Sécurité des images par tatouage numérique et cryptographie dans les applications médicales

Mayssa Tayachi

DOCTORAT BRETAGNE LOIRE / MATHSTIC

Université de Bretagne Occidentale

THÈSE DE DOCTORAT EN COTUTELLE DE

جامعة تونس المنار
UNIVERSITÉ DE TUNIS EL MANAR

L'UNIVERSITÉ DE BRETAGNE OCCIDENTALE
ET L'UNIVERSITE DE TUNIS EL MANAR

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

Par
Mayssa TAYACHI

Sécurité des images par tatouage numérique et cryptographie pour les applications médicales

Thèse présentée et soutenue à l'Université de Bretagne Occidentale, le 10 septembre 2021
Unité de recherche : Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance (Lab-STICC / UMR CNRS 6285)

Rapporteurs avant soutenance :

Florent RETRAINT	Professeur des Universités, Université de Technologie de Troyes
Dorra SELLAMI	Professeur, École Nationale d'Ingénieurs de Sfax

Composition du Jury :

Président :	Gouenou COATRIEUX	Professeur, IMT Atlantique
Examinateurs :	Florent RETRAINT	Professeur des Universités, Université de Technologie de Troyes
	Dorra SELLAMI	Professeur, École Nationale d'Ingénieurs de Sfax
Dir. de thèse :	Laurent NANA	Professeur des Universités, Université de Bretagne Occidentale
Co-dir. de thèse :	Faouzi BENZARTI	Professeur, École Nationale Supérieure d'Ingénieurs de Tunis
Co-encadrante de thèse :	Anca PASCU	Maître de conférences HDR Emérite, Université de Bretagne Occidentale

Remerciement

Je tiens à exprimer ma sincère gratitude à l'égard de mon directeur de thèse Mr. Laurent NANA, professeur des universités à l'Université de Bretagne Occidentale. Il m'a transmis son enthousiasme pour la recherche, et depuis toutes les années où j'ai travaillé avec lui, il n'a cessé de m'encourager et de me soutenir. Cela a grandement facilité le long parcours de ma thèse et contribué à la richesse de ce travail. Je suis vraiment heureuse de travailler avec vous sur le plan scientifique et humain.
Je remercie également mon deuxième directeur de thèse Mr. Faouzi BENZARTI, professeur à l'Ecole Nationale Supérieure d'Ingénieurs de Tunis (ENSIT) pour son encadrement tout au long de cette thèse, ses conseils, ses encouragements et ses qualités humaines.
J'exprime tous mes chaleureux remerciements à Mme Anca Christine PASCU, Maitre de conférences à l'Université de Bretagne Occidentale d'avoir codirigé et encadré cette thèse. Merci d'avoir suivi mon travail et de m'avoir donné de précieux conseils.
Mes sincères remerciements vont également à Mr. Wael ADI professeur à l'Université Technique de Braunschweig, qui m'a offert une opportunité de stage de mobilité et m'a donné accès au laboratoire et aux installations de recherche à l'Université Technique de Braunschweig. Je remercie également Dr. Saleh MULHEM chercheur à l'université de Lübeck pour les discutions fructueuses sur les aspects de cryptographie pour l'authentication de l'image médicale.
Je remercie chaleureusement Mme Dorra SELLAMI, Mr Florent RETRAINT et Mr Gouenou COATRIEUX d'avoir accepté de faire partie de mon jury de thèse. Je leur adresse mes sentiments les plus respectueux.
Je remercie également Mr Florent RETRAINT et Mme Dorra SELLAMI pour avoir bien voulu rapporter sur mon travail de thèse.
J'adresse aussi mes remerciements à tous les membres de mes laboratoires de recherche Lab-STICC et LR-SITI particulièrement, l'equipe IRIS, tous les professeurs, les doctorants, les secrétaires et les techniciens pour leur aides précieuses et leur sympathies.
J'adresse également toute ma profonde gratitude à ma mère Monia TAYACHI, mon père Hassen TAYACHI, ma sœur Chaima et mes frères Wassim et Firas, mon grand père Abdelkader et ma grande mère Zaara pour m'avoir soutenu et encouragé depuis le début.

J'aimerais bien remercier mon mari Nadhmi qui est toujours resté à mes côtés, pour son amour et sa compassion au cours de ces années.

TABLE DES MATIÈRES

Liste des figures

Liste des tableaux

Liste des acronymes

ROI Region Of Interest

DICOM Digital Imaging and Communications in Medicine

RONI Region Of Non Interest

SUC Secret Unckown Cipher

DCT Discrete Cosine Transform

DFT Discrete Fourier Transform

SVD Singular Value Decomposition

LSB Least Significant Bit

DWT Digital Wavelet Transform

LBP Local Binary Pattern

PSNR Peak Signal to Noise Ratio

SSIM Structural Similarity Index Mesure

BER Bit Error Rate

NC Normalised Correlation

ER Embedding Ratio

MSE Mean Squared Error

GIF Graphics Interchange Format

JPEG Joint Photographic Experts Group.

TIFF Tagged Image File Format

PNG Portable Network Graphics

BMP Best Management Practice

DIB Device Independent Bitmap

VR Value Representation

VL Value Length

VF Value Field

RGB Red Green Bleu

PACS Picture Archiving and Communication System

RIS Radiology Information System

HIS Hospital Information System

CT Computed Tomography

AQ Assurance Quality

LIS Laboratory Information System

EPR Electronic Patient Record

IWT (Integer Wavelet Transform)

WQM Weighted Quantization Method

PPG Point to Point Graph

QIM Quantization Index Modulation

DE Diffrence Expansion

PE Prediction Error

HVS Human Visual System

PCET Polar Complex Exponential Transform

QM Quantisation Matrix

QR Quick Response

PCA Principal Component Analysis

RLE Run-length encoding

DT-CWT Dual-tree complex wavelet transform

RSA Rivest–Shamir–Adleman

CA Certification Authority

AES Advanced Encryption Standard

RC4 Ron's Code

WPT Wavelet Packet Transform

SPIHT Set Partitioning in Hierarchical Trees

JWE JSON Web Encryption

SS Spread Spectrum

SCSQIM Scalar Costa Scheme Quantization Index Modulation

RDM Rational Dither Modulation

OTP One Time Pad

DIC Doctor's Identification et Code

CDF Cohen-Daubechies-Fauraue

MIM Man In the Middele

INTRODUCTION GÉNÉRALE

Les applications de télémédecine sont de plus en plus utilisées en raison du développement rapide de l'imagerie numérique et des technologies de l'information et de la communication. Les informations médicales qui comprennent des images médicales et les informations des patients sont extraites et transmises sur des réseaux non sécurisés entre les hôpitaux, qui sont situés à divers endroits, pour de nombreuses raisons, telles que le télédiagnostic, les traitements, les téléconférences entre cliniciens, la consultation médicale, l'apprentissage et la formation à distance. Les images médicales peuvent être manipulées intentionnellement et non intentionnellement par des utilisateurs non autorisés [121]. La protection des données médicales est nécessaire. Car ces données jouent un rôle important et parfois même vital dans la santé des patients. Leur détérioration peut être une cause directe ou indirecte de graves atteintes à la santé des patients. Pour les contenus multimédias de santé, la sécurité revient alors à assurer :

— La confidentialité (origine de l'information et de son attachement à un patient donné).

— La disponibilité.

— La fiabilité (une information fiable peut être utilisée en toute confiance par les praticiens. La fiabilité devient traçabilité quand il est possible de tracer une donnée tout au long de son existence).

— L'intégrité (cela revient à apporter les preuves que l'information n'a pas été modifiée partiellement par des personnes non autorisées).

— L'authenticité (cela revient à apporter les preuves que l'information n'a pas été modifiée totalement par des personnes non autorisées).

Ces exigences de sécurité sont générales et d'autres peuvent apparaître assez rapidement en fonction du contexte applicatif.
Plusieurs solutions informatiques ont été proposées pour protéger les données médicales comme : la cryptographie, la stéganographie et le tatouage numérique. La stéganographie et le tatouage numérique sont deux techniques de dissimulation d'informations qui im-

pliquent de cacher une information secrète appelée marque dans des données numériques de sorte que la marque puisse être détectée ou extraite plus tard. La stéganographie cache la marque secrète dans un signal porteur de telle sorte que personne en dehors du destinataire autorisé ne connaisse l'existence de l'information cachée (c'est-à-dire l'existence de la marque) alors que pour le tatouage, la marque masquée peut être visible et le signal porteur (l'image hôte) est l'information importante qui doit être transmise. Le tatouage numérique peut être défini comme un processus qui cache des informations secrètes appelées marques dans les données numériques, de sorte que la marque intégrée puisse être détectée ou extraite ultérieurement pour produire une confirmation de la validité des données [121]. Le tatouage numérique a été reconnu comme une approche clé pour l'identification, l'authentification et l'intégrité des données numériques. Le tatouage numérique a de plus en plus d'intérêt en raison du souci croissant d'authenticité, d'intégrité et de la protection du droit d'auteur du contenu numérique. La cryptographie est une technique consistant à chiffrer (coder) une information, de manière à la rendre accessible uniquement aux personnes autorisées, par le biais d'un processus de déchiffrement (décodage). Une de ses limites est qu'elle ne peut pas aider le propriétaire d'un contenu numérique à surveiller la façon dont un l'utilisateur gère le contenu après le décryptage. Le tatouage numérique peut efficacement répondre aux exigences essentielles de la télémédecine ou de la protection des images, y compris aux problèmes d'identification unique, d'authentification, de protection des droits d'auteur et de vérification de l'intégrité lors de la transmission via des réseaux non sécurisé et le stockage dans de grandes bases de données [143].

Problématique

Cette thèse traite trois problèmes :

— Le premier problème est le problème d'authentification et d'identification des images médicales transmises via un réseau non sécurisé. La plupart des travaux de recherche sur le tatouage numérique des images médicales visent à protéger des documents numériques ou des images médicales envoyés sur le réseau en termes de confidentialité et d'intégrité des données transmises. Mais le problème principal se situe au niveau de la marque insérée, qui doit être à la fois invisible, résistante aux différentes attaques. Par conséquent, pour le cas des images médicales, les facteurs invisibilité et robustesse contre les attaques seront des facteurs décisifs.

— Le deuxième problème abordé est celui de la modification ou de la manipulation des images médicales et plus particulièrement, la zone nécessaire au diagnostic (zone nommée la Région d'Intérêt / Region Of Interest (ROI) de l'image. Lors de l'échange des informations médicales relatives aux patients ainsi que la collection et la diffusion des données médicales, des altérations sur les images médicales peuvent être réalisables. Par exemple, la Figure 1 montre une maladie du foie d'un patient qui est modifiée en changeant la position de la région infectée du foie en utilisant un logiciel disponible (par exemple, l'outil Adobe Photoshop) [130]. De nombreux autres cas de manipulation peuvent être appliqués. La modification de la zone ROI de l'image peut entraîner un diagnostic erroné qui affecte la vie d'un patient. C'est pour cette raison qu'il est recommandé d'insérer la marque dans la partie qui n'est pas absolument nécessaire au diagnostic.

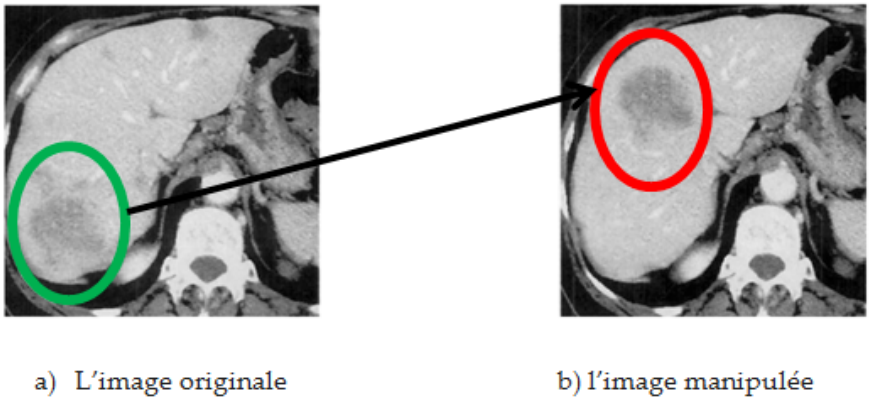


FIGURE 1 – Exemple d'une image médicale altérée

— Le troisième problème est relatif à la sécurité des dispositifs médicaux qui génèrent et traitent les images médicales utilisées par les personnes autorisées et non autorisées. Une des questions est comment assurer qu'une image émane d'une source fiable. Une autre question est celle de l'autorisation d'accès aux données uniquement aux personnes et dispositifs autorisés.

Contributions

Cette thèse a été orientée vers la conception et la mise en oeuvre d'approches de tatouage et de cryptographie pour répondre aux problématiques susmentionnées. Les principales contributions apportées dans ce cadre sont les suivantes :

1. **Une approche de zéro-tatouage pour l'authentification des images Digital Imaging and Communications in Medicine (DICOM)**
   Cette approche de zéro tatouage a pour but l'authentification des images DICOM. Elle fonctionne dans le domaine spatial. Son avantage est qu'elle n'insère pas la marque dans l'image. A partir des caractéristiques et des informations du patient extraites de l'image originale, elle génère une marque robuste qui est envoyée au récepteur pour la vérification de l'authenticité de l'image.
   La solution proposée assure une complexité de calcul plus faible que les solutions basées sur le domaine fréquentiel. La performance et l'efficacité de la solution proposée a été évaluée sous différentes attaques. Les résultats obtenus en termes d'imperceptibilité et de robustesse sont très satisfaisants.

2. **Une approche de tatouage double des images DICOM**
   Cette approche de tatouage d'image est basée sur la combinaison de la technique de construction de la marque du zéro-tatouage de la première approche et une technique de tatouage numérique pour l'insertion de la marque dans la partie RONI de l'image médicale afin d'éviter de modifier la partie anatomique de l'image dont le changement peut affecter le diagnostic médical. La méthode proposée fournit une solution d'authentification forte. En effet, elle offre deux manières d'authentifier l'image : soit par l'extraction de la marque, soit par l'extraction des caractéristiques de la partie anatomique de l'image. L'analyse des résultats expérimentaux obtenus avec la méthode proposée montre sa robustesse contre différentes attaques.

3. **Une approche d'authentification forte et résistante aux clones pour le système d'images médicales**
   Cette approche combine une technique de tatouage à expansion de différence avec une technique cryptographique basée sur des clés secrètes générées par un dispositif matériel (Hardware) résistant aux clones appelé Secret Unckown Cipher (SUC) (Chiffre Inconnu Secret) [2]. L'utilisation de SUC pour signer la marque renforce la sécurité des images médicales pendant leur transfert et leur stockage et élimine la reproductibilité et l'utilisation des images médicales par des personnes non autori-

sées.

Organisation de la thèse

Ce manuscrit de thèse est organisé en deux parties.
La première partie comporte deux chapitres (1 et 2) et aborde les notions fondamentales et un état de l'art sur le tatouage numérique d'images.

Le premier chapitre couvre les motivations de tatouage numérique, son schéma général, ses propriétés, ses classifications. En outre, il contient les différentes techniques de tatouage d'image numérique, les principes de diverses attaques contre les systèmes de tatouage d'images numériques. Les mesures de performance de tatouage d'images numériques sont également présentées dans ce chapitre.

Dans le chapitre 2 nous rappelons la définition des images médicales, ses types, ses formats les plus utilisés, sa gestion, ses risques et ses menaces. Dans la deuxième partie de ce chapitre, nous décrivons un état de l'art sur les différentes méthodes existantes de tatouage numérique qui sont proposées dans la littérature et visent à fournir l'authentification et l'identification des images médicales et nous discutons leurs limites et leurs intérêts de sécurité.

La deuxième partie du manuscrit est dédiée aux contributions de la thèse. Elle comporte trois chapitres (3, 4 et 5).

Dans le chapitre 3, nous décrirons une approche de zéro-tatouage pour l'authentification des images DICOM, qui vise à garantir l'authenticité des images médicales transmises par le biais d'un réseau public non sécurisé. La nouveauté de cette approche repose sur deux points principaux. Le premier point est l'extraction et la sélection des caractéristiques de l'image, appelées caractéristiques pertinentes, qui sont utilisées pour l'identification de l'image. Ces caractéristiques sont sélectionnées à partir d'un large ensemble de caractéristiques d'images, en utilisant une approche d'analyse statistique qui vise à sélectionner l'ensemble minimal discriminant de caractéristiques ayant la plus grande résistance aux attaques existantes. Le second point est le processus de construction de la clé qui est basé sur la combinaison d'informations extraites de l'en-tête des images DICOM, des caractéristiques pertinentes et d'un modèle Jacobien.

Le chapitre 4 présente une approche qui combine une méthode de zéro-tatouage dans la partie de région d'intérêt (ROI) de l'image et une méthode de tatouage numérique pour l'insertion de la marque dans la partie de la région de non intérêt (RONI) de l'image.

Dans cette approche des caractéristiques pertinentes extraites de l'image DICOM sont utilisées, d'une part, pour le zéro-tatouage basé sur le modèle Jacobien, et d'autre part, pour construire la marque qui est insérée dans la région de fond noir de l'image (RONI) en utilisant la technique d'interpolation linéaire ce qui permet de bien contrôler l'aspect imperceptibilité de la marque. La marque est insérée uniquement dans la zone de fond noir afin d'éviter d'affecter la partie anatomique (ROI) dont la modification peut entraîner un diagnostic erroné.

Dans le chapitre qui suit (chapitre 5), une nouvelle méthode résistante aux clones est proposée dont l'objectif est de renforcer la sécurité des images médicales. Le renforcement de la sécurité de l'image consiste à apporter les preuves de son intégrité, de ses origines et son attachement à un patient donné. Dans cette approche des informations sont extraites de l'image originale pour générer la marque. Ensuite, la marque est signée avec un dispositif de chiffrement physique SUC afin d'obtenir une marque signée résistante aux clones. La combinaison du SUC avec la marque garantit une confidentialité, une intégrité et une authenticité solides et offre un niveau élevé de sécurité au système d'imagerie médicale.

Le chapitre 6 conclut la thèse et décrit les travaux futurs.

Chapitre 1

Notions de base en tatouage numérique d'image

1.1 Introduction

Dans ce chapitre nous présentons en premier les motivations d'un système de tatouage numérique d'image, sa définition, son principe de fonctionnement, ses différentes étapes qui permettent l'insertion et l'extraction de la marque et ses principales propriétés. Nous introduisons ensuite une classification des techniques de tatouage numérique selon le type de données utilisées, le domaine d'insertion, la perception visuelle et la réversibilité. Une explication du principe de chaque technique de tatouage numérique est présentée par la suite. Après avoir expliqué les principes de chaque technique de tatouage, nous présentons brièvement les métriques d'évaluation des systèmes de tatouage en termes d'imperceptibilité et de robustesse. Après une étude des attaques auxquelles une image tatouée est potentiellement soumise est présentée. Une classification des attaques en deux types est considérée et expliquée : attaques de robustesse et attaques de sécurité. À la fin de ce chapitre, nous présentons les techniques qui combinent le tatouage numérique et la cryptographie pour la sécurité des images médicales.

1.2 Les motivations du tatouage numérique d'images médicales

La transmission des images médicales entre les hôpitaux, situés à divers endroits et différentes organisations administratives est devenu une pratique courante pour de nombreuses raisons.

Les exigences de sécurité des informations médicales découlent principalement des règles législatives et d'une éthique forte de la politique de sécurité, que les professionnels

et les patients concernés doivent suivre [108]. Cela nécessite trois fonctionnalités obligatoires : la confidentialité, la fiabilité et la disponibilité.
La confidentialité indique que seules les personnes autorisées, dans les situations normalement prévues, ont accès aux données. La fiabilité peut être décomposée en deux aspects :

— L'intégrité qui vérifie que les informations n'ont pas été modifiées.

— L'authentification qui garantit que les données appartiennent au bon patient et sont délivrées à partir de la source vérifiée.

La disponibilité définit la capacité des utilisateurs autorisés à utiliser le système d'information dans les situations normalement prévues d'accès et de pratique [32].
La confidentialité des données d'une image peut être obtenue en appliquant de nombreuses techniques telles que le cryptage, le contrôle d'accès et le pare-feu.
L'authentification nécessite la mise en œuvre de mesures pour découvrir si la confidentialité et / ou l'intégrité des données a été violée [120].
De nombreuses actions de manipulation ou de piratage des images médicales peuvent être appliquées lors de la transmission via des réseaux publics, mais le problème est de savoir comment les détecter ? Les techniques de tatouage numérique représentent une excellente solution pour protéger l'image médicale.

1.3 Qu'est-ce que le tatouage numérique ?

Le tatouage numérique est une technique permettant d'insérer dans un support numérique, de manière visible ou non visible, une information appelée marque.
La marque peut être une image, un texte, une vidéo, un audio ou bien une autre information numérique dans l'image hôte. La marque peut être insérée d'une manière visible ou invisible/ imperceptible sans altérer la qualité visuelle de l'image entière. Cette marque doit être résistante aux différentes attaques de traitement d'images. Elle peut être identifiée ou extraite ultérieurement pour produire une confirmation de la validité des données.
Pour la conception d'un algorithme de tatouage numérique performant, la marque insérée doit cependant respecter trois contraintes fondamentales : la robustesse, l'imperceptibilité et la capacité. Le tatouage numérique permet d'assurer un service de sécurité (copyright, intégrité, non répudiation, authentification, etc.).

1.4 Le schéma général du système de tatouage numérique

Le modèle de base du schéma de tatouage numérique se compose de trois éléments [108], [83] : le processus de génération de la marque, le processus d'insertion de la marque et le processus d'extraction de la marque. La génération de la marque est illustrée dans la figure 1.1, l'insertion de la marque est présentée dans la figure 1.2 tandis que l'extraction de la marque est présentée dans la figure 1.3.

1.4.1 Le processus de génération de la marque

La génération de la marque n'est pas une fonction standard. La marque doit être adaptée aux applications souhaitées. Dans les applications simples, les données insérées peuvent être un texte ou une image. Dans les applications développées, la marque peut avoir des propriétés particulières en fonction des objectifs souhaités.
Par exemple, dans les applications médicales, la marque peut avoir besoin des informations du patient ou des caractéristiques extraites de l'image hôte pour confirmer l'intégrité et l'authenticité des données tatouées. Donc, l'algorithme de génération est dépendant du but poursuivi bien qu'il soit soumis à certaines contraintes.

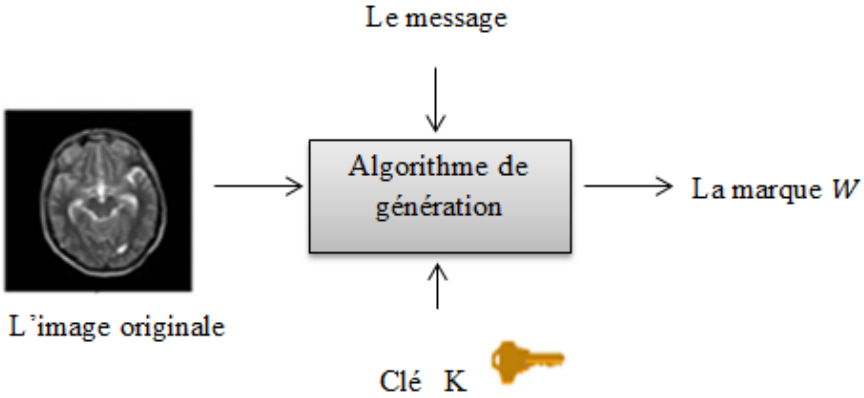


FIGURE 1.1 – le processus de la génération de la marque.

