériques consiste à y insérer une marque d'une manière invisible à l'œil humain, cette marque pouvant être détectée par un algorithme de traitement d'image. Cela sert entre autre à établir la propriété de ce document numérique. Le but de cette thèse est de proposer une technique de tatouage d'image lorsque celle-ci est imprimée sur un support physique puis numérisée à main levée avec la caméra d'un smartphone. Cela permettra de proposer de nouvelles applications nomades de tatouage, comme par exemple le contrôle mobile de documents officiels contenant une photo d'identité (ID) que nous souhaitons développer. Dans ce cas, la marque doit résister aux attaques liées au processus d'impression et numérisation avec une camera, dites attaques Print-Cam. Ces attaques très puissantes associent des modifications géométriques à des modifications de la valeur des pixels et peuvent rendre impossible la détection de la marque. La transformée de Fourier est utilisée comme domaine d'insertion de la marque, car cette transformée a des propriétés d'invariance contre certaines distorsions géométriques, rotation et translations dans le plan de l'image. La nouveauté de ce travail consiste à associer un tatouage d'image dans le plan de Fourier à 3 méthodes de correction : une correction géométrique de perspective basée sur la transformation de Hough, un filtre de Wiener pour réduire le flou et le bruit et enfin une correction colorimétrique pour réduire les dégradations de couleur. Les résultats obtenus sur des images ID montrent que la méthode proposée conduit à taux d'erreur total de 1%, contre 25% pour le meilleur de ses challengers. Ce taux d'erreur est compatible avec l'application sécuritaire visée.

Mots clés: Tatouage d'images, attaques Print-Cam, transformée de Fourier, déformation perspective, transformation de Hough, filtre de Wiener, variation colorimétrique

Abstract

Digital image watermarking consists in embedding information within the image which cannot be detected by the human visual system, but recovered with a software. The aim of this thesis is to propose a watermarking method when the watermarked image is printed on a physical support and then read freehandedly with a smartphone camera. In order to survive the Print-Cam process, the watermark must resist to multiple attacks. Those attacks occur during printing and capturing the image with a camera: in that case, the image might be rotated around the optical axis of the camera and translations may occur. Pixel value distortions are also present. These attacks may cause the loss of synchronization of the watermark and make the detection impossible. Hence, the main objective of the thesis is to develop a watermarking method that is robust to the Print-Cam attack in the context of an industrial security application for ID images. Fourier transform is used as this watermarking domain has invariance properties against some geometric distortions. Three main correction methods were integrated to deal with Print-Cam attacks: frame-based perspective rectification of the freehandedly captured images using detection of Hough lines, a Wiener filter to decrease image blurring and reduce noise, and adjustments to reduce color degradations. Results show that the method is highly robust with a total error rate of 1%, compared to a least 25% of errors for other methods, 1% of error rate being compatible with the targeted industrial application.

Keywords: image watermarking, Print-Cam attacks, Fourier transform, perspective deformation, Hough transform, Wiener filter, color correction.

List of publications

Journal publications:

- Khadija Gourrame, Hassan Douzi, Rachid Harba, Rabia Riad, Frédéric Ros, Meina Amar and Mohamed El Hajji: A zero-bit Fourier image watermarking for Print-Cam process. Journal Multimedia Tools and Applications Volume 78 Issue 2, January 2019 Pages 2621-2638.
- Meina Amar, Rachid Harba, Hassan Douzi, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Khadija Gourrame: Perceptual Image Watermarking based on a Mixed-scale Wavelet Representation. International Journal of Computer Applications 172, no. 8 (2017): 1-9.

Proceeding chapter publications:

- Khadija Gourrame, Hassan Douzi, Rachid Harba, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Meina Amar: Robust Print-Cam Image Watermarking in Fourier Domain. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 356-365.
- Meina Amar, Rachid Harba, Hassan Douzi, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Khadija Gourrame: A JND model using a texture-edge selector based on Faber-Schauder wavelet lifting scheme. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 328-336.

International conferences:

- Khadija Gourrame, Hassan Douzi, Rachid Harba, Frédéric Ros, Rabia Riad, and Mohamed El Hajji: Print-Cam resilient watermarking based on Fourier transform. 1th International Conference of Computer Science and Renewable Energies 2018, ICCSRE'2018, Ouarzazate, Morocco, November 22-24, 2018.
- Khadija Gourrame, Hassan Douzi, Rachid Harba, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Meina Amar: Robust Print-cam Image Watermarking in

Fourier Domain. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 356-365.

- Meina Amar, Rachid Harba, Hassan Douzi, Frédéric Ros, Mohamed El Hajji, Rabia Riad, and Khadija Gourrame: A JND model using a texture-edge selector based on Faber-Schauder wavelet lifting scheme. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 328-336.

Table of contents

List of figures

List of table

List of abbreviations

A/D	Analog /Digital
AWGN	Additive White Gaussian Noise
CCD	Charge-Coupled Device
CD	Compact Disc
CMJ	Cyan Magenta Jaune
N/A	Numérique/Analogique
DCT	Discrete cosine transform
DFT	Discrete Fourier transform
Dpi	Dots per inch
DWT	Discrete Wavelet Transforms
EQM	Erreur Quadratique Moyenne
FFT	Fast Fourier Transform
FMT	Fourier Mellin Transform
GGD	Generalized Gaussian Distribution
HVS	Human Visual System
IFMT	Inverse FourierMellin Transform
ILPM	Inverse Log Polar Mapping
JPEG	Joint Photographic Experts Group
JND	Just Noticeable Difference
LPM	Log Polar Mapping
LUT	Look Up Table
MP3	MPEG-1/2 Audio Layer 3
MPEG	Moving Picture Experts Group
PDF	Probability Density Function
PSNR	Peak Signal to Noise Ratio
PRND	Pseudo RaNDom
QIM	Quantization Index Modulation
RST	Rotation, Scaling and Translation

Chapter 1: Introduction

1.1 INTRODUCTION

"… seeing is not believing" is a well-known statement in the world of digital imaging [1], because any picture can be simply changed and wrongly used. The fast development of technology and the low cost of computer hardware and software nowadays provide widespread ways of producing, recording, editing, distributing and archiving digital multimedia content. In most cases human cannot be able to judge whether an image is authentic or fake with only visual inspection. The problem of data protection gain more attention with the improvement of technology. Along with enhancing defence techniques as cryptography, watermarking takes place as suitable and efficient solution for copyright protection, authentication, etc.

Since the 1990s, «digital data hiding" received special attention from the community of technology information and communication because it allows providing security solutions distribution of works. Digital watermarking is appeared as a new line of research that is part of this very recent scientific field and continues to grow in importance within the scientific community. Watermarking appears as an additional security means, to ensure authorized access, to facilitate the authentication of the content or to prevent illegal reproduction.

1.2 PROBLEM STATEMENT

In digital image watermarking, a message is inserted in a digital image in such a way that human eyes cannot see or detect the inserted message, but a software can detect the hidden message [2]. Watermarking is considered relatively brand-new discipline, compared with steganography. Steganography consists of hiding a message and transmitting it in a confidential manner within a data set. Watermarking differs from steganography mainly for its purpose but relies on similar techniques. Watermarking serves to secure a media rather than exchange messages. The research in watermarking is focused around three characteristics of the watermarking process as shows figure 1-1: capacity, imperceptibility and robustness. Capacity is the amount of information that is possible to be embedded in the image with a given method, imperceptibility tells how invisible the watermark is, and robustness describes how well the watermark

resists to attacks. By attacks, it is meant any modifications or perturbations that could render the detection of the mark a difficult issue. These properties heavily depend on the application and because these properties are conflicting to some extent, some trade-offs are unavoidable.

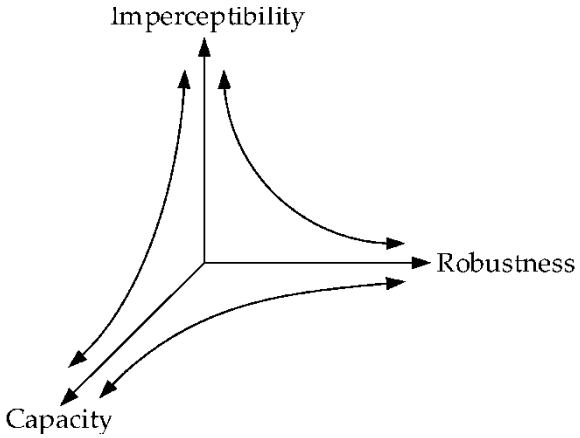


Figure 1-1- The trade-off between imperceptibility, robustness and capacity

Applications of watermarking are of high importance. To quote just a few, one may think of Copyright protection, source tracking (different recipients get differently watermarked content), Broadcast monitoring (television news often contains watermarked video from international agencies), video authentication.

New promising applications are under active investigations worldwide. The digital image can be printed on a physical support and freehandedly digitized with a smartphone camera. This allows embedded and mobile watermarking. Mobile watermarking application can range from shopping, games and teaching to various security related fields such as authentication of identity (ID) images on an official document as passports or ID cards (Figure 1-2).

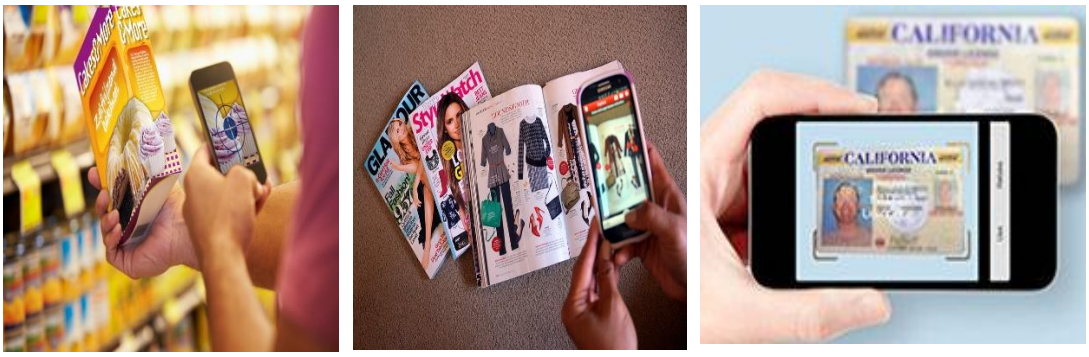


Figure 1-2- Different mobile applications of image watermarking on a physical support.

Unfortunately, the robust detection of this hidden information for mobile applications is not yet available nor widely studied. In this work, we will focus on the problem of reading hidden information, a watermark, from printed images on a physical support. In order to read the watermark from the printed image and to transform the content back to digital format, the image can be either scanned or photographed. We note that the process of printing the watermarked image and then detecting the watermark with a scanner represents the print-scan process. Likewise, when the printed image is captured freehandedly with a camera, the process is assigned as the Print-Cam process. Most of the studies about digital watermarking in the literature, up to now, has focused on purely digital images. Some research has been done on the print-scan robust watermarking systems, but few papers discuss the possible methods to freehandedly watermark detection with a smartphone camera [3]–[5]. Out of the existing methods, all are convenient for commercial use. In watermark in the print-scan process along with enduring digital to analog and analog to digital transformations, it must survive also geometric problem in form of rotation, scaling and translation distortions due to the scanning operation. These are represented as two-dimensional geometric problem related to the plane of the image. When the image is captured freehandedly with a camera, the watermark must survive to the same distortions as cited above, but also to an additional rotation related to the camera, the tilt angle distortion. This last distortion is particularly destructive. As a result, the synchronization between the watermark and the captured image get lost. Which lead to failure detection of the watermark. Image compression, paper quality, noises, lens focusing issues, light variations might create additional problems. All the possible

transformations or distortions that render the detection of the message a difficult issue are called attacks, either print-scan attacks, or Print-Cam attacks in our case.

1.3 OBJECTIVE OF THE THESIS

The main research goal of our contribution can be stated as follows: How to design a robust detection of the watermark from a printed image and freehandedly digitized with a smartphone camera? Until now, in most of the research literature, the camera is placed perpendicularly or with care to the printed image plan. Therefore, the main objective of the thesis is to develop robust methods for Print-Cam watermarking when the capturing process is performed freehandedly, that is when a tilt angle distortion also appears. In brief, the aim of this work is to introduce method for robust detection of the watermark with Print-Cam attacks, outperforming in term of detection rate those presented methods in the literature and able to handle industrial applications.

The thesis focuses on the robustness with respect to the impeccability condition of the watermark and especially on the robustness against Print-Cam attacks. These include the robustness to rotations in three dimensions due to the varying angles of capture. It is assumed here that the user has some knowledge of his/her camera phone. Some distortions may occur because of human malicious interaction. The question of how well the watermark survives malicious attacks will not considered here. Attacks to the physical object, such as ripping the image or considering scratches on it, will not be considered either. In this work, we will focus on ID images since these images are of interest for an industrial application we have in mind which is mobile control of official documents containing an ID image, as passports or ID cards.

1.4 THESIS ORGANIZATION

This thesis is organized into five chapters, including the Introduction current chapter. In the second chapter, we will present the state of the art of watermarking methods for digital images. First, we will describe digital watermarking and its different properties. Then we will discuss the general scheme of digital watermarking, describing in particular the different steps to insert and detect the watermark. For a better understanding of the physical phenomena that occur in the print-scan process as well as in Print-Cam process, we will characterize the printing and capturing process. Then we will identify the effects of printing and capturing an image. Finally, we will propose

a classification of watermarking methods according to the domain of insertion by focusing on Fourier-based methods.

The third chapter will present the related works in Print-Cam watermarking methods beside the general followed strategies to handle geometric problem in watermarking field.

The fourth chapter is primarily devoted to the description of a new watermarking method in the Fourier domain robust to Print-Cam attacks. This method is based on a pre-processing of the image before the insertion of the watermark. This pre-processing consists in a projective rectification, a blur correction followed by a colorimetric correction.

Last chapter presents the results of the proposed method on ID images. First, a simulated test will be described to illustrate the efficiency of the projective rectification compared to the existing Print-Cam watermarking methods in the literature. Second a real test will be presented where the captured devices will be iPhone6 and Samsung S5 smartphones. It is followed by a general conclusion and some perspectives are presented.

This thesis was conducted in the framework of a “cotutelle” between the University of Orléans and the University of Agadir. It was supported by CNRST-PPR2 project: "Development of a prototype authentication system based on face biometrics ". It was also supported by the SUREO 16042PRI project “Tatouage de photos d’identités numériques robuste aux attaques Print-Scan” with the Gemalto Company.

Chapter 2: Print-Cam Image Watermarking - Background

2.1 INTRODUCTION

In this chapter, the concept of digital image watermarking is explained through literature. To detect a watermark from a printed watermarked image, the image should be digitized with the help of scanner or mobile phone. Print-Scan system and Print-Cam system represent a case of watermarking system where the transmission phase, between watermark insertion and detection, goes from digital-to-analog and analog-to-digital domains. Further, we detail each system with related applications and attacks.

2.2 DIGITAL WATERMARKING

2.2.1 Based elements of watermarking system

Digital watermarking is the method of embedding information into a digital data, for example digital image, audio, video or text documents. The information is embedded into the digital data by performing invisible modifications to the content of the data. A generic watermarking system is shown in Figure 2-1:

- *Watermark embedding and watermark detection/extraction* are the core phases in watermarking system. Embedding process is about inserting information or signature called watermark into digital data content (that can be text document, video, audio or image) to produce a watermarked data. The inserted watermark is encoded and generated using a secret key. The same key (or different key depending on the needed application) is used to detect or extract the watermark from the input data in the detection phase.
- *Transmission phase* is the phase where the watermarked data goes through a transmission channel that may produce distortions due to attacks, producing distorted watermarked data. Attack is every modification affecting the watermarked data that makes detection process fails to detect the watermark. Attacks can be intentional and voluntary to remove the watermark for the unauthorised use of the data, also it can be unintentional related to the different signal operations during the transmission channel such as compression and

noises. We elaborate more details about different types of attacks in case of the image watermarking in the following of this chapter.

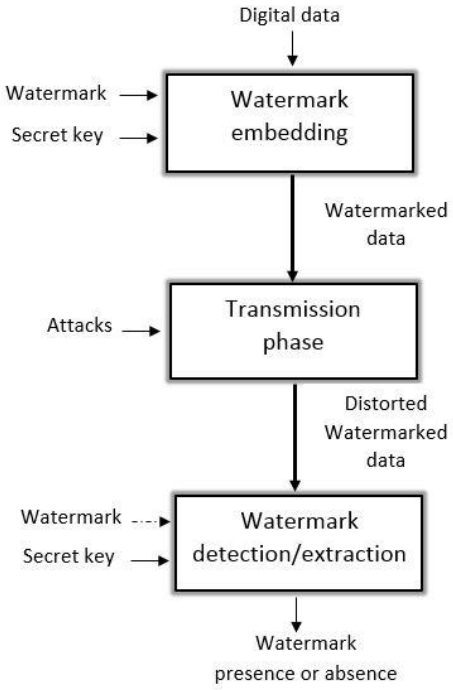


Figure 2-1: Generic of digital watermarking system.

- *Secret key:* all watermarking systems use secret key (one or more) to increase the security against intentional removal of the hidden watermark. Same watermark is used in watermark embedding and detection phases. If the key is known, this type of watermark is specified as public, and if the key is hidden, as private watermarks [2].

2.2.2 Different requirements in digital watermarking

There are various requirements that the design of watermarking algorithm should take in consideration. The importance of each requirement parameter depends on the served watermarking applications. Those parameters are explained as bellow:

2.2.2.1 Robustness

Watermark robustness measures the capability of the hidden watermark to survive any type of signal processing manipulations, including intentional and/or unintentional attacks. The first category of attacks aims at damaging the hidden information, while the second category do not explicitly intends to remove the watermark or making it unreadable. Not all watermarking techniques have the same level of robustness, some

techniques are robust against some signal manipulations and fails against other stronger attacks. The robustness can be classified as following:

- *Robust watermarking:* In this case, the watermarking system is designed to resist to different attacks that can occur to the digital document, and still the watermark is reliably detected under those manipulations.
- *Fragile watermarking:* the watermarking system is designed to be damaged at any kind of manipulations. This technique serves to detect any illegal manipulation, even slight modifications including incidental and intentional attacks. In this case, the extracted watermark is compared with the original watermark to identify if the digital data is modified or not.
- *Semi-fragile watermarking:* in this case, the watermarking system is designed to be robust against some attacks and fragile against some other specific attacks. It integrates the features of both robust and fragile watermarking.

2.2.2.2 Imperceptibility

When the watermark is embedded in a host medium such the watermark is not visible by human visual system (HVS) and/or human auditory system (HAS). The embedded watermark should not be sensitively detectable by any of the above human systems. Therefore, the watermark insertion process should not affect the quality of the host medium.

2.2.2.3 Capacity

It is a fundamental property of any watermarking technique. It represents the amount of information that a given technique is able to insert in the host medium. In general, capacity of watermarking techniques depends on many factors such as the particular used algorithm, the characteristics of the host medium and the attack strength.

2.2.2.4 Complexity

It characterizes the computational cost to embed, recover and detect the watermark information. In other word, it describes the effort and time needed for an efficient digital watermarking technique. It is recommended to design the watermarking algorithm as complex as possible for higher robustness. However, the complexity issue is more important for real time watermarking applications as for industrial applications.

2.2.3 Applications of digital watermarking

Several application scenarios related to Digital watermarking, are represented in this section. Watermark embedding has the goal to increase the security of the multimedia document. The added information (the watermark) can serve the functionality of different security fields as copyright protection, fingerprinting, multimedia authentication, and device control [2], [6].

2.2.3.1 Copyright protection

The protection of intellectual properties in digital world was one of the earliest motivations for developing and applying watermarking techniques. Watermarking is designed for copyright protection to identify both the source of the media as well as the authorized users. Embedding an invisible watermark to track the ownership and the recipients has attracted much interest in the printing and publishing industries. The copyright information (watermarks) requires higher level of robustness against intentional attempts to remove them. It can be visible to prevent end-users from mistreat the content as well as it can be invisible to detect the ownership in case of unauthorized reproduction of the content.

2.2.3.2 Fingerprinting (transaction tracking)

Watermarks are used in fingerprinting applications to trace unauthorised copies to the original owner of the digital documents. They are generally used along with copyright protection watermarks in transaction. A fingerprint (a watermark) is a unique identification signal for each copy that distinguish each recipient in the legal distribution process. The term comes from human fingerprint that uniquely identifies a person . In case of detection of illegal distribution, the extracted fingerprints from the copies allow to spot the recipients who are the sources of unauthorised distribution. Moreover, watermarks for fingerprints have same requirements as for copyrights watermarks.

2.2.3.3 Multimedia authentication

Embedding watermarks in digital documents can prove whether the content is modified or not. Typically, fragile and semi-fragile watermarking techniques are used as solution to control content integrity and authenticity. In this case, if the digital media is modified maliciously the fragile watermark will be destroyed, if the watermark can be retrieved or detected, the media is considered authentic otherwise, it is considered

as fake. Furthermore, some systems provide, in addition of detecting the tempered region, a restoration of the original content media. The design of (semi-)fragile watermarking techniques imposes strong requirements. It should balance between high robustness against standard processing such as compression and geometric transformations, and weak resistance (or fragile) to any intentional manipulations.

2.2.3.4 Device control

Device control watermarking applications are created to control access to resources using decoder devices. A watermarking system inserts an authorization code into a signal (e.g., radio and TV signals) and transmit it to a verifying device. In the device, the authorization code is extracted from the watermarked signal, which allows the user to perform authorized operations on the resource. Those operations may consist of permissions of executing a program, reading or copying a multimedia object. Control watermarks can also be used in audio signals to remotely control a device such us computer, robot or any kind of appliance. The device is supplied with suitable detector to identify the watermark signals, which can activate an action or change a state of the device.

There are many other applications that can be served by digital watermarking such as copy control, annotation watermarking, legacy enhancement, content filtering, forensics [2].

2.3 DIGITAL IMAGE WATERMARKING

Digital watermarking system, as mentioned earlier, consists of three general phases; embedding, detection and transmission phases. The design of watermarking technique is related tightly to the nature of the digital medium. In this paragraph, insertions and detection processes are explored in details along with the related attacks for digital image watermarking.