La figure 1.1 montre que les données originales (l'image originale), le message utilisateur spécifique et la clé secrète k sont trois paramètres qui peuvent être utilisés dans

l'algorithme de la génération de la marque. Certains ou tous ces paramètres sont nécessaires pour générer la marque. La sélection des paramètres requis dépend de l'application visée.

1.4.2 Le processus d'insertion de la marque

Le processus d'insertion de la marque se fait côté expéditeur. Dans cette étape, la marque est insérée aux données originales en appliquant un certain algorithme de tatouage et en utilisant une clé secrète k pour générer les données tatouées.

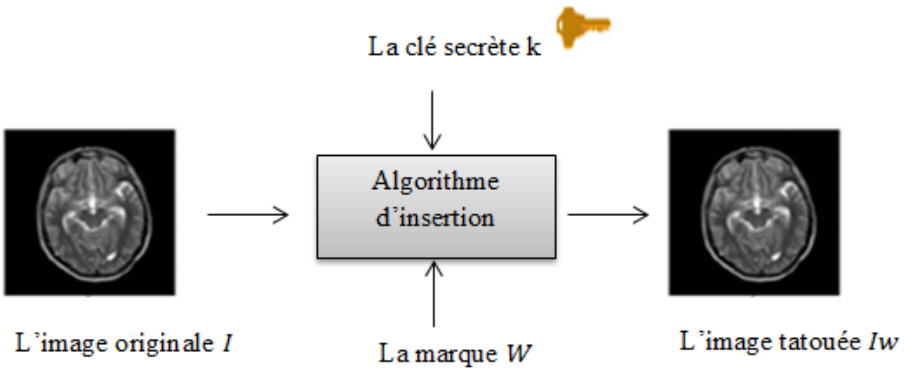


FIGURE 1.2 – le processus d'insertion de la marque.

1.4.3 Le processus d'extraction de la marque

Le processus d'extraction se fait en inversant l'algorithme d'insertion implémenté et en utilisant la clé secrète et / ou les données originales pour détecter / extraire la marque intégrée. La Figure 1.3 montre le principe du processus d'extraction de la marque.

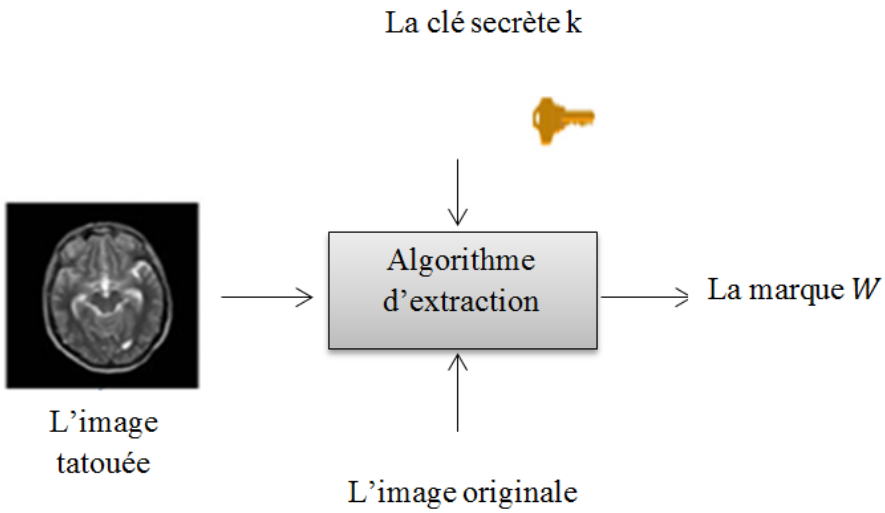


FIGURE 1.3 – le processus d'extraction de la marque.

1.5 Les propriétés d'un système de tatouage numérique performant

Plusieurs exigences sont essentielles pour la conception d'un système général de tatouage. Ces exigences incluent sept propriétés généralement utilisées. Elles peuvent être décrites comme suit :

— **La sécurité**
La sécurité caractérise la capacité de marquage à résister aux attaques malicieuses. Un système de tatouage est censé être sécurisé au sens que l'utilisateur non autorisé ne peut pas extraire la marque sans avoir des informations complètes sur l'algorithme et la clé secrète qui ont été utilisés pour insérer la marque. Le facteur de sécurité est crucial pour le système de tatouage et seule la personne autorisée peut extraire la marque.

— **La robustesse**
Cette exigence signifie la capacité du système de tatouage à résister à différentes attaques de traitement d'image. Ces attaques visent à supprimer ou détruire la marque insérée ou même à empêcher la marque de remplir son objectif attendu. Cox et al [36] définissent également la robustesse comme la capacité de détecter la

marque après des opérations de modification (traitement).

— **L'imperceptibilité ou l'invisibilité**
La marque doit être insérée avec la moindre dégradation de la qualité visuelle de l'image et d'une manière invisible autant que possible à l'œil humain pour qu'il ne puisse pas être détruit facilement par les pirates. Cox et al [36] définissent l'invisibilité comme une similitude visuelle entre l'image originale et l'image tatouée.

— **La capacité**
Cette propriété fait référence au nombre de bits qui peuvent être insérées sans affecter la qualité de l'image. Ce facteur définit le nombre de bits pouvant être incorporés sous forme de marque afin qu'ils puissent être efficacement découverts grâce au processus d'extraction. La capacité d'insertion dépend de l'application requise. Plusieurs applications de tatouage numérique ont différentes exigences de capacité selon le but recherché par le tatouage de l'image.
La capacité de tatouage est liée à deux autres propriétés importantes du système de tatouage, qui sont l'imperceptibilité et la robustesse. Ces trois propriétés sont fortement liées mais il est difficile de déterminer l'une à partir des autres. La relation entre elles est illustrée dans la figure 1.4. De toute évidence, une capacité élevée peut être obtenue en dégradant plus fortement l'image originale et en diminuant la robustesse. Par conséquent, un compromis approprié doit être trouvé en fonction de l'application [36].

— **La réversibilité**
Dans les domaines médicaux, si une image est modifiée pendant le processus de travail, cela peut conduire à des diagnostics erronés avec des implications graves pouvant aller jusqu'à la mort du patient.Par conséquent,la nécessité de récupérer strictement les données originales de l'image tatouée est élevée [66]. Les méthodes de tatouage réversibles ou sans perte satisfont à cette exigence en ce qu'elles garantissent l'extraction de la marque avec reconstruction exacte de l'image originale non modifiée [153]. Cependant, une image tatouée n'est pas exempte de distorsion, en particulier dans les techniques réversibles, mais l'image modifiée est utilisée comme couverture pour réaliser la marque, pas pour des fins de diagnostic. L'image récupérée est utilisée pour le diagnostic, la planification des interventions, etc [123].

— **La complexité**
Cette caractéristique du processus de tatouage est définie comme la durée du processus d'insertion et d'extraction de la marque. Les techniques de tatouage numérique

devront être de complexité très faible. Par exemple, dans le cas d'une application en temps réel des algorithmes rapides et efficaces sont nécessaires.

— **La fiabilité**

La fiabilité peut être décomposée en deux parties :

L'intégrité : est la capacité de prouver que les données n'ont pas été modifiées sans autorisation.

L'authentification : est la capacité d'identifier l'origine des informations et de confirmer que les données se réfèrent au bon patient.

Aujourd'hui, il n'y a pas de méthode de tatouage pour assurer toutes ces caractéristiques en même temps, donc d'une manière optimale. Cependant, en réalité, les exigences liées à chacun de ces attributs varient selon le contexte de l'application (par exemple, le contrôle d'intégrité, le suivi des copies illégales, la protection des droits d'auteur, etc). La méthode de tatouage sera choisie en fonction du compromis établi entre ces différents attributs.

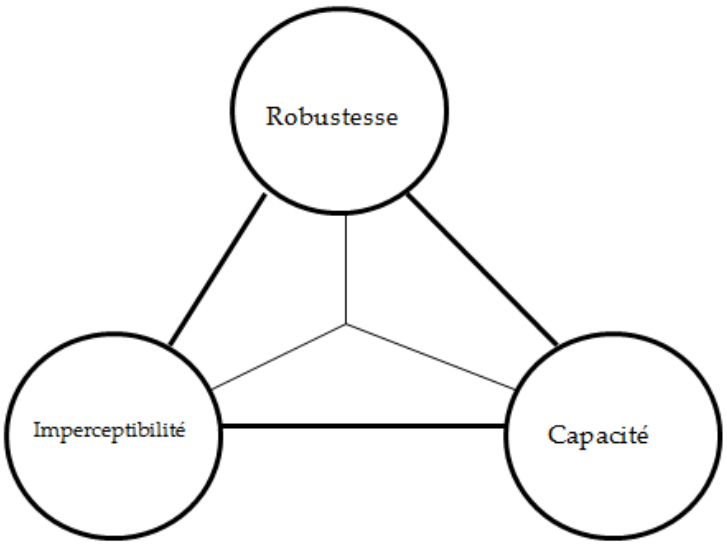


FIGURE 1.4 – Le triangle de compromis entre les trois caractéristiques essentielles : robustesse, capacité et imperceptibilité [121]

1.6 Classifications des systèmes de tatouage numérique

Les systèmes de tatouage numérique peuvent être classés suivant plusieurs critères notamment : le type des données utilisées, le domaine d'insertion, la perceptibilité humaine et la réversibilité. Ces classifications sont présentées dans la figure 1.5 .
Le tatouage numérique peut être appliqué sur différents types de données tels que le texte,

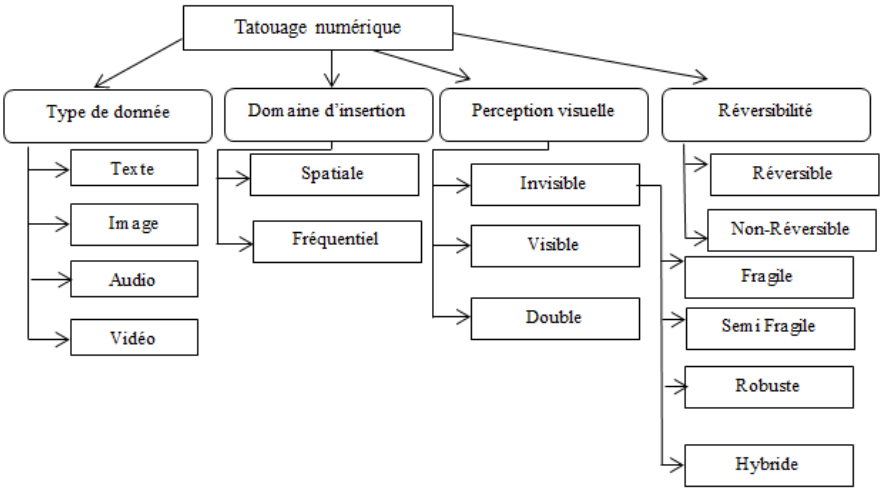


FIGURE 1.5 – Schéma de classification des types de tatouage numérique

l'image, l'audio et la vidéo. Les approches de tatouage numérique peuvent être conçues dans les domaines suivants : le domaine spatial (matrice de pixels), le domaine fréquentiel (les transformées). Selon la perception humaine, le tatouage numérique peut être classé en approches visibles, invisibles et doubles. Des approches de tatouage invisibles peuvent être classées en fonction de leur robustesse en quatre catégories : fragiles, semi-fragiles, robustes et hybrides. En plus des classifications précédentes, les approches de tatouage numérique peuvent être classées en réversibles et irréversibles.
La classification principale des approches de tatouage numérique est discutée dans les sous-sections suivantes.

1.6.1 Classification basée sur le type de données

Les données peuvent être de type texte, image, audio ou vidéo qui fait référence à l'insertion des marques dans un texte / une image / un audio / une vidéo afin de protéger le contenu des données contre la copie, la transmission ou la manipulation des données.

1.6.2 Classification basée sur la réversibilité

Les techniques de tatouage peuvent être classées en deux catégories, réversibles et irréversibles. Le tatouage réversible permet de retrouver ou de restaurer l'image originale à partir de l'image tatouée en appliquant une transformation inverse sans produire de changements. Il évite les distorsions irréversibles dans l'image originale en appliquant des techniques capables d'extraire l'image originale. Cependant, dans le tatouage irréversible (non réversible), il n'existe aucun moyen de trouver l'image originale à partir de l'image tatouée. La réversibilité est une exigence importante pour certaines applications qui traitent avec des données numériques sensibles telles que des applications médicales, militaires ou des applications dans le domaine législatif. Les approches de tatouage réversibles garantissent l'extraction de la marque insérée et les données originales exactement à partir du tatouage.

1.6.3 Classification basée sur la perception visuelle

En se basant sur la propriété de perception visuelle humaine, les approches de tatouage numérique sont classées en trois catégories : les approches visibles, invisibles et doubles.

— **Le tatouage visible**
Dans le tatouage visible, la marque est insérée dans les données originales de telle sorte qu'elle est visible à l'œil humain. Un tatouage visible est utilisé pour indiquer la propriété de données multimédias. Le logo ou le sceau des organisations, estampillé sur les documents, images ou vidéos, etc. pour l'identification du contenu et de la propriété sont les exemples les plus populaires de tatouage visibles. La figure 1.6 montre un exemple de tatouage visible d'une image médicale.

— **Le tatouage invisible**
Dans le tatouage invisible, la marque est insérée dans les données originales de manière à être imperceptible à l'œil humain. Dans la Figure 1.7 nous montrons un exemple de tatouage invisible d'une image médicale.

FIGURE 1.6 – Un exemple d'un tatouage visible d'une image médicale

FIGURE 1.7 – Un exemple de tatouage invisible d'une image médicale

— **Le tatouage double**
Dans certaines applications, les marques visibles et invisibles peuvent être appliquées ensemble. Cette procédure est appelée le tatouage double et dans cette situation, la marque invisible est considérée comme une sauvegarde pour le visible.

1.6.4 Classification selon le domaine d'insertion

Le domaine d'insertion est défini comme étant *la représentation numérique de l'image*. Il existe deux types de représentations : *le domaine spatial* et *le domaine fréquentiel*.
Dans une première approche, l'image numérique a été représentée comme une fonction $I(x, y)$ définie sur une matrice de pixels $M(x, y)$, $x = 1, \ldots n$; $y = 1, \ldots m$ et prenant des valeurs dans un ensemble de type $\{0, 2^1, 2^2, 2^n\}$ de niveaux de gris pour l'image noir et blanc ou dans un ensemble de type $M(x, y) \times \{l'espaceRGB\}$ pour l'image en couleur.
Cette représentation est appelée *domaine spatial*.
Le domaine fréquentiel est la représentation de l'image par une des fonctions associée à la fonction $I(x, y)$ et notamment *la transformée en cosinus discrète (Discrete Cosine Transform (DCT))*, *la transformée discrète en ondellettes (Digital Wavelet Transform (DWT))*, *La transformée de Fourier discrète (Discrete Fourier Transform (DFT))*, *La décomposition en valeurs singulières (Singular Value Decomposition (SVD))*.
L'étalement de spectre applique une autre transformation qui est une combinaison entre la fonction $I(x, y)$ ou une de ses transformées et en construisant un vecteur de variables aléatoires.
Les techniques de tatouage numérique peuvent être divisées selon le domaine d'insertion en deux groupes principaux : les techniques de tatouage dans *le domaine spatial* et les techniques de tatouage dans *le domaine fréquentiel*.

Le tatouage dans le domaine spatial

Une image dans le domaine spatial est représentée comme une fonction $I(x, y)$ définie sur une matrice $M(x, y)$ (le domaine des pixels) à valeurs dans un ensemble de niveaux de gris ou de couleurs. Dans les méthodes de tatouage qui utilisent cette représentation de l'image, la marque est insérée dans l'image originale en modifiant directement les valeurs des pixels de l'image.
Ces méthodes sont plus simples, plus rapides et moins couteuses en temps d'exécution. De plus, une marque peut être masquée plusieurs fois.

Cet avantage offre une robustesse supplémentaire contre toute attaque car la possibilité de supprimer toutes les marques est très faible.
Les techniques du domaine spatial peuvent avoir certains avantages, mais leur principal inconvénient est qu'elles ne peuvent pas survivre à certains types d'attaques géométriques et à de nombreuses opérations telles que l'application de méthodes de compression avec bruit et avec perte.
Quelques techniques classiques d'insertion de la marque dans le domaine spatial sont présentées ci-dessous :

La méthode du bit le moins significatif, Least Significant Bit (LSB)

La méthode du bit le moins significatif (Least Significant Bit (LSB)) représente l'une des techniques du domaine spatial les plus anciennes et les plus simples. Elle peut être appliquée à n'importe quelle forme de tatouage. Dans cette technique, le LSB de l'image originale est remplacé par la marque. Les bits de la marque sont codés dans une séquence qui sert de clé. Cette séquence doit être connue pour récupérer les bits insérés dans l'image originale. La valeur en pixels décimaux de l'image originale est d'abord convertie en binaire. Ensuite, les bits les plus à droite de chaque pixel sont remplacés par les bits de la marque.
Enfin, les pixels binaires modifiés sont retournés à leurs valeurs décimales originale. La Figure 1.8 montre un exemple de fonctionnement de la technique de tatouage LSB.

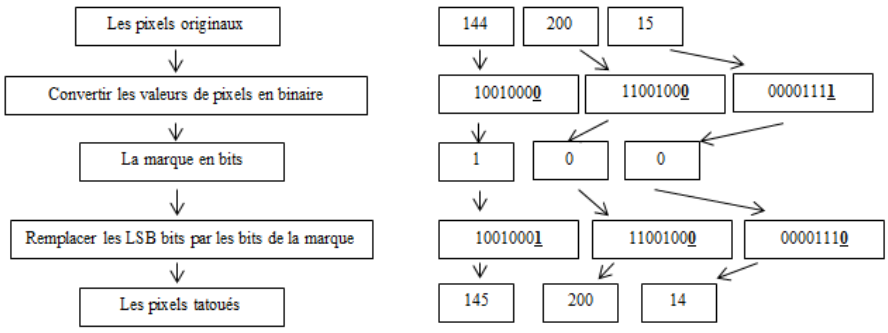


FIGURE 1.8 – La technique de tatouage LSB

Le modèle binaire local (LBP)

Le modèle binaire local (Local Binary Pattern (LBP)) est une méthode initialement conçue pour l'analyse de la texture, la reconnaissance d'objet / motif et une estimation de foule (crowd estimation)[27]. L'idée de base de LBP est de résumer la structure locale de l'image en comparant chaque pixel avec ses pixels de voisinage. Premièrement, l'image originale est partitionnée en blocs carrés non superposés. Deuxièmement, les différences de pixels locaux entre le pixel central et ses pixels adjacents dans chaque bloc sont calculées. Ensuite, ces pixels sont utilisés pour insérer les bits de la marque en utilisant le pixel central comme seuil. Le pixel de voisinage est étiqueté à 1 si son intensité est supérieure au seuil, sinon étiqueté à 0. À la fin de ce processus, LBP produit un code binaire de 8 bits de 0 à 255.
Les méthodes basées sur LBP sont robustes contre la variation de luminance et le réglage du contraste, mais fragiles avec d'autres opérations comme le bruitage et le filtrage. En d'autres termes, cette technique convient aux applications de tatouage semi-fragiles [100].

La technique de modification d'histogramme

Une autre technique de tatouage dans la catégorie du domaine spatial est la modification d'histogramme qui est basée sur les valeurs de pixels de l'image hôte pour construire l'histogramme de l'image et utilise la redondance des informations statistiques de l'image hôte pour masquer les données secrètes. Cette technique insère la marque en décalant le maximum et le zéro (ou le minimum s'il n'y a pas de zéro) de l'histogramme. Cette méthode peut être exécutée facilement, mais la capacité d'insertion est limitée par le nombre de points maximum qui apparaissent [62].

1.6.5 Le tatouage dans le domaine fréquentiel ou le domaine des transformées

Les techniques de tatouage numériques dans le domaine fréquentiel sont des méthodes utilisant des algorithmes basés sur l'insertion de la marque non pas directement dans la fonction de l'image $I(x, y)$, mais dans les coefficients des transformées de celle-ci. Dans ce domaine le tatouage est réalisé après une décomposition de la fonction de l'image $I(x, y)$ par des transformées telle que la transformée en cosinus discrète (Discrete Cosine Transform (DCT) [10], la transformée discrète en ondellettes (Discrete Wavelet Transform

- DWT) [9], la transformée de Fourier discrète (Discrete Fourier Transform - DFT) [64], la décomposition en valeurs singulières (Singular Value Decomposition - SVD) [9]. Les méthodes fréquentielles sont plus robustes à la compression et moins sensibles aux attaques géométriques.

La transformée en cosinus discrète (DCT)

La transformée en cosinus discrète (DCT) est l'une des principales méthodes mises en œuvre pour transformer les données du domaine spatial en domaine fréquentiel. L'image est divisée en blocs de $M \times N$ pixels. En appliquant cette technique, l'image sera segmentée en trois groupes : basses fréquences (BF), moyennes fréquences (MF) et hautes fréquences (HF). La plupart de l'énergie est concentrée dans la région des basses fréquences, tandis que la partie des hautes fréquences contient le moins d'énergie.
Les équations mathématiques de la transformation directe et inverse de la 2D-DCT sont présentées dans les équations (1.1) et (1.2) :

$$C(u,v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i,j) cos \frac{\pi(2i+1)u}{2M} \times cos \frac{\pi(2j+1)v}{2N} \tag{1.1}$$

$$f(i,j) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \alpha_u \alpha_v C(u,v) cos \frac{\pi(2i+1)u}{2M} \times cos \frac{\pi(2j+1)v}{2N} \tag{1.2}$$

Où u et v sont les positions horizontales et verticales (u=0,1,...,M-1 , v=0,1,...,N-1), $C(u,v)$ est le coefficient DCT de l' image, $f(i,j)$ est la valeur du pixel à la position (i,j) de l'image dans le domaine spatial, $M \times N$ est la taille de l'image. Les valeurs de α_u et α_v sont obtenues à partir des équations (1.3) et (1.4), respectivement.

$$\alpha_u = \begin{cases} \sqrt{1/M}, u = 0 \\ \sqrt{2/M}, 1 \leq u < M-1 \end{cases} \tag{1.3}$$

$$\alpha_v = \begin{cases} \sqrt{1/N}, v = 0 \\ \sqrt{2/N}, 1 \leq v < N-1 \end{cases} \tag{1.4}$$

Les coefficients DCT sont utilisés pour masquer la marque. Cette technique est robuste contre l'attaque de compression d'images JPEG car cette attaque est basée sur la technologie DCT. Cependant, DCT a une résistance faible aux attaques géométriques fortes comme la mise à l'échelle, le recadrage, la translation et la rotation, etc.

La transformée en ondelette discrète (DWT)

La transformée en ondelettes discrète (DWT) est une fonction mathématique qui associe à la fonction de l'image, $I(x, y)$ une autre fonction dont le domaine est exprimé en ondelettes. Dans le cas de l'image, cette fonction fournit une localisation spatiale appropriée et possède des caractéristiques multi-résolutions, qui sont similaires aux modèles théoriques du système visuel humain. Cette méthode est robuste contre les filtres médians et les filtres passe bas. Cependant, le tatouage utilisant cette transformée n'est pas résistant aux attaques géométriques [9]. La méthode DWT sépare l'image hiérarchiquement en quatre sous-bandes : LL, HL, LH et HH comme le montre la figure 1.9, où L = faible et H = élevé. La sous-bande LL comprend une approximation de l'image, tandis que les trois autres sous-bandes couvrent les détails manquants. De plus, la sous-bande LL résultant de n'importe quelle étape peut également être décomposée en continu pour atteindre un autre niveau jusqu'à atteindre le nombre requis de niveaux basés sur l'application.
Dans les systèmes de tatouage numérique, les niveaux de décomposition les plus faibles de l'image, sont les plus utilisés pour l'insertion de la marque.

La Figure 1.9 montre la décomposition en ondelettes à 2 niveaux de la technique DWT.

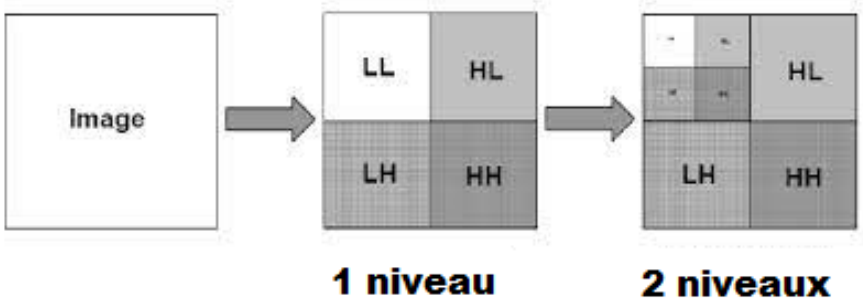


FIGURE 1.9 – La décomposition en ondelettes à 2 niveaux de résolution .

La transformé de Fourrier discrète (DFT)

La DFT désigne la technique la plus populaire pour convertir les images du domaine spatial en domaine fréquentiel [63]. Elle offre plus de robustesse contre les attaques géométriques. La DFT décompose l'image initiale sous une forme sinusoïdale et cosinusoïdale.

Par conséquent, l'insertion de la marque peut être implémentée de deux manières : l'insertion directe et l'insertion basée sur un modèle. On considère $f(x, y)$ une image de taille $M \times N$ avec $x = 0, 1, 2, \ldots, M-1$ et $y = 0, 1, 2, \ldots, N-1$. La transformée de Fourier Discrète et sa transformée inverse sont respectivement données par les équations (1.5) et (1.6)

$$F(u, v) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x, y) e^{-} j2\pi (\frac{ux}{N} + \frac{uy}{M}) \tag{1.5}$$

$$F(u, v) = \frac{1}{NM} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} F(u, v) e^{-} j2\pi (\frac{ux}{N} + \frac{uv}{M}) \tag{1.6}$$

Où : $F(u, v)$ est le coefficient de DFT, $u = 0, 1, 2, \ldots, M-1$, $v = 0, 1, 2, \ldots, N-1$.

1.6.6 Comparaison entre le domaine spatial et le domaine fréquentiel

Pour comprendre la différence entre le domaine spatial et le domaine fréquentiel, une étude comparative est effectuée dans cette sous-section. Commencent par la technique d'insertion de la marque dans le domaine spatial, la marque est directement insérée dans les pixels de l'image tandis que dans le domaine fréquentiel, la marque est insérée dans les transformés des coefficients de l'image. En termes de robustesse, prenons le domaine fréquentiel, la marque est plus robuste que dans le domaine spatial. L'imperceptibilité dans le domaine spatial est plus élevée et contrôlable dans le domaine spatial alors que dans le domaine fréquentiel l'imperceptibilité est faible et contrôlable. Parlant de la capacité, nous remarquons que la capacité est plus élevée dans le domaine fréquentiel que dans le domaine spatial. Ainsi que pour la complexité de tatouage dans le domaine fréquentiel, nous remarquons qu'elle est plus élevée que la complexité dans le domaine spatial. En termes de temps d'exécution, le temps d'exécution dans le domaine spatial est plus faible que le temps d'exécution dans le domaine fréquentiel. Le tableau 1.6.6 montre la différence entre le domaine spatial et le domaine fréquentiel.

	Domaine spatial	Domaine fréqeuntiel
Technique d'insertion	Directement dans les pixels de l'image	Dans les coefficients des transformées
Robustesse	Faible	Elevée
Imperceptibilité	Elevée et contrôlable	Faible et contrôlable
Capacité	Faible	Elevée
Complexité	Faible	Elevée
Temps d'exécution	Faible	Elevée

TABLE 1.1 – Comparaison entre le domaine spatial et le domaine fréquentiel

1.6.7 Les techniques basées sur la combinaison des domaines spatial et fréquentiel

Ce sont des techniques de tatouage permettant de fournir plus de marques et de réduire au minimum la distorsion de l'image tatouée. Elles se basent sur des algorithmes d'insertion de la marque dans la combinatoire de deux domaines spatial et fréquentiel. Le principe consiste à partitionner la marque de l'image hôte en deux parties, respectivement, pour l'insertion spatiale et l'insertion fréquentielle qui sont réalisées en fonction de la préférence de l'utilisateur et de l'importance des données.

1.7 Les métriques d'évaluation de la performance d'un système de tatouage numérique

Les performances de tout système de tatouage numérique d'image en termes d'imperceptibilité, de robustesse et de taux d'insertion sont exprimées à l'aide de métriques bien connues : le rapport signal /bruit (Peak Signal to Noise Ratio (PSNR)), l'indice de similarité (Structural Similarity Index Mesure (SSIM)), les coefficients de corrélation normalisés (Normalised Correlation (NC)), le taux d'erreur sur les bits (Bit Error Rate (BER)) et le taux d'incorporation (Embedding Ratio (ER)) [151] [171]. La description de ces métriques est effectuée dans cette section.

1.7.1 L'évaluation de l'imperceptibilité d'une image tatouée

Pour vérifier le critère d'imperceptibilité, l'image tatouée doit être de même qualité que l'originale c-à-dire que l'image tatouée et l'originale soient perceptuellement équiva-

lentes. Les mesures visuelles de la qualité d'image sont effectuées sur le calcul de proximité de l'image tatouée par rapport à l'image originale ou bien sur la distorsion ou niveau de dégradation introduit par d'autres traitements sur l'image. Parmi ces mesures, nous trouvons des métriques basées sur la comparaison des pixels entre l'image hôte et l'image tatouée. Parmi les métriques basées sur la différence des pixels, nous citons : le rapport signal/bruit (PSNR), l'erreur quadratique moyenne (Mean Squared Error (MSE)) et l'indice de similarité (SSIM).

L'erreur quadratique moyenne (MSE)

L'erreur quadratique moyenne (Mean Square Error) compare l'image originale et l'image tatouée pixel par pixel. Elle est représentée par la formule suivante :

$$MSE(I, \bar{I}) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I_w(i,j))^2 \tag{1.7}$$

Où $I(i,j)$ est la valeur de la luminance du pixel (i,j) de l'image originale et $I_w(i,j)$ est celle de l'image tatouée, les deux images étant de taille $(M \times N)$. La MSE renseigne sur la dégradation ou niveau de distorsion introduite au niveau des pixels entre l'image hôte I et l'image tatouée I_w. Plus la MSE est grande, plus le niveau de distorsion est élevé. Une MSE de valeur faible est mieux appréciée.

Le rapport signal-bruit (Peak Signal to Noise Ratio) PSNR

Le PSNR (Peak Signal to Noise Ratio) est généralement utilisé pour estimer la qualité de l'image originale et tatouée. Une valeur PSNR plus élevée indique que les deux images sont plus similaires les unes aux autres. Cette métrique est déterminée en décibels (dB). Le PSNR est défini par :

$$PSNR(I, I_w) = 10 \log_{10} \left[\frac{255^2}{MSE} \right] dB \tag{1.8}$$

Où I est l'image originale. I_w est l'image tatouée, MSE est la quadratique moyenne. Une valeur de PSNR inférieure à $30db$ signifie que l'image contient des dégradations visuelles ou perceptibles.

La mesure de l'indice de similarité structurelle (Structural Similarity Index Measurement (SSIM))

Le SSIM mesure la similitude entre deux images dans un modèle basé sur la perception qui considère la dégradation de l'image comme un changement perçu des informations structurelles. Les informations structurelles sont les informations véhiculées par les interdépendances entre les pixels spatiaux adjacents de l'image. Ces interdépendances entre les pixels spatiaux adjacents ont beaucoup d'informations sur la structure d'objets dans la scène de perception visuelle. SSIM est calculé en incorporant des caractéristiques perceptuelles importantes, notamment le masquage de luminance et le masquage de contraste. Le masquage de luminance par lequel les distorsions de l'image ont tendance à être moins visible dans les régions lumineuses de l'image, tandis que le masquage de contraste par lequel les distorsions deviennent moins visibles dans les zones d'activité très importantes ou texturées dans l'image. Le SSIM est calculé selon l'équation 1.9.

$$SSIM(I, I_w) = \frac{(2\mu_I\mu_{I_w} + C_1)(2\sigma_{II_w} + C_2)}{(\mu_I^2 + \mu_{I_w}^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} \tag{1.9}$$

La moyenne de SSIM est également calculée selon l'équation 1.10.

$$mSSIM(I, I_w) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} SSIM(I_{ij}, I_{wij}) \tag{1.10}$$

Où μ_I est la moyenne de l'image originale I, μ_{I_w} est la moyenne de l'image tatouée I_w, σ_{II_w} est la covariance de I et I_w, σ_I^2 est la variance de I, $\sigma_{\tilde{I}}^2$ est la variance de I_w, $\mathrm{C}_1=(\mathrm{K}_1 L)^2, C_2 = (K_2 L)^2$ sont deux variables pour stabiliser la division avec un dénominateur faible, (L la plage dynamique des valeurs des pixels (est généralement de $2^{\#\,bits\,per\,pixel}$-1), K_1=0.01 et K_2=0.03 par défaut, $M\times N$ est la taille de l'image.

1.7.2 L'évaluation de la robustesse de la marque extraite

Les métriques suivantes peuvent être appliquées pour mesurer la fiabilité et la robustesse de la marque extraite contre les attaques.

Le taux d'erreur sur les bits (Bit Error Rate (BER))

La métrique du taux d'erreur sur les bits (BER) mesure le pourcentage de bits erronés de la marque extraite par rapport au nombre total de bits de la marque originale. Plus le

BER est faible, meilleure est l'efficacité du système de tatouage [56]. Le BER est défini par l'équation suivante :

$$BER(w, w') = \frac{1}{M \times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(w(i,j) \bigoplus w'(i,j)\right] \times 100 \tag{1.11}$$

Où $w(i,j)$ représente la valeur du pixel (i,j) dans la marque originale w, $w'(i,j)$ représente la valeur du pixel (i,j) dans l'image tatouée w' et $M \times N$ est la taille de la marque.

Le ratio de précision (Accuracy Ratio AR)

Le ratio de précision Accuracy Ratio (AR) peut également être utilisé pour évaluer la correspondance entre la marque originale insérée et la marque extraite. Il représente la relation entre les bits corrects et les bits totaux de la marque originale. Il peut être exprimé par l'équation suivante :

$$AR = \frac{CB}{NB} \tag{1.12}$$

Avec CB représente le nombre de bit corrects et NB est le nombre de bits totaux de la marque originale.

Le coefficient de normalisation (Normalization Coefficient NC))

Le coefficient de normalisation (Normalization Coefficient (NC)) mesure la similitude (ou la distance) entre la marque originale et la marque extraite. Les valeurs de NC sont dans l'intervalle $[-1, 1]$; si $NC = 1$, cela signifie que deux images sont absolument identiques, si $NC = 0$ cela signifie que deux images sont complètement différentes, si $NC = -1$ cela signifie que deux images sont complètement anti-similaires. NC est calculé selon l'équation 1.13.

$$NC(w, w') = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(w_{ij} - \mu_w) \times (w'_{ij} - \mu_{w'})}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(w_{ij} - \mu_w)^2}\sqrt{(\sum_{i=1}^{M}\sum_{j=1}^{N}(w'ij - \mu_{w'})^2}} \tag{1.13}$$

Où w_ij est le pixel (i,j) de la marque originale w, w'_ij est le pixel (i,j) de la marque extraite w', μ_w est la moyenne de la marque originale w et μ'_w est la moyenne de la marque extraite w'. $M \times N$ est la taille de la marque.

1.7.3 L'évaluation du taux d'insertion de la marque

Le taux d'insertion (ER), mesure le pourcentage des données insérées (bits de la marque ou coefficients de la marque) dans l'image hôte [171]. Un algorithme idéal présente d'excellentes performances s'il atteint une charge utile de la marque plus élevée, une imperceptibilité plus élevée et une plus grande robustesse. La charge utile d'insertion est calculée selon l'équation suivante :

$$ER = \frac{T}{M \times N} \tag{1.14}$$

Où T est le nombre total des bits secrets insérés et $M \times N$ est la taille de l'image hôte.

1.8 Les attaques en tatouage numérique

Afin de pouvoir estimer la robustesse, les performances et l'efficacité d'un schéma de tatouage, il est nécessaire de regarder les différentes attaques qui menacent les critères susmentionnés. Dans la littérature, plusieurs classifications des attaques de tatouage ont été proposées. Celles présentées par Cox et al [36] sont généralement les plus populaires. La Figure 1.10 montre un schéma de classification des attaques.

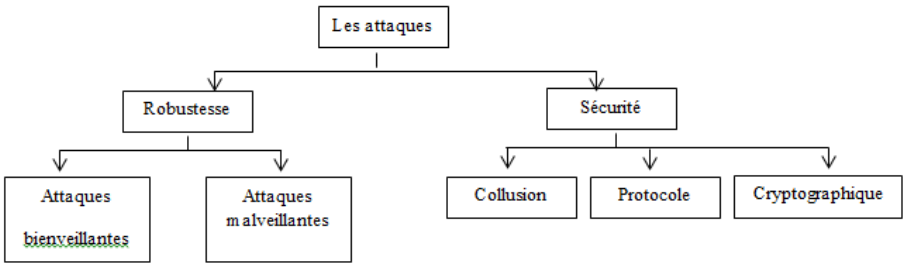


FIGURE 1.10 – Classification des attaques de tatouage [36]

1.8.1 Les attaques sur la robustesse

Il existe deux types d'attaques qui affectent la robustesse de l'algorithme de tatouage [36] : les attaques bienveillantes et les attaques malveillantes.

1.8.2 Les attaques malveillantes

Ce sont des manipulations destinées à supprimer, empêcher la détection de la marque ou rendre la marque inutilisable. Tous les attaquants peuvent utiliser consciemment toutes les attaques malveillantes pour atteindre leurs objectifs.
Les attaques impliquant le filtrage, la compression, l'ajout de bruit, la quantification sont appelées attaques simples [85]. Parmi les autres attaques de ce type les plus connues nous citons :

— **L'attaque de désynchronisation**
l'attaque de désynchronisation est généralement créée par les transformations géométriques. Ce type d'attaque rend impossible la détection et la récupération de la marque. Cette dernière reste dans l'image tatouée et attaquée.

— **L'attaque de la mosaïque [116]**
Dans cette attaque, il s'agit de découper l'image tatouée en plusieurs "imagettes" afin que chacune porte un fragment de la marque et ainsi, la détection et la récupération de la marque deviennent impossibles.

1.8.3 Les attaques bienveillantes

Les attaques bienveillantes regroupent les manipulations sur l'image tatouée dont le but est de permettre une meilleure exploitation de l'image et qui ne sont pas destinées à détruire la marque ou à empêcher sa détection. Ils s'agit d'opérations normales liées à l'utilisation ou à la diffusion de l'image marquée comme dans [166] :

— **La compression**
Pour stocker des images numériques ou les transmettre, il faut passer par la compression pour réduire la taille des fichiers images. Cette compression peut être fatale pour la marque puisque les deux algorithmes sont antagonistes [168] : l'objectif de la compression vise à réduire certaines composantes de l'image et à ne garder que celles nécessaires à sa compréhension. Si la marque est présente dans les hautes fréquences, elle sera alors détruite par l'opération de quantification propre à la compression avec perte. Ainsi, les marques doivent être insérées dans les régions de fréquence basse ou moyenne de l'image malgré le risque de distorsion.

— **Le filtrage**
Le filtrage est une opération nécessaire pour nettoyer une image bruitée et ainsi améliorer sa qualité. L'opération de lissage sur une image, visant à atténuer le bruit,

se fait par un filtre passe-bas qui permet d'atténuer les composantes hautes fréquences de l'image tatouée et donc de dégrader les composantes haute fréquence de la marque. L'utilisation d'un filtre passe-haut, dans le cadre d'attaques bienveillantes n'est pas nécessaire car il retient le bruit.

— **Les transformations géométriques**
Les transformations géométriques incluent le zoom, la réduction de la taille de l'image, la rotation, le recadrage. Elles provoquent une désynchronisation entre la marque dans l'image et le détecteur qui doit connaître la position exacte de la marque dans l'image.

— **L'ajout de bruit**
Le bruit peut être ajouté à une image marquée lorsqu'elle est transmise dans un canal bruité. L'effet de cet ajout avec des proportions importantes aura un effet masquant sur la marque et pourra donc gêner son extraction ou sa détection. Il existe deux types de bruit : le bruit gaussien, qui ajoute des valeurs générées de manière aléatoire à chaque pixel de l'image, et le bruit de sel et poivre, qui consiste à transformer au hasard des pixels de l'image en pixels noirs ou blancs.

1.8.4 Les attaques sur la sécurité

Parmi les attaques liées à la sécurité du tatouage, nous citons :

— **L'attaque de protocole**
Elle vise à rendre la marque inutilisable en mettant en doute son authenticité et non à la détruire. Elle entre en jeu lorsque le propriétaire de l'image originale marque son œuvre et la met en circulation. L'attaquant crée un faux original en soustrayant la marque du propriétaire de l'image tatouée et en marquant le faux original avec sa propre marque. Il peut ainsi usurper le droit du propriétaire légal de l'image en extrayant sa marque du faux original, en cas de litige entre le propriétaire légal et l'usurpateur [37].

— **L'attaque de collusion**
Elle consiste à construire, à partir de plusieurs versions de documents tatoués par des clés différentes, un document qui ne contient plus de signal de tatouage. Il existe deux grandes familles d'attaques de collusion [146] :

- Plusieurs attaquants peuvent collecter différentes images contenant le même tatouage. Le but est d'estimer la marque et de la supprimer après chaque image.
- Lorsque la même image est tatouée avec différentes marques, il suffit de les moyenner pour obtenir une estimation de l'image originale.

— **L'attaque cryptographique**
Elle utilise le principe de la cryptographie. Certaines de ces attaques visent à découvrir la clé secrète utilisée pour insérer la marque en essayant de manière exhaustive toutes les clés possibles (l'algorithme est public selon le principe de sécurité Kerchoff).

1.8.5 Bancs de tests

Il existe différents bancs de tests permettant de tester la résistance des schémas de tatouage. On citera :

— StirMark Benchmark [118]

— Checkmark

— Optimark

— Certimark

Pour tester la résistance des schémas de tatouage proposés, nous avons utilisé le banc de test StirMark [118] .

StirMark Benchmark

Stirmark Benchmark est un outil générique pour des tests de robustesse du tatouage d'image [117]. La première version de StirMark a été publiée en 1977, puis plusieurs versions ont suivi améliorant l'attaque originale en introduisant une liste de tests plus longue. Il consiste à combiner plusieurs attaques de type : rotation, fenêtrage, rehaussement du signal, changement d'échelle, découpages, transformations linéaires et des transformations géométriques. L'objectif de StirMark est de présenter un service public indépendant automatisé avec des profils d'évaluation étendus pour évaluer rapidement les bibliothèques de tatouage. StirMark. Benchmark 4.0 est disponible gratuitement en tant que code source binaire en C / C ++. Ce programme peut être facilement compilé en utilisant Microsoft Visual Studio Express.

1.9 Tatouage numérique et cryptographie

Dans le tatouage d'images médicales, des informations telles que le logo de l'hôpital, les informations du patient et la signature du médecin sont insérées dans l'image médicale pour le but de confidentialité, d'authentification et le diagnostic. Le tatouage numérique offre des avantages supplémentaires : le contrôle d'accès, l'évitement du détachement, la confidentialité, la non répudiation, l'indexation, l'économie de mémoire et de la bande passante [109]. Le tatouage numérique pourrait être polyvalent pour fournir une localisation de sabotage, une auto-récupération et une vérification de la propriété.

Malgré ses avantages, le tatouage numérique présente certaines faiblesses ; par exemple, il ne masque pas les informations ni de l'image elle-même ni de la marque [15].

Les approches de cryptographie protègent les données pendant la transmission. La personne qui a la clé secrète et l'algorithme peut décrypter les données dans un format utile. Mais après le décryptage, les données ne sont plus protégées et il est très difficile de vérifier leur intégrité et leur origine. Ce type de protection est appelé méthode de protection à priori. Les approches de tatouage sont venues comme une technique de protection complémentaire pour prouver l'intégrité, l'authenticité et l'origine, etc.
Après le décryptage des données, nous avons toujours la possibilité d'identifier si les données sont falsifiées ou si elles sont sous leur forme originale. Ce type de protection est appelé méthode de protection postérieure [19].

Les limites susmentionnées de la cryptographie et du tatouage montrent que chacune de ces approches prise individuellement ne suffit pas pour offrir un haut niveau de sécurité. Différentes approches ont été proposées pour tirer parti de la complémentarité entre mécanismes de cryptage et de tatouage. Leur objectif fondamental est d'assurer la confidentialité des données grâce au chiffrement, tout en ajoutant de nouvelles fonctionnalités de sécurité par le tatouage numérique.

Techniquement, selon la façon dont le tatouage et le chiffrement sont combinés, nous suggérons de distinguer cinq catégories principales de méthodes combinant le tatouage et le chiffrement [19] :

— Tatouage suivi du cryptage
— Cryptage suivi du tatouage
— Tatouage /décryptage conjoint
— Tatouage /cryptage conjoint
— Tatouage cryptage commutatif

Dans les sous-sections suivantes, nous présentons pour chacune des catégories le principe de fonctionnement ainsi que quelques exemples de méthodes.

1.9.1 Les techniques de tatouage suivi du cryptage

Cette méthode consiste simplement à insérer d'abord la marque dans les données originales et puis les données tatouées sont cryptée [86]. Côté récepteur, les données tatouées et cryptées sont décryptées, puis la marque est extraite. La marque insérée ne peut être extraite qu'après le décryptage. La principale application pour laquelle ces méthodes ont été proposées est la protection des droits d'auteur. La Figure 1.11 présente le processus du tatouage (insertion de la marque) suivi du cryptage côté expéditeur. La Figure 1.12 présente le processus du décryptage suivi du tatouage (extraction de la marque) côté récepteur.

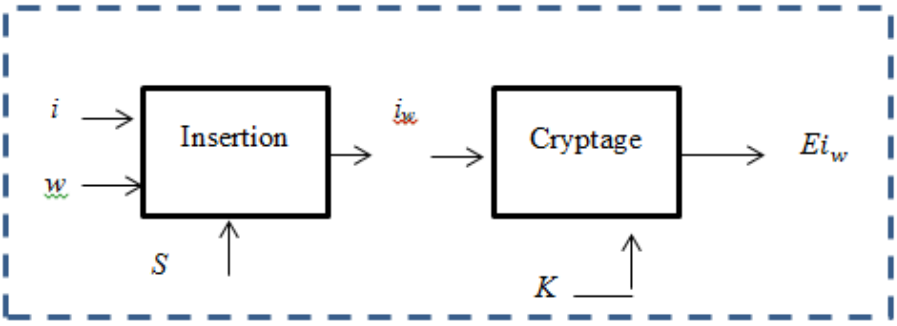


FIGURE 1.11 – Le processus de tatouage suivi du cryptage coté expéditeur

Avec i,w et S sont les données originales, i_w et k sont respectivement les données tatouées et la clé secrète de l'algorithme de cryptage et décryptage. Ei_w est la donnée tatouée cryptée et Di_w est la donnée tatouée décryptée.