2.3.1 Basic image watermarking system

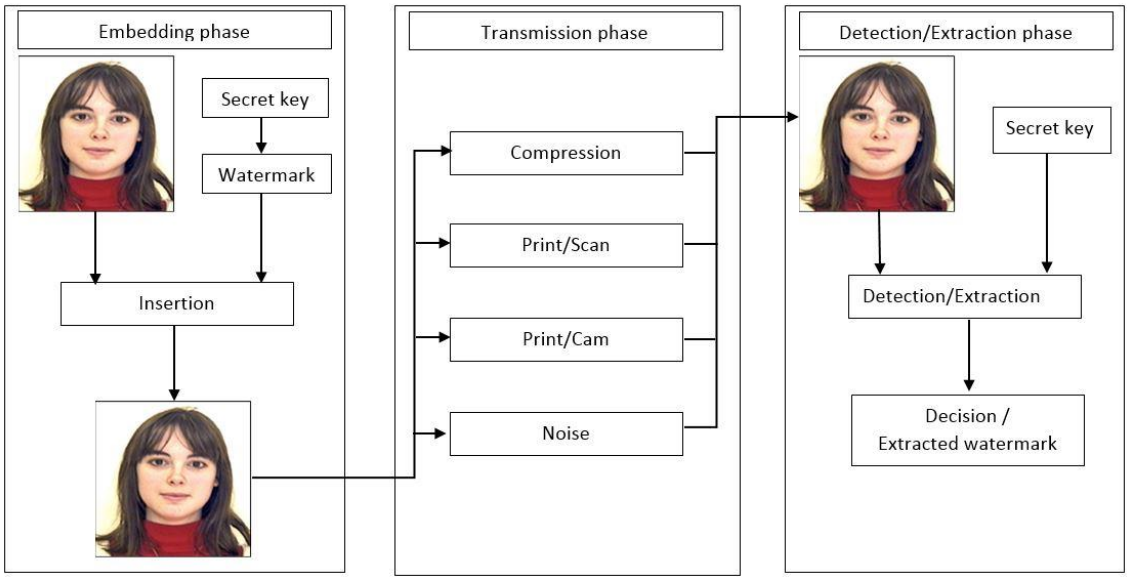


Figure 2-2: Generic of digital image watermarking system.

2.3.1.1 Embedding phase

In embedding phase, the original image I_0 is merged with a collection of bits that represents the watermark W. This merging operation produces new watermarked image I_w. The watermarked images are visually similar to the original images. The watermark W is generated using a secret key K. The watermark is adjusted by watermark modification or scaling [cox] to maintain the imperceptibility requirement. Additive and substitutive watermarking are the main insertion operations that combine the watermark with the original image.

- *Additive watermarking:* to perform the embedding of the watermark, the additive approach adds the watermark value into the components of the image. Additive watermarking can be mathematically defined by one of the following equations [2]:

$$I_w = I_0 + \alpha \times W, \quad (2\text{-}1)$$

$$I_w = I_0(1 + \alpha \times W), \quad (2\text{-}2)$$

$$I_w = I_0 \times e^{\alpha \times W}. \quad (2\text{-}3)$$

Where factor α controls the strength of watermark insertion to balance between the imperceptibility and robustness requirements. In this operation, the

watermark can be added directly to the pixels of the original image or to the components of the image after a frequency transformation.

- *Substitutive watermarking:* in this case, the watermark is substituted to the components of the image. In order to insert one value of the watermark, substitutive method replaces one piece of information of the original image, a feature or a characteristic of it, with another that is delivered from a dictionary that encodes the desired watermark value. Accordingly, watermark detection and extraction stands in the image feature re-reading or interpolation. The substitutive watermarking approach takes several forms as Least Significant Bits (LSB) substitution [7], Quantization Index Modulation (QIM) [8] and histogram substitution [9].

2.3.1.2 Detection/extraction phase

The goal of image watermarking system is permanently introducing some information into the original image and then trying to detect or extract it as reliably as possible. Analogically if the watermark embedder is considered as transmitter in a communication chain then a watermark detector or extractor will be the receiver. The purpose of detection process is deciding whether the image under test contains a watermark or not (zero-bit watermarking scheme), whereas for extracting process is extracting the watermark that the image may carry (multi-bit watermarking scheme). There are two protocol types followed for detection or extraction phase:

- *Blind watermarking:* A watermarking technique is said to be blind if extraction or detection of the watermark does not require the access of the original image. Blind watermarking is more used in most applications, since the unmodified original image is usually not available for the watermark extraction or detection.
- *Non-blind watermarking:* A watermarking technique is said to be non-blind if the original image is needed for the extraction or detection of the watermark. Non-blind watermarking is more robust than the blind one because it is evident that the watermark can be extracted or detected easily using both the original image and the watermarked image.

2.3.1.3 Transmission phase

Transmission phase represents the intermediate phase between the embedding and detection/extraction phases, where the watermarked images are exposed to several

attacks. In digital image watermarking, attacks are a set of operations or/and modifications that occurs to the watermarked image and makes the watermark undetectable. Attacks in image watermarking field can be classified as four classes, image processing attacks, synchronization attacks, cryptographic attacks and protocol attacks:

- *Image processing attacks:* this class of attacks include image degradation, image enhancement and image compression. Image degradation operations can damage watermarked image by removing a part of it, hence damaging the watermark. Examples of those operations are different type of noise insertion and cropping. Image enhancement are generally convolution that can remove the watermark from the image, such as smoothing, sharpening, histogram equalization, median filtering, Gaussian filtering, and contrast enhancement (changing the brightness of the image). In case of image compression, the watermark can be recovered by an inverse operation if the watermarked image is compressed with a lossless compression method. In the contrary, lossy compression such as JPEG and JPEG2000 compressions, apply irreversible changes to the image. Therefore the watermark may be lost and return may not be possible.
- *Synchronization attacks:* this class of attacks does not intend to remove the watermark itself, but to distort it through spatial alterations of the watermarked image. These attacks make the watermark detector loses the synchronization with the embedded information. However, the watermark itself is physically present in the image. Synchronization attacks are done by performing geometric transformations to the watermarked image. For example rotation, translation, scaling, affine transformation and projective transformation.
- *Cryptographic and Protocol attacks:* these attacks are categorized as intentional attacks. Cryptographic attack method tries to find out the secret key used for watermark insertion based on exhaustive key search approaches. Since many watermarking schemes use secret key it is crucial to keep the key's length secure. Protocol attacks have the goal of creating protocol ambiguity in the watermarking process, which can cause ambiguity regarding true ownership such as copy attack [2].

Attacks are very important to be studied and understood in watermarking system, in order to identify the weaknesses of watermarking technique, and improve its robustness.

2.3.2 Different insertion domains

Digital image watermarking is the concept of inserting a pattern of bits into a digital image, usually in an imperceptible way. The transparent watermark is added by changing the image pixels. Those changes can be in spatial domain, which involve directly the pixels of the image or in frequency domain by modifying the frequency representation of the image like using Fourier or wavelet coefficients.

2.3.2.1 Spatial domain

For watermarking techniques in spatial domain, the watermark is embedded directly by modifying the pixel values of the original image. The used values in this case are the values of color channels, luminance or brightness signals of the digital image [10]. Watermarking in spatial domain has the advantage of low complexity and ease of implementation however; it is less robust to attacks such as noise and compression. Many watermarking techniques are proposed in spatial domain. LSB is one of the earliest methods in spatial domain. The binary representation of the watermark, in this technique, is replacing the LSB of each pixel with one bit of the watermark sequence. Correlation-based technique is another watermarking technique used in spatial domain using the correlation properties of additive random noise patterns. The watermark in this case is embedded according to the following equation:

$$I_w(x,y) = I_0(x,y) + \alpha \times W(x,y). \qquad (2\text{-}4)$$

The pseudo-random pattern $W(x,y)$, scaled with a strength factor α is added to the original image $I_0(x,y)$, and resulting the watermarked image $I_w(x,y)$. To retrieve the watermark, the correlation between the pseudo-random pattern and the suspected watermarked image is evaluated. If the correlation value is more than a calculated threshold t, the watermark is detected; otherwise, the image does not hold a watermark. Moreover, Patchwork is watermarking technique developed by Bender et al. [11] pseudo-random statistical model. The watermark is imperceptibly inserted with a specific statistic and Gaussian distribution into the luminance values of the original image.

2.3.2.2 Transformed domain

Watermarking techniques in frequency domain exploit significant coefficients and regions of the original imager after a frequency transformation. Watermarking techniques in frequency domain are more robust and more complex than techniques in spatial domain. In transform domain techniques, the watermark can be inserted into selected coefficients of the transformed image [12]. In order to retrieve the watermarked image, an inverse transform of the modified coefficients needs to be taken. Using discrete wavelet transform (DWT) most of the information contained in the original image is concentrated into the LL sub band, it is called approximate image. Moreover, the other sub bands contain some details like the edge and textures, which are represented by large coefficients in the high frequency sub-bands. The most vertical detail information corresponding to horizontal edges is represented in LH. While the horizontal detail information from the vertical edges is represented by HL. The LL (low pass) sub-band can be further decomposed to another level of the same previous decomposition. This process can be continued until the desired level of decomposition determined by the application [13]. Therefore, the watermark embedding can be done in one or many sub-bands of the same level or including many levels depend on the application and proceeded protocol of the watermarking method. For discrete cosine transform (DCT), the image is divided into parts of different frequencies low, high and middle frequency coefficients [14]. The middles frequency part can handle better the watermarking process because if provides an additional resistance to image compression while avoiding significant changes in the original image [2]. Discrete Fourier transform (DFT) is widely used in watermarking field [15], [16]. It serves to select decent coefficients from the transformed image for embedding the watermark in order to balance between the invisibility and the robustness. More other transforms are used in watermarking techniques like singular value decomposition (SVD) [17], discrete Hadamard transform (DHT) [18], Fourier-Mellin Transform (FMT) [19], Radon transform (RT) [20], and quaternion Fourier transform (QFT) [21].

2.3.3 Evaluation of watermark

The efficiency of digital image watermarking algorithms is mainly evaluated based on its imperceptibility and robustness.

2.3.3.1 Mean Square Error (MSE)

MSE is a visual quality measure. It contains the additive squared error between the original image and the watermarked image [22]. The MSE can be defined as:

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (I_0(x,y) - I_w(x,y))^2 \quad (2\text{-}5)$$

Where $I_0$and $I_w$are respectively the original and the watermarked images with the size $M \times N$. The lower value of MSE illustrates that the visual quality of the watermarked image is close to the original one.

2.3.3.2 Structural Similarity Index Measure (SSIM)

The general form of SSIM [23] is defined as:

$$SSIM = [l(x,y)]^{\alpha}.[c(x,y)]^{\beta}[s(x,y)]^{\gamma}. \quad (2\text{-}6)$$

Where $l(x,y), c(x;y) and\ s(x,y)$ are luminance measurement, contrast measurement and structure variations between pairs of local square windows $x\ and\ y$ of the original image and the watermarked image respectively. The parameters $\alpha, \beta\ and\ \gamma$ represent the relative importance of each measurement. The SSIM values changes between 0 (total difference) and 1 (total similarity). The mean of SSIM evaluates the global similarity between the original image and the watermarked image.

2.3.3.3 Peak Signal to Noise Ratio (PSNR)

The invisibility requirement in image watermarking field is measured using PSNR [24]. Which is defined as:

$$PSNR = 10 \times log_{10}\left(\frac{d^2}{MSE}\right). \quad (2\text{-}7)$$

Where d is the maximum pixel value of the image. In case if the image pixels are coded with 8 bits then in this case $d = 255$. MSE is the mean square error between the original image and the watermarked image. The higher PSNR value illustrates that the watermarked image is visually similar to the original image, which indicates that the watermark in more imperceptible. In general, the watermarked image with PSNR greater than 40 dB is acceptable [24].

2.3.3.4 Normalized Correlation (NC)

NC is one of measurement that evaluates robustness of watermarking technique [2]. NC value evaluates the similarity and the difference between the inserted watermark

and the extracted watermark. The more NC value is close to 1, the extracted watermark is considered as similar to the inserted one in the image. However if NC value is close to 0, the extracted watermark is different form the inserted one. NC is defined as:

$$NC = \frac{\sum_{x=1}^{L}\sum_{y=1}^{K} W_{inserted}(x,y)W_{extracted}(x,y)}{\sum_{x=1}^{L}\sum_{y=1}^{K}[W_{inserted}(x,y)]^2}, \quad (2\text{-}8)$$

Where $W_{inserted}$ and $W_{extracted}$ are the inserted watermark and extracted watermark respectively of size $L \times K$.

2.3.3.5 Bit Error Rate (BER)

The BER determines the ratio of the number of incorrectly extracted watermark bits and total number of the sequence bits of the inserted watermark. Ideally, BER value should be equal to 0.

$$BER = \frac{Number\ of\ incorrect\ bits}{Total\ number\ of\ bits}. \quad (2\text{-}9)$$

2.4 PRINT-SCAN IMAGE WATERMARKING

During the Print-Scan process, the watermarked image suffers from many modifications. Both invisible and visible distortions are presented in this system. In the following, we detail both printing and scanning systems and the produced distortions in relation with watermarking process.

2.4.1 Print-Scan watermarking system

The watermarked image in Print-Scan system is first printed into a paper of book, magazine or ID cards. Then, the image is digitized using a scanner for the watermark detection (figure 2-3). Printer and scanner in this system are the main materials in the transmission phase (figure 2-1) of the watermarking system.

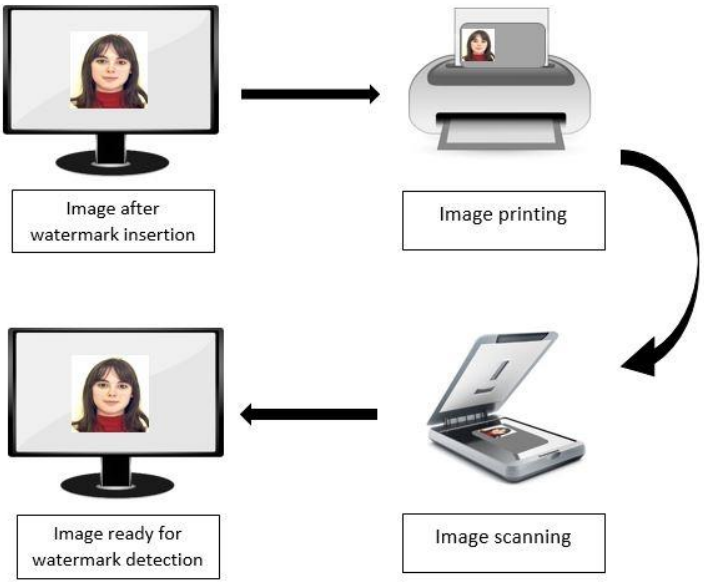


Figure 2-3: Print-Scan image watermarking system.

2.4.1.1 Printing process

In general, printing means recreating text or image on paper, cards or other materials. A printer is the tool that communicate with computer in order to produce the image output on physical print media as magazines, books or ID cards. Many printing technologies are developed. In the following, we present the main technologies of the recent printer devices [25]:

- *Laser printers:* this type of printer utilizes a laser beam to produce an image on a drum (or a cylinder). The light of the laser modifies the electrical charge on the drum wherever it shoots. The drum is then rolled through a storage of toner, which is gathered by the charged portions of the drum. Finally, the toner is transferred to the paper through a combination of heat and pressure. The standard monochrome laser printers use single toner, while the color laser printers use four toners to print in full color. The main characteristics of laser printers is their resolution, how many dots per inch (dpi) they manage. The available resolutions range from 300 dpi at the low end to 1,200 dpi at the high end. Laser printers produce very high quality print and are capable of printing an almost unlimited variety of fonts.
- *Inkjet printers:* In the inkjet printing mechanism, the print head has several tiny jets. As the paper moves past the print head, the jets spray droplets of ink onto

it, forming the characters and images. There is usually one black ink cartridge and one so-called color cartridge containing ink in primary pigments (cyan, magenta, and yellow). Some inkjet printers can make full color hard copies at 600 dpi or more. The resolution in inkjet printers is primarily related to the size of the jets, the smaller jets size allows smaller droplets that produce higher resolution [26].

- *Dye-sublimation printers:* A dye–sublimation printer uses the heating process in printing mechanism, in order to transfer dye to solid objects. This type of printers work by heating solid ink so that it can be transferred on a solid surface, such as plastic or ceramic. These printers are used for printing photos and ID cards, as well as for fabrics. Dye-sublimation printers use a special overcoating instead of black with the other standard ink colors, so dye-sublimation uses the CMYO (cyan, magenta, yellow, and overcoating) system, yet some printers do use black ink. The inks are transferred on the surface one color at a time. These printers produce continuous tones compared with inkjet printers where the tones can vary with several stopping. As a result, reproducing photos with dye-sublimation printers are much more accurate than with inkjet printers [27].

- *Thermal printers:* this type of printers creates a hardcopy of an image by selectively

  heating areas of thermal paper. Thermal printing does not make use of ink or toner comparing many other printing types but mainly depends only on thermal papers for producing the images. The surface turns black in the regions where it is heated to create the image. Thermal printers are efficient and faster in printing monochromic ones compared to other forms of printing, however, they usually do not print out colors well. During the printing operation, if the printer becomes too heated, the printing may not be precise and accurate [28].

2.4.1.2 Scanning process

A scanner is a tool that captures a hard copy input (image, a document etc.) and converts it to a digital image, allowing to save the data on a computer and reuse it for watermark extraction or detection. They are many types of scanners as; flatbed scanners, sheet-fed scanners, handheld scanners, and drum scanners. Almost all types of scanners have same basic principle (Figure 2-4). First, the document is placed on

the glass plate and the cover is closed. The inside of the cover is usually flat white or black. It affords a uniform background so the scanner software can use as a reference point for controlling the dimension of the scanned document. Then, a lamp is used to illuminate the document. A belt linked to the stepper motor, that it moves gradually the scan head across the paper. The scan head combines mirrors, lens, filter and CCD array. The mirrors are used to reflect the image of the scan sequentially ending by a reflection onto the lens. Next, the lens focuses the image over a filter on the CCD array. The ADC is used to digitize the image. Finally, the digital image is sent to the host computer.

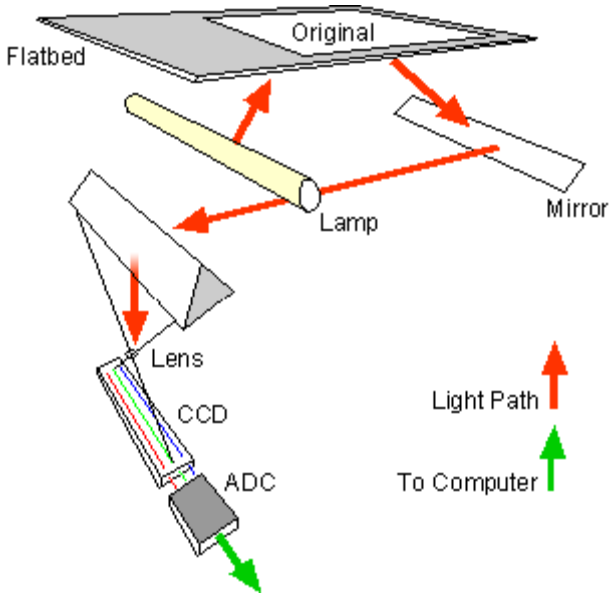


Figure 2-4: Basic scanning mechanism [25].

2.4.2 Print-Scan attacks

Print–Scan process produces several serious attacks, which introduce distortions on the watermarked image. The output digital image after the Print-Scan process is actually modified even if it looks similar for human eyes. In [29], Solanki *et al.* described different types of distortions and attacks that occur to the image after Print-Scan process (Figure 2-5). These distortions are described as below:

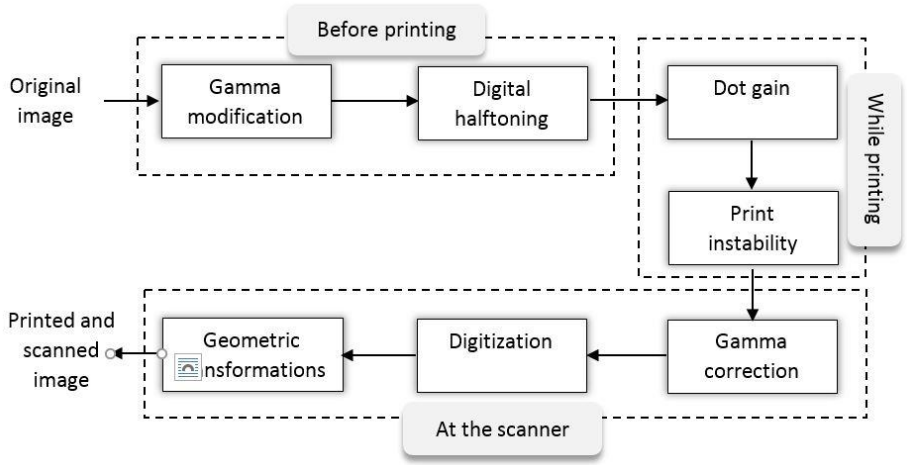


Figure 2-5: Distortions in Print-Scan process [29].

- *Gamma tweaking:* is a non–linear transformation emerged in printers. The transfer characteristics of the printers can be changed to adjust the printed image. Gamma tweaking is used to make sure that the printed image appears the same as on a monitor.
- *Digital halftoning:* halftoning is the process of converting an image into binary image. This process is executed before the action of printing. Each pixel in the digital image is represented as a halftone cell in most of halftoning methods.
- *Dot gain:* A phenomenon occurs when the digital halftone is executed dot-by-dot. Hence, the printed image to look darker than expected mainly because of optical or electrostatic causes.
- *Print instability:* unexpected correlated noises that happen during the printing process. Print instability represents the minor variations that appears in the printer's output like, for example, the horizontal imperfections.
- *Scanner gamma correction:* the scanned image should be acceptable to the human visual system (HVS). Using gamma correction, the grey level of the output pixels is raised at the power $1 = \gamma$, where γ is the gamma value of the monitor representing the scanned image.
- *Digitization:* the conversion from analog to digital form leads to quantization errors. Combining the nonlinear adjustment in early steps in Print-Scan process, the quantization errors are amplified.

- *Geometric transformations:* main transformations that arise during the scanning are cropping, rotation, scaling and translation. These geometric transformations are mainly related to the position of the printed image in the scanner. They still existed even with the careful scanning of the user.

2.5 PRINT-CAM IMAGE WATERMARKING

Similarly, to Print-Scan process, the watermarked image in Print-Cam process suffers from many modifications. More degradations are presented in this system mainly related to the use of mobile phone while capturing. In the following, we focus on capturing system and the produced distortions in relation with watermarking process.

2.5.1 Print-Cam watermarking system

The watermarked image in Print-Cam system is first printed into a paper of book, magazine or ID cards. Then, the image is digitized using a camera of smartphone freehandedly for watermark detection (figure 2-6). Likewise, in this system printer and smartphone's camera are the main materials in the transmission phase (figure 2-1) of the watermarking system.