1.9.2 Les techniques du cryptage suivi du tatouage

Dans cette approche, la marque cryptée est insérée dans les données originales cryptées. De l'autre côté, le décodeur doit extraire la marque cryptée et les données originales cryptées puis les décrypter. Dans la figure 1.13, nous expliquons la phase de cryptage–insertion

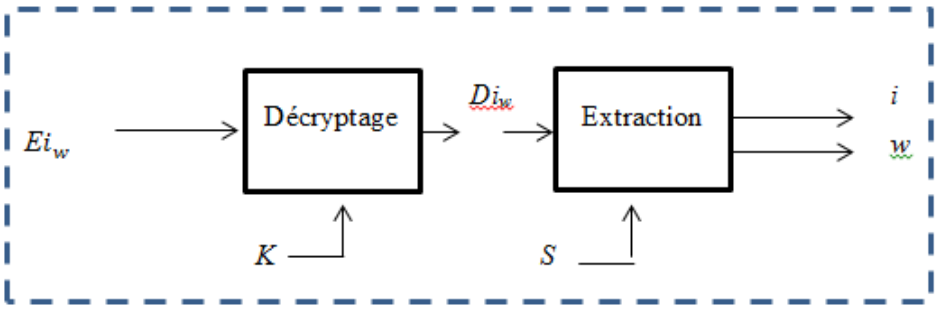


FIGURE 1.12 – Le processus de tatouage suivi du suivi du décryptage coté récepteur

du processus de cryptage suivi du tatouage . La figure 1.14 explique quant à elle la phase d'extraction-décryptage de ce processus.

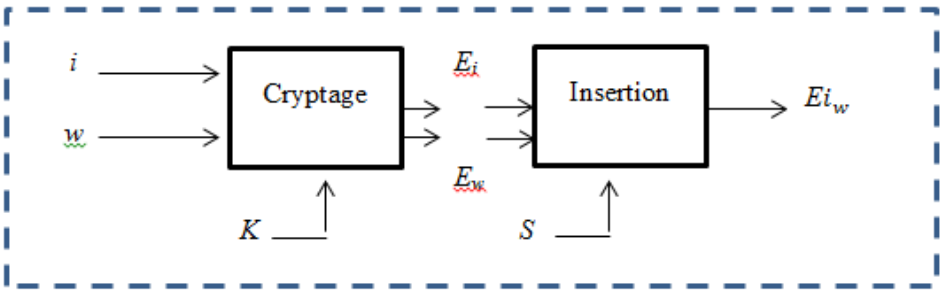


FIGURE 1.13 – Le processus du cryptage suivi du tatouage : phase de cryptage-insertion

Où E_i et E_w sont respectivement les données originales cryptées et les données cryptées tatouées.

1.9.3 Tatouage-décryptage conjoint

La méthode de tatouage-décryptage conjoint est considérée comme une méthode d'insertion sécurisée, où la technique du tatouage numérique est appliquée aux données décryptées côté récepteur. L'expéditeur crypte les données et les transmet via Internet, le

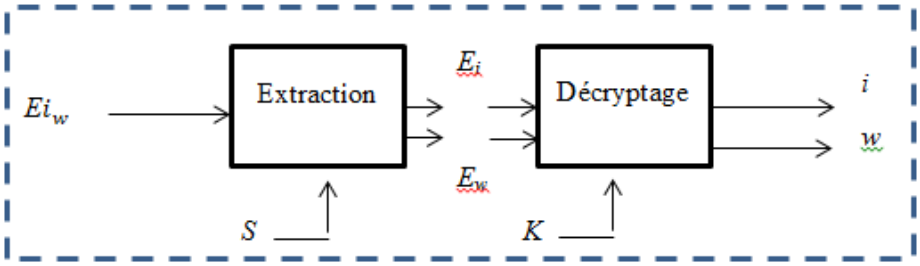


FIGURE 1.14 – Le processus du cryptage suivi du tatouage : phase d'extraction-décryptage

récepteur reçoit les données cryptées et les informations spécifiques uniques sur la clé déchiffrée (clé de déchiffrement spécifique au client (CPDK)). Le processus de décryptage et le processus de tatouage sont fait du côté récepteur, ce qui signifie que le résultat décrypté avec le CPDK spécifique du récepteur produit une copie de contenu personnalisée du récepteur.

La technique de tatouage-décryptage conjoint limite l'utilisation de la bande passante et réduit la complexité du processus d'extraction de la marque du côté du serveur (expéditeur). De plus, elle est utile pour le suivi médical, les empreintes digitales et les applications d'identité de propriété [25]. La figure 1.15 montre le diagramme général de la technique du tatouage décryptage conjoint.

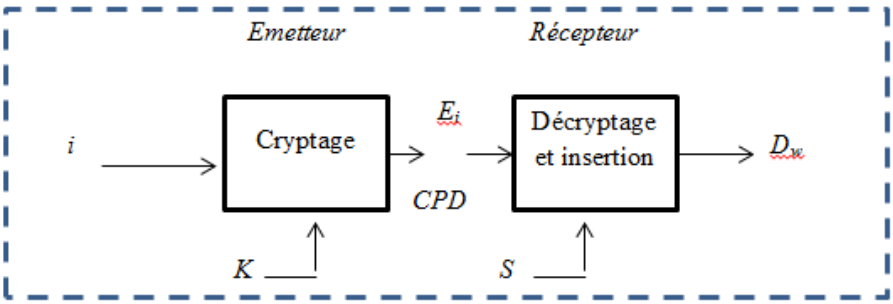


FIGURE 1.15 – Diagramme général de la technique de tatouage-décryptage conjoint

Où $CPDK$ est la clé unique spécifique de décryptage et D_w est la donnée décryptée tatouée.

1.9.4 Tatouage cryptage conjoint

Dans la méthode de tatouage cryptage conjoint, la marque est intégrée via le processus de cryptage, ce qui signifie la combinaison du tatouage et du cryptage ensemble côté expéditeur. Du côté du récépteur, la marque peut être extraite dans le domaine spatial après le décryptage, ou dans le domaine crypté à partir de l'image cryptée, ou bien dans tous les deux domaines [19].
Le schéma général de la technique de tatouage-cryptage- conjoint est illustré dans la figure 1.16.

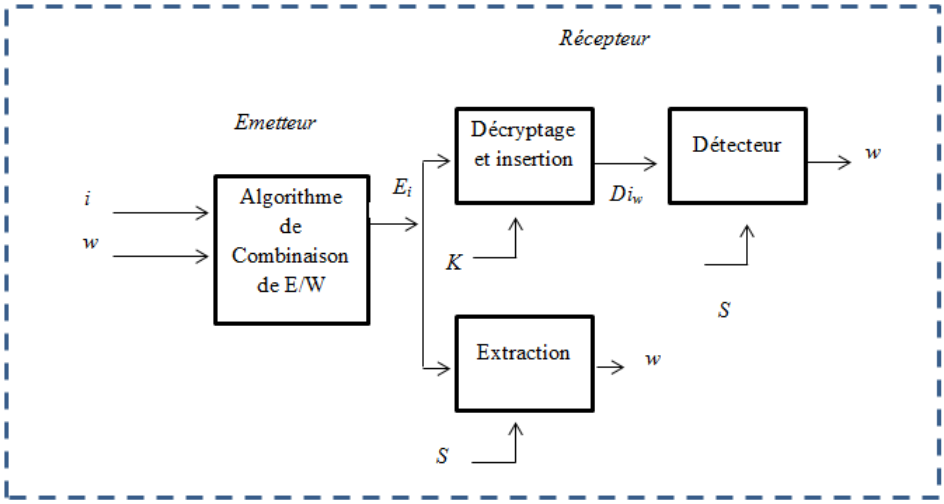


FIGURE 1.16 – Diagramme général de Tatouage-cryptage-conjoint

1.9.5 Les techniques de tatouage cryptage commutatif

Ces techniques sont souvent basées sur un cryptage partiel ou un cryptage invariant. Dans ce dernier cas, les données originales sont cryptées de sorte que certaines de ses fonctionnalités restent invariantes aux processus de cryptage et de décryptage. Ces fonctionnalités sont utilisées pour l'insertion de la marque.

1.10 Conclusion

Dans ce chapitre, nous avons présenté les notions de base d'un système de tatouage numérique, son schéma général, ses principales propriétés et sa classification, ses métriques d'évaluation, une classification de ses attaques. Finalement les méthodes combinant le tatouage numérique et la cryptographie ont été présentées. Ce chapitre nous a permis d'identifier les grandes lignes menant à la conception d'un système de tatouage numérique ainsi qu'un système combinant le tatouage numérique et la cryptographie et a révélé la diversité des techniques combinant le tatouage numérique et la cryptographie utilisées.
Le prochain chapitre sera dédié à un état de l'art sur le tatouage numérique des images médicales avec une étude plus détaillée sur les approches existantes de tatouage numérique.

Chapitre 2

Etat de l'art sur le tatouage numérique des images médicales

2.1 Introduction

La sécurité des informations médicales est aujourd'hui une nécessité, découlant des règles législatives. Ces règles donnent des droits au patient et des devoirs aux professionnels de la santé. Les soins de santé modernes aujourd'hui sont basés sur le partage des informations médicales dans des réseaux non sécurisés comme Internet accessible aux médecins ou spécialistes. L'image médicale est l'une de ces informations, elle est considérée comme un noyau principal dans le domaine de la télémédecine. Elle est utilisée pour l'analyse clinique et le diagnostic médical. Toute modification de l'image médicale volontairement ou pas affectera le diagnostic du spécialiste. Pour ces raisons, il est nécessaire de fournir des conditions de sécurité pour ces échanges afin de garantir l'intégrité et l'authenticité des images médicales lors de la transmission. Les techniques de tatouage numérique, font partie des solutions les plus importantes pour protéger l'image médicale.

Dans ce chapitre nous présentons en première partie les notions de base du traitement d'images médicales telles que : la définition des images médicales, ses quatre différents types les plus utilisés couramment par les médecins. Il s'agit de l'image issue de la radiographie, du scanner, de l'échographie et de l'imagerie par résonance magnétique. Nous présentons ses caractéristiques et ses différents formats de représentations. Nous décrivons par la suite les systèmes de gestion des images médicales, les zones Région d'intérêt (Region of interest (ROI)) et Région de non-intérêt (Region of Non Interest (RONI)) constituant une image médicale ainsi que les risques et les menaces liées à la sécurité des images médicales. Finalement, nous décrivons l'importance de la télémédecine.

La deuxième partie de ce chapitre est réservée à un état de l'art sur les techniques de tatouage numérique des images médicales, qui sont catégorisées en quatre groupes : les techniques de tatouage pour minimiser les distorsions, les techniques de tatouage

réversibles, les techniques de zéro-tatouage et les techniques de tatouage hybrides. Un bilan des techniques de tatouage est ensuite présenté à la fin de ce chapitre.

2.2 Les images médicales

L'imagerie médicale fait référence à tous les moyens physiques ou techniques que la médecine utilise pour visualiser les organismes du corps humains pour le but du diagnostic et du traitement d'un grand nombre de pathologies dans le cadre de la santé numérique [52]. L'image médicale permet de fournir une représentation visuelle d'informations ou de données de propriétés médicales perceptibles. Elles peuvent être interprétées structurellement (description de la structure (forme)) ou fonctionnellement (description de la fonction de l'organe). Dans un contexte plus large, l'imagerie médicale comprend tous les moyens et les techniques pour acquérir, stocker, traiter et interpréter des informations médicales sous forme d'images.

2.2.1 Les types des images médicales

Il existe quatre types d'imagerie médicale les plus couramment employées en médecine qui reposent sur l'utilisation des méthodes tomographiques basées soit sur les rayons X soit sur la résonance magnétique (IRM), les méthodes échographiques utilisant les ultrasons et la radioactivité.

La radiographie

Le principe de la radiologie est basé sur l'utilisation des rayons X, en enregistrant sur un film l'image projetée de transparence aux rayons X d'une région anatomique. La sortie est une impression sur un film photographique des différences de densité d'un organe. Le film sera plus ou moins noirci selon l'organe radiographié : les os apparaîtront blancs, les tissus mous seront dans différents tons de gris et l'air sera noir. La radiographie est souvent utilisée en orthopédie, en rhumatologie et en orthodontie pour étudier les traumatismes osseux, les déformations du squelette ou les implantations dentaires. Elle permet également d'observer des anomalies sur certains organes comme des infections bactériennes ou virales ou encore des tumeurs au niveau des poumons ou des seins (mammographie). La Figure 2.1 montre un exemple d'une image radiographique.

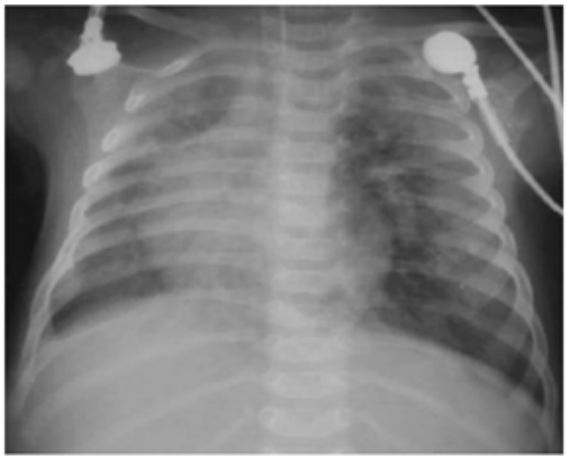


FIGURE 2.1 – Image radiographique

L'échographie

L'échographie est dérivée du principe du sonar. Les images résultent de l'émission et la réflexion des ultrasons sur les organes pleins de l'abdomen, le cœur et tous les organes non masqués par le squelette (globe oculaire, cerveau chez le nouveau-né) ou par les gaz. L'échographie peut être utilisée pour observer la fonction des organes comme évaluer la vitalité et la forme du fœtus pendant la grossesse. La Figure 2.2 montre un exemple d'images échographiques.

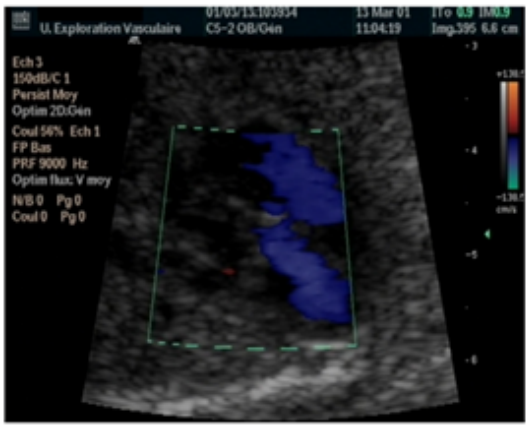


FIGURE 2.2 – Image échographique

Scanner

Le scanner repose également sur l'utilisation des rayons X mais permet d'obtenir des images tridimensionnelles des organes ou des tissus (os, muscles ou vaisseaux) sous forme de coupes. A l'aide de scanner on visualise une modification de volume ou une anomalie de structure (infections, hémorragies, tumeur, ganglions, embolie). En cancérologie, il permet de suivre la réponse à la chimiothérapie. Il peut également être utilisé pour guider les drainages et les biopsies. La Figure 2.3 montre un exemple d'une image scanner.

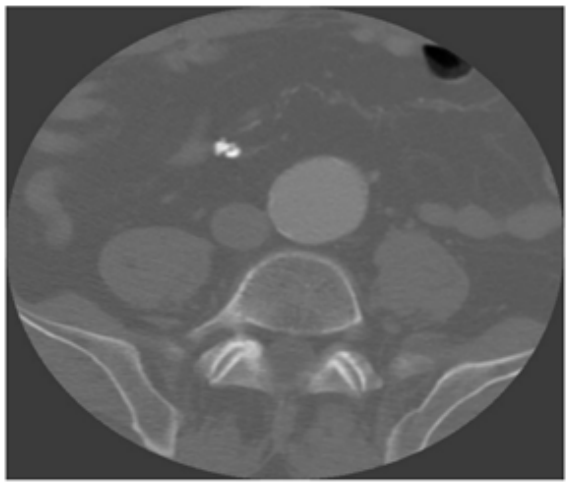


FIGURE 2.3 – Image scanner

Imagerie par résonance magnétique (IRM)

L'imagerie par résonance magnétique (I.R.M.) est basée sur le phénomène de résonance magnétique nucléaire (R.M.N.). En visualisant différentes structures. Par résonance magnétique, on peut obtenir des images en coupe et des représentations tridimensionnelles dans tous les plans spatiaux en visualisant différentes structures ; en particulier en neuro-imagerie (cerveau, moelle épinière) et les tissus mous (viscères, muscles et tendons). Le dispositif permet également d'exclure les procédures de diagnostic d'arthroscopie, au cours desquelles des incisions sont pratiquées pour visualiser un dysfonctionnement articulaire. La Figure 2.4 montre un exemple d'une image IRM du cerveau.

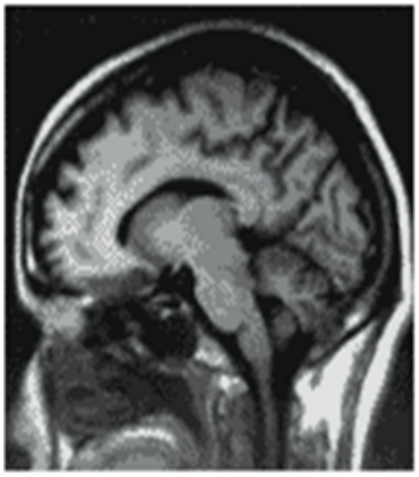


FIGURE 2.4 – Image IRM

2.2.2 Les formats de représentation des images médicales

Les images médicales peuvent être représentées par les formats de fichiers majeurs standardisés les plus utilisées sur le marché : Best Management Practice (BMP), Graphics Interchange Format (GIF), Joint Photographic Experts Group. (JPEG), Portable Network Graphics (PNG), Tagged Image File Format (TIFF) et DCM.

Le format BMP

Le format BMP est l'un des formats les plus simples. Un fichier BMP est un fichier bitmap, c'est-à-dire un fichier d'images graphiques stockant les pixels sous forme de tableau de points et gérant les couleurs soit en couleurs vraies, soit grâce à une palette indexée. Le format BMP a été conçu de telle manière qu'on obtienne un bitmap indépendant du périphérique d'affichage (Device Independent Bitmap (DIB)).

Le format GIF

Le format GIF est le plus couramment utilisé sur le Web, il est limité à 256 couleurs, donc il ne convient pas aux photos très colorées où il y a beaucoup de nuances, d'autre part pour insérer des logos, des icônes et même une banderole, le rapport qualité / taille est imbattable. C'est un format Compuserve utilisant la technologie de compression (Lempel-Ziv-Welch). C'est un format standard pour les images médicales à haute définition (par

exemple, lésions cliniques, pathologie anatomique). Le format GIF ne peut être utilisé qu'en mode couleur indexées, non pas RVB.

Le format JPG ou JPEG

Le format JPEG est le format le plus particulièrement utilisé pour les photos scannées contenant plusieurs couleurs. En fait, en jouant sur la qualité de l'image, JPEG réduit sa taille. Il ne gère pas la transparence comme le GIF, mais il dépasse jusqu'à 256 couleurs. La technologie de compression utilisée est plus destructrice que le GIF. Le taux de compression d'image peut varier de 1 à 99%. C'est un format utilisé pour les images à moyenne ou basse définition (par exemple, les champs chirurgicaux/opératoires).

Le format TIFF

Le format TIFF est un format graphique plus ancien qui permet de stocker des images bitmap de grande taille (plus de 4 Go après compression) sans perte. Le format TIFF permet de stocker des images en noir et blanc (niveaux de gris), des images en couleur (jusqu'à 32 bits par pixel) et des images indexées. De plus, le format TIFF permet l'utilisation de plusieurs espaces de couleurs. Ce format a été créé à l'origine pour l'échange entre différents systèmes d'exploitation. Ce format se trouve généralement dans le programme d'acquisition du scanner à plat.

Le format PNG

Le format PNG permet de stocker des images en niveaux de gris (la profondeur de codage par pixel va jusqu'à 16 bits), en couleurs réelles (la profondeur de codage par pixel est jusqu'à 48 bits), ainsi que des images indexées, faisant usage d'une palette de 256 couleurs.

Le format DICOM

Les images médicales sont enregistrées sous un format de stockage et d'échange appelé Digital Imaging Communication in Medicine (DICOM) qui contient, outre l'image elle-même, des métadonnées la caractérisant (identité du patient, date et heure d'acquisition, type d'appareil, paramètres d'acquisition détaillés, etc.). L'objectif principal du standard DICOM est de faciliter les transferts d'images accompagnées de leurs dossiers médicaux entre les machines de différents constructeurs. En effet, avant la généralisation

de ce format, chaque constructeur de matériel d'imagerie utilisait un format de données propriétaire, entrainant d'importants problèmes de gestion et de maintenance (incompatibilités, coût, perte d'information) dans les établissements de santé. La structure basique d'un fichier DICOM est illustrée dans la Figure 2.5. Généralement un fichier DICOM

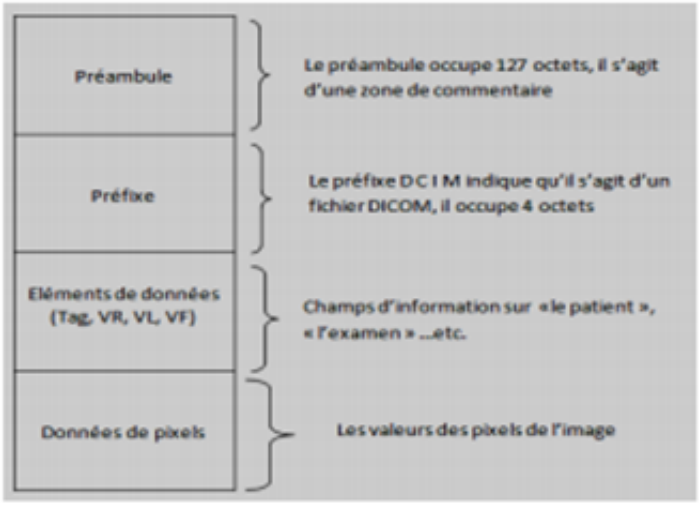


FIGURE 2.5 – Structure du fichier DICOM

se compose de deux parties les informations de l'en-tête et celles des pixels de l'image. L'organisation de l'information contenue dans les fichiers DICOM est sous une forme séquentielle. Chaque information élémentaire est constituée de 4 champs de données (Tag, Étiquette, Value Representation (VR), Value Length (VL), Value Field (VF) [160]. Un aperçu d'un exemple d'entête d'un fichier DICOM est donné par la Figure 2.6.

2.2.3 Les caractéristiques des images médicales

Les phénomènes physiques impliqués dans l'acquisition d'images médicales ont des particularités propres à chaque mode, et peuvent s'exprimer sous les formes suivantes au niveau de l'image : la taille de l'image, la résolution, le bruit, le contraste etc.

— **La taille des images**
En imagerie médicale, la taille de l'image dépend généralement du capteur rentrant dans l'acquisition et de la zone anatomique à imager. Par exemple, En IRM, le format d'image change plus que tout autre type d'image avec des formats matriciels

Etiquette	Description	VR	VL (Octets)	VF
0002,0000	Group Length	UL	4	204
0002,0010	Transfer Syntax UID	UI	20	1.2.840.10008.1.2.1
0002,0012	Implementation Class UID	UI	20	1.3.12.2.1107.5.8.2
0008,0020	Study Date	DA	8	20160117
0008,0030	Study Time	TM	14	092406.897000
0008,0060	Modality	CS	2	CT
0008,1010	Station Name	SH	8	somaris4
0009,0010	Private Creator	LO	14	SPI RELEASE 1
0010,0010	Patient's Name	PN	26	XXXX YYYYY
0010,0020	Patient ID	LO	6	242/07
0018,0090	Data Collection Diameter	DS	6	000500
0019,0015	Private Creator	LO	20	SIEMENS CM VA0 ACQU
0020,0010	Study ID	SH	6	000001
0028,0100	Bits Allocated	US	2	16
7FE0,0010	Pixel Data	OW	524288	0000 0034 0424 0000 004A 0000 0000 048C 043C 0548 046C 05D3 ...

FIGURE 2.6 – Aperçu de l'entête d'un fichier DICOM

carrés et non carrés (par exemple 64×64, 64×128, 128×128, 128×192, 256×512, 512×512, 512×1024, ...).

— **La résolution spatiale**

La résolution d'image fait référence au nombre de pixels par pouce qui détermine la qualité de l'image. C'est ce qu'on appelle les points par pouce (dpi (dots per inch)). Dans la plupart des cas, plus la résolution est élevée plus la qualité d'image est meilleure et plus la représentation des détails contenus dans l'image est clairs. La résolution d'image peut toujours être réduite. En augmentant la résolution on n'améliorera pas la qualité de l'image.

Si le système d'imagerie peut afficher des objets de plus en plus petits dans l'image, il a une plus grande résolution spatiale. Selon chaque type d'image, un ou plusieurs facteurs entraîneront la limitation de la résolution spatiale. Par exemple, prenons le cas des images radiographiques, la limitation de la résolution spatiale est liée aux caractéristiques physiques du capteur. La plus grande longueur d'onde des rayons X est d'environ un dix milliardième de mètre. Cependant, le capteur ne peut pas représenter toutes ces informations.

— **Le contraste**

C'est l'opposition évidente entre deux zones de l'image, c'est à dire c'est la différence entre les niveaux de gris de l'image, plus précisément entre les zones claires et le zones sombres de l'image. Une image en niveau de gris uniforme n'a pas de contraste.

— **Le bruit dans les images médicales**
Le bruit est considéré comme un phénomène aléatoire qui peut être ajouté à l'image originale de telle sorte qu'il provoque la distorsion de l'intensité des pixels, de sorte que le signal d'image est déformé localement. Les causes de bruits sont diverses en citant par exemple :

- Le mal fonctionnement d'un capteur utilisé (optique, électronique)
- La qualité d'échantillonnage (mouvement de caméra ou de scène).
- Les interférences atmosphériques etc.

En général, les principales sources de bruit sont divisées en deux catégories : le bruit anatomique et le bruit d'acquisition.

— **La couleur**
La fonction de couleur traite le degré de sensibilité de chaque espace colorimétrique de l'image originale aux yeux humains. L'importance de la fonction de couleur pour la perception visuelle humaine est due à la structure biologique de la rétine humaine. La couleur fait référence à la capacité des objets à réfléchir des ondes électromagnétiques de différentes longueurs d'onde. L'œil humain peut détecter les couleurs en tant que combinaison des couleurs primaires (rouge, vert et bleu). La longueur d'onde du rouge est de 700 nm (nano-mètres), pour le vert est 546,1 nm, et pour le bleu est 435,8 nm. Nous pouvons trouver des images médicales en niveaux de gris et des images médicales couleurs [129].

- Les images médicales au niveaux de gris : sont représentées par des pixels qui peuvent prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Les valeurs de pixels peuvent être comprises par exemple entre 0 et 255. Chaque pixel est donc représenté par un octet.
- Les images médicales couleur : les applications médicales utilisent parfois des images en couleur. La représentation des couleurs s'effectue de la même manière que les images monochromes avec cependant quelques particularités. En effet, il faut tout d'abord choisir un modèle de représentation. On peut représenter les couleurs à l'aide de leurs composantes primaires RVB (Rouge Vert Bleu) (Red Green Bleu (RGB) en anglais). La Figure 2.7 montre un exemple de représentation d'une image médicale au niveau de gris et une image médicale en couleur.

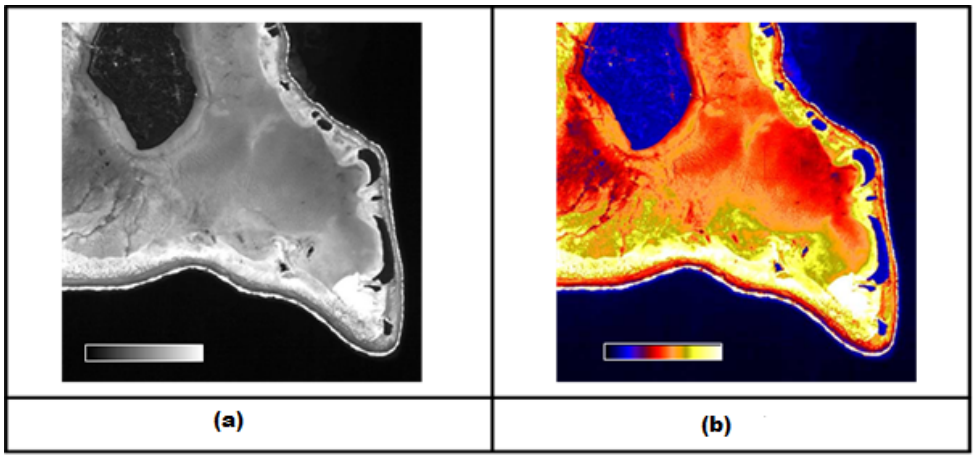


FIGURE 2.7 – Exemple de représentation d'une image médicale en niveau de gris (a) et en couleur (b).

— **La luminance**
C'est le degré de luminosité de chaque point de l'image. Également défini comme le quotient de l'intensité lumineuse d'une surface par rapport à l'aire apparente de cette surface. Pour la perception visuelle du spectateur à distance, le terme luminosité est remplacé par le mot brillance, qui correspond à l'éclat d'un objet.
Une sorte d'ensemble de caractéristiques de bonne luminosité est :

— Des images brillantes

— Un bon contraste

— Pas de parasites

À partir de ces caractéristiques des images médicales qui peuvent être regroupées en termes de contraste, de bruit, de résolution, de couleur etc., des normes et des directives liées à l'affichage, au stockage, au partage et au diagnostic peuvent être dérivées. En effet, des systèmes informatiques dédiés à la technologie médicale sont nécessaires au traitement de ces données. Ce sera le sujet des paragraphes suivants.

2.3 Les systèmes de gestion des images médicales

Le traitement, l'analyse et la gestion doivent également être pris en considération. En particulier, les images médicales sont partagées entre différentes applications liées à la prise en charge des patients à l'hôpital ou dans d'autres services de santé. En fait, les hôpitaux modernes utilisent des équipements de diagnostic et des systèmes d'information

automatisés (SI). Ces systèmes sont situés dans diverses parties du bâtiment de l'hôpital. Cependant, ils travaillent ensemble pour fournir de nombreuses fonctions, telles que la facturation, l'imagerie, les médicaments, la gestion et le diagnostic.
Dans cette section, nous présenterons les différentes catégories de systèmes d'information médicaux ainsi que les 2 systèmes d'information médicaux les plus utilisés.

2.3.1 Les systèmes d'informations médicaux : fonction et catégories

La fonction d'un système d'information médical est de fournir des installations pour le stockage, la récupération, la transmission et l'évaluation des informations. En médecine, il existe différentes catégories de systèmes d'information : les systèmes pour les médecins généralistes et les spécialistes (cardiologues, ophtalmologistes, dentistes, etc.), les systèmes pour les unités hospitalières tels que radiologie, exploration fonctionnelle, laboratoire et les systèmes d'information hospitaliers. Parmi les systèmes d'informations médicaux, nous donnons une brève description de deux systèmes les plus utilisés : le système d'archivage et de communication PACS et le système d'information hospitalier Hospital Information System (HIS).

2.3.2 Le système d'archivage et de communication (PACS)

PACS est l'acronyme de "Picture Archiving and Communication System". Il s'agit d'un ensemble d'équipements informatiques reliés en réseau qui peuvent être utilisés pour l'acquisition, l'archivage, l'impression, la consultation et l'interprétation des images radiologiques, de plus il est relié à un système informatique de radiologie ou d'hôpital (Radiology Information System (RIS) ou HIS) pour l'identification du patient et la présentation des informations cliniques pertinentes [72]. La Figure 2.8 montre l'architecture d'un système PACS. Un PACS se compose de quatre composants principaux : les modalités d'imagerie telles que la Computed Tomography (CT), l'IRM et les ultrasons etc., un réseau sécurisé pour la transmission des informations concernant les patients, des postes de travail pour l'interprétation des images et des archives pour le stockage et la récupération des images et des rapports médicaux. L'objectif principal de PACS était de mieux gérer les services de radiologie et de donner l'accès aux images aux services cliniques demandeurs pour le diagnostic, la consultation et l'édition des rapports. Comme le montre la Figure 2.8, les modalités envoient les données à un poste de travail d'assurance qualité (Assurance

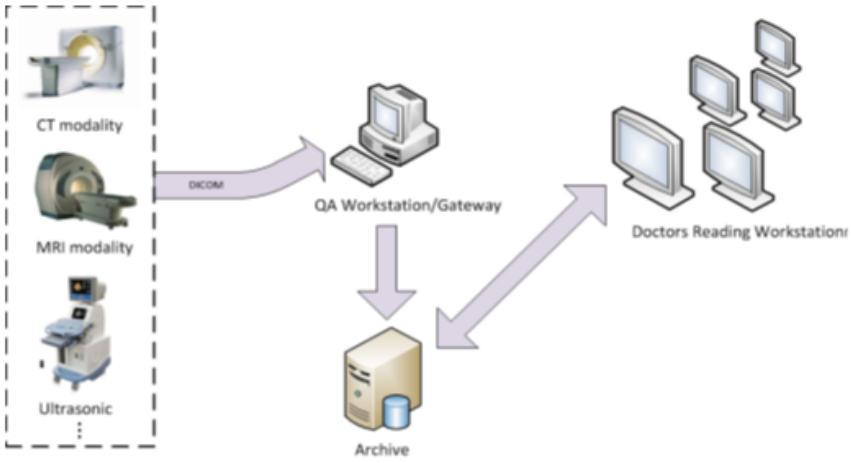


FIGURE 2.8 – L'architecture d'un système PACS [72]

Quality (AQ)), parfois appelé passerelle PACS. Le poste de travail AQ est un point de contrôle pour s'assurer que les données démographiques des patients sont correctes ainsi que d'autres attributs importants d'une étude donnée.
Si les informations de l'étude sont correctes, les images sont transmises au système d'archivage pour rangement. Le dispositif de stockage central (archives) stocke les images et dans certains cas, les rapports, d'autres mesures et informations attachées aux images. La prochaine composante du flux de travail PACS est la lecture des postes de travail. Le poste de lecture est l'endroit où le radiologue examine l'étude du patient et formule son diagnostic. Normalement lié au poste de travail de lecture, il se trouve un ensemble de rapports qui aide le radiologue à faire le rapport final. En plus du flux de travail mentionné, il existe normalement un logiciel de création de CD / DVD utilisé pour la distribution des données aux patients ou aux médecins traitants.

2.3.3 Le système d'information hospitalier (SIH)

Un Système d'Information Hospitalier (SIH), (Hospital Information System HIS), est un système d'information complet et intégré conçu pour gérer les aspects administratifs, financiers et cliniques d'un hôpital. Ce système comprend le traitement d'information sur papier ainsi que les machines de traitement des données [72]. Il peut être composé de composantes logicielles distinctes avec des extensions spécifiques ainsi que d'une grande variété

de sous-systèmes dans les spécialités médicales (par exemple, le Système d'Information de Laboratoire (Laboratory Information System (LIS)) et le Système d'Information de Radiologie (Radiology Information System (RIS)).

2.4 La télémédecine

Parallèlement aux progrès des technologies informatiques, de communication et d'imagerie, il y a eu une augmentation de l'utilisation des applications de la télémédecine basée sur l'échange d'informations médicales (données, voix et images fixes ou vidéo) utilisant des équipements de télécommunication. Elle a déjà été utilisée avec succès dans un certain nombre de domaines de la médecine. La télémédecine permet à un médecin ou à un spécialiste d'un site de dispenser des soins de santé, de diagnostiquer des patients, de fournir une assistance préopératoire, de fournir une thérapie ou de consulter un autre médecin ou du personnel paramédical dans des sites éloignés. Ainsi, l'objectif de la télémédecine est de fournir des soins de santé spécialisés à des sites distants en sous-effectif et de fournir des soins d'urgence avancés grâce aux technologies modernes de télécommunication et d'information [23]. En télémédecine, où un médecin peut ne pas être en mesure de rencontrer un patient face à face, il est important que le médecin obtienne des images vidéo de qualité suffisamment élevée du patient pour poser un diagnostic correct [107]. En télémédecine, la qualité perceptuelle de l'image reçue est importante [23]. Cependant, le volume de données à transférer, à stocker et à manipuler étant si énorme (par exemple, l'imagerie du corps entier par exemple), certains traitements peuvent être appliqués à condition que la modification apportée n'affecte pas le résultat du diagnostic. La compression d'image sans perte [107] est un exemple d'un tel traitement conduisant à des exigences de bande passante de transmission moins exigeantes. Les progrès de la compression des données médicales réalisés dans les systèmes d'imagerie, les systèmes de stockage et la télémédecine rendent la compression dans ce domaine particulièrement intéressante. Cependant, cette compression doit être adaptée aux spécificités des données biomédicales qui contiennent des informations de diagnostic.

2.5 La région d'intérêt (ROI) et la région de non intérêt (RONI) dans les images médicales

La plupart des images médicales se composent de deux parties appelées la Région d'Intérêt (Region of Interest (ROI)) et la Région de Non-Intérêt (Region of Non-interest (RONI)). La ROI contient les informations importantes que les médecins utilisent pour le diagnostic. C'est aussi la région dont l'intégrité doit être strictement contrôlée. La modification d'un pixel, même unique, dans la ROI de l'image médicale peut, dans certains cas, affecter les informations globales contenues dans l'image, et peut donc influencer le diagnostic et par conséquent, menacer la santé ou même la vie du patient. D'autre part, la partie RONI de l'image ne contribue pas au diagnostic, elle peut être utilisée pour l'insertion de la marque. Il existe deux types de séparation de la ROI de la RONI.

Le premier type de séparation est basé sur le fait que la RONI est la partie du fond noir de l'image qui contient seulement les pixels noirs. Tout le reste c'est la partie ROI qui est la partie diagnostic ou appelée aussi la partie anatomique de l'image.

Tandis que dans le deuxième type de séparation, la zone ROI est généralement marquée par un médecin ou un radiologue de manière interactive et se présente sous n'importe quelle forme irrégulière.
En fonction de l'image, elle peut être définie par un polygone dessiné ou un outil de sélection assisté par ordinateur. Le reste de l'image est la partie RONI. Elle peut contenir non seulement des pixels noirs mais aussi des pixels aux niveaux de gris. La Figure 2.9 montre un exemple de premier type de séparation de la partie ROI (la partie diagnostic) et RONI (la partie de fond noir) d'une image médicale. Les Figures 2.10 et 2.11 montrent le deuxième type de séparation de ROI et RONI d'une image médicale. La partie ROI est sélectionnée par un polygone rouge.

Dans certains cas de tatouage numérique, la séparation de l'image originale en deux zones : la zone ROI et la zone RONI est nécessaire. Plusieurs méthodes de séparation de ROI et RONI sont proposées dans la littérature. Ces méthodes peuvent être soit d'une manière automatique [126] ou par un spécialiste ou un médecin [78]. Du côté récepteur, la technique de séparation doit être réversible pour que le receveur récupère la même sortie de séparation de l'image tatouée sous l'hypothèse que l'image n'a pas été modifiée. Ales Rocek et al [132] ont utilisé dans leur approche de tatouage numérique une méthode de recherche de la zone RONI d'une manière automatique. La méthode de détection est basée sur la comparaison de paires de vecteurs voisins. Les vecteurs contiennent des valeurs de

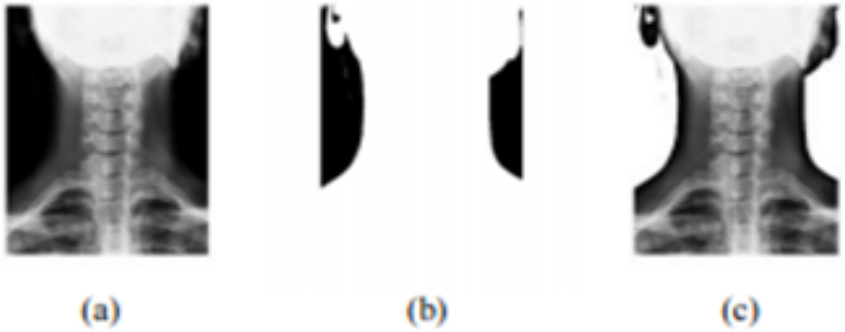


FIGURE 2.9 – Exemple illustratif de RONI (Region de non intérêt) et ROI (Région d'intérêt) dans une image radiographique. (a) image d'une colonne cervicale (1510 × 1191 pixels) ; (b) image du Fond noir (RONI), (c) l'objet anatomique (ROI) [113].

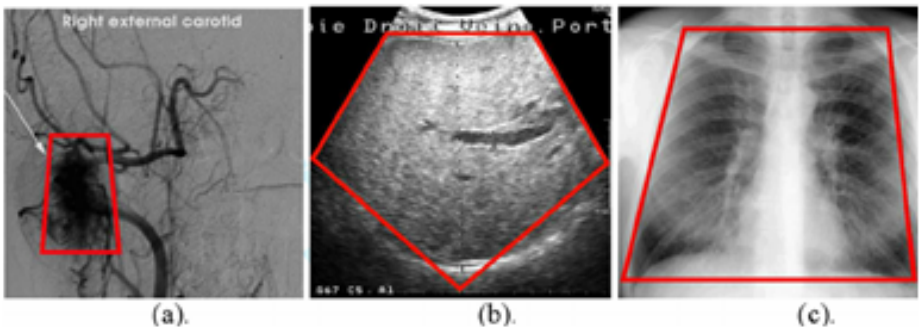


FIGURE 2.10 – Sélection de la zone ROI des images médicales. (a) une image IRM. b) une image échographique, (c) une image radiographique [54].

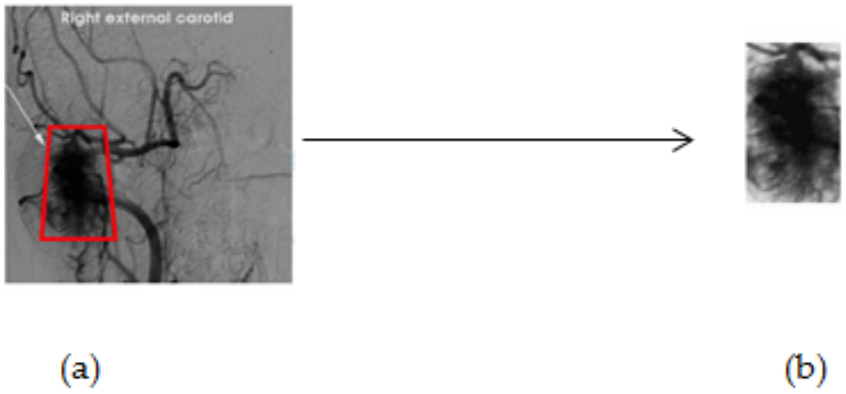


FIGURE 2.11 – (a) l'image originale, (b) la zone ROI [54]

pixels des lignes et des colonnes. La comparaison est faite dans chaque direction - du haut, du bas, de la droite et de la gauche - des bords au centre de l'image. Le long de chaque vecteur, la frontière entre ROI et RONI est l'endroit sur le vecteur qui diffère du point précédent de plus que le seuil spécifié. Des informations détaillées se trouvent dans l'article [132]. Une détermination plus précise de RONI en tenant compte des contours des objets peut être utilisée, comme dans [90]. Ritu Agrawal et al [140] ont utilisé une technique de séparation de ROI et RONI pour détecter les tumeurs à partir d'images cérébrales IRM et CT. Pour trouver la zone ROI à partir de l'image originale une méthode de segmentation c-means floue est appliquée. Dans certains travaux, la ROI est prise comme une forme de carré [45], [169], [79], qui couvre la moitié du total de la zone d'image comme dans [150]. Par exemple dans les images de taille 512×512 pixels, un carré de taille 256×256 a été pris qui couvre presque toute la zone ROI. Un schéma développé par Fotopoulos et al [45] et Jasni et al [169] utilise aussi un rectangle pour définir la ROI de l'image médicale. Dans Siau-Chuin Liew et al [79], quatre rectangles sont utilisés pour former une pyramide pour la ROI. Cette méthode permet à la ROI d'être définie avec plus de précision en raison de caractéristiques de l'image de l'échographie et d'avoir plus d'espace pour la RONI.

2.6 Risques et menaces liés à l'image médicale

Lors de l'échange, du partage ou même du stockage des images médicales et de données de patients, celles-ci peuvent être soumises à de multiples menaces ou risques. Dans cette

section, nous donnons une idée sur ces risques pour montrer d'une part l'importance de la protéger et permettre une meilleure compréhension des mécanismes de déploiement permettant d'atteindre un niveau de sécurité élevé que nous discutons dans les chapitres suivants.

Ces risques peuvent être divisés en trois catégories : les accidents, les erreurs, les malveillances [42][11], et séparables suivant la nature des menaces (physique, technique, environnementale, humaine,...) [26]. Ces risques affectent quatre attributs de sécurité indépendamment ou conjointement tels que l'intégrité, la confidentialité et la disponibilité que nous avons détaillé au chapitre 1.

— **Les accidents**

Ce sont les problèmes liés à l'environnement du système d'information (SI) ou à son fonctionnement normal qui entrent dans cette catégorie. Il peut s'agir :

- Du dysfonctionnement du matériel, des logiciels, de l'environnement technologique (coupure de courant, perte du réseau, support mémoire défaillant, etc).
- De la destruction partielle ou totale du matériel, des logiciels (catastrophes naturelles : tremblement de terre [8], risques physiques : feu, etc).
- De la négligence ou la défaillance/absence des personnels techniques chargés de la manipulation ou de la maintenance du système, etc.

Quoique nous fassions, ces risques existeront toujours et nous ne pouvons que tenter d'en limiter les conséquences.

— **Les erreurs**

Les sources d'erreur les plus courantes au niveau d'un Système d'Information (SI) sont les suivantes :

- Les erreurs de saisie.
- Les erreurs dans la transmission des informations par le SI.
- Les erreurs de manipulation des fonctions d'exploitation du SI.
- Les erreurs résultant de la mauvaise utilisation du SI.

Ces erreurs constituent un vaste domaine où la responsabilité des utilisateurs et des intervenants est importante mais où les erreurs de conception des logiciels et des systèmes jouent un rôle important.

— **Les malveillances**
Si des erreurs s'avèrent à risque, elles ne sont pas à des fins malveillantes. Une fois que les facteurs humains apparaissent, il est difficile d'évaluer leur portée. De plus, trouver des exemples est particulièrement difficile. La malveillance peut être utilisée pour extorsion ou gain économique. Les altérations malveillantes peuvent aller de la suppression de preuves d'ordonnances ou d'erreurs de diagnostic jusqu'à l'engagement de la responsabilité d'un tiers.
Par conséquent, elles peuvent être le résultat des destructions physiques directes, complète ou partielle des fichiers et des logiciels ou de leurs sauvegardes, ou le résultat de détournements indirects (virus, bombes logiques), voire de vol d'identité ou d'intrusion d'un tiers permettant d'accéder au fonctionnement du système informatique.

Les différents risques auxquels sont confrontés les informations médicales et les systèmes d'information SI doivent être déterminés pour définir les objectifs de sécurité.