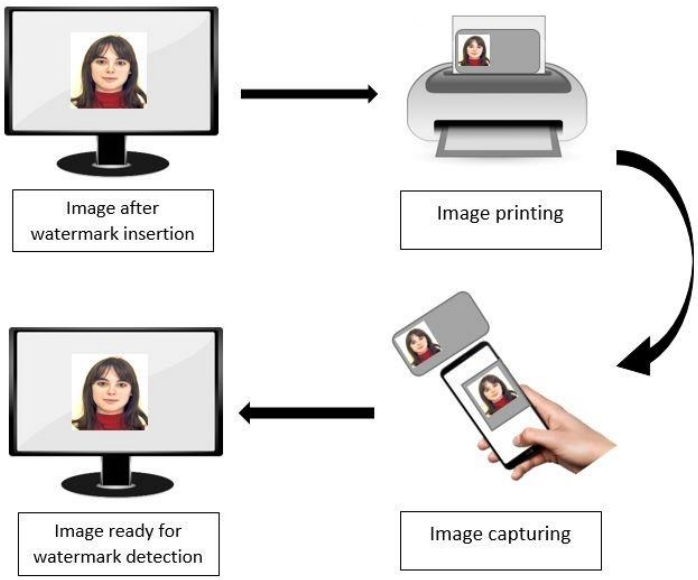


Figure 2-6: Print-Cam image watermarking system.

2.5.1.1 Print-Cam watermarking applications

In this chapter, we discussed earlier the general applications for digital watermarking. Yet, the huge growth of using smartphones create new possibilities of watermarking

applications especially for industrial fields. The biggest advantage of using smartphones is that it is not limited to a specific time and place. Therefore, the watermark in Print-Cam system is free from the time and place conditions, means that it can be detected or extracted at anytime and anywhere. In the following, some of the main possible scenarios are listed:

- *Online shopping* [30]: with one click from smartphone's camera of an item in a magazine, catalogue or newspaper, the user can get the internet URL where he can buy the item directly just by reading the watermark in the captured images.
- *ID card authentication*: with one picture of the ID card with mobile phone the security agent, for example, can check the authentication of the card.
- *Retrieving information*: print-cam watermarking technique enables the user to retrieve information about a product as book, cosmetic product or medication by taking picture of the package of the item.

Commercially, Digimarc is the most famous print-cam watermarking international company, provides security and brand protection from companies using watermarking and business possibilities with their applications [31].

2.5.1.2 Capturing process

The basic components of a smartphone's camera are:

- *Sensor* [32]**:** it is the part of the camera that 'captures' the image. An integrated circuit mainly consists of photodetectors (the core component that captures light), amplifiers, transistors, and some form of processing hardware and power management. The sensor provides all the necessary data, when the smartphone's camera software requests an image. Smartphone camera sensors universally use CMOS (complementary metal-oxide-semiconductor) or CCD (charged-coupled device). CCD sensors have been of a higher quality.

Figure 2-7: Camera module from the Galaxy S5 and a Samsung S5K2P2XX 1/2.6” sensor with an f/2.2 lens [32].

- *Lens:* it reduces and focuses the light in front of the camera to adjust to the small size of the sensor, so the image looks crisp and clear. As an illustration, the lens in smartphone’s camera is a collection of multiple plastic or glass elements, with glass usually affording a higher quality, sharper result. Each element has a specific function as shaping the light to fit the size of the sensor, correcting issues, or providing the final focus point.

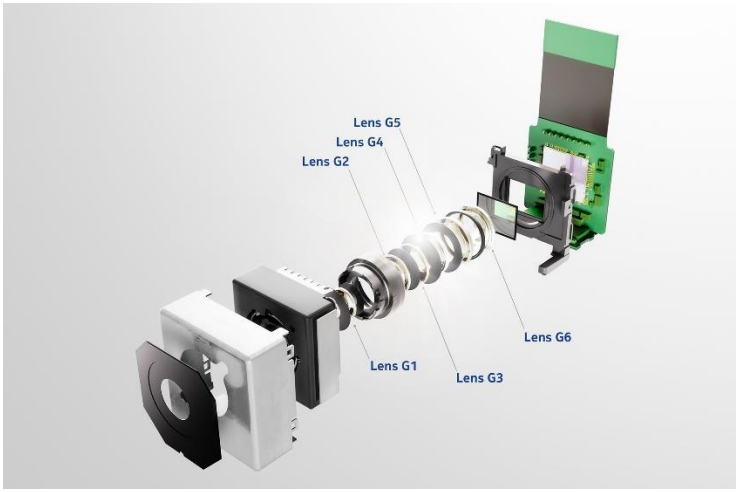


Figure 2-8: Camera construction of Nokia [32].

Sensor and lens are the crucial hardware parts part of the camera. The characteristics of these components create a set of features of the camera; thus, they control the quality of the captured image. Camera’s features are resolution, focus, image stabilization, aperture and focal length.

2.5.2 Print-Cam attacks

In Print-Cam process, the watermarked image is first printed and then captured with a digital camera or a camera of a camera phone, the attacks in this process can be considered as an amplification of attacks in print-scan process. In other words, the attacks appearing in print-scan process are all possible attacks in the Print-Cam process. In addition, the print-cam process delivers various other attacks on watermark including:

- *Geometric transformations:* Perspective or projective distortions caused by the relative position of the camera and the printed image. It is a combination of four main geometric distortions; rotation, translation, scale, and tilting of the optical axis.
- *Motion blur*: Mostly caused by the shaking of the user's hand while taking the picture. It is difficult to detect the watermark in this kind of images.
- *Lighting effect:* The changes of illumination can affect the captured image quality thus it can destroy the watermark. In addition, multiple light sources, direction of the light, shadows, flashlight, flatness, color of the light and light reflection, all have an impact to detection failure of the watermark [33].
- *Lens distortions*: They are caused by the optical design of the lenses in the smartphones. In general, there are three known types of optical distortion – barrel, pincushion and mustache / moustache (also known as wavy and complex) [34].

All the previous attacks can be classified under controlled and uncontrolled attacks. In such way that the controlled attacks, as attacks related to materials (printer, smartphone's camera), can be predicted and fixed. However, uncontrolled attacks, like geometric distortions and light, are hard to predict and fix.

Chapter 3: Literature Review

3.1 INTRODUCTION

In this chapter, research literature related to the thesis is presented. The first chapter introduced digital image watermarking in general and detailed description about Print-Cam process and attacks. Geometric distortions are among the main challenging issues produced by Print-Cam process for watermarking methods. In this chapter, the section 3.1 investigates the general image watermarking techniques against geometric transformation. These techniques are classified into four categories; exhaustive search, invariant domains, watermark re-synchronization and image re-synchronization. Section 3.2 presents previous proposed work specifically related to Print-Cam watermarking methods. Section 2.3 summarises a synthesis of the presented state of the art.

3.2 IMAGE WATERMARKING TECHNIQUES AGAINST GEOEMETRIC DISTORTIONS

Geometric distortions do not actually erase the watermark from the image. Instead, they destroy the synchronization between the watermark and watermark detector. Many approaches have been developed to deal with the synchronization problem produced by the geometric attacks, are generally belong to the following categories:

3.2.1 Exhaustive search

Considering all possible geometric deformations, exhaustive search approach performs accordingly the watermark detection process over the geometrical inverse transformation. The watermark is recovered by searching each possible geometric distortion transformation. The watermark detection is completed by choosing the maximum correlation value of all hypothetical distortion parameter and then compared with the appropriated threshold value. Obviously, this approach suffers from the computational constraints considering searching size. It enlarges with the complexity of the geometric distortion level. Exhaustive search may also need a careful study of false possible probability that increases with the size of the search [35], [36].

Usually, studied geometric distortions are limited to translation, scaling and rotation. To limit the range of tested parameters, some presumptions on the severity of

the distortion are made. In order to focus on more complex transform while controlling reasonable computational cost, detection can sometimes be operated on smaller regions of the image [37], [38]. Further reducing the search space, strong hypotheses can be made on the relative continuity or smoothness of the deformation [39]. Another way to limit search space is to use periodically structured watermarks [40], [41]. It enables to limit search for synchronization problem over one repetition period.

3.2.2 Invariant domains

One of the means to get rid of spatial synchronization constrains is to build a watermark in insensitive space to geometric distortions. This space is known as invariant domain. In the following, we list most used transformed domains with advantageous geometric properties.

3.2.2.1 Fourier domain

DFT is one of the powerful tools in digital signal processing. Fourier transform allows of decomposing a signal (such us an image) into a sum of basic signals, which have the property of beings easy to implement and observe. These signals are periodic and complex, in order to allow finding, studying and analysing an amplitude and phase of the system.

The DFT of an image $f\ (m,n)$ of size $M\ \times\ N$ is defined by:

$$F(u,v) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)e^{-j2\pi(\frac{um}{M}+\frac{vn}{N})}, \tag{3-1}$$

where (u,v) are the spatial frequencies for position (m,n). From the transform of Fourier, it is possible to reconstruct the original image exactly by taking the inverse of Fourier transform as presented in equation (3-2).

$$f(m,n) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{j2\pi(\frac{um}{M}+\frac{vn}{N})}. \tag{3-2}$$

The obtained image after applying DFT are in complex form. In general, magnitude M and the phase P are calculated to represent the complex form by the following equations:

$$M(u,v) = |F(u,v)| = \sqrt{(Re(u,v)^2 + Im(u,v)^2)}, \tag{3-3}$$

$$P(u,v) = \arg\big(F(u,v)\big) = tan^{-1}\left(\frac{Im(u,v)}{Re(u,v)}\right). \tag{3-4}$$

where Im and Re respectively represent the imaginary and the real parts of the Fourier transform of the Image f. In general, we represent only the magnitude whose illustrated in Figure 1-10.

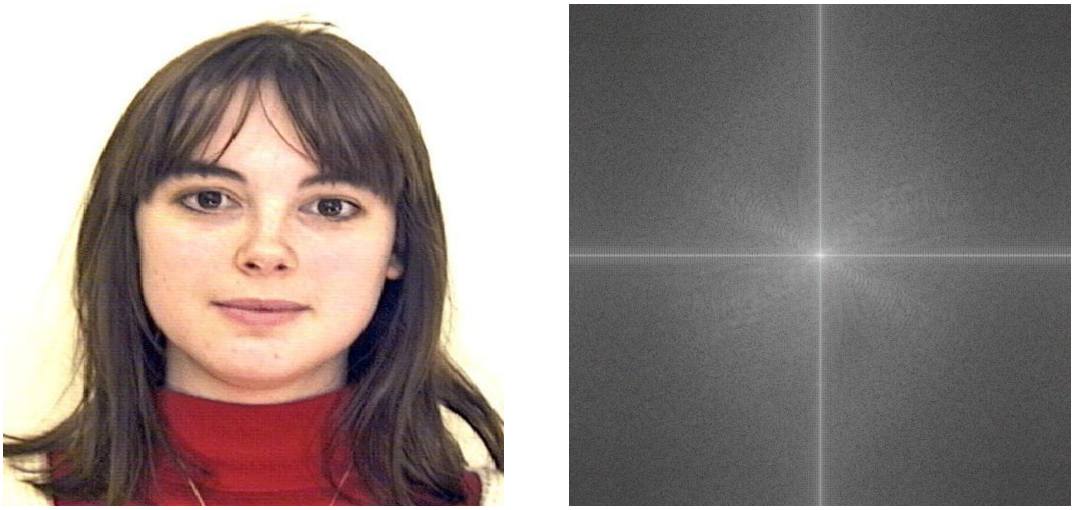


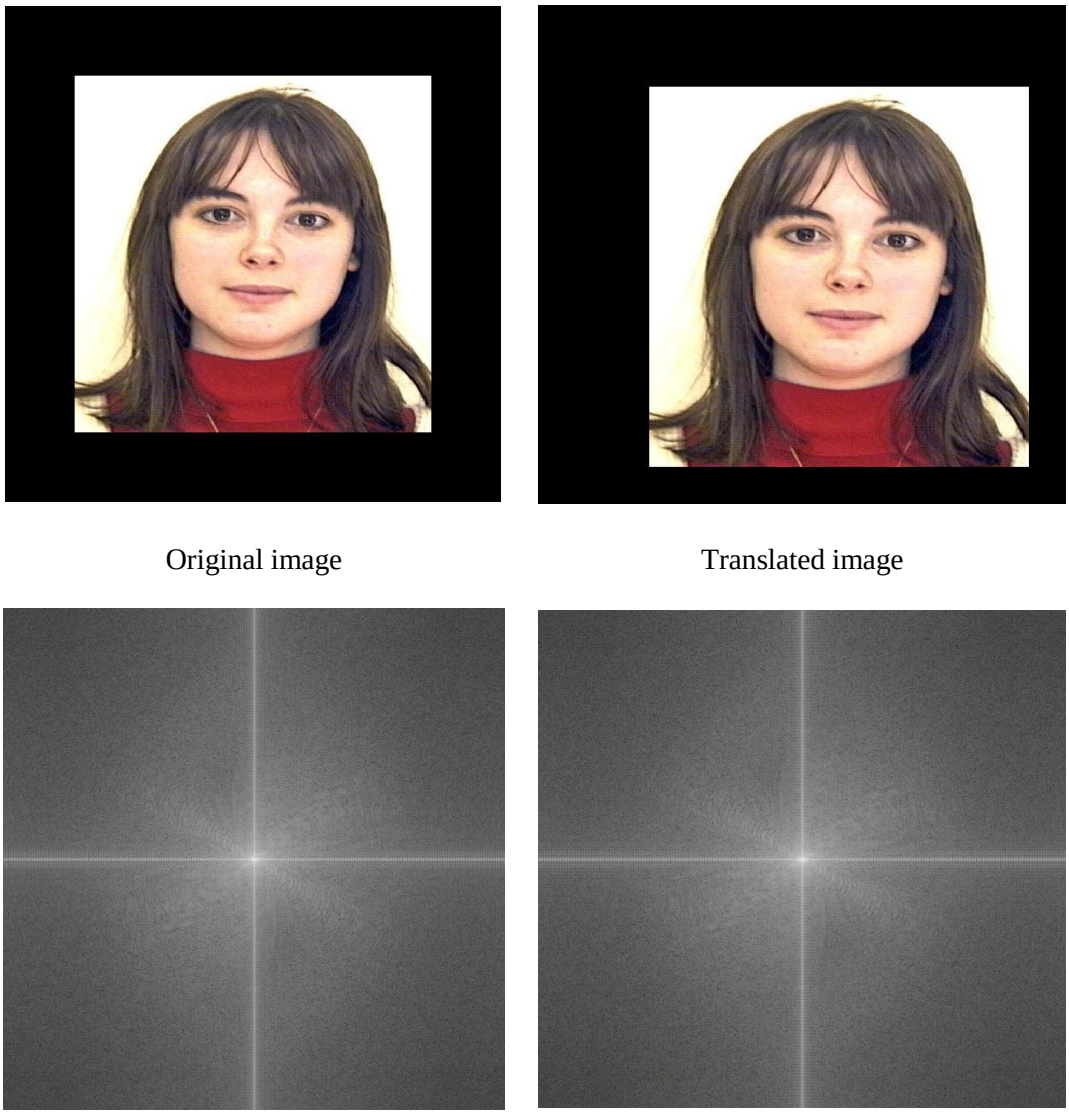
Figure 3-1- An image and its magnitude of DFT.

Watermarking algorithms in Fourier domain take the advantage of Fourier transformation properties against geometric distortions. Those properties are described below:

- *Translation:* spatial shifts of the image generate a linear shift in the phase component of Fourier transform. However, the magnitude component is not affected from the linear translation in spatial domain.

$$f(x+a, y+b) \underset{FT}{\leftrightarrow} |F(u,v)| \exp\big(-j(au+bv)\big), \tag{3-5}$$

  where $f(x,y)$ is the image in spatial domain, $F(u,v)$ is the transformed image in frequency domain and (a,b) denotes the translation factor.



Original image | Translated image

Fourier magnitude of the original image | Fourier magnitude of the translated image

Figure 3-2: Comparison between Fourier magnitude of an image and translated image

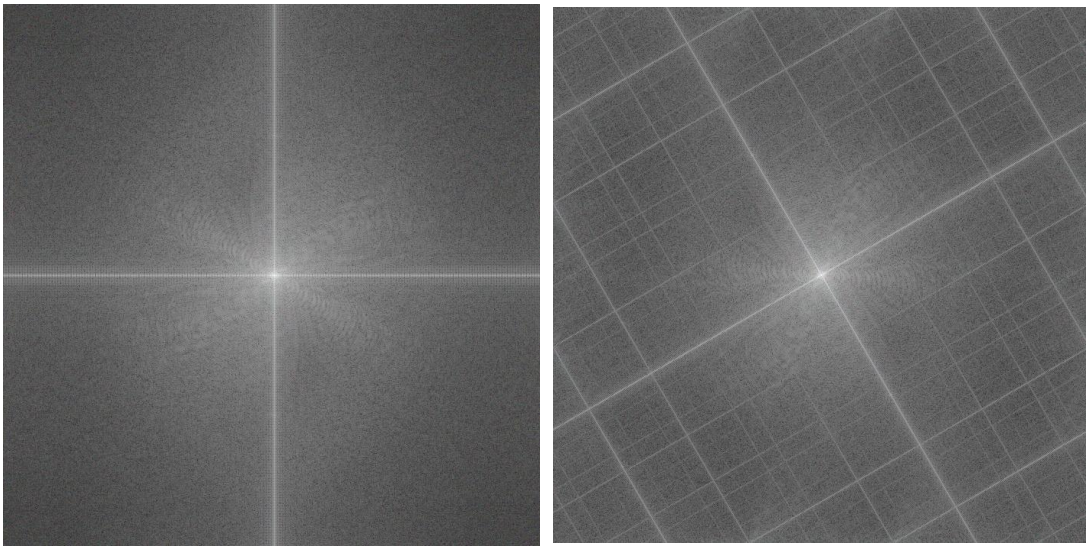
- *Scaling:* Scaling in the spatial domain with a factor k of the image causes an inverse scaling in the frequency domain as expressed in the following equation:

$$f(k.x, k.y) \underset{FT}{\leftrightarrow} \frac{1}{|k|} F\left(\frac{u}{k}, \frac{v}{k}\right). \tag{3-6}$$

- *Rotation:* Rotation of an image through an angle θ in the spatial domain causes the Fourier representation to be rotated through the same angle.

$$f(x.cos\theta - y.sin\theta, x.sin\theta + y.cos\theta) \underset{FT}{\leftrightarrow} F(u.cos\theta - v.sin\theta, u.sin\theta + v.cos\theta). \tag{3-7}$$

Original image | Rotated image with 30°



Fourier magnitude of original image | Fourier magnitude of rotated image

Figure 3-3: Comparison between Fourier magnitude of an image and rotated image

Watermarking methods in Fourier domain take the advantage of two characteristics over spatial domain. The watermark is distributed over the entire image after the Fourier transformation back to the spatial domain, which allows the implementation of stronger watermarks with less perceptual influence [15]. In addition, Fourier magnitude has strong geometric properties. As explained previously, the magnitude is invariant to translation hence the watermarking in this space is robust against spatial translation. To handle the problem of rotation, watermarking methods are proposed in literature where the watermark is inserted in circular manner in the magnitude.

Solachidis and Pitas [42] proposed a watermarking algorithm in Fourier domain robust against translation, rotation and scaling (RST). As we explained earlier, the use of DFT domain makes the algorithm robust against translation. The robustness against rotation is gained by embedding circularly symmetric watermark. In addition, the algorithm is robust against scaling. In the proposed algorithm, DFT is applied on grayscale image with dimension $N \times N$. The inserted watermark consists of 2-D circular symmetric sequence with values ± 1 and has zero mean value. The watermark is embedded with a ring shape covering the middle frequencies in the Fourier magnitude (Figure 3-3).

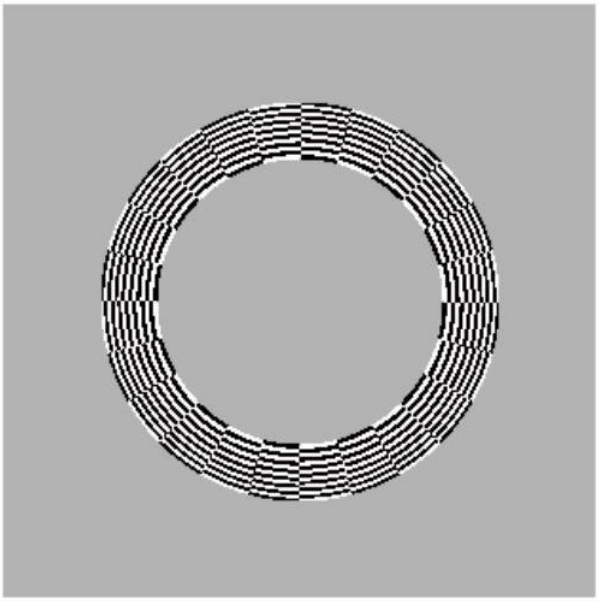


Figure 3-4: Shape of the watermark in DFT domain [42]

The circular pattern of the watermark is mathematically expressed as follow:

$$W(r,\theta) = \begin{cases} 0 & if\ r < R_1 and\ r > R_2 \\ \pm 1 & if\ R_1 < r < R_2 \end{cases} , where \begin{cases} r = \sqrt{u^2 + v^2} \\ \theta = \arctan\left(\frac{v}{u}\right), \end{cases} \quad (3\text{-}8)$$

u and v are the Cartesian coordinates of the watermark. With S sectors and N homocentric sub-rings of radius $r \in \lfloor R_1, R_2 \rfloor$ are forming the ring of $S.N$ pieces. Each piece is assigned with the same value 1 or -1. The watermark embedding is achieved with the following operation

$$M_W(u,v) = M(u,v) + \alpha.W(u,v), \quad (3\text{-}9)$$

where M_W is the coefficients of the watermarked magnitude, M is the coefficients of non-watermarked magnitude and α is the strength factor of the watermark. The

magnitude is rounded to 0 if it becomes negative. The watermarked image is retrieved by applying the inverse DFT.

For detecting the watermark, the correlation c is used to detect the presence of the watermark between the Fourier magnitude of the questioning image M^* and the watermark W:

$$c = \sum_{i=1}^{N}\sum_{j=1}^{N} W(u,v)M_W(u,v), \tag{3-10}$$

we get:

$$c = \sum_{i=1}^{N}\sum_{j=1}^{N} (W(u,v)M(u,v) + \propto W(u,v)W(u,v)) . \tag{3-11}$$

Considering that W and M are independent, and W has zero mean value, the mean value of c is:

$$\mu = \begin{cases} \pi(R_2^2 - R_1^2)\alpha & if\ the\ watermark\ is\ present \\ 0 & otherwise\ the\ watermark\ is\ not\ present \end{cases}. \tag{3-12}$$

Furthermore, the correlation is normalised according to the non-zero value of the μ which results a value in the range [0,1] ($c' = c/\mu$). The obtained value is compared with a threshold t; the watermark is considered as present in the image if it is more than the threshold t, otherwise, the watermark is considered as absent in the image. The threshold value is pre-determined by testing false alarms and non-detections.

Licks and Jordan [43] proposed another watermarking method based on Fourier domain with a circular insertion of the watermark. They used random numbers in order to predefine 1 and -1 ones as the watermark signal values and they do not use sectors as the previous method. However, in this case the watermark would not be circularly symmetric. In this approach, the algorithm is robust against linear translations. If the image is rotated then the magnitude suffers from rotation with the same angle. As a result, a circular translation with the same angle will occur to the watermark. Therefore, in the detection phase, cross-correlation is computed to detect the presence of the watermark in the image. For the improvement of this algorithm, Poljiack *et* al.[44] determined an optimal radius for watermark insertion to minimize quality degradation. In addition, PSNR is used as metric to evaluate the visual quality of the watermarked image. For detection process, maximum of a cross-correlation between

the watermark and the image is computed and compared with a threshold value to detect the presence of the watermark in the image.

3.2.2.2 Log-polar transform

Log-Polar transform is an image-processing tool known for its rotation and scaling properties [45], [46]. It is a sampling method used to convert image from the Cartesian coordinates $I(x,y)$ to the log-polar coordinates $LP\,(\rho,\theta)$. The mathematical expression of the mapping procedure is shown below:

$$(x,y) \xleftrightarrow{Polar\ transform} (r,\theta) \xleftrightarrow{log-polar\ transform} (\rho,\theta)$$

$$\begin{cases} x = rcos\theta \\ y = rsin\theta \end{cases} \leftrightarrow \begin{cases} r = \sqrt{x^2+y^2} \\ \theta = tan^{-1}\dfrac{y}{x} \end{cases} \leftrightarrow \begin{cases} \rho = \log(r) = log\sqrt{x^2+y^2} \\ \theta = tan^{-1}\dfrac{y}{x} \end{cases} \qquad (3\text{-}13)$$

where (x,y) represents the sampling pixel in the Cartesian coordinates, (r,θ) represents the radius and the angular position in the polar coordinates and (ρ,θ) represents the log-radius and the angular position in the log polar coordinates. Log-polar sampling is accomplished by mapping image pixels in the Cartesian to the log-polar coordinates according to equations (3-8) (figure 3- 4).

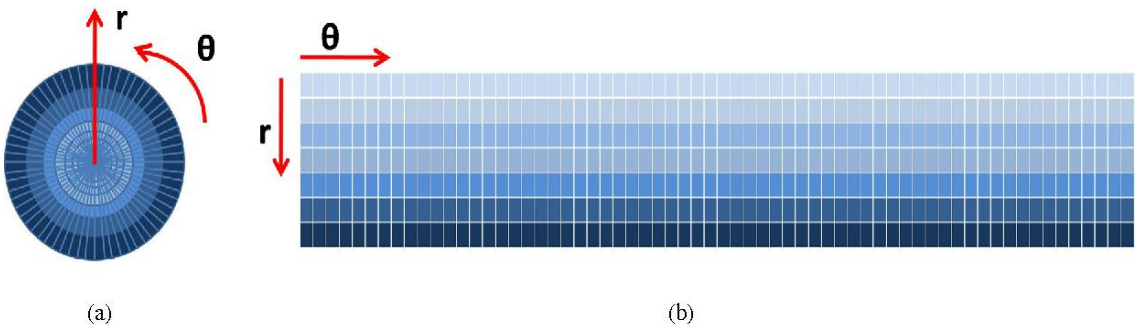


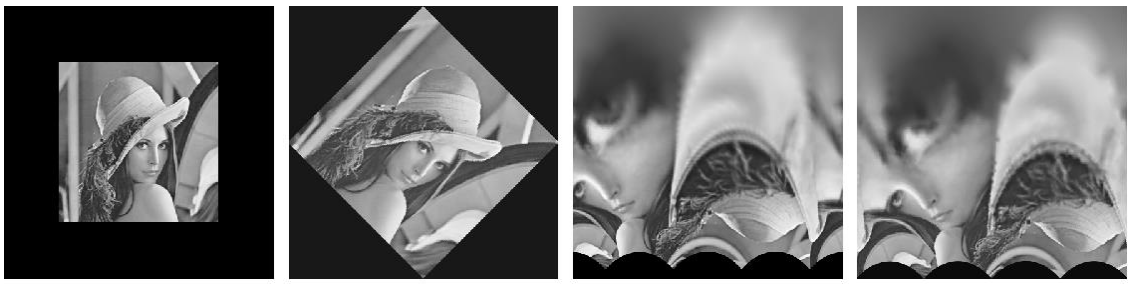
Figure 3-5- Log-polar transform sampling in the Cartesian Coordinates, (b) the resulting sample distribution in the angular and log-radius directions [47].

The geometric advantage of using log-polar transform over the Cartesian coordinates representation is that any rotation and scale in the Cartesian coordinates is converted into a translation in the angular and the log-radius directions of the log-polar coordinates, respectively, as shown below:

- *Scaling:* scaling in the spatial domain with a factor k of the image in Cartesian coordinates is converted into translation according the log-radius axis in the log-polar coordinates. as mathematically expressed in the following equation:

$$(k.x, k.y) \leftrightarrow (k.r, \theta) \leftrightarrow (\log(k.r), \theta) = (\rho + \log(k), \theta). \quad (3\text{-}14)$$

- *Rotation:* Rotation of an image with an angle φ in Cartesian coordinates causes translation according the angular axis in the log-polar coordinates.



(a) (b) (c) (d)

Figure 3-6: (a) The original image *Lena*, (b) the scaled and rotated image of (a), (c) the log-polar transformed image of (a), and (d) the log-polar transformed image of (b) [47].

3.2.2.3 Fourier-Mellin domain

Fourier-Mellin transform of an image f in polar coordinates (r, θ) can be expressed as follow:

$$FM(u, v) = \frac{1}{2\pi} \int_0^{2\pi} \int_0^{\infty} f(r, \theta) r^{-jv-1} e^{-ju\theta} \, dr d\theta, \quad (3\text{-}15)$$

where (u, v) are the transform coordinates in Fourier-Mellin domain. The integral related to r variable represent the expression of Mellin transform such that:

$$M(-jv) = \int_{-\infty}^{\infty} g_\theta(r) r^{-jv-1} dr, \quad (3\text{-}16)$$

where $g_\theta(r) = f(r, \theta)$. The equation (3-16) can be simplified using integral by substitution technique as explained in the following:

Set log polar coordinates with $\begin{cases} \rho = \ln(r) \\ r = e^{\rho} \end{cases}$ this means $\mathrm{d}\rho = \frac{dr}{r}$. Applying the change of variable into equation (3-16) the result equation becomes:

$$FM(u,v) = \frac{1}{2\pi}\int_{0}^{2\pi}\int_{-\infty}^{\infty} f(e^{\rho},\theta)e^{-jv\rho}e^{-ju\theta}\,d\rho d\theta. \quad (3\text{-}16)$$

Now making $s(\rho,\theta) = f(e^{\rho},\theta)$, the equation (3-16) becomes:

$$FM(u,v) = \frac{1}{2\pi}\int_{0}^{2\pi}\int_{-\infty}^{\infty} s(\rho,\theta)e^{-j(v\rho+u\theta)}\,d\rho d\theta, \quad (3\text{-}17)$$

which is the mathematical expression of Fourier transform of a function s in log-polar coordinates. As a result, Fourier-Mellin transform can be expressed as Fourier transform of a function in log-polar coordinates.

In image processing field, Fourier-Mellin domain is described by Ruanaidh and Pun [19]. Figure 3-6 illustrates the process of obtaining the RST transformation invariant from a digital image. The watermark takes the form of two-dimensional spread spectrum signal in the RST transformation invariant domain. First, DFT is applied and then followed by a Fourier-Mellin transform (FMT- A log-polar mapping (LPM) followed by a Fourier transform). The invariant coefficients selected for their robustness to image processing are marked using a spread spectrum signal. The inverse mapping is computed as an inverse Fourier transform (IDFT) followed by an inverse Fourier-Mellin transform (IFMT- An inverse log-polar mapping (ILPM) followed by an inverse IDFT). The inverse transformation from RST invariant domain to the image domain uses the phase computed during the forward transformations from image domain to the RST invariant domain.

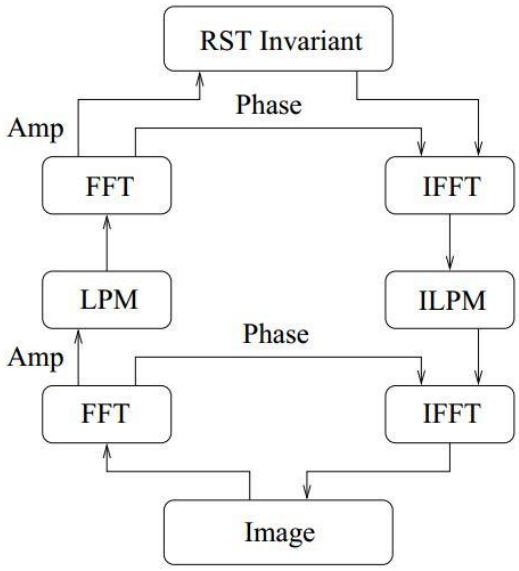


Figure 3-7: Prototype of RST invariant watermarking scheme based on Fourier-Mellin transform [19].

To detect the watermark, the image is transformed to the RST invariant domain and the watermark is decoded.

The purpose of using log-polar mapping is to find a representation in which rotation and scaling operations are converted to linear shifts, as explained in the previous paragraph. This transformation maps the spatial coordinatesx axis (x, y) to polar axis (ρ, θ) equation (3-8). Hence, if we apply Fourier transform to the log-polar representation, we obtain a rotation and scale invariant domain because of the shift invariance property of Fourier transform. The problem in this theoretically RST invariant method is related to its implementation. When applied on a digital image, the transformations require a lot rounding because of the trigonometric and logarithmic operators. This rounding causes a large amount of loss in the data, which results in huge amount of image quality loss. In practice, this solution can be implemented for small RST deformations, but it is inapplicable as soon as the image undergoes to real geometrical deformations. Moreover, problems of approximation due to the discrete nature of the images, plus the reduction of the embedding space make the watermark weakly resistant to low-pass filtering and lossy compression [48].

3.2.3 Watermark re-synchronization

Image features represent an invariant reference to geometric distortions, which solve the problem of watermark synchronization. In this case watermark location is related

to image semantics rather than image spatial coordinates [49]. This section reviews watermark synchronization methods using image features to extract the patches. Those methods can be divided into two categories: feature point-based synchronization and region-based synchronization.

3.2.3.1 Feature point-based synchronization

Feature-based synchronization method first described by Kutter et al. [49]. They extract feature points using a scale interaction technique based on 2D continuous wavelet. These points are utilized to segment the image, using a Voronoi diagram partitioning of the image such that all pixels in the image were closer to the location of the feature points. The spread spectrum watermark is embedded into each segment separately. This method is robust to most attacks. It however fails to synchronize the location of the watermark because the feature points from the scale interaction technique are sensitive to changes of image scale. Similarly, Bas et al. [50] proposed a synchronization method. Using differential features of the image, they extract feature points by applying the Harris corner detector. The feature points are decomposed into a set of disjoint triangles by Delaunay tessellation that is the straight line dual of the corresponding Voronoi diagram collected by joining all pairs of points. The result triangles are watermarked by the additive spread-spectrum method on the spatial domain (Figure 3-7). The weakness of this method is that Harris corner detector uses differential features, which are sensitive to image noise. As a result, the set of extracted feature points from the original and attacked images do not match. Therefore, the set of triangles from the feature points of the original and attacked images differ significantly and the resulting patches do not correspond. Tang and Hang [51] use for watermark synchronization, intensity-based feature extraction with image normalization. First, they extract feature points using the Mexican Hat wavelet scale interaction method that determines feature points by identifying changes in intensity in the image. By using the feature points as centers, disks of fixed radius R are normalized to achieve geometric-distortion invariance. These normalized disks are watermarked on the frequency domain. Although this method works well in response of most attacks, it fails against scaling distortion, because radius of the disks are fixed in such a manner that different contents are used for normalization. With Ye et al. [52], scale invariant feature transform (SIFT) is used to produce circular regions for watermark insertion. This type of watermarking method requires that the group of

feature points used for insertion process should be found the same in the detection process, which is non-trivial especially in the presence of projective transformations.

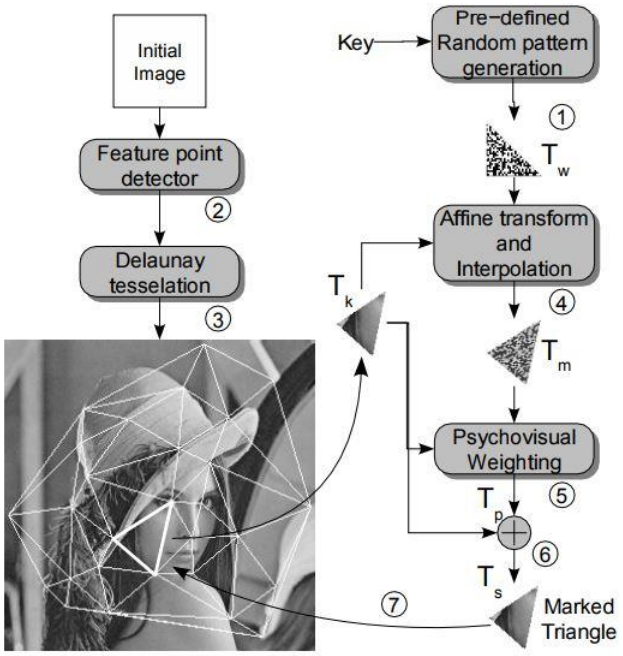


Figure 3-8: feature based watermarking insertion proposed by Bas et al. [50].

3.2.3.2 Region based synchronization

Nikolaidis and Pitas [53] described an image-segmentation based synchronization method. An adaptive k-mean clustering technique is applied to segment images and select a set of the largest regions. The bounding rectangles of these regions are adopted as the patches for watermarking. The segment regions are failed to resist sever geometric attacks. Considering image segmentation depends on image contents, geometric attacks such as projective transformations critically affect the segmentation results. Moreover, in case the images have complex texture, extraction of patches become more complex.

For watermark synchronization using image semantics, the robustness of the methods is highly dependent to the exact extraction of the patches. When the patches differ during watermark insertion and detection, it is impossible or difficult to prove existence of the watermark. Hence, it is important to select carefully the features to be extracted for determining the patches.

3.2.4 Image re-synchronization using template-based techniques

Image re-synchronization methods are achieved with Synchronization or registration pattern that is embedded into cover image to simplify watermark search. One of the most direct solutions to solve the synchronization attacks is composed of inserting templates along with the watermark or embedding a periodic watermark pattern into the image. Generally, templates with known structure helps to reflect the geometric distortion. These additional templates [54] are used as artificially embedded references for resynchronization goal only. The template-based approach performs the watermark retrieval process by approving the presence of a watermark and estimating and rectifying the severe geometric transformation of the watermarked image [55]. Therefore, the synchronization pattern is classified and provided resilience to geometric attacks [50].

Fourier domain, not only a watermark embedding space, but also it is used as template embedding space. Peireira et al. [56] proposed a watermarking method using the concept of a template which carries no information on itself. In this scheme, the embedding process consists of two-part a spread spectrum signal as watermark and a template. The watermark signal is embedded using DFT along with a template. In this case, template enables to understand the geometric transformation applied to the watermarked image in order to synchronize the watermark. This method is capable of solving the RST transformation only. Kang et al. [57] suggested a template based watermarking scheme using both DWT and DFT. In this proposed method, the watermark is embedded in the coefficient of the LL band of the DWT domain and a template in the middle frequency component of the DFT domain. Their scheme achieved robustness against JPEG compression and affine transform. However, it was not robust against some common image processing attacks

The template-based algorithms generally are relevant to adaptive determination in the strength of the templates for reducing the search space. Meanwhile, the template is restricted to the number of embedded patterns, which contributes to be the counterpart of unaccepted false positive probabilities in the parameter estimation of the applied geometric transformation. In addition, the process of the successful watermark detection, similarly as feature-based algorithms, relies to the precise detection of the template because the detection error tolerance is highly influenced by the inaccuracy of the detected position. Although an amount of progress for utilizing

template-based watermarking techniques, they are sensitive to the perceptual similarity between the original and watermarked image. The embedding of the watermark with the template should take the insertion position and strength into account carefully. Usually, templates are used to be inserted as pseudorandom noise patterns and under some specific operations, as filtering operators, can filter potentially out the local maxima. Then, the applied templates are damaged easily by the malicious attack and the applied various geometric transformations are hard to be recognized during the template detection process. In brief, the major limitation is that this kind of approach has a severe effect on the resistance of higher level of geometric transformations engaging with threats and risks of the template attack [48].

3.3 PRINT-CAM IMAGE WATERMARKING RELATED WORKS

In 2004, Nakamura et al. [58] and Katayama et al. [59] were among the first papers to argue the need for Print-Cam image watermarking. They proposed a watermarking embedding and detection method in the spatial domain for camera-equipped cellular phones that resisted to geometrical distortions by using frame synchronization. The geometric correction is achieved with following equations:

$$\begin{cases} x' = \dfrac{a_1 x + b_1 y + c_1}{a_0 x + b_0 y + c_0}, \\ y' = \dfrac{a_2 x + b_2 y + c_2}{a_0 x + b_0 y + c_0}, \end{cases} \tag{3-15}$$

where (x', y') are frame positions in the original picture, (x, y) are detected frame position in the camera picture and $(a_0, b_0, c_0; a_1, b_1, c_1; a_2, b_2, c_2)$ are the matrix parameters of the geometric transformation. Corners of the frame was detected using an exhaustive search of the left and right sides of the image. They relied on thresholding and judged a point to be part of the frame if the result on the frame detection filter at that point was greater than the predefined threshold. However, the correct threshold changes from image to image and even over the same image with lighting variation and therefore defining right threshold values is difficult even with adaptive threshold estimating methods. Moreover, their method was robust to small geometric distortions. Correspondingly, Liu and Shieh (2011) [60] suggested an improvement of the watermarking method used by Nakamura et al. [58] by controlling the watermark strength using the Watson model for JND (Just Noticeable Difference) calculation. This improved the capacity by reducing the size of the watermark blocks.

Their experiment of two different position-detection patterns influenced by 2D-barcodes drew a conclusion that a frame is the most efficient tool for the synchronization of a watermark signal.

Takeuchi et al. [61], in 2005, also applied a frame on the watermarked image to overcome geometric distortions, using guided scrambling techniques for the watermark embedding. Their method showed an improvement in robustness against geometric lens distortion, but like the previous papers, it resists to small geometric distortions.

Kim et al. [62], in 2006, proposed a embedding process in the spatial domain. They used a spatial template to predict geometric distortions. This technique showed good results in terms of watermark detection. However, they used a tripod in the capturing process to reduce the geometric deformations. In 2008, Nuutinen and Oittinen [63] experiment a watermark embedding scheme in spatial domain using block-by-block technique. A bit was inserted by changing intensity values between two adjacent blocks. The bit was extracted by comparing the mean intensity values of the neighboring blocks. The method was robust to strong geometric distortions. The authors used a capturing distance of 10 cm and the image was captured perpendicularly. Their work was a combination of designing the watermarking method and testing the method in different color spaces and perceptibility of the watermark in the color spaces. As a result, they concluded that the Y-channel of the YCbCr transformed image is the most robust, but still the blue channel of RGB (Red, Green, Blue) works better respecting the imperceptibility requirement. Similarly, in 2010 Takimoto et al. [64] mentioned that HVS is least sensitive to the blue color. They proposed a circular synchronization template, which was inserted in the blue channel. The method was tested on captured images with a camera phone but no information about testing protocol or capturing angles was stated.

The term of Print-Cam process was used for the first time in 2008 by Pramila et al. [3]. They proposed a discrete wavelet transform (DWT) based watermarking technique, drawing on work by Keskinarkaus et al. [65]. The embedding technique was originally proposed for the print-scan process. The multibit message was embedded in the Haar wavelet transform domain with spread spectrum techniques with:

$$\begin{cases} y^{Cm}(n) = y^{C}(n) + \beta . m(k), & messagebit = 1, \\ y^{Cm}(n) = y^{C}(n) - \beta . m(k), & messagebit = 0, \end{cases} \quad (3\text{-}16)$$

where m is the watermark sequence, y^C is the approximation coefficients or detail coefficients of the wavelet transformed image, and β is embedding strength coefficient. The watermark was extracted by cross-correlating the same m-sequence and thresholding the result. If the cross-correlation value was above the threshold, the detected value was 1 otherwise it was 0. Geometric synchronization is retrieved using frame detector filter as in figure 3-8 in order to find the four corners of the frame and estimate the geometric parameter in the equation (3-10). As the images had to be captured with care, their method showed resistance to strong geometric distortions.

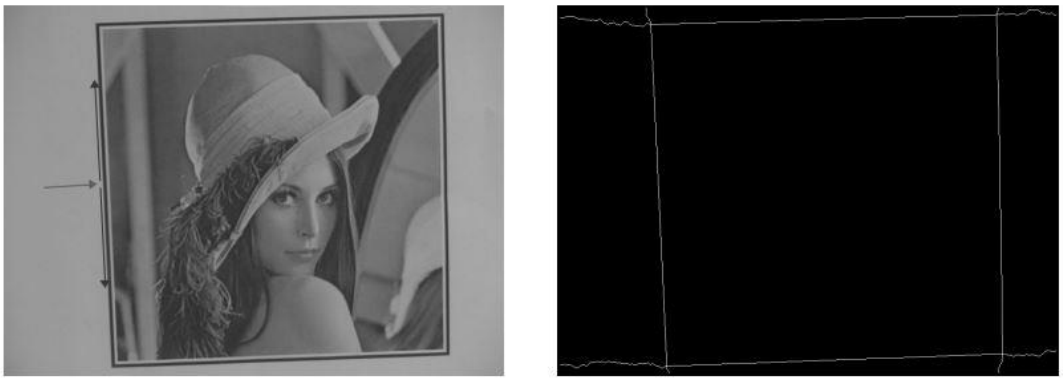


Figure 3-9: The frame is determined by searching along a crosswise line and advancing up and down the side of the frame. The second image shows the detected frame [3].