Dans la section suivante, une liste des travaux existants sur le tatouage numérique des images médicales sera analysée. Cette enquête vise à comprendre et souligner les avantages et les limites des techniques de tatouage numérique existantes concernant l'intégrité et l'authenticité des images médicales.

2.7 Les méthodes existantes de tatouage numérique des images médicales

Il existe quatre méthodes de tatouage d'images médicales : les méthodes classiques, les méthodes de tatouage des régions d'intérêt (ROI) et des régions de non-intérêt (RONI), les méthodes de tatouage réversibles, les méthodes de zéro-tatouage et les méthodes de tatouage hybrides. Dans les sections suivantes, les approches de tatouage, leurs utilisations et leurs résultats sont présentés. À la fin de cette section, un bilan sur les approches de tatouage numériques existantes est fait pour examiner et synthétiser la spécificité de chaque approche.

2.7.1 Les méthodes classiques

Dans les méthodes conventionnelles de tatouage, la marque est insérée dans toute l'image originale en remplaçant certains détails comme LSB. Lors de la mise en œuvre

d'un schéma de tatouage numérique pour une image médicale, les images ne doivent pas être modifiées de façon perceptuelle car aucun médecin n'acceptera d'utiliser l'image dégradée pour prendre une décision, quelle que soit la taille d'altération. D'où l'algorithme de tatouage de préférence doit être réversible [44].

2.7.2 Les méthodes de tatouage des régions d'intérêt (ROI) et des régions de non-intérêt (RONI)

Les images médicales pouvaient être divisées en deux régions ROI et RONI. La région ROI comprend la région informative qui est utilisée pour le diagnostic et doit être stockée sans aucune distorsion. Cependant, la région RONI est la région qui ne contient pas des informations importantes pour le diagnostic, elle représente généralement le fond noir de l'image, mais parfois elle peut contenir des parties grises présentant un léger intérêt [141].

Dans le tatouage dans la région ROI, des techniques du domaine spatial ou fréquentiel sont utilisées pour masquer la marque. La marque codée peut être robuste ou fragile suivant l'objectif et l'application. Ces marques sont mises en œuvre d'une manière particulière sans impact sur la qualité visuelle de l'image [34], [93] . L'utilisation de la région ROI pour intégrer la marque peut déformer les pixels par conséquent entraîner le mauvais diagnostic [34]. D'autre part, le tatouage dans la région RONI insère les marques dans des zones sans importance pour conserver le diagnostic, mais ils ont plusieurs inconvénients tels qu'ils peuvent être mis en œuvre que si RONI existe dans l'image, la quantité d'informations à être intégrée dépend de la taille de la zone RONI et la partie ROI peut ne pas être protégée contre les attaques malveillantes.

Memon et al. [93] ont proposé une technique de tatouage fragile pour assurer l'intégrité de l'image médicale radiologique. Cette technique évite la distorsion de la région ROI de l'image en intégrant les informations de la marque dans la région RONI de l'image. La marque est composée par des informations sur le patient, du logo de l'hôpital et d'un code d'authentification calculé à l'aide d'une fonction de hachage. Un cryptage de la marque est effectué pour assurer l'inaccessibilité des données aux adversaires. Une technique de séparation automatique de ROI et RONI a été appliquée par l'utilisation d'un carré ou une ellipse. Ensuite, un brouillage des pixels dans la zone RONI à l'aide d'une clé a été appliqué. Pour insérer la marque dans les pixels brouillés de la zone RONI, les auteurs ont utilisé la technique de LSB. Ensuite, un re-brouillage des pixels dans la RONI a été fait pour les ramener à leur position d'origine. Finalement, l'image tatouée

a été obtenue par une combinaison de ROI et RONI. Les résultats obtenus montrent que la méthode proposée est robuste contre les attaques suivantes : le bruit Gaussien, le filtre médian, la compression JPEG, l'égalisation d'histogramme et l'attaque de copie. En termes d'imperceptibilité, l'approche proposée a une valeur moyenne de PSNR égale à 54.52 dB.

Memon, et al.[95] ont proposé une méthode de tatouage hybride qui insère deux marques, une marque robuste est insérée dans la région de non-intérêt (RONI) pour assurer la sécurité et la confidentialité et une marque fragile est insérée dans la région d'intérêt (ROI) pour le contrôle d'intégrité. La méthode proposée insère les informations de la région ROI dans la région RONI à l'aide de la méthode d'insertion basée sur des blocs dans le domaine fréquentiel en utilisant la technique (Integer Wavelet Transform) (IWT). L'image originale est divisée en ROI et RONI en utilisant l'algorithme proposé dans [24] pour sélectionner la région ROI. La région ROI est définie par le médecin. Ensuite, la région RONI est divisée en blocs de taille $N \times N$, pour éviter le sous-débordement et le débordement. Une carte de localisation est générée pour incorporer la marque par blocs en laissant les blocs suspects. La marque robuste est insérée dans les coefficients de haute fréquence tel que HL, LH et HH tandis que la marque fragile est insérée dans la zone ROI en utilisant la méthode LSB. Finalement une combinaison de ROI et RONI a été faite pour obtenir l'image tatouée. Les résultats expérimentaux montrent que la méthode proposée est robuste contre les attaques suivantes : le bruit Gaussien, le filtre médian, la compression JPEG et l'attaque de copie. Le PSNR obtenu dans cette méthode est égal à 59.89 dB.

Une technique d'authentification des images médicales est proposée par Tareef et al. [150]. L'image médicale est divisée en deux régions ROI et RONI. La région ROI est sélectionnée par le médecin en utilisant un carré et le reste de l'image est considéré comme la partie RONI. Cette méthode insère deux marques dans la RONI de l'image. La première marque est le dossier électronique du patient (EPR) et la deuxième marque est la partie ROI de l'image. Le codage Sparce Coding (SC) est appliqué pour encoder les deux marques : l'EPR et la région ROI afin d'avoir une compression élevée avec une qualité élevée de reconstruction de la marque. Ensuite, Le codage de l'EPR et du ROI est inséré conjointement dans la partie RONI de l'image en utilisant la technique d'insertion SVD pour atteindre deux objectifs de sécurité : la protection et l'authentification des données. Les résultats expérimentaux montrent que la technique proposée n'offre pas seulement un bon taux de correction de sabotage mais aussi une grande robustesse contre les attaques

compression JPEG, le bruit Gaussian, l'attaque flou (blurring) et l'attaque de seuil dur (Hard Threshold).

Jasni Mohamad Zain et al. [169] ont présenté un tatouage réversible dans la région de non-intérêt (RONI) de l'image pour vérifier l'authenticité et l'intégrité des images DICOM. Cette méthode est également basée sur la séparation du ROI et du RONI. La marque est générée à partir de la partie ROI de l'image en créant une valeur de hachage en utilisant SHA-256 de l'image entière. Après cela, la marque est insérée dans les bits les moins significatifs (LSB) de la partie RONI. Cette approche est réversible. La marque et l'image originale seront récupérées et le SHA-256 de l'image récupérée sera comparé à la marque extraite à des fins d'authentification.

Dans [140], une technique du tatouage robuste et sans perte d'image médicale basée sur la modulation M-Ary a été proposée par M. Sharma et al. Une séparation des parties ROI et RONI est effectuée à l'aide d'une méthode de segmentation de type floue appelée fuzzy c means. Le dossier électronique du patient (Electronic Patient Record (EPR)) est utilisé comme une marque et il est inséré dans les coefficients de transformation discrète en cosinus (DCT) de la bande de fréquence moyenne de la partie RONI.

2.7.3 Les méthodes du tatouage réversible

L'insertion de la marque, peu importe la banalité de la modification peut entraîner une dégradation de la qualité d'image hôte. Dans les applications, telles médicales où les exigences d'authentification sont souvent essentielles, il existe généralement des contraintes strictes sur la fiabilité des données qui empêchent toute déformation dans l'opération de tatouage. Par exemple, la modification de l'image médicale d'un patient peut affecter la vie du patient en provoquant des erreurs de diagnostic et de traitement. En conséquence, des techniques de tatouage réversibles ont été développées qui peuvent arrêter cette lacune en appliquant une technique qui peut récupérer à la fois la marque insérée et l'image originale. Des techniques de tatouage réversibles peuvent être utilisées pour l'authentification et l'intégrité de l'image, tandis que l'avantage de la réversibilité protège la qualité de l'image [67]. La technique de tatouage réversible peut être considérée comme un cas particulier du tatouage numérique [67]. La figure 2.12 illustre un schéma de tatouage réversible simple.

Une classification des méthodes de tatouage réversible est évoquée dans la section suivante.

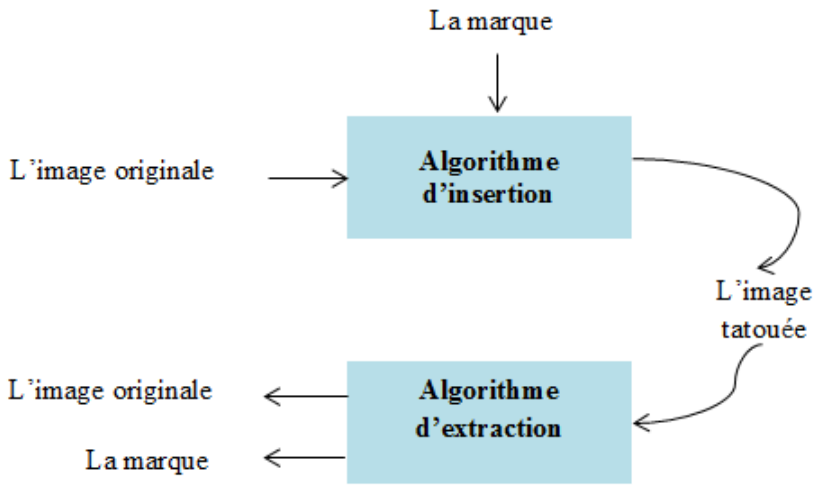


FIGURE 2.12 – Schéma basique d'un tatouage réversible

Classification des méthodes de tatouage réversible

Quelques défis majeurs rencontrés par les chercheurs dans ce domaine sont également décrits.

Pan et al.[112], ont classé diverses approches de tatouage réversibles en deux classes ; additif et substitutif, basé sur la méthode d'insertion. La comparaison est effectuée par une analyse empirique des approches de tatouage réversibles sélectionnées sur des images médicales.

Caldelli et al. [21] ont fourni un autre examen, qui classe les techniques de tatouage réversibles, sur la base des propriétés de tatouage, c'est-à-dire robuste, fragile et semi-fragile.

Bien que différentes catégories de techniques de tatouage réversibles soient rapportées dans la littérature, il est difficile de tracer une frontière précise entre les différentes catégories de techniques de tatouage réversibles. Cependant, une chose commune à toutes ces approches est de créer un espace pour cacher l'information et insérer la marque.

Nous avons examiné les nouvelles techniques de tatouage réversibles émergentes et nous les avons classées en quatre groupes : des techniques basées sur la compression, des techniques basées sur la modification d'histogramme, des techniques basées sur la quantification et des techniques basées sur l'expansion. Nous analysons brièvement les trois premiers groupes ; tandis que le tatouage réversible basé sur l'expansion est discuté

en détail. La raison est que les techniques de tatouage réversible basées sur l'expansion sont très prometteuses pour atteindre une capacité élevée à une qualité d'image donnée et sont efficaces sur le plan des calculs. Nous avons utilisé cette technique dans l'approche proposée dans le chapitre 5.

À cette fin, plusieurs techniques de tatouage basées sur l'expansion sont discutées.

Tatouage réversible basé sur la compression

Afin de récupérer l'image originale, nous devons stocker les informations essentielles pour la récupération de l'image originale et la marque. Ainsi, en cas de tatouage réversible, des données supplémentaires doivent être insérées et par conséquent nécessite plus d'espace par rapport au tatouage conventionnel pour l'insertion des données. Une approche simple consistera à compresser une partie de l'image pour l'insertion de données. Plusieurs schémas de tatouage réversibles sont signalés en utilisant cette approche.

Yang et al.[167] ont proposé une technique de compression à haute capacité pour le tatouage d'images dans le domaine de transformée de cosinus discret (DCT). Ainsi, une structure de discrimination de bloc basée sur deux essais est incorporée pour surmonter le problème de débordement / sous-dépassement.

Celik et al. [24] ont proposé une approche basée sur la compression. Les valeurs d'intensité des pixels dans l'image originale sont d'abord quantifiées en appliquant une quantification scalaire de niveau L. Ensuite, les restes obtenus sont compressés en utilisant un codec d'image adaptatif sans perte basé sur le contexte (CALIC). Les informations de tatouage sont concaténées avec celui-ci. À la fin, les données à insérer sont ajoutées à l'image quantifiée pour obtenir l'image tatouée.

Xuan et al.[165] ont développé une technique de tatouage réversible utilisant la fonction de compression sur les coefficients d'ondelettes entières. La fonction de compression est utilisée pour compresser les coefficients dont les valeurs sont supérieures à un certain seuil. Ce processus se traduit par une augmentation de la capacité d'insertion. Cependant, cela augmente également les données auxiliaires.

Memon et al. [97] ont appliqué une simple optimisation de seuil pour améliorer la capacité de l'approche de Xuan et al.[165]. D'un autre côté, Arsalan et al. [12] ont utilisé la fonction de compression [165] de Xuan et al. en combinaison avec un algorithme génétique pour développer une technique de tatouage réversible à haute capacité. Dans leur approche, l'image originale est d'abord transformée en domaine fréquentiel en prenant une transformée en ondelettes entières puis divisée en blocs. L'opération de compression est

effectuée sur chaque coefficient d'un bloc, dont la valeur est supérieure à un certain seuil. Chaque bloc a sa propre valeur de seuil. La matrice de seuil optimale / quasi-optimale est élaborée à l'aide d'un algorithme génétique et intégrée comme information auxiliaire. La technique d'Arsalan et al.[12] offre de bonnes performances en termes de compromis capacité / imperceptibilité, mais elle consomme plus de temps.

Tatouage réversible basé sur la modification d'histogramme

De nombreux chercheurs ont effectué des recherches dans le domaine du tatouage réversible basé sur la modification d'histogramme [[47],[57],[60],[67],[68],[74],[77],[76],[81],[67], [82], [39]].

Initialement, Vleeschouwer et al. [39] ont présenté une approche de tatouage réversible basée sur l'interprétation circulaire. Dans leur approche, l'image est divisée en plusieurs blocs de pixels voisins. Ensuite, chaque bloc est divisé en deux zones et les histogrammes correspondants sont calculés. Un composant principal est calculé pour chaque zone et est positionné sur un cercle suivant une position angulaire correspondant à l'histogramme. L'approche permet que les deux composants principaux des zones d'un bloc soient proches sur le cercle. L'insertion du bit de marque se fait en tournant le composant principal de la première zone dans le sens des aiguilles d'une montre ou dans le sens inverse selon que la valeur du bit soit 1 ou 0.

Ni et al. [106] ont développé une nouvelle approche de tatouage réversible basée sur la modification d'histogramme d'image. Avant l'insertion de la marque, une paire de pics et de points zéro est sélectionnée dans l'histogramme de l'image originale. Seuls les pixels avec des valeurs entre le pic et le point zéro subissent une modification pendant le processus d'insertion. Cependant, la capacité d'insertion est limitée au nombre de pixels présents au point de pointe dans l'histogramme de l'image originale.

Lin et al. [81] ont présenté une approche de tatouage réversible à plusieurs niveaux qui utilisent l'histogramme de différence d'image pour l'insertion des données. La différence d'image est générée en prenant la différence de deux pixels adjacents de l'image originale. L'image originale est divisée en un certain nombre de blocs qui ne se chevauchent pas, puis le bloc de différence correspondant à chaque bloc d'image est généré. Pour l'insertion de données, la méthode de modification d'histogramme est appliquée à chaque bloc de différence. Mais cette technique souffre de surcharge d'une grande quantité de données, c'est-à-dire de stocker les informations de valeur de crête pour chaque bloc.

Tsai et al. [82] ont proposé une approche subtilement différente de [81]. La différence

entre un pixel de base et tous les autres pixels dans le bloc est utilisée plutôt que la différence de pixels adjacents. Cependant, la méthode de prédiction utilisée dans [82] est moins précise et la nécessité de conserver les valeurs des pixels de base inchangés réduit la capacité d'insertion de la marque.

Kim et al. [68] ont proposé une nouvelle méthode qui exploite la corrélation spatiale entre les images sous-échantillonnées. Une image sous-échantillonnée de référence est d'abord sélectionnée parmi plusieurs images sous-échantillonnées, puis les différences entre la référence et les autres images sous-échantillonnées sont générées. L'insertion de la marque est ensuite effectuée en modifiant l'histogramme de différence.

Kamran et al. [67] ont également signalé une nouvelle approche qui utilise le concept de sous-échantillonnage pour l'amélioration de la performance. L'échantillonnage à la baisse fournit deux versions sous-échantillonnées de l'image originale, à savoir la référence et la dissimulation des données. Les blocs sont générés en utilisant ces deux versions sous-échantillonnées. L'insertion de la marque est réalisée dans les blocs par la technique de modification d'histogramme. De plus, pour rendre la technique aveugle, Kamran et al. [67] a intégré la carte de localisation (LM) dans l'image tatouée.

Tatouage réversible basé sur la quantification

Les techniques de tatouage basées sur la quantification sont en général robustes. Cependant, les approches de tatouage réversible basées sur la quantification sont pour la plupart de nature fragile.

Cheung et al. ont proposé une stratégie de quantification séquentielle (SQS) pour l'intégration des données [30]. La stratégie de quantification séquentielle (SQS) rend la modulation d'une valeur de pixel dépendante des pixels précédents. La méthode réversible d'insertion des données est utilisée avec la technique de stratégie de quantification séquentielle (SQS) pour la rendre plus appropriée aux fins d'authentification.

Saberian et al. [134] ont présenté une approche basée sur la méthode de quantification pondérée (Weighted Quantization Method (WQM)), qui peut être appliquée aussi bien dans le domaine spatial que dans le domaine fréquentiel. Contrairement à d'autres approches, la distorsion provoquée par cette approche ne dépend pas de la charge utile. Cette approche montre que la méthode de quantification pondérée WQM offre une capacité d'insertion élevée, lorsqu'elle est appliquée à la transformation de graphe point à point (Point to Point Graph (PPG)).

Lee et al. [73] ont proposé une technique de tatouage réversible basée sur la quanti-

fication vectorielle en utilisant la modification d'histogramme pour atteindre une grande capacité d'insertion. Les techniques conventionnelles de tatouage basées sur la modulation d'indice de quantification (Quantization Index Modulation (QIM)) ne sont pas réversibles en général, en raison des distorsions irréversibles provoquées dans l'image tatouée en raison du processus de quantification.

Ko et al.[69] ont développé un algorithme de tatouage basé sur la modulation d'indice de quantification QIM pour les systèmes de tatouage d'images médicales, ce qui assure la récupération de l'image originale. Cette technique offre de meilleurs résultats en terme de BER et NC que la méthode QIM proposée dans [69].

Tatouage réversible basé sur l'expansion

Le concept de tatouage réversible basé sur la différence d'expansion (Diffrence Expansion (DE)) a d'abord été introduit en 2003 [35]. Il a offert une nouvelle façon aux techniques de tatouage réversibles. Le schéma proposé insère un bit de la marque dans les LSBs de la valeur de différence de deux pixels. Les paires de pixel sélectionnées peuvent être soit deux voisines quelconques (horizontales ou verticales) ou deux pixels sélectionnés dans un cadre d'un modèle prédéfini. Une explication de cette technique de tatouage est présentée dans la figure 2.13.

Alattar [7] a étendu l'approche précédente en cachant deux bits dans les différences d'un triplet de pixels. L'algorithme proposé utilise des triplets spatiaux et spectraux de pixels pour cacher une paire de bits pour augmenter la capacité d'insertion. Un triplet spatial désigne trois pixels choisis dans la partie spectrale ou couleur correspondante de l'image. D'une autre part, le triplet spectral peut être n'importe quelle valeur de trois pixels choisis parmi diverses composantes spectrales.

Alattar [6] a développé une approche de tatouage réversible en utilisant la technique de la différence d'expansion (DE) de quads d'images couleur. Cette méthode insère trois bits dans le DE d'un groupe de quatre pixels. La méthode la plus simple de sélection des quads consiste à supposer que 2×2 pixels adjacents sont un quad. La capacité de masquage maximale du système proposé est estimée à 0,75 bpp. Cependant, la capacité est estimée inférieure car certains quads peuvent ne pas être utilisables en raison de problèmes de débordement / sous-dépassement. Par exemple, la différence peut être (plus de 255 ou moins de 0) pour des images en niveaux de gris de profondeur 8 bits.

Alattar [58] a généralisé le précédent algorithme en implémentant DE de vecteurs, au lieu de paires, triplets et quads, pour améliorer la capacité d'insertion des images en

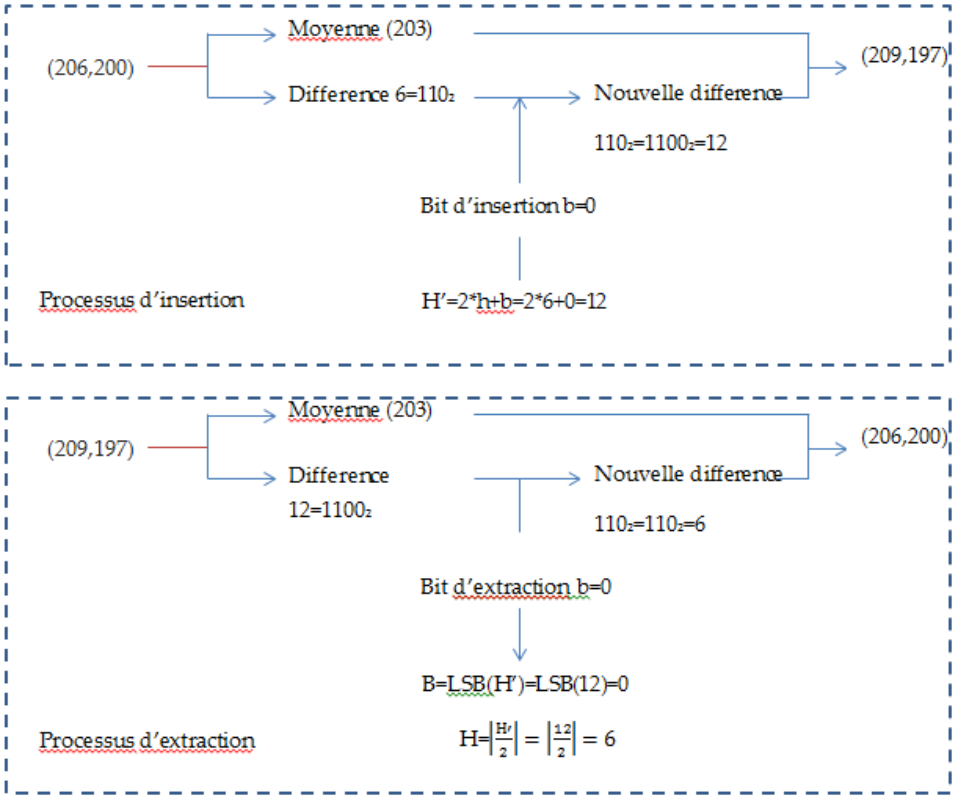


FIGURE 2.13 – Principe de la technique de tatouage réversible DE

couleur. Le système proposé cache plusieurs bits dans la différence de chacun des vecteurs de pixels connectés.