In 2009, Pramila el al. [66] proposed a Print-Cam watermarking method to extract a watermark from binary image. The watermark is a small binary image (logo) which is protected with (15, 11) Hamming error coding and inserted in the binary image using flippability scores of the pixels and block-based relationship. The frame is added to the image in order to overcome projective distortions and lens distortions are corrected by calibrating the camera. The obtained results for this proposed method are shown for images captured freehandedly by rotation the camera within the range -2 and +2 degrees. For correct extraction of the watermark in this method, the image needs to be perfectly inverted from the distortion pixel by pixel. In 2012, Pramila et al. [67] proposed a different print-cam watermarking method with no frame. Instead, they used a watermarking method based on pseudorandom sequences and autocorrelation function in the spatial domain for color images. They used the same watermarking method in 2016 with an all-in-focus imaging technique to solve the unfocused image problem in the capturing process [4].

Horiuchi et al. [68], in 2009, proposed an image watermarking method based on spatial domain using a template in the frequency domain print-cam process. In principle, the watermark is inserted in the spatial domain by superimposing the message transformed by the inverse discrete Fourier transformation on the image as shown in figure 3-9. However, The paper does not show the robustness of the method against geometric distortions.

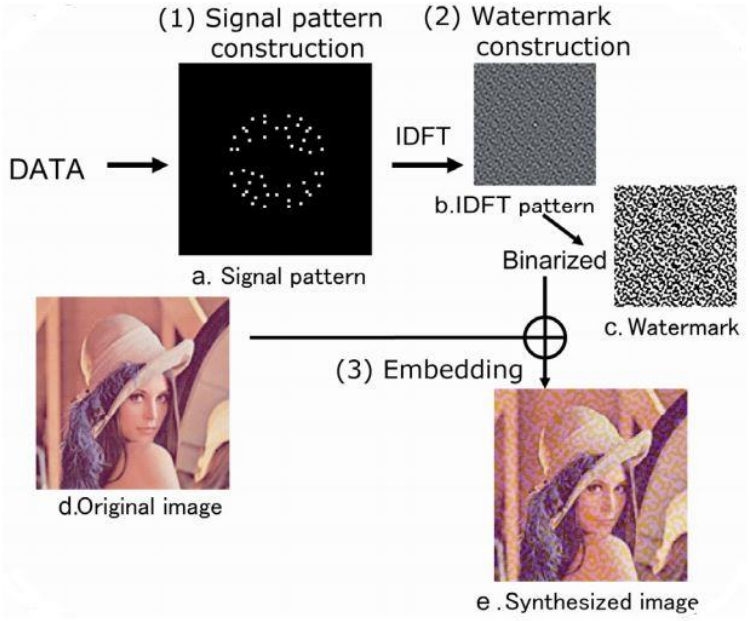


Figure 3-10: Watermark embedding process proposed by Horiuchi et al. [68].

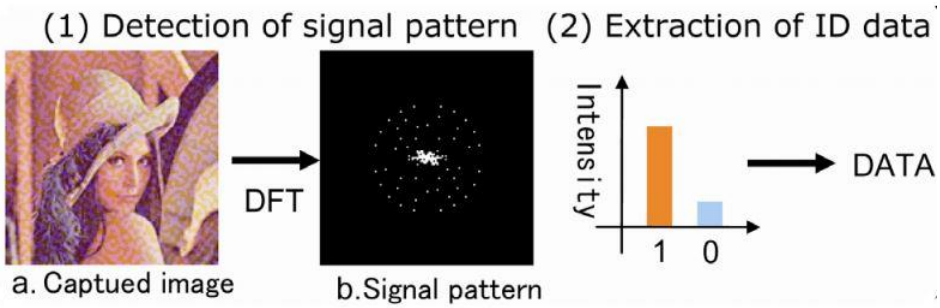


Figure 3-11: Watermark Extraction process proposed by Horiuchi et al. [68].

In 2012, Thongkor et Amornraksa [69] applied the existing print-cam watermarking schemes to images of Thai ID cards. The system used a spatial domain watermarking method, and the embedding process was performed in the blue color channel of the picture by applying the following equation (3-12) and (3-13):

$$B'(i,j) = B(i,j) + W(i,j)\, s\, L(i,j), \tag{3-20}$$

$$L(i,j) = 0.299R(i,j) + 0.587G(i,j) + 0.114B(i,j), \quad (3\text{-}21)$$

where $B(i,j)$ and $B'(i,j)$ represent respectively blue channel components of the original and watermarked image at the coordinate (i,j), $W(i,j)$ is the embedded watermak, s represents the embedding strength factor. $L(i,j)$ is the luminance component of each of each embedding pixel where $R(i,j)$, $G(i,j)$ and $B(i,j)$ represents respectively Red, Green and Blue color components at the coordinates (i,j). For extraction process the estimated watermarked bit $w'(i,j)$ at (i,j) is obtained by the following equation:

$$w'(i,j) = B'(i,j) - B"(i,j), \quad (3\text{-}17)$$

where $B'(i,j)$ is the blue channel pixel of the watermarked image at coordinates (i,j) and $B"(i,j)$ is the average of $B'(i,j)$ nearby watermarked image pixels. Zero value is set as threshold if $w'(i,j)$ is negative the watermark bit is estimated as 0 and if it is positive it is estimated as 1. The authers used the original image to rectify the distorted image geometrically by selecting manually the feature points from both original and watermarked image to estimate the geometric transformation matrix. Although the method gave good results, it is a non-blind method that requires original image for each geometric correction process. Under the same conditions, Thongkor et Amornrksa [5] suggested in 2014, an improvement of their previous method using a JND model for embedding process and an automatic registration technique, but this technique still requires adjusting the original watermarked image with the captured image for geometric registration.

In 2013, Delgado-Guillen et al. [70] proposed a watermarking method for mobile platforms based on Fourier and log-polar transformations. Also in 2015, Ouyang et al. [71] proposed a modified version of Fourier-Mellin based watermarking method using quaternion Fourier transform. However, both their results did not cover robustness against projective distortions. In 2016, Moritani et al. [72] proposed embedding method based on block division and code diffusion in DCT domain for captured image. They used Sobel edge detector to detect the edges of the image to correct the perspective distortion. The method was designed for unknown resolution and number of blocks of the original watermarked image. They inserted markers in the DFT domain to indicate resolution and number of blocks in which the watermark was embedded. In 2017, H. AL-Otum et Shalabi [73] proposed a spatial watermarking method for smartphone using quick respond code, same for Takishita et al. [74]

proposed a watermarking method based on DWT transform for 2D code, however the presented tests do not cover the projective deformations. Nam-Tuan Le [75] proposed spatial based watermarking method where the projective deformations are corrected using multiple captures of the same picture.

3.4 SYNTHESIS OF THE PRESENTED METHODS

Print-Cam image watermarking system is a watermarking system that includes the processing of printed and phone-captured images. Attacks related to this system can be classified as attacks related to the materials, in this case the printer and the camera of the smartphone, like blur, noises, color variation and geometric distortion in form of lens distortion. In addition, there are attacks related to the user, which produce the projective distortion from taking picture freehandedly. Finally, attacks related to environments that produce light variation from taking pictures in dark environment or with one or many sources of lighting. Robustness of a watermarking method is the core requirement that indicates the efficiency of the method for application. Geometric attack represents one of the major problems that disturbs the robustness of image watermarking technique.

In Print-Cam system, the geometric attacks are in form of projective transformation, which is a combination of rotation, scaling, translation and tilting of the optical axis of the camera. In general, geometric attacks are handled over years in watermarking field with one or a combination of four major strategies: exhaustive search, invariant domain, feature based scheme and template-based scheme. Exhaustive search is a simple method but the less efficient because it consumes more of time computation to process all the possible parameter values of the distortion. For invariant domain, up to our knowledge there is no domain utilized in watermarking field that is invariant to projective transformation. The highest geometric invariant domain was Log-polar transform, which is invariant to rotation, translation and scaling (RST). Further, most of proposed feature-based methods require the presence of original image for geometric registration, which leads to a non-blind scheme. In addition, template-based methods involve additional data insertion for the template or fix a known reference as a template for geometric registration which is not possible for all kind of images.

Comparing Print-Scan image watermarking methods, related works to Print-Cam methods are not as widely studied in watermarking field even with the huge advancement of the technologies of smartphones and its cameras. Mostly the reason for that is related to the unsolved problem of the projective transformation. Hence, few works are proposed over years related to Print-Cam system. However, there is no universal method that solve all problems related to the system. As observations of the related works, spatial and wavelet transform watermarking methods are the most used embedding domains for the Print-Cam process and almost there is an absence of using Fourier transform as embedding space for Print-Cam system. Yet, the Fourier based watermarking method is known to be more resistant to geometric distortions (except scale changes and tilt of optical axis distortions). Template based method in form of frame synchronization of the image is designed in the majority of the proposed works.

Chapter 4: Print-Cam image Watermarking Method

4.1 INTRODUCTION

In this chapter, we will first describe watermarking method in Fourier domain. This method provides the robust, imperceptible and blind detection needed for ID images. The focus is to present a robust watermarking method against the main attacks in Print-Cam system; geometric distortion, blur and colour degradations.

The proposed system is presented in Figure 4-1. The watermark is first embedded in the input image. After the print-cam process, the captured image is treated with three different correction steps: a frame-based perspective registration, a Wiener filter to decrease image blurring and adjustment to eliminate colour degradations. Finally, the decision is taken, during the detection process, whether the pre-processed image is watermarked or not. The adapted watermarking method is summarized in Figure 4-1.

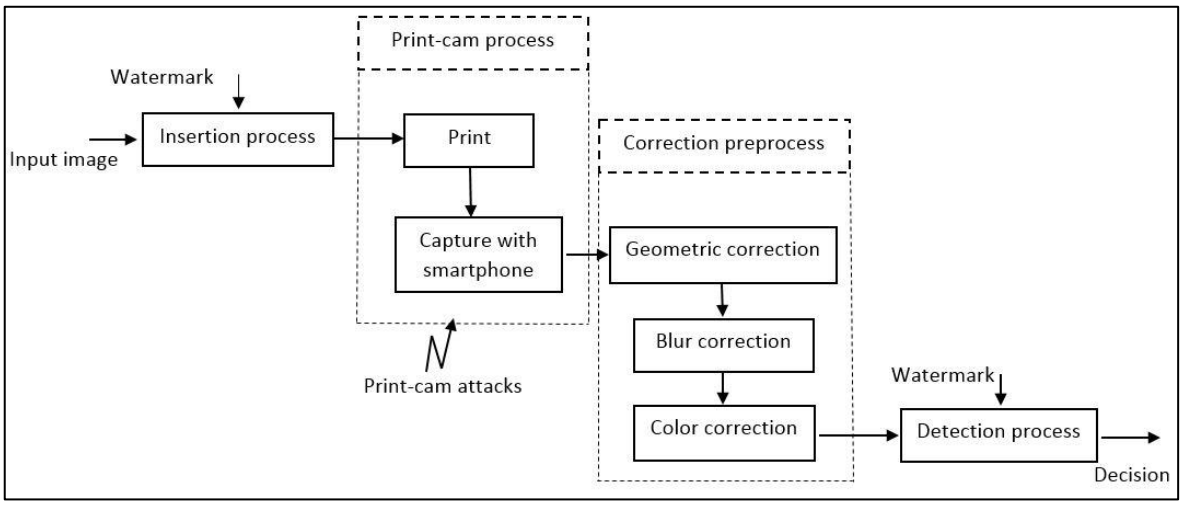


Figure 4-1: Print-cam watermarking process

4.2 FOURIER BASED WATERMARKING METHOD

Several watermarking methods based on the Fourier transform have been developed over years [76], [15], [16]. Generally, the watermark is inserted in the magnitude

coefficients of the DFT of the image. The Figure 4-2 shows a general scheme of watermarking in Fourier domain. Initially, the Fourier transform is applied to the original image. Only the luminance channel is concerned in the case of color images. Then, the watermark is inserted in some magnitude coefficients of the Fourier transform of the image, the phase is not modified. Finally, the watermarked image is reconstructed from the watermarked magnitude and the phase by applying the inverse of Fourier transform. Watermark detection is performed by calculating the cross-correlation between the coefficients of both watermark and Fourier magnitude of the image. In this case, the original image is not needed for detection phase. Licks and Hordan [43] are the first suggested an insertion of a circular watermark in the Fourier transformation to resist the rotation of the image. Poljicak et al. [15] proposed insertion in an optimal radius circle that maximizes the PSNR. Riad et al. [77] improved the circular insertion along with the optimal radius by reducing the variance of the selected magnitude coefficients for better detection.

4.2.1 Insertion method

Watermark embedding is performed in the DFT magnitude of the luminance channel of the original image. In the case of colour images, the luminance is obtained by a transformation of the space RGB colors to space Ycbcr. A symmetric watermark is inserted along a circle of radius r in the DFT magnitude [77], The watermark is generated from a pseudo-random sequence v using a secret key k which represents the seed of the pseudo random generator of +1 and -1. The vector v of l elements is of zero mean and unit variance. Knowing the radius of the circle where the watermark better be inserted, the watermark W is created using the following equation:

$$W(x_i, y_i) = v(j)\left[\frac{1}{9}\sum_{s=1}^{l+1}\sum_{t=1}^{l+1} M(x_i + s, y_i + t)\right], \qquad (4\text{-}1)$$

where $W(x_i, y_i)$ are the coefficients of the watermark, $v(j)$ represents the element of the sequence v with coordinate j, and $M(x_i, y_i)$ are the coefficients the Fourier magnitude of the original image. For more stability, smoothing of the coefficient M is introduced with its eight neighbours as shown the equation 4-1.

Coordinates (x_i, y_i) are obtained from the following equation:

$$x_i = \left(\frac{m}{2} + 1\right) + round(rcos\left(\frac{j.\pi}{l}\right)), \quad (4\text{-}2)$$

$$y_i = \left(\frac{n}{2} + 1\right) + round(rsin\left(\frac{j.\pi}{l}\right)), \quad (4\text{-}3)$$

where m and n represent the size of the image, r is the radius of the circle where the watermark will be inserted and l length of the vector v. Moreover, the application of a dedicated low-pass filtering on the embeddable coefficients of the DFT magnitude improves the detection rate. Hence, the watermark W of l elements is inserted in the filtered coefficients as follows:

$$M_W = M_f + \alpha \times W, \quad (4\text{-}4)$$

where M_W is the magnitude of the watermarked DFT coefficient, M_f is the original one after filtering the embeddable coefficients using a Gaussian filter, and α is the strength parameter. The choice of α is related to the invisibility of the watermark. In the proposed method, the watermark is spread over all the image pixels taking into account the peak signal-to-noise ratio (PSNR) metric. Therefore, an adaptive strength α is determined to obtain the desired value of PSNR, in general equal to 40dB [15], [24]. The final watermarked image is reconstructed by applying the inverse DFT to obtain the luminance of the watermarked image from which color image is recovered using the unmodified chrominance components.

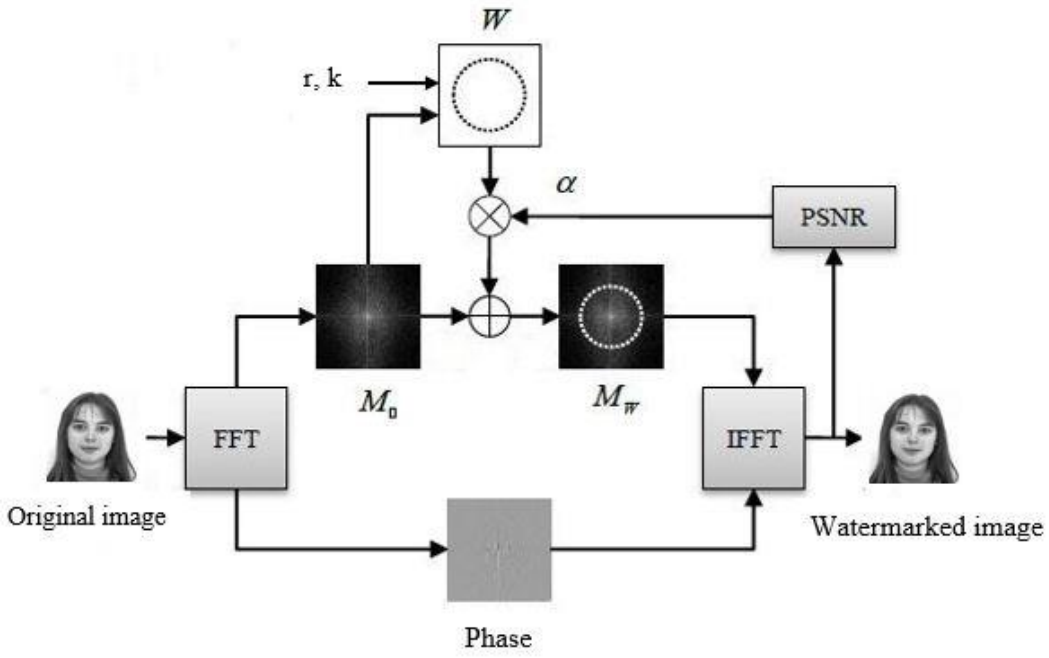


Figure 4-2- Watermark detection in Fourier domain.

4.2.2 Detection method

4.2.2.1 Watermark detection

The decoder performs a blind watermark detection. As a result, the original image is not required in the detection phase. The only requirement is the key k used in insertion phase to generate vector v and the image to be tested. The blind decoder needs only the captured image and the watermark W generated by the key k using Pseudo Random number (PRND) Figure 4-3. First, the DFT is applied to the luminance of the captured image. Then, the coefficients are extracted from the magnitude along the radius r. The maximum of the normalized cross-correlation $Cmax$ is computed between the extracted coefficients F and the sequence W of the watermark:

$$C_{Max} = \underset{0\le j\le N-1}{\text{Max}}\left(\frac{\sum_{i=0}^{N-1}(W(i)-\bar{W})(F(i+j)-\bar{F})}{\sqrt{\sum_{i=0}^{N-1}(W(i)-\bar{W})^2 \sum_{i=0}^{N-1}(F(i+j)-\bar{F})^2}} \right), \qquad (4\text{-}5)$$

where N is the sequence length, $\bar{W}$ and $\bar{F}$ are the means of the watermark and extracted Fourier coefficients respectively. The watermark is said to be present if the maximum value of the normalized cross-correlation exceeds a threshold t.

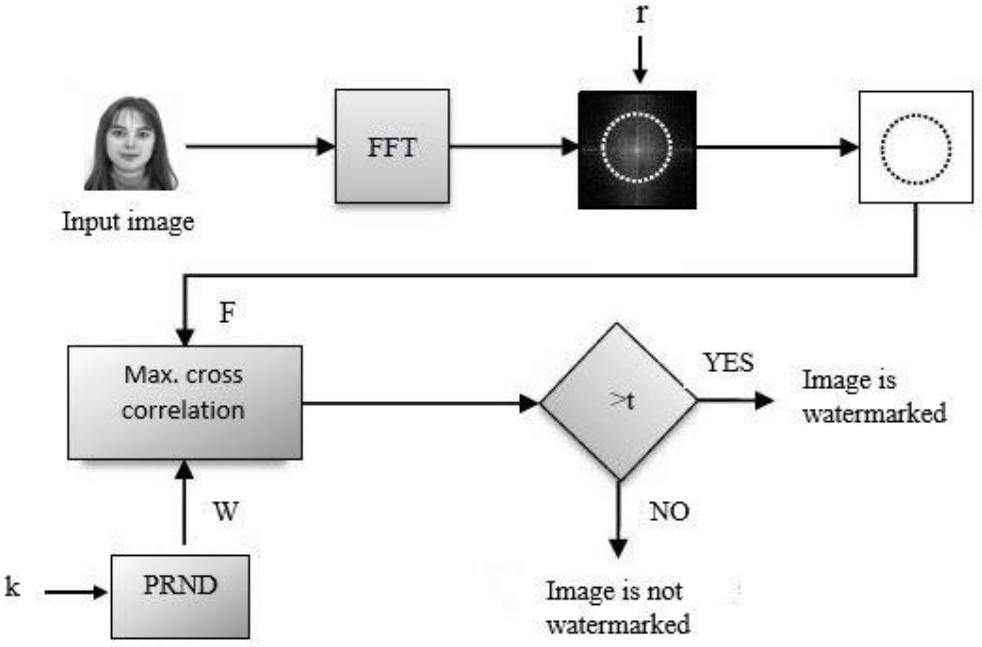


Figure 4-3:Watermark detection in Fourier domain.

4.2.2.2 Threshold estimation

Detection of watermark can be achieved by using statistical methods. Therefore, choosing an appropriate statistical model, for each watermarking domain, is of a great

importance. In general, the detection theory problems are often formulated as a classical hypothesis testing problem; with the null hypothesis ($H0$) for image without watermark, and the alternative hypothesis ($H1$) for image containing the watermark [78].

The threshold decision or the criterion response must be taken based on observations of a set of watermarked and non-watermarked images. To obtain an optimum solution for such a problem with respect to some criteria, many researchers have used the Bayesian hypothesis testing approach where the criterion is a minimization of Bayesian risk. This minimization leads to a decision based on the likelihood ratio (or log-likelihood ratio) $l(x)$ defined as:

$$l(x) = \frac{p(x \mid H_1)}{p(x \mid H_0)}, \tag{4-6}$$

where $p(x|H_i)$ is the probability density function (pdf) of the host feature x under the hypothesis H_i. The following Figure 4-4 present example of pdf under H_0 and H_1.

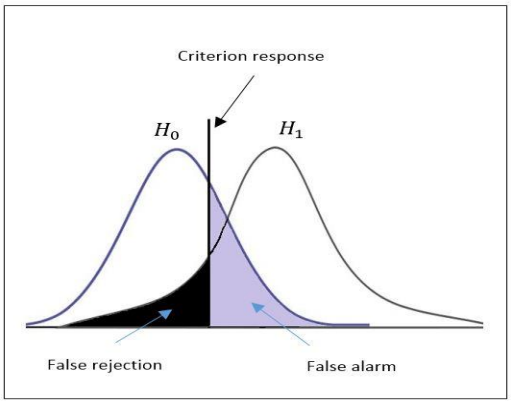


Figure 4-4: Illustration of distribution of density probability function (pdf) under hypothesis H0 and H1

From the above formulation, the decision is made by comparing the likelihood ratio against a detection threshold t. In general, in order to compute $l(x)$ (via this, we determine the detector structure) and t (for analyzing errors), it requires that the statistical distribution of the coefficients of the magnitude, the watermark, the embedding rule as well as the attacks behaviours are fully characterized. Thus, it is very complicated for real application.

The threshold (criterion response value) is chosen according to some application-dependent criteria, either to minimize the false rejection (when the watermarked image detected as non-watermarked) and false alarm (when the non-watermarked image detected as watermarked) or to find a trade-off between them.

However, analysis of the false rejection is often difficult since we have to deal with attack modelling as well as embedding scheme. It would be therefore better to deal with the false alarm. Furthermore, for many applications, the false alarm is considered more important criterion and have to be strictly bounded. So, the threshold is finally defined by placing a constraint on the false alarm (also called Neyman-Pearson criterion [79]). The probability of false alarm is defined as:

$$P_{fa} = P(x > t|H_0) = \int_{t}^{+\infty} pdf\,(H_0)\,, \tag{4-7}$$

where P_{fa} is the probability false alarm.

In the literature, optimum detectors are only derived under oversimplified assumptions such as in AWGN channels where both the host and the attack noise are modelled as white Gaussian processes [6]. Such an assumption has been proved impractical through a number of works [80]–[82] where most of different insertion domains are well fitted by the generalized Gaussian distribution especially for spatial domain. This detector is optimal only when the distribution of data samples is Gaussian. But, studying the statistical properties of wavelet coefficients, for example, demonstrates that the Gaussian distribution cannot capture the wavelet coefficients density efficiently [83]. According to the distribution used for the wavelet coefficients, different types of detectors can be obtained. And several different priors have been considered for the wavelet coefficients in watermark detection such as Laplacian distribution [84], generalized Gaussian distribution, [85], modified Gauss–Hermit [86], Bessel K form [87]. Most of the above models assume that the wavelet coefficients are independent and identically distributed. However, these conditions are impractical and allows only an evaluation on the "effectiveness" rather than the robustness of the watermarking system [88]. As we are testing in this work a perceptual watermarking method in both wavelet and spatial domain, where the watermark is modulated by a non-linear JND function such as: $y = x + JND(x).w$. We consider just the "random watermark false alarm" [33], where the detector output follows a Gaussian distribution due to the central limit theorem:

$$P_{fa} = P(x > t|H_0) = \int_{t}^{+\infty} pdf\,(H_0) = \frac{1}{\sqrt{\pi}} \int_{t/\sqrt{2}\,\sigma_{H_0}}^{+\infty} e^{-s^2} ds\,. \tag{4-8}$$

In order to compute P_{fa}, we need to know σ_{H_0}(variance of set non-watermarked of images) as demonstrated in [89].

For instance, Miller and Bloom [35] proposed another theoretical model for the calculation of pdf, which is later demonstrated to be more adapter to Fourier watermarking domain [15], [16], [90]. For a cross correlation coefficient C of a watermark with size L, and non-watermarked image, the pdf in this model can be modeled as:

$$P_{fa} = P(C > t|H_0) = \frac{\int_0^{\cos^{-1}(t)} sin^{L-2}(u)\ du}{2\int_0^{\pi/2} sin^{L-2}(u)\ du} \tag{4-9}$$

For the testing part of this study, we fix the value of the false alarm, so that each tested domain will have its own specific threshold value for the sake of the objectivity of the test

4.3 PROJECTIVE REGISTRATION

In this section, the projective geometry is discussed in detail. Projective transformation is produced from the action of taking picture with a camera of smartphone freehandedly. Therefore, the camera geometry is needed to be explored as well as the mathematical representation of the projection from the 3D world coordinates of the printed image to the 2D coordinates of the captured image. Those details will help to specify the properties of 2D projective transformation so it can be used for the design of the projective rectification process.

4.3.1 Projective rectification process

There exist geometric relations between the object and the camera positions while capturing process. In this paragraph, we will explain these geometric relations in form of parameter estimations of whole process. Then we will reveal some of methods used for the geometric rectification.

The operation of taking points coordinates from a 3D world and map it in imaging plan, which is a 2D plan, is called projective transformation as shown in Figure 4-5:

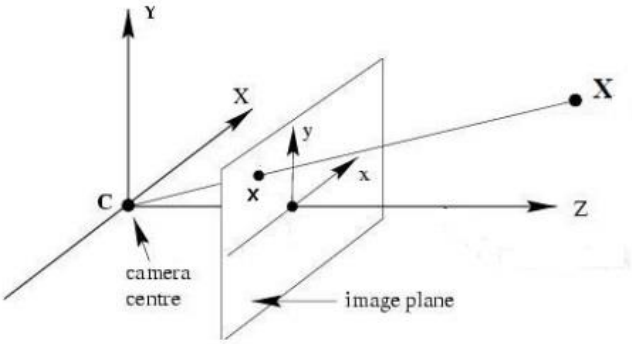


Figure 4-5: Geometric projection process

In a projective space where the points at infinity exist and predefined, the projective transformation become a linear transformation, and can be presented in form of mathematical relation, as the following equation:

$$p = H \times P \tag{4-10}$$

where P is a world coordinates, p is its corresponding image coordinates, and H with dimention 3×4 a projective matrix that describes the transformation from the 3D to 2D spaces. Similarly, the capturing process of an image using a camera can be simulated by a projective transformation as follows:

$$\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = K \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} M \begin{pmatrix} X \\ Y \\ Z \\ 1 \end{pmatrix} \tag{4-11}$$

M gives the 3D position and pose of the camera, therefore has eight degrees of freedom, which represent the extrinsic camera parameters. In a minimal parametrization. K is independent of the camera position. It contains the intrinsic parameters of the camera [15]. In particular, perspective transformation or 2D projective transformation is the projection from 2D plan in 3D world into 2D plan, and this is exactly our case since our capturing process is defined as taking a picture of a printed image, which is a 2D object. Then the relation of the perspective transformation becomes:

$$\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = H \begin{pmatrix} X \\ Y \\ 1 \end{pmatrix} \tag{4-12}$$

H defines the 3×3 perspective matrix [91].

4.3.2 Geometric image rectification

The perspective distortions are created from the fact of changing the positions of the camera and the object during capturing process. Therefore, the matrix M in the equation 4-11 is the responsible matrix that parametrizes the perspective distortion. So, from the mathematical view, to delete the geometric effect, we have to invert the transformation. So that many mathematical methods are suggested in [92]. In the following we present the most powerful and useable techniques are used to rectify this kind of geometric deformation.

- **Four corners method:** From the equation (4-12), the projective matrix has 8 degree of freedom hence only 8 unknown parameters to estimate. The system equation that we need to solve is:

$$\begin{cases} x = \dfrac{h_{11}X + h_{12}Y + h_{13}}{h_{31}X + h_{32}\ Y + 1}, \\ y = \dfrac{h_{21}X + h_{22}Y + h_{23}}{h_{31}X + h_{32}\ Y + 1}. \end{cases} \qquad (4\text{-}13)$$

With correspondences four points, H can be uniquely computed [91].

- **Parallel lines method:** the projective homography can be understood to be the product of three components – similarity (H_s), affine (H_a), and projective (H_p), i.e., H = Hs Ha H_p. so to invert the perspective transformation, the method remove the projective and affine components to obtain the similarity transformed version of the original image. This method is more detailed in the reference [92].

For our adapted method we will use concept of the frame method, to apply the 4 "corner strategy" to overcome the perspective distortions. Since the second method is already assigned particularly to the document or text type images.

To estimate the *H* matrix. Feature point detection techniques, such as SIFT and SURF, are more suitable for non-blind watermarking methods [5]. As this is not the case here, a frame synchronization method by detecting the Four corners of the ID image. The projective matrix H has 8 degrees of freedom hence there are 8 unknown parameters to estimate.

First the Hough transform is used to detect frame lines of the image, then the four corners are estimated as the intersections of those lines. The projective matrix is

estimated by solving the system of equations 4-13 with the corresponding four points. Finally, the inverse transformation is applied on the image to remap the rectified image.

To correct the geometric effect, we need to estimate the four corner positions. Therefore, the steps of this process are as follow:

Step 1: Detect the four corners: we use Hough line to detect the frame of ID image, then we get the four points from the intersections of those lines.

Step 2: Estimate the projective matrix: with corresponding four points, we solve the system equation 4-13.

Step 3: Apply the invert transformation in the whole image, to remap the rectified image.

An example is given in Figure 4-6:

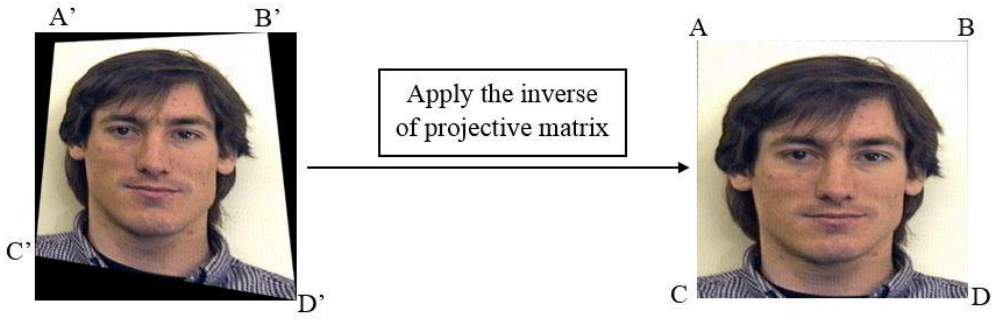


Figure 4-6: Projective rectification

4.4 BLUR AND COLOR CORRECTIONS

4.4.1 Blur correction

Removing blur from images is still an active research field. In general, the image blurring process is commonly modelled as the convolution of a clear image with a blur kernel (Point Spread Function PSF) plus noise:

$$I_{out} = h * I_{in} + n, \tag{4-14}$$

where $*$ denotes the convolution operator, I_{in} denotes the clear image, I_{out} denotes the available blurry observation, h is the blur kernel and n represents the image noise. Image deblurring methods can be classified into two categories: blind image deblurring [29], and non-blind image deblurring. The latter is dependent on prior

knowledge of the system and of its parameters. In this work we used a Wiener filter [15], [16] since the print-cam watermarking system is known. The PSF of the system and its noise variance must first be estimated.

Figure 4-7 shows the PSF estimated from the average of 10 printed and captured point sources for iPhone6 and Samsung S5.

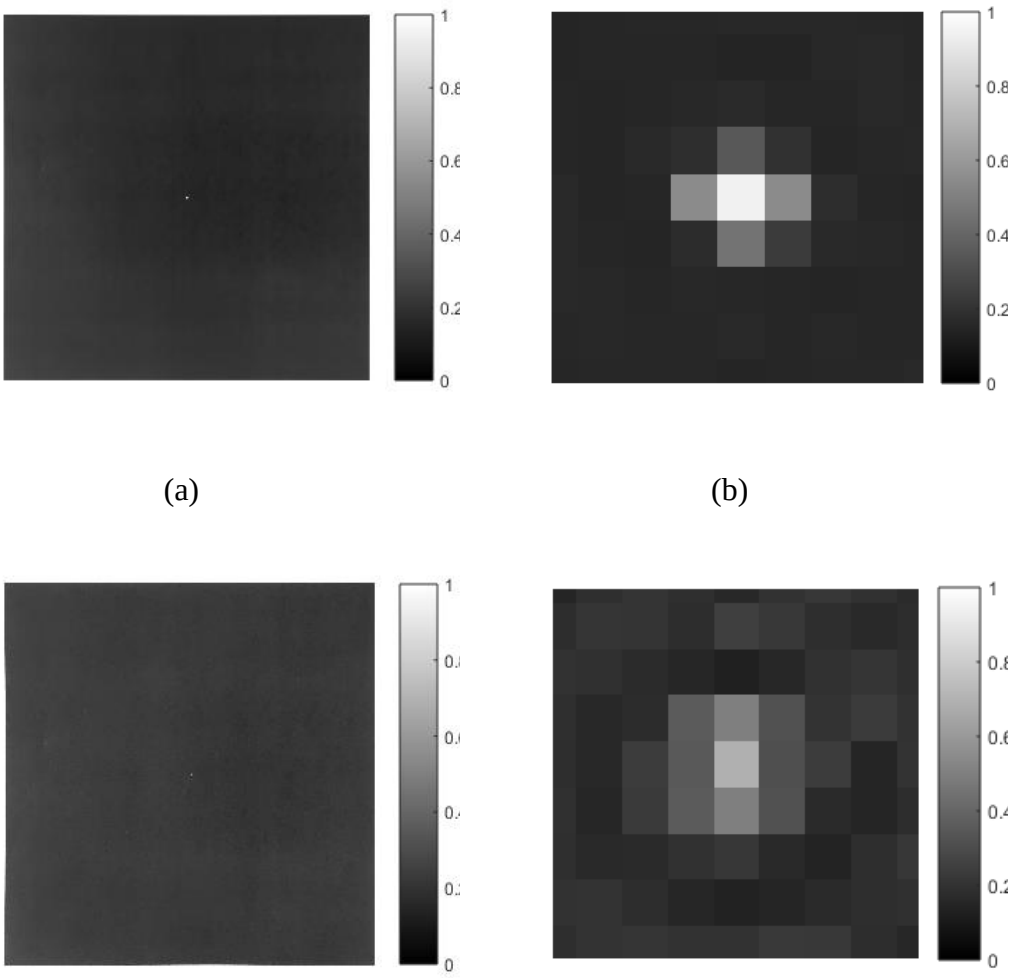


Figure 4-7: Estimated PSF of tested print-cam system with iPhone 6 (a) and zoom (b), and Samsung S5 (c) and zoom (d)

Noise variance was estimated from four printed and captured images of uniform gray level, respectively 50, 100, 150, 200. Image variance was computed for each tested gray level. The mean of the image variance is the final noise variance. We found a standard deviation of 4.9 pixels for the iPhone 6 and 4.5 for the Samsung S5.

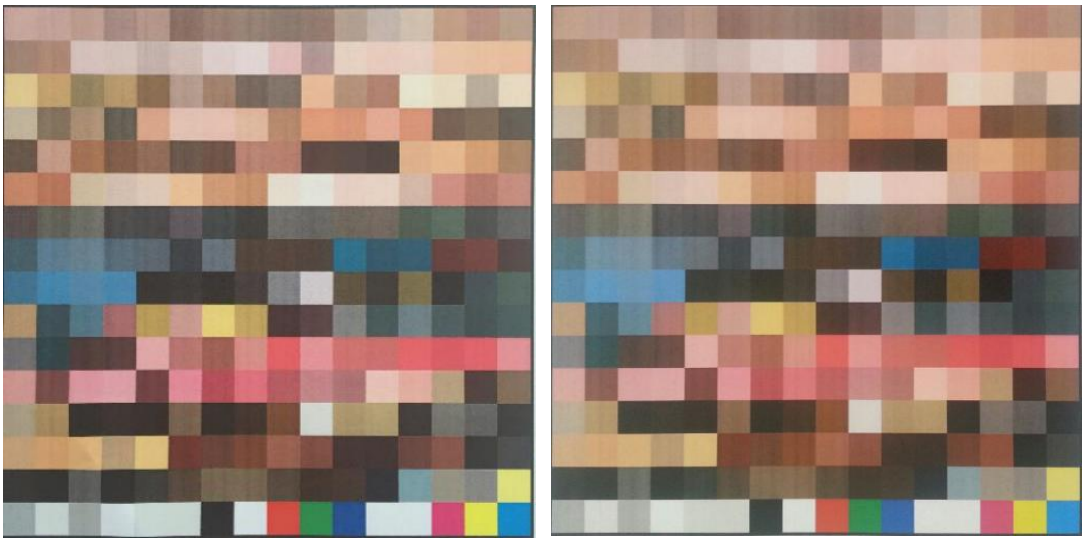
4.4.2 Color correction

Colour distortion is a result of many factors occurring during the print-cam process. Many approaches have been used for colour correction, such as classical gamma correction [93], and polynomial correction [16], [94]. For all these methods, the colour correction is established first by estimating the colour distortion function then applying the inverse of this function to the distorted image in a given colour domain (RGB, HSV,…). In this work we used polynomial 4^{th} order correction method by solving the following equation in the RGB domain:

$$\begin{cases} R' = a_0 + a_1 R + a_2 R^2 + a_3 R^3 + a_4 R^4, \\ G' = b_0 + b_1 G + b_2 G^2 + b_3 G^3 + b_4 G^4, \\ B' = c_0 + c_1 B + c_2 B^2 + c_3 B^3 + c_4 B^4, \end{cases} \quad (4\text{-}15)$$

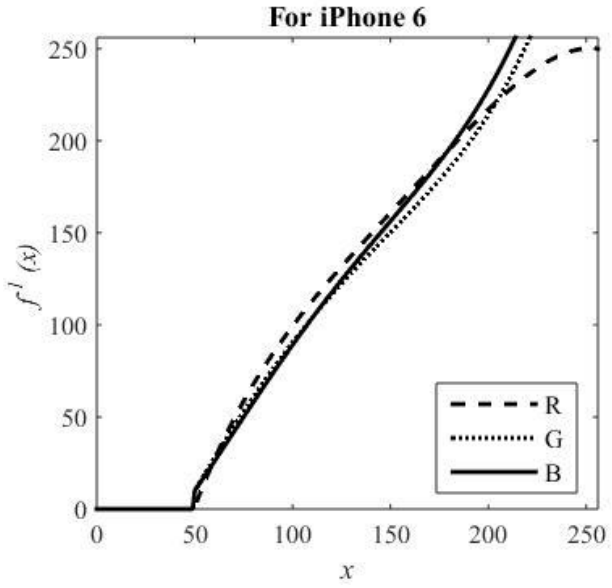
where The R, G and B denote the original Red, Green and Blue color signals, R', G' and B' denote the distorted output color signals and (a_i), (b_i), (c_i) for $i \in [0,4]$ are the 4^{th} polynomial coefficients to be estimated for respectively R, G and B channels . To estimate the used function a color palette with specific color collections (shown in Fiure 4-8). This collection represents 256 colour tones in ID images, especially different skin and hair colour tones [16]. The estimated inverse function of the RGB component for the testing print-cam system with iPhone 6 and Samsung S5 is shown in Figure 4-9.

(a)

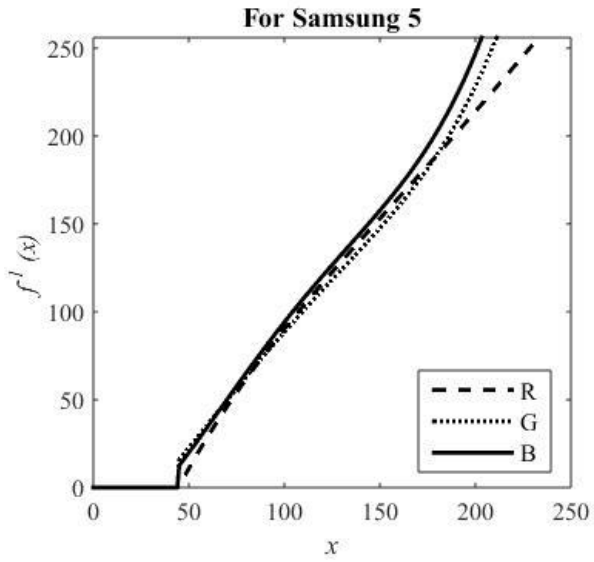


(b) (c)

Figure 4-8: The testing targets of the color palette with known color distribution; (a) original palette, captured palette with (b) iPhone 6 (c) Samsung S5



(a)



(b)

Figure 4-9: Inverse transfer function for each colour component of Print-Cam system with (a) iPhone 6 (b) Samsung S5

Chapter 5: Results

5.1 INTRODUCTION

In this section, the proposed Fourier based method is compared with the following five methods:

- Spatial-1 is the watermarking method in [75], where the technique is based on block insertion in the Cb channel of the YCbCr colour image representation,
- Spatial-2 is the watermarking method in [5], where block insertion of the watermark was in the blue channel of RGB image representation using JND (just noticeable difference) to control the insertion strength,
- DWT-1 in [73], the watermark insertion is basically done on the horizontal and vertical sub-bands of the first level of the wavelet transform,
- DWT-2 in [3], the watermark is embedded on the horizontal detail coefficients of the first sub-band level using Haar wavelet,
- FMT is the modified Fourier-Mellin based watermarking method in [71], where the watermark is inserted in the mid frequencies of the quaternion Fourier transform followed by the log-polar transform.

We present two tests: a first simulated test where we apply only simulated perspective deformations on ID images. Only the frame-based perspective correction is applied. In the second test, we apply real print-cam attacks on ID watermarked images printed on a paper and digitized using smartphones freehandedly (iPhone 6 and Samsung S5). Perspective correction is associated to the blur and colour corrections. Additional results are also shown.

The image database used in this work is the PICS images (Psychological Image Collection at Stirling)-Aberdeen 1. It contains pictures of the color faces *s* of 90 people Ian Craw at Aberdeen, with variations in lighting and in different positions. The resolution of the images varies between 336×480 and 624×544. All images have been resized to 512 512, which allows the use of the FFT algorithm.