Un développement significatif de la technique DE introduit par Thodi et Rodriguez [154], s'appelle (Prediction Error (PE)) expansion. Dans cette méthode, PE est utilisé au lieu de DE de deux pixels adjacents car l'erreur est plus légère que la différence entre les valeurs de pixels. Le processus d'insertion se fait en développant les valeurs de PE. Pour éviter les problèmes de débordement / sous-dépassement, seuls les pixels extensibles sont choisi pour le processus d'insertion. Une carte de localisation compressée des emplacements d'insertion sélectionnés est également combinée avec la marque en blocs.

Thodi et Rodríguez [155] ont amélioré leur approche précédente en combinant le décalage PE et l'histogramme au lieu de la carte de localisation. La méthode de décalage d'histogramme nécessite une carte de débordement / sous-dépassement, qui nécessite relativement moins d'espace que la carte de localisation. Cette approche a réduit la déformation à de faibles quantités de masquage et modéré le problème de contrôle de la capacité causé par la carte d'emplacement.

2.7.4 Les méthodes de zéro-tatouage

La méthode de zéro-tatouage ne modifie pas l'image originale pour insérer la marque mais elle utilise des caractéristiques importantes et uniques extraite de l'image originale pour construire la marque qui peut être utilisée ultérieurement pour identifier l'image originale. Cela équilibre volontairement le conflit entre l'imperceptibilité et la robustesse de la marque contre les attaques. C'est une bonne méthode alternative de tatouage pour n'apporter aucune distorsion de la qualité d'image originale. La conception d'un zéro-tatouage est basée sur l'extraction de caractéristiques robustes et uniques de l'image originale.

Ces caractéristiques sont déduites de propriétés des domaines spatiaux ou fréquentiels et la plupart d'entre eux sont corrélés avec les principes du système visuel humain (Human Visual System (HVS)), la propriété de texture, la transformation des valeurs singulières (SVD), la distribution d'énergie des basses fréquences (DWT) et les informations exprimées au moyen des coefficients de la transformée en cosinus (DCT) sont des exemples de fonctionnalités d'images utilisées pour extraire des caractéristiques afin de générer un zéro-tatouage.

De plus, la transformation exponentielle complexe (Polar Complex Exponential Transform (PCET)), les moments d'exposants quaternion (QEMs), et les moments de Bessel-

Fourier [164] sont trois méthodes de transformation qui fournissent quelques caractéristiques robustes qui sont exploitées pour construire un zéro-tatouage pour l'authentification d'image. De nombreuses approches de zéro-tatouage ont été proposées pour résoudre les problèmes d'identification, d'authentification et de contrôle d'intégrité. Nous décrivons brièvement des récents travaux de zéro tatouage utilisant les images médicales.

Musab Ghadi et al. [50] ont proposé une approche de zéro-tatouage pour authentifier les images médicales transmises via un réseau de santé non sécurisée sur la base de paramètres extraits de l'image originale. L'image originale est partitionnée en blocs de 8×8 qui ne se chevauchent pas, un processus de soustraction cumulative entre les valeurs de pixels de l'image originale est appliqué, ensuite, une matrice de quantification (Quantisation Matrix (QM)) de fichier JPEG est extraite pour générer une matrice finale de taille 8×8. Le processus de soustraction commence par soustraire le premier bloc 8×8 de l'image originale et le bloc 8×8 de la matrice QM. La valeur moyenne du bloc 8×8 résultant est utilisée comme une clé k et sera une entrée du modèle Jacobien pour générer un zéro-tatouage.

V.Seenivasagam et al. [138] ont proposé un système de zéro-tatouage pour l'authentification d'image et le contrôle d'accès aux dossiers de santé électroniques (DSE) dans un environnement de téléradiologie. Cette approche utilise le domaine composite Transformation de Contourlet (CT) et la Décomposition en Valeurs Singulières (SVD). Les détails d'identification du patient et un lien vers les données du patient encodés dans un code (Quick Response (QR)) sont utilisés comme une marque. De plus, pour réduire les frais généraux de calcul, la marque est découpée en éliminant la région blanche de l'image. Le résultat est la marque de taille 77×77. La robustesse du système de zéro-tatouage est attribuée au partage maitre (Master Share). Dans ce système, les auteurs ont utilisé les moments invariants de Hu [39] pour créer le partage maitre (master share) qui représente les caractéristiques essentielles de l'image hôte. Ensuite, une fonction de générateur de nombres triangulaires (TNG) qui peut coder de manière unique une paire d'entiers est utilisée pour combiner le partage maitre (Master share) et la marque brouillée avec la transformation d'Arnold pour générer le partage secret (secret share). La marque peut être générée par le personnel autorisé uniquement en possession de la clé secrète partagée.

Les auteurs de [161] ont proposé une approche de zéro-tatouage robuste basé sur la transformation exponentielle de complexe polaire (PCET) [125] et de la cartographie logistique [163]. L'approche proposée a commencé par brouiller la marque W à l'aide de la méthode d'Arnold de brouillage [65] et la graine (seed) S pour améliorer la robustesse,

le résultat est W_s. Ensuite, le PCET est appliqué sur l'image originale I pour obtenir les coefficients PCET. La carte logistique est ensuite utilisée pour sélectionner au hasard un ensemble de coefficients PCET pour construire un vecteur caractéristique $\vec{A}$. Le vecteur $\vec{A}$ est converti en séquence binaire 1D, et la séquence résultante est remodelée en tant qu'image caractéristique I_F. L'opération XOR entre l'image caractéristique I_F et l'image de la marque brouillée W_s sont appliquées pour générer une image de vérification de zéro-tatouage W_V. La valeur de hachage HVSK du W_V, la graine S et la clé secrète K utilisée dans la méthode de cartographie logistique, sont calculées en utilisant l'algorithme Message-Digest 5 (MD5) [156]. Par la suite, le l'horodatage T est ajouté à HVSK pour générer HVSKT. Le HVSKT devient une unique identification pour générer un zéro-tatouage et elle est envoyée à un tiers de confiance via un canal sécurisé. Le processus de vérification de zéro-tatouage commence par la vérification de la validité des paramètres de sécurité : W_V, graine S et la clé secrète K. Si les paramètres sont validés, le vecteur caractéristique A de l'image attaquée I est construit en utilisant la méthode PCET et la clé de carte logistique K. La séquence binaire du vecteur de caractéristiques extrait A est remodelée en une image de caractéristiques I_F^*. L'opération XOR entre I_F^* et W_V est appliquée pour générer une image brouillée $W*_s$, et une transformation d'Arnold inversée utilisant la graine S est appliquée pour obtenir la marque vérifiée W. Cette approche est robuste contre les attaques de rotation, la mise à l'échelle, la compression, les attaques de bruit, l'affûtage et le flou.

Les auteurs dans [75] ont proposé un algorithme robuste de zéro-tatouage d'image basé sur la transformation discrète en ondelettes (DWT) et l'analyse en composantes principaux (Principal Component Analysis (PCA)). Dans l'algorithme proposé, l'image originale est d'abord transformée avec DWT, et sa bande LL est divisée en blocs d'image non chevauchée avec chaque bloc d'image transformé en vecteur, puis il applique l'analyse des composants principale PCA sur l'ensemble de vecteurs. Enfin, il construit la séquence de zéro-tatouage en jugeant la polarité positive et négative du coefficient qui a la valeur absolue maximale dans chaque vecteur analysé. La robustesse de l'algorithme proposé aux processus d'image donnés est analysée, et les résultats montrent que l'algorithme proposé est robuste aux attaques de traitement de signal conventionnel, comme le bruit, le filtrage, la compression JPEG et le recadrage, etc.

Baoru Han et al. [55] ont proposé un algorithme de zéro-tatouage pour les applications médicales données pour assurer la robustesse, la sécurité et l'invisibilité. Cette technique repose sur la transformée en ondelettes discrètes tridimensionnelles, la transformée de

Fourier tridimensionnelle et le réseau neuronal chaotique Hermite. Le nouveau réseau de neurones chaotique Hermite est utilisé pour générer la séquence chaotique pseudo-aléatoire pour le brouillage (scrambling). L'image médicale tridimensionnelle est transformée par la transformée en ondelettes discrète en trois dimensions et la transformée de Fourier discrète en trois dimensions. Ensuite, les coefficients de fréquence basse et intermédiaire sont sélectionnés comme caractéristiques des données médicales pour créer un zéro-tatouage. Cet algorithme a une bonne résistance aux attaques géométriques telles que le bruit gaussien, la compression JPEG, le cisaillement virement de bord et attaque par zoom.

2.7.5 Les méthodes de tatouage hybrides

Les méthodes de tatouage hybride consistent à combiner deux méthodes de tatouage différentes ou plus pour améliorer la performance des systèmes de tatouage. En combinant convenablement des méthodes particulières de la bonne manière, les inconvénients de chaque méthode seront éliminés et leurs forces seront mises en évidence. Cela pourrait éliminer les obstacles à l'utilisation d'un seul type de tatouage en pratique pour sécuriser les images médicales, car chaque type de tatouage a des avantages et des limites.

Ales Rocek et al. [132] ont proposé une approche entièrement réversible pour la sécurité des images médicale en combinant les avantages des trois approches : Le tatouage réversible, le zéro-tatouage et le tatouage dans la partie RONI. L'idée de base est que l'image originale est divisée en deux parties : ROI et RONI. RONI est la partie de l'image où les petits changements ne faussent pas les informations médicales. Le ROI est le reste de l'image. L'extraction de la partie RONI a été réalisée automatiquement par la méthode présentée dans [131]. La ROI est sécurisé par une approche de zéro-tatouage. L'information nécessaire pour retirer la marque de la partie ROI sécurisée est appelée le partage secret (Secret Share), qui est insérée comme une marque dans la partie RONI à l'aide d'un tatouage réversible. Cela sécurise l'image sans changer ses parties les plus importantes et permet une reconstruction complète de l'image originale ainsi que la vérification de son authenticité. Le concept de tatouage dans la partie ROI est basé sur le principe de zéro-tatouage. Elle est issue de la méthode décrite dans l'article [14], qui combine la robustesse de tatouage en utilisant le domaine d'ondelettes complexe à double arbres (dual-treecomplex wavelet domain) et les avantages de la cryptographie visuelle. Le processus de tatouage utilise la transformation en ondelettes complexes d'arbres doubles (Dual-tree complex wavelet transform (DT-CWT)) [104] pour créer une matrice binaire B basée sur les coefficients de sous-bande bas-bas (LL). À partir de la matrice B et de la marque, le partage secret est

ensuite généré à l'aide de la cryptographie visuelle. La même procédure est utilisée pour extraire la marque pour générer un partage public (public share). Après chevauchement (ou logique), le partage secret, les partages publiques et la marque sont obtenus comme résultat. Ensuite, la marque est insérée dans la partie RONI par la technique de tatouage numérique réversible RCM (Reversible Contrast Mapping) qui remplace les bits les moins significatifs des paires de pixels transformées. Le LSB du premier point de chaque paire est utilisé pour indiquer si la paire est transformée ou non. Une valeur de 1 indique qu'elle est transformée, la valeur 0 indique qu'elle n'est pas transformée.

Asaad F. Qasim et al. [122] ont développé une approche de tatouage robuste pour confirmer l'intégrité et l'authenticité des images de résonance magnétique (IRM) du cerveau et pour vérifier que les altérations peuvent être détectées et suivies en arrière. Dans cet article, une approche qui combine la technique de tatouage réversible aveugle et la technique de tatouage dans ROI /RONI est présentée pour détecter les changements intentionnels et non intentionnels dans les images médicales. L'image originale est divisée en deux parties ; la région d'intérêt (ROI) et la région de non intérêt (RONI). A partir de l'entête de l'image DICOM, seuls les champs de métadonnées essentiels, qui contiennent les informations et les données des patients décrivant l'image qui ne change pas pendant la distribution, ont été employés pour générer une marque d'authentification AW. La signature numérique de l'image originale aussi est calculée et encodée par l'algorithme de Message Digest (MD5) pour offrir une marque d'intégrité IW. Ensuite, les deux marques IW et AW sont concaténées et converties en forme binaire. Pour améliorer la capacité d'insertion et réduire le niveau de distorsion, la marque est compressée par la technique de codage de longueur de course (Run-length encoding (RLE)). RLE est facile et rapide à mettre en œuvre, ce qui en fait une bonne alternative à d'autres algorithmes de compression complexes.

Abhilasha Sharma et al. [140] ont proposé une méthode basée sur deux techniques de tatouages dans le domaine de transformation populaires, la technique de transformé en ondelettes discrètes (DWT) et la technique de transformé en cosinus discrète (DCT). Dans le processus d'insertion, l'image médicale originale est divisée en deux parties distinctes, la région d'intérêt (ROI) et la non-région d'intérêt (NROI). Plusieurs marques sous forme d'image et de texte sont insérées dans la partie ROI et la partie RONI. Afin d'améliorer la sécurité de la marque texte, La technique de cryptage (Rivest–Shamir–Adleman (RSA)) est appliquée à la marque texte avant l'insertion et les données EPR cryptées sont insérées dans la partie RONI de l'image médicale originale. Pour l'insertion de la marque les auteurs

ont appliqué la technique de DWT de deuxième niveau sur ROI et RONI pour obtenir les sous-bandes LL2, LH2, HL2 et HH2. Puis ils ont appliqué un DWT de troisième niveau sur l'image de la marque et la transformation DCT à la sous-bande LL3 du DWT de l'image de la marque. Puis ils ont formatée la transformation DCT de la marque à l'aide de la fonction module pour obtenir la marque «W1» ensuite ils ont sélectionné le fichier de données du dossier patient électronique (EPR) comme marque de texte et ils ont crypté la marque à l'aide de cryptographie à clé publique pour obtenir la deuxième marque «W2». La transformée en cosinus discrète inverse (IDCT) et la transformée en ondelettes discrètes inverses de deuxième niveau (IDWT) sont utilisées pour insérer la marque dans la partie ROI. Et ils ont appliqué l'inverse de deuxième niveau de transformé en ondelettes discrète (IDWT) pour la marque texte insérée dans la région RONI. Pour obtenir l'image tatouée ils ont fusionné les parties ROI et RONI insérées dans l'image originale. La performance de la méthode proposée est évaluée pour des attaques de traitement d'image et le résultat souhaité est obtenu sans dégradation significative et perceptuele de la marque extraite.

Imane Assini et al [13] ont proposé une méthode de tatouage robuste qui combine trois techniques de tatouages : la transformée en ondelettes discrètes (DWT), la transformée en cosinus discrète (DCT) et la décomposition en valeurs singulières (SVD). Cette approche est destinée pour insérer une marque invisible dans une image médicale. L'image originale est divisée en troisième niveau de coefficients DWT puis transformée par DCT et SVD. La même technique est appliquée à la marque. La valeur singulière de la marque est insérée dans la valeur singulière des sous-bandes haute fréquence du DWT de troisième niveau de l'image originale. Cependant, l'insertion de la marque dans ces zones permet de renforcer la robustesse du système de tatouage sans nuire à la qualité de l'image tatouée. Pour produire l'image médicale tatouée l'inverse de DCT et de DWT est appliqué.

Lou et Sung [84] ont décrit deux méthodes de transformation (DCT et DWT) pour incorporer une marque aléatoire dans une image. Après la décomposition de troisième niveau de l'image originale par DWT, DCT est appliqué aux sous-multiples paramètres de Fourier fractionnaire discret (MPDFRF) et DWT. Dans le processus d'insertion, l'image originale est décomposée en quatre sous-bandes d'ondelettes en utilisant DWT. Après chaque sous-bande est segmentée en blocs, la transformation MPDFRF est appliquée à chaque bloc. L'image de la marque est ensuite insérée dans les blocs. Les résultats expérimentaux montrent le bon visuel d'imperceptibilité et de la robustesse contre les attaques connues.

Hadi et al. [53] ont proposé une méthode basée sur deux méthodes de transformation,

Fresnel et DWT. Avant d'insérer la marque, l'image originale est d'abord transformée par la transformation de Fresnel pour générer l'image originale chiffrée. Après la deuxième décomposition de l'image originale à l'aide de DWT, les informations de copyright cryptées sont insérées dans l'image originale décomposée. La méthode utilise une séquence chaotique comme clé pour crypter les informations de copyright.

Nakhaie et Shokouhi [105] ont proposé une méthode de mesure objective de la qualité sans référence basée sur la technique du spectre étalé et DWT utilisant le traitement de la partie ROI. Dans le processus d'insertion, l'image originale est d'abord divisée en deux parties séparées, ROI et RONI, ensuite, DWT et DCT sont appliquées sur ROI et RONI , respectivement. La marque binaire est insérée dans la transformation DCT de la partie RONI de l'image originale.

Thanushkodi [158] a proposé une méthode de tatouage en domaine fréquentiel pour vérifier l'intégrité et l'authenticité des images médicales. Dans le processus d'insertion, DCT est d'abord appliqué à l'image originale pour générer une matrice de transformée. Une image hybride transformée est obtenue ensuite en appliquant la transformation en ondelettes de Daubechies sur la matrice transformée résultante. Maintenant, la valeur de bit le moins significatif (LSB) de chaque deux octets de l'image hybride transformée est calculée suivis de l'opération XOR. En outre, chaque valeur de pixel de la marque binaire est comparée à la valeur XOR résultante pour obtenir une image tatouée. Le processus d'extraction est l'inverse du processus d'insertion. La technique de transformation en ondelettes Daubechies utilisée par les auteurs est utile pour l'analyse locale, mais elle a une surcharge de calcul plus élevée.

Singh et al. [144] ont présenté une méthode de tatouage multiple sécurisée basée sur DWT, DCT et SVD. À des fins d'authentification d'identité, la méthode proposée utilise l'image médicale comme une marque image et le dossier personnel et médical du patient comme une marque texte. Afin d'améliorer la sécurité de la marque texte, le cryptage est appliqué à la représentation ASCII de la marque texte avant l'insertion. Les résultats expérimentaux ont montré que la méthode est robuste pour divers traitements de signal et attaques "Checkmark". Pour améliorer les performances de la méthode proposée, DWT peut être appliqué sur la marque au lieu de DCT comme proposé dans [144].

Zear et al. [170] ont proposé une technique de tatouage hybride robuste et sécurisée par transformées en ondelettes discrètes (DWT), transformée en cosinus discrète (DCT), décomposition en valeurs singulières (SVD) et le réseau de neurones. Deux informations différentes de la marque texte sont compressées et codées par le code de correction d'erreur

arithmétique et le code de correction d'erreur de hamming respectivement. La marque texte codée et compressée est insérée dans l'image originale. De plus, la transformée d'Arnold est appliquée sur la marque image avant d'être insérée dans l'image hôte. La performance de l'algorithme a été largement évaluée en termes de PSNR, NC et BER.

2.8 Bilan sur les approches de tatouage existantes

Dans la section précédente, nous avons présenté une revue des techniques de tatouage d'images existantes. Celles-ci ont été classées en quatre catégories : tatouage classique, tatouage des régions ROI et RONI, tatouage réversible, zéro-tatouage et tatouage hybride. Il est à noter que ces méthodes ne sont pas spécifiquement destinées ou adaptées à des modalités précises d'imagerie médicale. Dans cette section, nous discutons diverses questions liées à chaque approche.

De nombreuses techniques ont été proposées dans la littérature pour le tatouage des images médicales utilisant à la fois les domaines spatial et fréquentiel. Ces techniques insèrent la marque dans l'image entière ou dans les parties ROI ou RONI de l'image en mettant en œuvre des méthodes réversibles ou irréversibles. Par comparaison avec les techniques de domaine fréquentiel qui conviennent aux applications de vérification de propriété, les techniques basées sur le domaine spatial sont moins complexes et fournissent une capacité et une qualité visuelle plus élevées. Cependant, les méthodes du domaine spatial sont fragiles et ne peuvent pas survivre à de nombreuses opérations les rendant inappropriées pour l'intégrité et l'authentification. En outre, il est à noter que les techniques du domaine fréquentiel qui sont basées sur DCT et DFT sont rarement utilisées pour le tatouage d'images médicales et la majorité des études préfèrent les techniques basées sur DWT car il offre une correspondance précise avec le système visuel humain.

Le changement d'un seul bit dans une image médicale pourrait être un problème pour un diagnostic correct. En utilisant le tatouage RONI uniquement, les marques sont stockées uniquement dans des parties qui ne contiennent pas d'informations importantes pour le diagnostic, mais cela présente plusieurs inconvénients tels qu'il ne peut être appliqué que s'il existe une partie RONI dans l'image, de plus, la taille de la marque dépend de la taille de la partie RONI. La sélection de la partie RONI peut être automatique ou manuelle. La fiabilité de la détection automatique de zones importantes dépend de la méthode choisie. En pratique, différentes méthodes de sélection automatique de RONI sont principalement utilisées [[127], [124], [148]].

La nécessité de rechercher la partie RONI rend le tatouage plus difficile et peut provoquer des erreurs avec les processus d'étiquetage ROI manuels et automatiques. L'adéquation de ces méthodes dépend des caractéristiques de l'image (possibilité d'avoir une RONI, taille de la RONI, etc).
Les exigences médicales sont extrêmement strictes avec la qualité des images médicales et ne permettent pas la modification non clinique. Les méthodes de tatouage irréversibles restent soumises à l'acceptation par les radiologues tandis que les images originales restent généralement privilégiées à des fins de diagnostic. Le tatouage réversible est basé sur le processus d'insertion de la marque dans une image médicale, la transmission de l'image tatouée et l'extraction complète de la marque de l'image se fait du côté du destinataire. Après l'extraction de la marque, l'image originale est entièrement restaurée et inchangée. Une fois la marque retirée de l'image, l'image n'est plus protégée. De toute évidence, il est nécessaire de transmettre ces valeurs différentielles de manière sécurisée. Ces différences sont utilisées du côté du destinataire pour retirer la marque et reconstruire l'image originale [[128], [59]]. Comme un avantage de cette méthode, nous pouvons mentionner la possibilité de sécuriser l'image entière par des méthodes de tatouage robustes et une capacité plus élevée que le tatouage RONI. Le principal inconvénient est la nécessité de créer un autre canal pour le transport sécurisé des informations différentielles.
Dans le zéro-tatouage, la marque n'est pas insérée directement dans les données tatouées, mais elle est conservée séparément pour une comparaison ultérieure. En conséquence, il peut être considéré comme sans perte car aucune donnée n'est modifiée, il est principalement utilisé pour assurer la protection des droits d'auteur. Il est basé sur une autorité de certification (Certification Authority (CA)) [[148],[59]]. Les principaux avantages sont une grande robustesse et une non distorsion de l'image tatouée. Le gros inconvénient est la nécessité de construire un système basé sur une autorité de certification CA assez complexe pour le stockage et la comparaison de la marque.
Dans le cas de tatouage hybride, en combinant convenablement des méthodes particulières de la bonne manière, les inconvénients de chaque méthode seront éliminés et leurs forces sont mises en évidence. Une comparaison de ces techniques concernant la méthode d'insertion, la robustesse, la capacité, l'imperceptibilité, la réversibilité et l'objectif est également illustrée dans le tableau 2.1.