5.2 SIMULATED TEST

5.2.1 Testing protocol

This section presents the comparison of the watermark detection between the proposed method and the methods listed in the above, using 500 ID digital images from PICS database. Perspective attacks are simulated. Both methods are implemented under the same protocols and conditions. The steps of the test are shown in the following Figure 5-1:

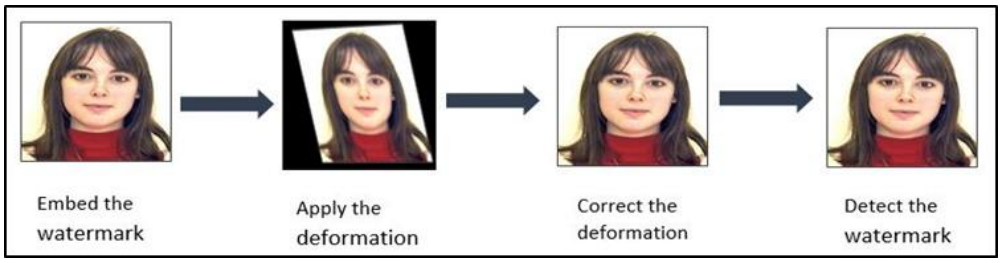
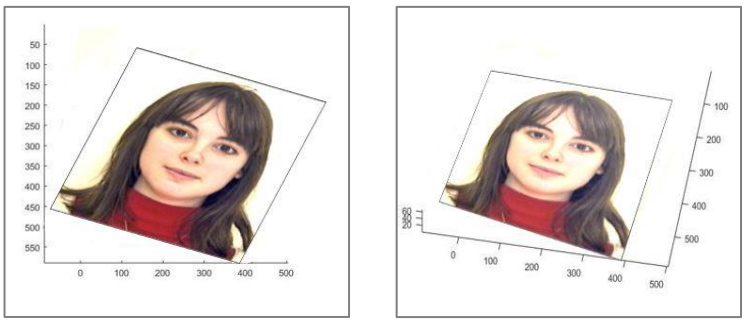


Figure 5-1: the process of simulated test

For the perspective distortions, the simulation of 3D rotation of the image (3 rotations around *x, y,* and *z* axis) is used simultaneously with the simulation of camera position (view point position) that defines polar angles θ and φ (polar angle in the *x-y* plane, polar angle above or below the *x-y* plane). Those angles are measured in degrees. The following Figure 5-2 shows examples of simulated perspective distortions:



(a) (b)

Figure 5-2: (a) - 3D rotation (5°, -2°, 10°) with view-point (0°, 90°). (b) - 3D rotation (5°, -2°, 10°) with view-point (10°, 60°).

The 500 ID images were deformed under random values of perspective attacks similar to those occurring when taking an image freehandedly with a smartphone. The rotation values around the *x, y,* and *z* axes were respectively taken from the intervals [-5°, 5°], [-5°, 5°], and [-10°, 10°]. View point values of θ and φ were respectively between [0°, 10°] and [60°, 90°]. We corrected the geometric deformation using frame-based perspective correction.

5.2.2 Results

The probability of true positive detection as a function of the detection threshold is shown in Figure 5-3. Three cases are of interest:

- Without projective deformations,
- With projective deformations,
- With projective deformations followed by geometric corrections.

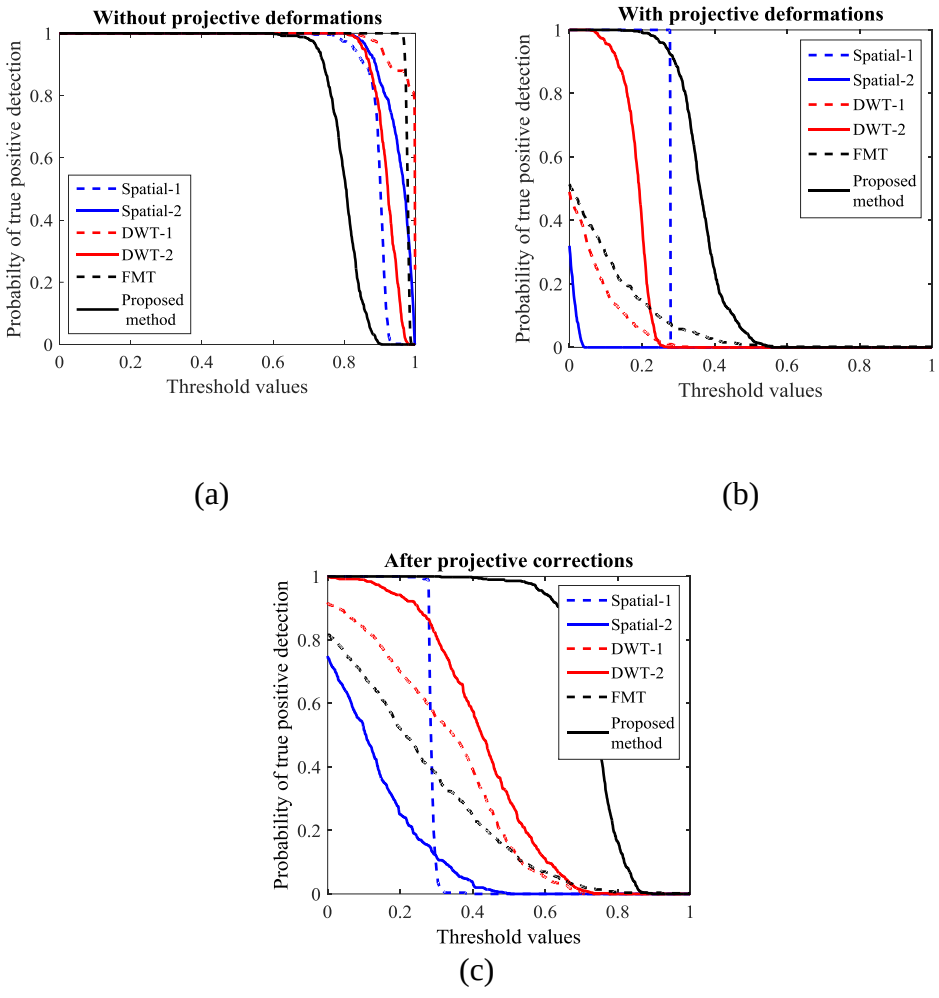


Figure 5-3- Probability of true positive detection as a function of the threshold values before (a), after (b) the perspective attacks and (c) after the perspective corrections.

Results show that the DWT, spatial and Fourier-Mellin based methods are better than the Fourier one in the case where no perspective or projective attack occurs.

The probability of true positive detection of the Fourier method outperforms the other tested methods in the case of perspective attacks (Figure 5-3- (b)). Finally, the quality of the detection after geometrical correction for Fourier is almost identical to

the quality when no attack was present. This is not the case for the other two methods. This can be explained as follows. The geometric correction is not perfect, and some residual rotations and translation still survive. The Fourier method is naturally adapted to rotation and translation attacks and is less sensitive than DWT or spatial methods to these residual attacks. For the case of Fourier-Mellin based method, although the transform is geometrically strong (RST invariant), the detection rate is very weak compared to the results of the proposed method. The main issue is related to the computational errors. They are due to log-polar transform and the inverse transform along with interpolation error produced by projective deformations and its corrections [90].

To confirm these preliminary results, tests in real situations were conducted and are reported in the next section. The methods Spatial-2 and DWT-2 are selected for the comparison in the real test based on the better performance of each domain in the simulated test.

5.3 REAL TEST

5.3.1 Testing protocol

We tested the three methods in real conditions. The number of the tested data is 480 ID images (240 are marked and 240 are not marked). The images were printed on a paper support with a Konica Minolta C284 printer (Dot-Matrix type) with a resolution of 200 dpi and size 44×44 mm for the printed ID image. Then captured freehandedly with iPhone6 and Samsung S5 with a resolution of 8 megapixels and 16 megapixels respectively (remember that the acquisition is freehanded). The camera of the two devices are set by default parameters: no filter, no flash light during the capturing process. The pictures have been captured under daylight illumination. The steps of this test are shown in the following Figure 5-4:

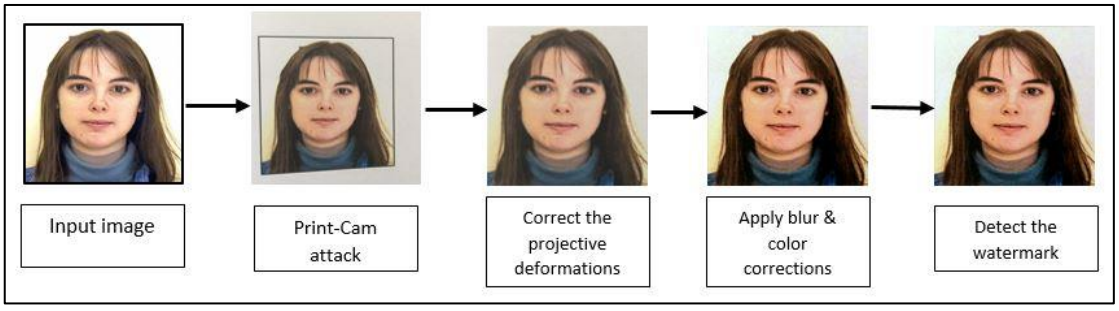
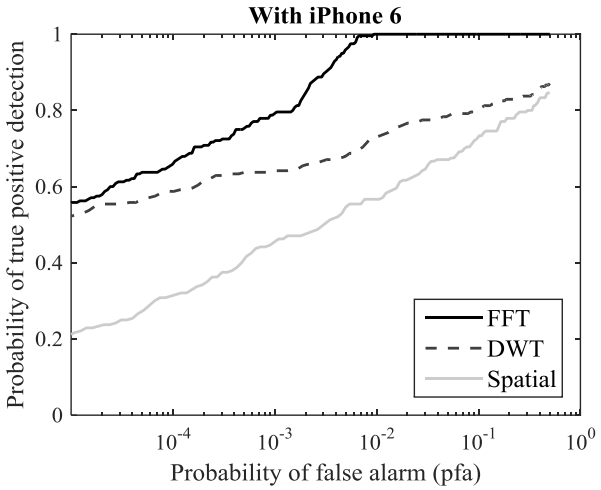


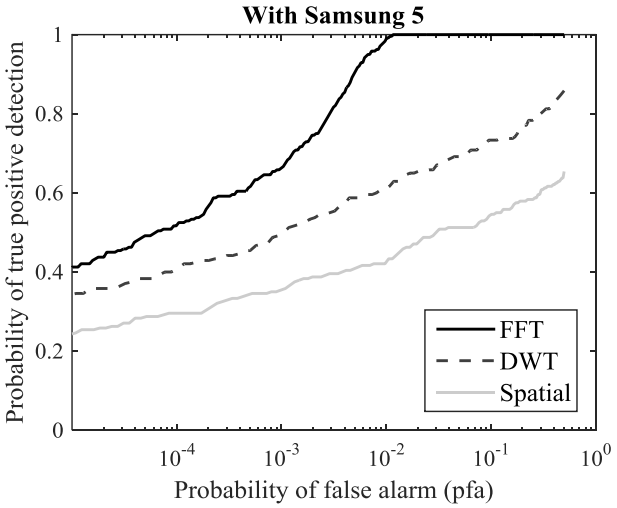
Figure 5-4- Process of the test

5.3.2 Results

In Figure 5-5, the proposed Fourier watermarking method, noted FFT, with the complete correction process, is compared with the other two tested methods DWT-2 noted as DWT and Spatia-2 noted as Spatial in terms of ROC curves.



(a)

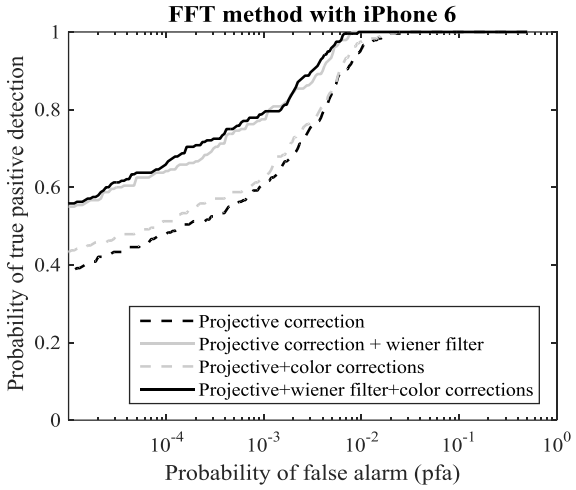


(b)

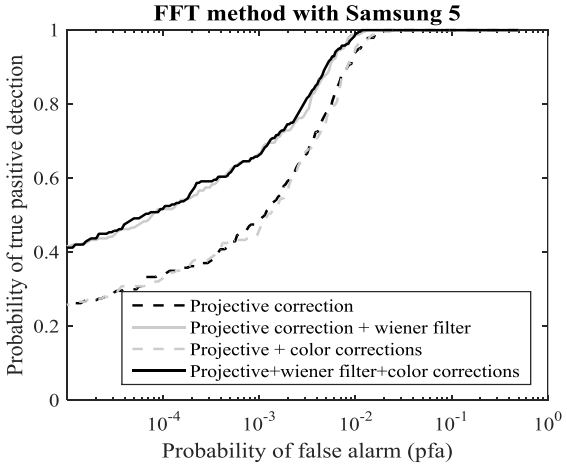
Figure 5-5: Comparison of ROC curves between the three methods with corrections for (a) iPhone 6 and (b) Samsung S5

The performance of the watermarking method in the FFT domain is better than those of watermarking methods in other domains. These results confirm the results obtained during the simulated test.

As an additional result, the following ROC curves show the impact of the blur and color corrections. The projective correction was also applied. Only results for the Fourier method are presented since the results for the other two methods (DWT and spatial) are identical.



(a)



(b)

Figure 5-6: Comparison of ROC curves for different adapted corrections in Fourier domains with (a) iPhone 6 and (b) Samsung S5

Results show that the Wiener filter associated to the color corrections improves the detection rate. They also demonstrate the strong positive impact of blur correction compared to the color correction.

As a final result, the following table shows the minimal errors for the three methods and for the two smartphones.

Methods	**FFT**		**DWT**		**Spatial**	
Smartphones	**i6**	**S5**	**i6**	**S5**	**i6**	**S5**
Minimal error rate	**1.02%**	**1.07%**	25.52%	35.31%	36.77%	52.35%

Table 5-1: Minimal error rate for the three methods and the two smartphones

Results clearly show the ptomising performances of the proposed method with a minimal error rate of 1.02% and 1.07% for respectively iPhone 6 and Samsung S5. These numbers are to be compared with the other results (25.52% in the best case). Lastly, few differences were found between the two smartphones (iPhone6 and Samsung S5), although the former led to fewer errors when considering the Fourier method.

Chapter 6: Conclusion

6.1 CONCLUSION

This thesis focussed on watermarking ID images printed on a physical support and freehandedly digitized using a smartphone camera. The printing operation followed by digitization produce powerful so called print-cam attack that results in difficulties recovering of the watermark. The main features expected from the proposed watermarking algorithm are invisibility and robustness against this print-cam attack.

This thesis report started with a chapter on watermarking background; we discussed the different phases of designing a watermarking method followed by a chapter on the state of the art of image watermarking related to print-cam process. First, we have presented a brief description on watermarking strategies against geometric distortions, which were exhaustive search, invariant domains, watermark re-synchronization and image re-synchronization. Then we discussed the designed watermarking method in literature for print-cam process. Among the methods of robust watermarking to transformations, we get motivated to choose watermarking methods in the Fourier domain. This domain of insertion is characterized by its strong resistance against some geometric attacks, namely translations and rotations in the image plane.

To reach our objective we have presented a detailed study of the distortions produced during the print-cam process and the attacks or problems related to this process. We also discussed the proposed models and the developed solutions for eliminating or reducing them. These distortions are divided mainly into two categories; geometric transformations affecting the position of pixels as well as distortions that affect the pixel value. With respect to pixel value distortions several models have been proposed but ultimately few counterattacks have been developed.

Our contribution in the field of image watermarking is shown in the fourth chapter. The approach developed belongs to additive schemes with blind detection in the Fourier space. In print-cam process, stronger attacks occur compared to print-scan process. Geometric distortion in this case is the most critical problem. This attack is modelled as a projective distortions. It is produced by freehandedly taking a picture

with a camera. Projective distortion is a combination of geometric transforms as rotations, translations, scaling and the tilting of the optical axis. In addition, there are other attacks as blurring, noise and colour variations. An analysis of these problems has driven us to propose a set of corrective approaches associated to the classical Fourier watermarking strategy. It involves addressing these distortions of print-cam attacks in three phases. The first is projective registration with frame-based technique using Hough transform for line detection. As a result most of the geometric deformations are corrected. The second is a blur and noise reduction using an adapted Wiener filter. This is possible because we were able to measure the PSF of the printing and digitization process as well as its noise. The third is colorimetric correction using a transcoding function. Once again, a measurement of the colour transfer function allowed such a rectification. Finally, the imperceptibility of the mark was insured by choosing a PSNR due to the watermark insertion fixed to 40dB.

This method was tested on ID images and compared to five other methods of the literature. Results on simulated projective attacks show that our method outperformed other ones. We recall figure 5-3 that illustrates this result. It is clearly seen that our method, the black curve, has much better true positive detection capabilities than the 5 other ones.

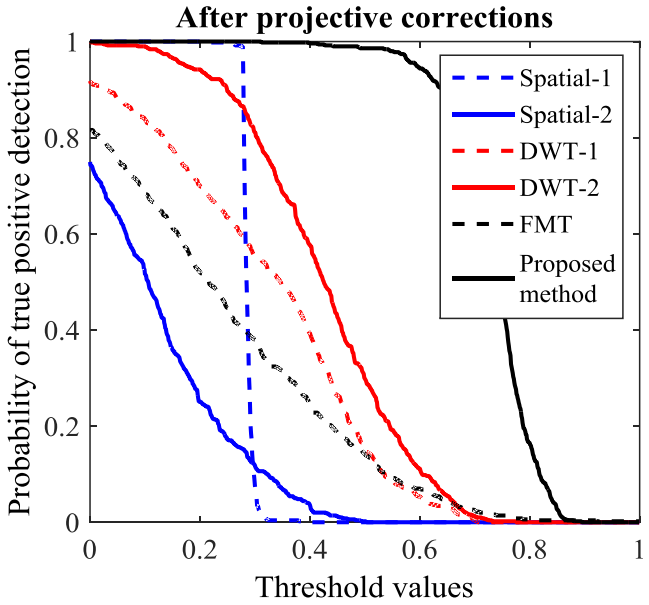


Figure 6-1: Probability of true positive detection as a function of the threshold values after the projective attacks followed by the projective corrections.

We also tested our method in a real situation when ID images were printed on paper and captured with two smartphones, namely Iphone6 and Samsung S5. The comparative study presented in chapter 5, shows that the method proposed in this work is more effective than those of the literature methods. We note that the combination of corrective methods significantly improves the detection rate. We recall figure 5-5 that illustrates this result. It is clearly seen on these ROC curves that our method, the black curve, has much better performances than two other challengers (DWT and Spatial) for the Samsung S5 smartphone (results are similar for the iPhone 6). As a final result, the total error rate is of 1%, compared to more than 25 % for the 2 other methods. It is compatible with industrial applications.

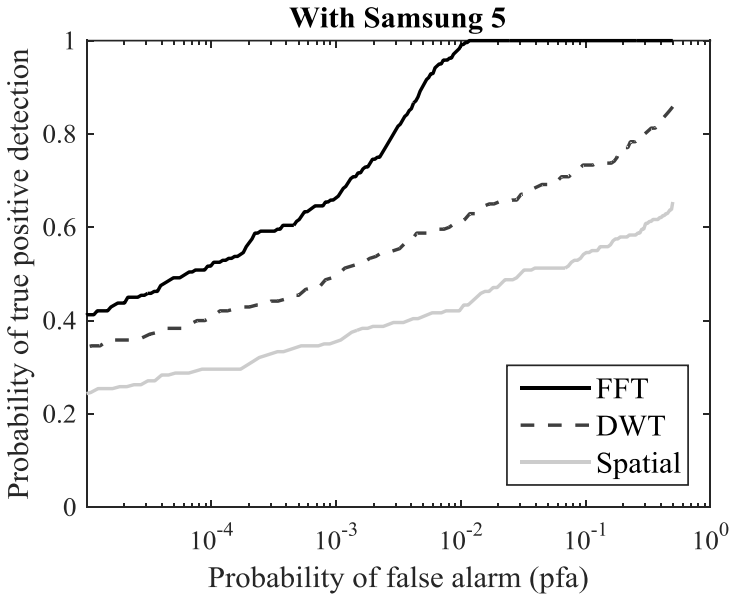


Figure 6-2: ROC curves between the three methods with corrections for Samsung S5

6.2 FUTURE WORKS

The watermarking method proposed in this work does not take into account the psycho visual aspect when inserting the mark. Numerous works exploiting the psycho visual masks (sensitivity to contrast, luminance adaptation…) exist and have demonstrated their effectiveness. In our future work, our approach will be to build a psycho-visual model that takes the most common properties of the human visual system to determine the threshold of visual detection (JND). The objective being to improve the efficiency of our approach while maintaining its simplicity.

The industrial application we have in mind is a mobile control of official documents containing an ID image, as passports or ID cards. In a near future we intend to develop the embedded version of our method on android and iOS targets.

Finally, this thesis shows that digital image watermarking can be successfully used in connecting the analog world to the digital one. In the future, we will look forward using neural network to solve efficiently the projective distortions. This would increase the number of possible applications and bring the print-cam robust watermarking closer to consumers and content providers.

References

[1] H. Farid, « Seeing is not believing », *IEEE Spectr.*, vol. 46, n° 8, p. 44–51, 2009.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, et T. Kalker, *Digital watermarking and steganography*. Morgan kaufmann, 2007.

[3] A. Pramila, A. Keskinarkaus, et T. Seppänen, « Watermark robustness in the print-cam process », *Proc IASTED Signal Process. Pattern Recognit. Appl. SPPRA 2008*, p. 60–65, 2008.

[4] A. Pramila, A. Keskinarkaus, V. Takala, et T. Seppänen, « Extracting watermarks from printouts captured with wide angles using computational photography », *Multimed. Tools Appl.*, vol. 76, n° 15, p. 16063–16084, 2017.

[5] K. Thongkor et T. Amornraksa, « Robust image watermarking for camera-captured image using image registration technique », in *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, 2014, p. 479–483.

[6] M. Barni et F. Bartolini, *Watermarking systems engineering: enabling digital assets security and other applications*. New York: Marcel Dekker, 2004.

[7] S. Heidari et M. Naseri, « A novel LSB based quantum watermarking », *Int. J. Theor. Phys.*, vol. 55, n° 10, p. 4205–4218, 2016.

[8] A. Phadikar, S. P. Maity, et B. Verma, « Region based QIM digital watermarking scheme for image database in DCT domain », *Comput. Electr. Eng.*, vol. 37, n° 3, p. 339–355, 2011.

[9] J. Hwang, J. Kim, et J. Choi, « A reversible watermarking based on histogram shifting », in *International Workshop on Digital Watermarking*, 2006, p. 348–361.

[10] A. K. Singh, N. Sharma, M. Dave, et A. Mohan, « A novel technique for digital image watermarking in spatial domain », in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 2012, p. 497–501.

[11] W. Bender, D. Gruhl, N. Morimoto, et A. Lu, « Techniques for data hiding », *IBM Syst. J.*, vol. 35, n° 3.4, p. 313–336, 1996.

[12] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*, Second edition. Boca Raton: Taylor & Francis, CRC Press, 2017.

[13] N. Kashyap et G. R. Sinha, « Image watermarking using 3-level discrete wavelet transform (DWT) », *Int. J. Mod. Educ. Comput. Sci.*, vol. 4, n° 3, p. 50, 2012.

[14] C. Das, S. Panigrahi, V. K. Sharma, et K. K. Mahapatra, « A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation », *AEU-Int. J. Electron. Commun.*, vol. 68, n° 3, p. 244–253, 2014.

[15] A. Poljicak, L. Mandic, et D. Agic, « Discrete Fourier transform-based watermarking method with an optimal implementation radius », *J. Electron. Imaging*, vol. 20, n° 3, p. 033008, 2011.

[16] R. Riad, R. Harba, H. Douzi, F. Ros, et M. Elhajji, « Robust fourier watermarking for id images on smart card plastic supports », *Adv. Electr. Comput. Eng.*, vol. 16, n° 4, p. 23–30, 2016.

[17] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, et R.-J. Chen, « An improved SVD-based watermarking technique for copyright protection », *Expert Syst. Appl.*, vol. 39, nº 1, p. 673–689, 2012.
[18] S. P. Maity et M. K. Kundu, « DHT domain digital watermarking with low loss in image informations », *AEU-Int. J. Electron. Commun.*, vol. 64, nº 3, p. 243–257, 2010.
[19] J. J. O. Ruanaidh et T. Pun, « Rotation, scale and translation invariant spread spectrum digital image watermarking », *Signal Process.*, vol. 66, nº 3, p. 303–317, 1998.
[20] E. Maiorana, P. Campisi, et A. Neri, « Biometric signature authentication using radon transform-based watermarking techniques », in *2007 Biometrics Symposium*, 2007, p. 1–6.
[21] P. Bas, N. Le Bihan, et J.-M. Chassery, « Color image watermarking using quaternion Fourier transform », in *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03).*, 2003, vol. 3, p. III–521.
[22] A. M. Eskicioglu, P. S. Fisher, et S.-Y. Chen, « Image quality measures and their performance », 1994.
[23] G. P. Renieblas, A. T. Nogués, A. M. González, N. Gómez-Leon, et E. G. del Castillo, « Structural similarity index family for image quality assessment in radiological images », *J. Med. Imaging*, vol. 4, nº 3, p. 035501, juill. 2017, doi: 10.1117/1.JMI.4.3.035501.
[24] A. Cheddad, J. Condell, K. Curran, et P. Mc Kevitt, « Digital image steganography: Survey and analysis of current methods », *Signal Process.*, vol. 90, nº 3, p. 727–752, 2010.
[25] A. Smoaca, « ID Photograph hashing: a global approach », PhD Thesis, Saint-Etienne, 2011.
[26] M. Singh, H. M. Haverinen, P. Dhagat, et G. E. Jabbour, « Inkjet Printing-Process and Its Applications », *Adv. Mater.*, vol. 22, nº 6, p. 673‑685, févr. 2010, doi: 10.1002/adma.200901141.
[27] H. S. Elsayad et S. El-sherbiny, « A Study into the Influence of Paper Coatings on Paper Properties and Print Quality of Dye Sublimation Thermal Prints », *Polym.-Plast. Technol. Eng.*, vol. 47, nº 2, p. 122‑136, janv. 2008, doi: 10.1080/03602550701581126.
[28] K. Nolde et M. Morari, « Modeling and Control of Thermal Printing », *IEEE Trans. Control Syst. Technol.*, vol. 18, nº 2, p. 405‑413, mars 2010, doi: 10.1109/TCST.2009.2017025.
[29] K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, et I. El-Khalil, « `Print and Scan' Resilient Data Hiding in Images », *IEEE Trans. Inf. Forensics Secur.*, vol. 1, nº 4, p. 464‑478, déc. 2006, doi: 10.1109/TIFS.2006.885032.
[30] B. Perry, B. MacIntosh, et D. Cushman, « Digimarc MediaBridge: the birth of a consumer product from concept to commercial application », in *Security and Watermarking of Multimedia Contents IV*, avr. 2002, vol. 4675, p. 118‑124, doi: 10.1117/12.465267.
[31] « Digimarc | The Barcode of Everything ». https://www.digimarc.com/ (consulté le avr. 08, 2019).
[32] « Know Your Smartphone: A Guide to Camera Hardware », *TechSpot*. https://www.techspot.com/guides/850-smartphone-camera-hardware/ (consulté le avr. 08, 2019).

[33] A. Pramila, A. Keskinarkaus, et T. Seppänen, « Camera based watermark extraction-problems and examples », in *Proceedings of the finnish signal processing symposium*, 2007.
[34] P. Chotikawanid et T. Amornraksa, « Image watermarking against lens flare effects », in *Eighth International Conference on Graphic and Image Processing (ICGIP 2016)*, 2017, vol. 10225, p. 102251D.
[35] M. L. Miller et J. A. Bloom, « Computing the probability of false watermark detection », in *International Workshop on Information Hiding*, 1999, p. 146–158.
[36] J. F. Lichtenauer, I. Setyawan, T. Kalker, et R. L. Lagendijk, « Exhaustive geometrical search and the false positive watermark detection probability », in *Security and Watermarking of Multimedia Contents V*, 2003, vol. 5020, p. 203–214.
[37] A. Tefas et I. Pitas, « Multi-bit image watermarking robust to geometric distortions », in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, 2000, vol. 3, p. 710–713.
[38] F. H. Hartung, J. K. Su, et B. Girod, « Spread spectrum watermarking: Malicious attacks and counterattacks », in *Security and Watermarking of Multimedia Contents*, 1999, vol. 3657, p. 147–158.
[39] S. Baudry, P. Nguyen, et H. Maître, « Estimation of geometric distortions in digital watermarking », in *Proceedings. International Conference on Image Processing*, 2002, vol. 2, p. II–II.
[40] M. Maes, T. Kalker, J.-P. Linnartz, J. Talstra, F. G. Depovere, et J. Haitsma, « Digital watermarking for DVD video copy protection », *IEEE Signal Process. Mag.*, vol. 17, n° 5, p. 47–57, 2000.
[41] D. Delannay et B. Macq, « Generalized 2-D cyclic patterns for secret watermark generation », in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, 2000, vol. 2, p. 77–79.
[42] V. Solachidis et L. Pitas, « Circularly symmetric watermark embedding in 2-D DFT domain », *IEEE Trans. Image Process.*, vol. 10, n° 11, p. 1741–1753, 2001.
[43] V. Licks et R. Hordan, « On digital image watermarking robust to geometric transformations », in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, 2000, vol. 3, p. 690–693.
[44] A. Poljicak, L. Mandic, et D. Agic, « Discrete Fourier transform-based watermarking method with an optimal implementation radius », *J. Electron. Imaging*, vol. 20, n° 3, p. 033008, 2011.
[45] H. Araujo et J. M. Dias, « An introduction to the log-polar mapping [image sampling] », in *Proceedings II Workshop on Cybernetic Vision*, 1996, p. 139–144.
[46] G. Wolberg et S. Zokai, « Robust image registration using log-polar transform », in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, 2000, vol. 1, p. 493–496.
[47] R. Matungka, Y. F. Zheng, et R. L. Ewing, « Image registration using adaptive polar transform », *IEEE Trans. Image Process.*, vol. 18, n° 10, p. 2340–2354, 2009.
[48] H. Tao, L. Chongmin, J. M. Zain, et A. N. Abdalla, « Robust image watermarking theories and techniques: A review », *J. Appl. Res. Technol.*, vol. 12, n° 1, p. 122–138, 2014.
[49] M. Kutter, S. K. Bhattacharjee, et T. Ebrahimi, « Towards second generation watermarking schemes », in *Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348)*, 1999, vol. 1, p. 320–323.

[50] P. Bas, J.-M. Chassery, et B. Macq, « Geometrically Invariant Watermarking Using Feature Points », *IEEE Trans. Image Process.*, vol. 11, nº 9, p. 1014‑1028, sept. 2002, Consulté le: sept. 09, 2019. [En ligne]. Disponible sur: https://hal.archives-ouvertes.fr/hal-00166590.
[51] C.-W. Tang et H.-M. Hang, « A feature-based robust digital image watermarking scheme », *IEEE Trans. Signal Process.*, vol. 51, nº 4, p. 950–959, 2003.
[52] X. Ye, X. Chen, M. Deng, et Y. Wang, « A SIFT-based DWT-SVD blind watermark method against geometrical attacks », in *2014 7th International Congress on Image and Signal Processing*, 2014, p. 323–329.
[53] A. Nikolaidis et I. Pitas, « Region-based image watermarking », *IEEE Trans. Image Process.*, vol. 10, nº 11, p. 1726–1740, 2001.
[54] S. Stankovic, I. Djurovic, et I. Pitas, « Watermarking in the space/spatial-frequency domain using two-dimensional Radon-Wigner distribution », *IEEE Trans. Image Process.*, vol. 10, nº 4, p. 650–658, 2001.
[55] W. Lu, H. Lu, et F.-L. Chung, « Feature based watermarking using watermark template match », *Appl. Math. Comput.*, vol. 177, nº 1, p. 377–386, 2006.
[56] S. Pereira, J. J. Ruanaidh, F. Deguillaume, G. Csurka, et T. Pun, « Template based recovery of Fourier-based watermarks using log-polar and log-log maps », in *Proceedings IEEE International Conference on Multimedia Computing and Systems*, 1999, vol. 1, p. 870–874.
[57] X. Kang, J. Huang, Y. Q. Shi, et Y. Lin, « A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression », *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, nº 8, p. 776–786, 2003.
[58] T. Nakamura, A. Katayama, M. Yamamuro, et N. Sonehara, « Fast watermark detection scheme for camera-equipped cellular phone », in *Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia*, 2004, p. 101–108.
[59] A. Katayama, T. Nakamura, M. Yamamuro, et N. Sonehara, « New high-speed frame detection method: Side Trace Algorithm (STA) for i-appli on cellular phones to detect watermarks », in *Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia*, 2004, p. 109–116.
[60] J.-C. Liu et H.-A. Shieh, « Toward a two-dimensional barcode with visual information using perceptual shaping watermarking in mobile applications », *Opt. Eng.*, vol. 50, nº 1, p. 017002, 2011.
[61] S. Takeuchi, A. Kunisa, K. Tsujita, et Y. Inoue, « Geometric distortion compensation of printed images containing imperceptible watermarks », in *2005 Digest of Technical Papers. International Conference on Consumer Electronics, 2005. ICCE.*, 2005, p. 411–412.
[62] W. Kim, S. H. Lee, et Y. Seo, « Image fingerprinting scheme for print-and-capture model », in *Pacific-Rim Conference on Multimedia*, 2006, p. 106–113.
[63] M. Nuutinen et P. Oittinen, « Digital Watermarking Technologies Based on Color Modulation for Linking Applications », *Graph. Arts Finl.*, vol. 37, nº 2‑3, p. 1–14, 2008.
[64] H. Takimoto, S. Yoshimori, Y. Mitsukura, et M. Fukumi, « Invisible calibration pattern based on human visual perception characteristics », in *2010 20th International Conference on Pattern Recognition*, 2010, p. 4210–4213.
[65] A. Keskinarkaus, A. Pramila, T. Seppänen, et J. Sauvola, « Wavelet domain print-scan and JPEG resilient data hiding method », in *International Workshop on Digital Watermarking*, 2006, p. 82–95.

[66] A. Pramila, A. Keskinarkaus, et T. Seppänen, « Reading watermarks from printed binary images with a camera phone », in *International Workshop on Digital Watermarking*, 2009, p. 227–240.
[67] A. Pramila, A. Keskinarkaus, et T. Seppänen, « Toward an interactive poster using digital watermarking and a mobile phone camera », *Signal Image Video Process.*, vol. 6, nº 2, p. 211–222, 2012.
[68] T. Horiuchi, M. Wada, R. Saito, et S. Tominaga, « Improvement on information capacity of watermarked images by using multi-valued area of embedded signals », in *Proceedings: APSIPA ASC 2009: Asia-Pacific Signal and Information Processing Association, 2009 Annual Summit and Conference*, 2009, p. 765–768.
[69] K. Thongkor et T. Amornraksa, « Digital image watermarking for photo authentication in Thai national ID card », in *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, 2012, p. 1–4.
[70] L. A. Delgado-Guillen, J. J. Garcia-Hernandez, et C. Torres-Huitzil, « Digital watermarking of color images utilizing mobile platforms », in *2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013, p. 1363–1366.
[71] J. Ouyang, G. Coatrieux, B. Chen, et H. Shu, « Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping », *Comput. Electr. Eng.*, vol. 46, p. 419–432, 2015.
[72] Y. Moritani, A. Yoshihara, N. Jinda, et M. Muneyasu, « Data detection method from printed images with different resolutions using tablet device », in *2016 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 2016, p. 1–6.
[73] H. Al-Otum et N. E. Al-Shalabi, « Copyright protection of color images for android-based smartphones using watermarking with quick-response code », *Multimed. Tools Appl.*, vol. 77, nº 12, p. 15625–15655, 2018.
[74] S. Takeshita, T. Maehara, et S. Ono, « Digital watermark design for two-dimensional codes displayed on smart phone screen using multi-objective optimization and optical simulation », in *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, 2017, p. 201–214.
[75] N.-T. Le, « Invisible watermarking optical camera communication and compatibility issues of IEEE 802.15. 7r1 specification », *Opt. Commun.*, vol. 390, p. 144–155, 2017.
[76] F. Ros, J. Borla, F. Leclerc, R. Harba, et N. Launay, « An industrial watermarking process for plastic card supports », in *2006 IEEE International Conference on Industrial Technology*, 2006, p. 2809–2814.
[77] R. Riad, F. Ros, R. Harba, H. Douzi, et M. El Hajji, « Pre-processing the cover image before embedding improves the watermark detection rate », in *2014 Second World Conference on Complex Systems (WCCS)*, 2014, p. 705–709.
[78] P.-B. Nguyen, A. Beghdadi, et M. Luong, « Robust watermarking in DOG scale space using a multi-scale JND model », in *Pacific-Rim Conference on Multimedia*, 2009, p. 561–573.
[79] Q. Yan et R. S. Blum, « Distributed signal detection under the Neyman-Pearson criterion », *IEEE Trans. Inf. Theory*, vol. 47, nº 4, p. 1368–1377, 2001.

[80] A. Briassouli et M. G. Strintzis, « Locally optimum nonlinearities for DCT watermark detection », *IEEE Trans. Image Process.*, vol. 13, nº 12, p. 1604–1617, 2004.
[81] Q. Cheng et T. S. Huang, « An additive approach to transform-domain information hiding and optimum detection structure », *IEEE Trans. Multimed.*, vol. 3, nº 3, p. 273–284, 2001.
[82] M. Mitrea, F. Prêteux, A. Vlad, et C. Fetita, « The 2D-DCT coefficient statistical behaviour: a comparative analysis on different types of image sequences », *J. Optoelectron. Adv. Mater.*, vol. 6, nº 1, p. 95–102, 2004.
[83] M. Amirmazlaghani et H. Amindavar, « Two novel Bayesian multiscale approaches for speckle suppression in SAR images », *IEEE Trans. Geosci. Remote Sens.*, vol. 48, nº 7, p. 2980–2993, 2010.
[84] T. M. Ng et H. K. Garg, « Maximum-likelihood detection in DWT domain image watermarking using Laplacian modeling », *IEEE Signal Process. Lett.*, vol. 12, nº 4, p. 285–288, 2005.
[85] A. Nikolaidis et I. Pitas, « Asymptotically optimal detection for additive watermarking in the DCT and DWT domains », *IEEE Trans. Image Process.*, vol. 12, nº 5, p. 563–571, 2003.
[86] S. M. Rahman, M. O. Ahmad, et M. N. S. Swamy, « A new statistical detector for DWT-based additive image watermarking using the Gauss–Hermite expansion », *IEEE Trans. Image Process.*, vol. 18, nº 8, p. 1782–1796, 2009.
[87] Y. Bian et S. Liang, « Locally optimal detection of image watermarks in the wavelet domain using Bessel K form distribution », *IEEE Trans. Image Process.*, vol. 22, nº 6, p. 2372–2384, 2013.
[88] M. Amirmazlaghani, « Additive watermark detection in the wavelet domain using 2D-GARCH model », *Inf. Sci.*, vol. 370, p. 1–17, 2016.
[89] P. B. Nguyen, A. Beghdadi, et M. Luong, « Perceptual watermarking using a new Just-Noticeable-Difference model », *Signal Process. Image Commun.*, vol. 28, nº 10, p. 1506–1525, 2013.
[90] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, et Y. M. Lui, « Rotation, scale, and translation resilient watermarking for images », *IEEE Trans. Image Process.*, vol. 10, nº 5, p. 767–782, 2001.
[91] R. Hartley et A. Zisserman, *Multiple view geometry in computer vision*. Cambridge university press, 2003.
[92] L. Jagannathan et C. V. Jawahar, « Perspective correction methods for camera based document analysis », in *Proc. First Int. Workshop on Camera-based Document Analysis and Recognition*, 2005, p. 148–154.
[93] M. D. Grossberg et S. K. Nayar, « Modeling the space of camera response functions », *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 26, nº 10, p. 1272–1282, 2004.
[94] V. Cheung, S. Westland, D. Connah, et C. Ripamonti, « A comparative study of the characterisation of colour cameras by means of neural networks and polynomial transforms », *Color. Technol.*, vol. 120, nº 1, p. 19–25, 2004.

List of publications

Journal publications:

- Khadija Gourrame, Hassan Douzi, Rachid Harba, Rabia Riad, Frédéric Ros, Meina Amar and Mohamed El Hajji: A zero-bit Fourier image watermarking for Print-Cam process. Journal Multimedia Tools and Applications Volume 78 Issue 2, January 2019 Pages 2621-2638.
- Meina Amar, Rachid Harba, Hassan Douzi, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Khadija Gourrame: Perceptual Image Watermarking based on a Mixed-scale Wavelet Representation. International Journal of Computer Applications 172, no. 8 (2017): 1-9.

Proceeding chapter publications:

- Khadija Gourrame, Hassan Douzi, Rachid Harba, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Meina Amar: Robust Print-Cam Image Watermarking in Fourier Domain. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 356-365.
- Meina Amar, Rachid Harba, Hassan Douzi, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Khadija Gourrame: A JND model using a texture-edge selector based on Faber-Schauder wavelet lifting scheme. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 328-336.

International conferences:

- Khadija Gourrame, Hassan Douzi, Rachid Harba, Frédéric Ros, Rabia Riad, and Mohamed El Hajji: Print-Cam resilient watermarking based on Fourier transform. 1th International Conference of Computer Science and Renewable Energies 2018, ICCSRE'2018, Ouarzazate, Morocco, November 22-24, 2018.
- Khadija Gourrame, Hassan Douzi, Rachid Harba, Frédéric Ros, Mohamed El Hajji, Rabia Riad and Meina Amar: Robust Print-Cam Image Watermarking in

Fourier Domain. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 356-365.

- Meina Amar, Rachid Harba, Hassan Douzi, Frédéric Ros, Mohamed El Hajji, Rabia Riad, and Khadija Gourrame: A JND model using a texture-edge selector based on Faber-Schauder wavelet lifting scheme. Lecture Notes in Computer Science (Vol 9680). Springer proceeding 2016, pp. 328-336.

Khadija GOURRAME

Développement d'une technique de tatouage d'images robuste aux attaques Print-Cam

Résumé: Le tatouage d'images numériques consiste à y insérer une marque d'une manière invisible à l'œil humain, cette marque pouvant être détectée par un algorithme de traitement d'image. Cela sert entre autre à établir la propriété de ce document numérique. Le but de cette thèse est de proposer une technique de tatouage d'image lorsque celle-ci est imprimée sur un support physique puis numérisée à main levée avec la caméra d'un smartphone. Cela permettra de proposer de nouvelles applications nomades de tatouage, comme par exemple le contrôle mobile de documents officiels contenant une photo d'identité (ID) que nous souhaitons développer. Dans ce cas, la marque doit résister aux attaques liées au processus d'impression et numérisation avec une camera, dites attaques Print-Cam. Ces attaques très puissantes associent des modifications géométriques à des modifications de la valeur des pixels et peuvent rendre impossible la détection de la marque. La transformée de Fourier est utilisée comme domaine d'insertion de la marque, car cette transformée a des propriétés d'invariance contre certaines distorsions géométriques, rotation et translations dans le plan de l'image. La nouveauté de ce travail consiste à associer un tatouage d'image dans le plan de Fourier à 3 méthodes de correction : une correction géométrique de perspective basée sur la transformation de Hough, un filtre de Wiener pour réduire le flou et le bruit et enfin une correction colorimétrique pour réduire les dégradations de couleur. Les résultats obtenus sur des images ID montrent que la méthode proposée conduit à taux d'erreur total de 1%, contre 25% pour le meilleur de ses challengers. Ce taux d'erreur est compatible avec l'application sécuritaire visée.

Mots clés: Tatouage d'images, attaques Print-Cam, transformée de Fourier, déformation perspective, transformation de Hough, filtre de Wiener, variation colorimétrique.

Development of a robust image watermarking technique under print-cam attack

Abstract: Digital image watermarking consists in embedding information within the image which cannot be detected by the human visual system, but recovered with a software. The aim of this thesis is to propose a watermarking method when the watermarked image is printed on a physical support and then read freehandedly with a smartphone camera. In order to survive the Print-Cam process, the watermark must resist to multiple attacks. Those attacks occur during printing and capturing the image with a camera: in that case, the image might be rotated around the optical axis of the camera and translations may occur. Pixel value distortions are also present. These attacks may cause the loss of synchronization of the watermark and make the detection impossible. Hence, the main objective of the

thesis is to develop a watermarking method that is robust to the Print-Cam attack in the context of an industrial security application for ID images. Fourier transform is used as this watermarking domain has invariance properties against some geometric distortions. Three main correction methods were integrated to deal with Print-Cam attacks: frame-based perspective rectification of the freehandedly captured images using detection of Hough lines, a Wiener filter to decrease image blurring and reduce noise, and adjustments to reduce color degradations. Results show that the method is highly robust with a total error rate of 1%, compared to a least 25% of errors for other methods, 1% of error rate being compatible with the targeted industrial application.

Keywords: image watermarking, Print-Cam attacks, Fourier transform, perspective deformation, Hough transform, Wiener filter, color correction

Laboratoire IRF-SIC, Faculté des Sciences d'Agadir. Université Ibn Zohr, BP 8106 – Cité Dakhla, 80000 Agadir, Maroc.

Laboratoire PRISME – Pôle IRAuS, Axe Image et Vision. Polytech'Orléans, 12 Rue de Blois, BP 6744 45067 Orléans Cedex 2 France.