Les méthodes	Les domaines d'insertion	La robustesse	L'imperceptibilité	La capacité	La réversibilité	L'objectif
Les méthodes classiques	Domaine spatial	Fragile	Elevée	Elevée	Non	Intégrité et authentification
	Domaine fréquentiel	Robuste	Basse	Basse	Non	Protection de la propriété
Les méthodes ROI et RONI	Domaine spatial	Fragile	Elevée	Dépendant	Non	Intégrité et authentification
	Domaine fréquentiel	Robuste	Basse	Dépendant	Non	Protection de la propriété
Les méthodes réversibles	Les méthodes basées sur la compression	Fragile	Elevée	Elevée	Réversible	Intégrité et authentification
	Les méthodes basées sur la quantification	Robuste	Basse	Basse	Réversible	Protection de la propriété
	Les méthodes basées sur l'expansion	Semi fragile	Elevée	Elevée	Réversible	Intégrité et authentification
	Les méthodes basées sur la compression	Fragile	Elevée	Elevée	Réversible	Intégrité et authentification
Les méthodes de zéro-tatouage	Domaine spatiale	Robuste	Elevée	Elevée	Réversible	Intégrité et authentification
	Domaine fréquentiel	Robuste	Elevée	Elevée	Réversible	Intégrité et authentification

TABLE 2.1 – Comparaison des approches de tatouage existantes

2.9 Les méthodes existantes de combinaison du tatouage numérique et de la cryptographie

Il existe dans la littérature des techniques combinant le tatouage et la cryptographie pour assurer un haut niveau de sécurité des transmissions d'images médicales. Dans cette section nous présontons un état de l'art sur les différentes méthodes existantes qui com-

binent le tatouage numérique et la cryptographie.

2.9.1 Les méthodes de tatouage suivi du cryptage

Rajendra Acharya et al [1] ont proposé une technique pour entrelacer le texte d'information du patient et le document graphique pour un stockage efficace. La marque est conçue pour entrelacer les informations du patient avec des images médicales pendant la compression JPEG, afin de réduire les frais généraux de stockage et de transmission. Les données textuelles sont cryptées à l'aide d'une technique logarithmique avant d'être entrelacées avec des images dans le domaine fréquentiel pour assurer une plus grande sécurité. Les signaux graphiques sont également entrelacés avec l'image. La technique est testée pour différentes images.

J.M. Rodrigues et al [133] ont proposé une nouvelle méthode de masquage de données cryptographiques sans perte pour l'image médicale. Elle est basée sur la décomposition et le contenu de l'image. Dans cette méthode les informations du patient sont insérées dans l'image d'une manière hautement indéchiffrable sans ni augmentation de taille ni changement du contenu original. L'idée principale est de décomposer l'image médicale en deux sous-images et d'appliquer à chaque sous-image un processus différent afin de gagner de l'espace et de la confidentialité des informations. Elle peut être utilisée pour intégrer le diagnostic et / ou la maladie historique dans des images médicales du patient à des fins de transfert en toute sécurité. La méthode proposée permet de masquer des informations de l'ordre de 8% de la taille de l'image originale sans augmentation, l'entropie est égale à 7,9 bits / pixel.

Dans [61], les auteurs ont également proposé une double approche de tatouage suivi du cryptage pour prouver l'authenticité et l'intégrité des images médicales. La transformation DWT à deux niveaux est appliquée aux données originales. La marque est insérée dans la sous-bande bas-haut basée sur la technique LSB où la sous-bande bas-haut est à nouveau divisée en plusieurs blocs, puis les informations médicales (en tant que deuxième marque) sont insérées dans ces blocs en utilisant la technique LSB. Finalement, l'image tatouée est cryptée à l'aide des algorithmes RSA , Advanced Encryption Standard (AES) et Ron's Code (RC4).

Un autre travail de tatouage suivi du cryptage est présenté dans [149]. Le tatouage est basé sur les méthodes suivantes : la transformation de paquets en ondelettes (Wavelet Packet Transform (WPT)) et la décomposition en valeurs singulières (SVD), tandis que les données tatouées sont cryptées en fonction du partitionnement défini dans les arbres

hiérarchiques (Set Partitioning in Hierarchical Trees (SPIHT)) fournis en développant le framework (JSON Web Encryption (JWE)), afin d'assurer la confidentialité des données et la propriété du contenu.

2.9.2 Les méthodes du cryptage suivi du tatouage

W. Puech et al. [119] ont proposé une méthode qui combine le cryptage d'image et la technique de tatouage pour une transmission sécurisée des images médicales. Cette méthode est basée sur la combinaison des clés privées, des clés publiques, de chiffrement par clé secrète et le tatouage. L'algorithme de cryptage avec clé secrète est appliqué à l'image. La clé secrète est cryptée avec une méthode de cryptage basée sur des clés publiques-privées. Ensuite, cette clé secrète est intégrée dans l'image cryptée à l'aide de la méthode de tatouage DCT.

Solanki et al. [145] ont proposé une autre approche de cryptage suivi de tatouage afin de protéger les informations de patients stockées dans les images médicales. En cryptage /phase d'insertion, l'image tatouée est cryptée à l'aide de l'algorithme RSA (Rivest–Shamir–Adlema) tandis que l'image originale est améliorée sur la base du seuil de la zone de haute intensité. L'insertion de la marque se fait en fonction de l'algorithme Haar DWT (Digital Wavelet Transform). Lors de la phase d'extraction/décryptage, l'image originale et l'image tatouée sont décomposés par la méthode HAAR DWT, puis la marque est décryptée en utilisant l'algorithme RSA.

Dans [147], les auteurs ont présenté une technique de cryptage suivi de tatouage pour les images JPEG afin de préserver la confidentialité du contenu. Les auteurs ont appliqué une technique de chiffrement de flux asymétrique (asymetric stream cipher) pour le cryptage. Le chiffrement de flux codé obtenu a été inséré dans les coefficients de l'image hôte en se basant sur la transformation en ondelettes discrète DWT. La marque peut être extraite à partir de l'image cryptée ou à partir de l'image décryptée. Dans cette recherche, les auteurs ont appliqué diverses approches de tatouage telle que l'approche (Spread Spectrum (SS)), (Scalar Costa Scheme Quantization Index Modulation (SCSQIM)) et la modulation de vibration rationnelle (Rational Dither Modulation (RDM)).

Dans [135], une approche hybride de cryptage et de tatouage d'image est proposée dans laquelle le cryptage est effectué à l'aide de la méthode (One Time Pad (OTP)) tandis que le tatouage est effectué en fonction de la méthode des transformées en ondelettes discrètes DWT. La clé a été construite à partir de chaque bloc de 8×8 de l'image. La marque est cryptée à l'aide de la fonction XOR, puis les auteurs insèrent la marque cryptée dans

l'image originale dans la sous-bande de fréquence moyenne des coefficients DWT. Les faiblesses de cette technique sont les suivantes : la clé est extrêmement volumineuse à partager, la manière de produire la clé est fragile et le les résultats d'imperceptibilité sont inacceptables. De plus, les auteurs n'ont pas mesuré la robustesse de leur algorithme de tatouage contre les attaques.

2.9.3 Les méthodes de tatouage-décryptage conjoint

Dalel Bouslimi et al [20] ont proposé un système de tatouage-décryptage conjoint dans le but de vérifier la fiabilité des images et d'identifier la personne à l'origine d'une distribution illégale. Ce système associe une méthode de tatouage commune, basée sur la modulation d'indice de quantification (QIM), et une approche conjointe de tatouage-décryptage. Côté émetteur, la marque est insérée comme preuve de fiabilité de l'image avant de l'envoyer cryptée. À la réception, une autre marque qui est une preuve de traçabilité, est intégrée lors du processus de décryptage.

2.9.4 Les méthodes de tatouage cryptage conjoint

Dalel Bouslimi et al. [18] ont proposé un algorithme de tatouage cryptage conjoint dans le but de protéger les images médicales. Cette technique est basée sur le chiffrement de flux RC4 et le chiffrement par bloc. Ils ont inséré deux messages contenant le code d'authenticité (AC), qui sera accessible dans les domaines spatiaux et chiffrés. L'insertion et l'extraction dépendent de deux clés du tatouage. L'une d'elles est utilisée dans le domaine chiffré tandis que l'autre est utilisée dans le domaine spatial. Les résultats expérimentaux ont montré une faible distorsion de l'image et une capacité suffisante pour intégrer une preuve de fiabilité.

Une autre approche du tatouage cryptage conjoint a été proposée également par Bouslimi et al. [17]. L'algorithme du tatouage comprend deux techniques de tatouage : la technique du bit du poids faible LSB et la technique de la modulation d'indice de quantification, tandis que l'algorithme de cryptage est basé sur le chiffrement de flux RC4.

2.9.5 Les techniques de tatouage cryptage commutatif

Dans [136], l'image est cryptée au moyen d'une permutation aléatoire des positions des pixels sans changer leurs valeurs de gris. Cette dernière est tatouée en utilisant un

schéma de tatouage basé sur un histogramme avant ou après le processus de cryptage [31]. Néanmoins, ces fonctionnalités «invariantes» ou «non cryptées» peuvent être exploitées pour une attaque.

Roland Schmitz et al. [137] ont proposé une approche de tatouage cryptage commutatif. Un chiffrement de permutation est utilisé pour crypter les données multimédias. Par conséquent, tout schéma de tatouage non localisé qui ne dépend que de statistiques globales des données multimédias peut être combiné avec le chiffrement de permutation pour former un schéma du tatouage cryptage commutatif.

M. Cancellaro et al. [22] ont proposé un schéma du tatouage cryptage commutatif pour les images numériques. La propriété commutative du procédé proposé permet de chiffrer une image tatouée sans interférer avec la marque embarquée ou de tatouer une image chiffrée permettant toujours un déchiffrement parfait. Les deux opérations sont effectuées sur un domaine de transformation : la transformation de Haar (Tree Structured Haar transform). La dépendance clé du domaine de transformation adopté augmente la sécurité du système global. En fait, sans la connaissance de la clé génératrice, il n'est pas possible d'extraire des informations utiles de l'image chiffrée tatouée. Les résultats expérimentaux ont montré la robustesse de la méthode proposée contre les attaques de recadrages (cropping attacks).

2.10 Conclusion

Dans ce chapitre une notion générale de l'image médicale a été abordée avec une présentation sur l'ensemble des formats d'images utilisés pour la visualisation d'une partie d'un corps humain ou d'un organe donné afin d'apporter plus de précision à un diagnostic médical. En effet et à titre d'exemple la radiologie et l'échographie fournissent des informations et l'IRM fournit des images de grande qualité et des informations sur l'état biologique des tissus.

D'un point de vue informatique, les méthodes de tatouage numérique des images ont donné lieu à un certain nombre d'applications médicales dont le but est d'aider le médecin à travers la sécurisation des images médicales et des données de patients .

Plusieurs approches de tatouage d'images sont présentées dans ce chapitre. Ces approches sont classées en quatre catégories : la première regroupe l'ensemble d'approches de tatouage ROI/RONI, la deuxième l'ensemble d'approches de tatouage réversibles, la troisième l'ensemble d'approches de zéro-tatouage et la quatrième les approches de tatouage

hybride.

Les systèmes de tatouage ROI/RONI intègrent des marques dans les régions qui n'ont pas d'incidence sur le diagnostic médical. Les méthodes de tatouage réversible assurent la récupération de l'image originale précisément après l'extraction de la marque intégrée. Les méthodes de zéro-tatouage sont basées sur l'extraction de quelques caractéristiques robustes de l'image pour construire une marque et les approches de tatouage hybride combinent différentes méthodes de tatouage parmi les précédentes.

À la fin de ce chapitre, nous avons présenté les approches existantes combinant le tatouage numérique et la cryptographie qui sont classées en cinqs catégories notamment : le tatouage suivi du cryptage, le cryptage suivi du tatouage, le tatouage /décryptage conjoint, le tatouage /cryptage conjoint et le tatouage cryptage commutatif.

Nous nous sommes également intéressés aux applications de télémédecine où les besoins de sécurité de contenus doivent être précisés en fonction de règles législatives récentes. Le prochain chapitre porte essentiellement sur la description d'une approche de zéro-tatouage pour l'authentification des images médicales qui constitue la première contribution de cette thèse.

Chapitre 3

Une approche de zéro-tatouage pour l'authentification d'images DICOM basée sur le modèle Jacobien

3.1 Introduction

Avec le développement récent du télé-diagnostic et de la télémédecine, la quantité d'images médicales transférées à travers le réseau hospitalier a été considérablement augmentée. Ces images médicales sont généralement au format DICOM (Digital Imaging and Communications in Medicine). Le besoin des solutions pour l'authentification et la confidentialité de ces données est critique.

Ce chapitre présente une approche de zéro-tatouage pour l'authentification et l'identification des images DICOM. Le zéro-tatouage ne modifie pas les informations de l'image et satisfait donc le besoin de conserver les informations de diagnostic essentielles. La nouveauté de l'approche proposée repose sur deux points principaux. Le premier est l'approche de sélection des caractéristiques d'images, appelées caractéristiques pertinentes, qui sont utilisées pour l'identification de l'image. Ces caractéristiques sont sélectionnées à partir d'un large ensemble de caractéristiques d'images, en utilisant une approche d'analyse statistique qui vise à sélectionner l'ensemble minimal discriminant de caractéristiques ayant la plus grande résistance aux attaques existantes. Le second est le processus de construction de la clé basé sur la combinaison d'informations extraites de l'en-tête des images DICOM, des caractéristiques pertinentes et d'un modèle Jacobien. Cette clé est celle envoyée au récepteur pour l'authentification de l'image médicale. Les résultats expérimentaux montrent que l'approche proposée présente de très bonnes performances en termes d'authentification et d'identification des images médicales même en cas d'attaques

géométriques et non géométriques.

Ce chapitre est organisé comme suit. La section 3.2 présente les notions de base utilisées dans cette approche, ainsi que le principe du modèle Jacobien. La section 3.3 présente l'approche proposée, y compris le processus de génération et d'extraction de la marque. Les résultats expérimentaux sont illustrés dans la section 3.4. L'analyse du système proposé est discutée dans la section 3.4.2. L'étude comparative est abordée dans la section 3.5. La section 3.6 conclut le chapitre.

3.2 Les notions de base

Cette section présente les notions de base utilisées dans l'approche de zéro-tatouage proposée. Ces notions sont des paramètres statistiques utilisés pour la construction de la clé.

3.2.1 Les paramètres statistiques

Il existe de nombreuses caractéristiques statistiques descriptives utilisées pour analyser une image [92], [87], [75].

Elles peuvent être classées en catégories de caractéristiques statistiques du premier ordre, du deuxième ordre ou d'ordre supérieur [111].
Les caractéristiques statistiques de premier ordre décrivent la distribution du niveau de gris de l'image et les propriétés d'estimation (par exemple, la variance, la moyenne, l'asymétrie, l'aplatissement, etc.) des valeurs de pixel individuelles en supprimant l'interaction spatiale entre les pixels de l'image. Les caractéristiques statistiques du second ordre et d'ordre supérieur estiment les propriétés d'au moins deux valeurs de pixel se produisant à des emplacements spécifiques les unes par rapport aux autres, par exemple la matrice de cooccurrence. Dans ce travail, nous nous concentrons sur l'utilisation des caractéristiques statistiques de premier ordre de l'image. La raison principale est qu'elles nécessitent potentiellement moins de temps de calcul que les caractéristiques d'ordre supérieur.

Les caractéristiques statistiques du premier ordre sont utilisées dans cette approche, nous citons : l'histogramme de l'image, la moyenne, le maximum, le minimum, l'asymétrie, l'entropie, la plage, l'aplatissement, la variance, la médiane, la racine carré (RMS) et l'énergie. Elles sont présentées ci-après.

Notons $f(x, y)$ la fonction associée à une image de taille $N \times M$. Les variables x et y peuvent respectivement prendre les valeurs $x = 0, 1, \cdot; N - 1$ et $y = 0, 1, \cdot, M - 1$. La fonction $f(x, y)$ peut prendre des valeurs discrètes $0, 1\cdot, G-1$, où G correspond au nombre total de niveaux d'intensité dans l'image.

a) **L'histogramme d'intensité**

L'histogramme d'intensité est une fonction indiquant le nombre de pixels dans l'image entière pour chaque niveau d'intensité.

$$\text{h(i)} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \delta(f(x, y), i), where \begin{cases} i = 0, 1, \ldots, G-1 \\ x = 0, 1, \ldots, N-1 \\ y = 0, 1, \ldots, M-1 \end{cases}$$

(3.1)

Où $\delta(j, i)$ est la fonction Kronecker delta

$$\delta(j, i) = \begin{cases} 1, j = i \\ 0, j \neq i \end{cases} \tag{3.2}$$

L'histogramme de l'image est un simple résumé des informations statistiques contenues dans l'image. Étant donné que le calcul de l'histogramme du niveau de gris implique des pixels uniques, l'histogramme est considéré comme des paramètres statistiques de premier ordre de l'image. La densité de probabilité d'apparition approximative des niveaux d'intensité est obtenue en divisant les valeurs $h(i)$ par le nombre total de pixels dans l'image.

$$p(i) = h(i)/NM, o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.3}$$

b) **La moyenne**

La moyenne est l'intensité moyenne du niveau de gris de l'image. Si la moyenne est élevée, cela signifie que l'image est lumineuse. Si la moyenne est faible alors l'image est sombre. La moyenne peut être définie comme suit :

$$\mu = \sum_{i=0}^{G-1} ip(i), o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.4}$$

c) **La variance**

La variance donne la quantité de fluctuations du niveau de gris à partir de la valeur moyenne du niveau de gris de l'image, elle mesure la différence entre chaque i (intensité du niveau de gris) et la moyenne.

$$\sigma^2 = \sum_{i=0}^{G-1}(i-\mu)^2, o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.5}$$

d) **L'Écart type**

L'écart type est un paramètre statistique qui mesure la dispersion d'une variable statistique par rapport à sa moyenne. Il est calculé comme la racine carrée de la variance.

$$\sigma = \sqrt{\sigma^2}\sum_{i=0}^{G-1}(i-\mu^3)p(i) \tag{3.6}$$

e) **L'asymétrie (skewness)**

L'asymétrie est la mesure de la distribution des niveaux de gris autour de la moyenne. La valeur de l'asymétrie sera positive ou négative. La valeur négative indique que les données sont plus étalées à gauche de la moyenne qu'à droite. La valeur positive indique que les données sont plus étalées vers la droite. L'asymétrie est définie comme suit :

$$\mu_3 = \sigma^-3\sum_{i=0}^{G-1}(i-\mu^3)p(i), o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.7}$$

f) **Le coefficient d'aplatissement (Kurtosis)**

Le coefficient d'aplatissement est utilisé pour mesurer le pic de la distribution des valeurs d'intensité autour de la moyenne. La valeur élevée du coefficient d'aplatissement indique que le pic de la distribution est net et que la queue est plus longue et grasse. La faible valeur du coefficient d'aplatissement indique que le pic de la distribution est arrondi et que la queue est plus courte et plus fine.

Le coefficient d'aplatissement est défini comme suit :

$$\mu_4 = \sigma^-4\sum_{i=0}^{G-1}(i-\mu^4)p(i) - 3, o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.8}$$

g) **L'énergie**

La fonction d'énergie mesure l'uniformité de la distribution du niveau d'intensité. Si

la valeur est élevée, alors la distribution est à un petit nombre de niveaux d'intensité. L'énergie peut être définie comme suit ;

$$E = \sum_{i=0}^{G-1} [p(i)^2], o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.9}$$

h) **L'entropie**

L'entropie mesure l'uniformité de la distribution des intensités de niveaux de gris de l'image globale et indique la magnitude des informations de l'image. Une entropie très faible indiquerait que les pixels de l'image ont tous à peu près la même valeur. Une entropie plus élevée signifie que l'histogramme est plus proche d'une distribution uniforme.

$$H = -\sum_{i=0}^{G-1} p(i) log_2[p(i)], o\grave{u}\{i = 0, 1, ..., G-1\} \tag{3.10}$$

i) **Le maximum**

La fonction maximum décrit la valeur d'intensité maximale d'une image.

$$I_{max} = max\{f(x, y)\} \tag{3.11}$$

j) **Le minimum**

La fonction minimale décrit les valeurs d'intensité minimale d'une image.

$$I_{min} = min\{f(x, y)\} \tag{3.12}$$

k) **La plage**

La plage correspond à la différence entre les valeurs les plus élevées et les plus basses dans un ensemble de nombres. Pour calculer la plage, soustrayez le plus grand nombre du plus petit nombre de l'ensemble.

$$Plage = I_{max} - I_{min} \tag{3.13}$$

l) **La médiane**

La médiane est la valeur qui sépare la moitié inférieure et supérieure du tableau trié de valeurs de pixels de l'image.

m) **La moyenne quadratique (RMS)**

La fonction RMS est la racine carrée de la moyenne de la somme de toutes les valeurs

de pixels au carré.

$$RMS = \sqrt{\frac{1}{NM}\sum_{x=1}^{N}\sum_{y=1}^{M} f(x,y)^2} \tag{3.14}$$

n) **Le coefficient de variation**

Le coefficient de variation peut être utilisé pour mesurer la dispersion d'un ensemble de valeurs. Le coefficient de variation (C.V) peut être calculé par la formule suivante :

$$C.V = \frac{standard\,deviation}{mean} = \frac{\sigma}{\mu} \tag{3.15}$$

3.2.2 Le modèle Jacobien

Le modèle Jacobien est une matrice définie à partir d'une fonction vectorielle F et d'un point donné $(x_1, \ldots, x_n)R^n$. C'est la matrice des dérivées partielles du premier ordre d'une fonction vectorielle. Soit F une fonction définie de R^n à R^m, par ses m fonctions composantes à valeurs réelles, comme suit : modèle Jacobien est une matrice définie à partir d'une fonction vectorielle F et d'un point donné $(x_1, \ldots, x_n)R^n$. C'est la matrice des dérivées partielles du premier ordre d'une fonction vectorielle.
Soit F une fonction définie de R^n à R^m, par ses m fonctions composantes à valeurs réelles, comme suit :

$$F : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rightarrow \begin{pmatrix} f_1(x_1, \cdots, x_n) \\ \vdots \\ f_m(x_1, \cdots, x_n) \end{pmatrix}$$

Les dérivées partielles de ces fonctions à un point M, si elles existent, peuvent être organisées dans une matrice à m lignes et n colonnes, appelée matrice Jacobienne de F.

$$J_F(M) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

3.3 Description de l'approche proposée

Dans cette section, nous présentons le schéma proposé qui vise à construire un zéro-tatouage pour assurer l'authentification et l'identification des images DICOM lors de la transmission via un réseau de santé non sécurisé, ou pendant son utilisation ou son

stockage dans une base de données. Le système de zéro-tatouage proposé est basé sur l'extraction des caractéristiques de l'image hôte à l'aide d'une analyse statistique, l'extraction du nom du patient à partir de l'en-tête de l'image DICOM, la transformation des initiales du nom du patient (première lettre du prénom et du nom de famille) en une matrice binaire de taille 16×16, la génération d'une matrice de taille 16×16 à partir de l'image originale par un processus de soustraction cumulative et l'utilisation de cette matrice pour définir des fonctions Jacobiennes et générer une matrice Jacobienne. La matrice Jacobienne est utilisée pour construire une marque. L'organigramme de l'approche du zéro-tatouage proposé est illustré à la Figure 3.1. Les caractéristiques extraites de l'image originale ont été choisies parmi un grand ensemble de paramètres statistiques de premier ordre en appliquant une analyse statistique préliminaire sur une base de données de 100 images médicales et en sélectionnant le plus petit ensemble de paramètres offrant les meilleures capacités d'authentification des images même en cas d'attaques géométriques et non géométriques. Les images de la base de données ont été sélectionnées de manière à être aussi représentatives que possible des différents types d'images médicales utilisées pour le diagnostic. Nous présenterons d'abord cette étape d'analyse statistique préliminaire, puis nous présenterons les différentes étapes de l'approche du zéro-tatouage proposée.

3.3.1 Étape de prétraitement : sélection des caractéristiques à l'aide de l'analyse statistique

Le prétraitement est crucial dans le travail présenté dans ce chapitre. Il vise à trouver des caractéristiques appropriées à partir de l'image hôte pour une identification parfaite des images. Après le calcul des paramètres statistiques du premier ordre (moyenne, maximum, minimum, asymétrie, entropie, plage, kurtosis, variance, médiane, racine quadratique moyenne (RMS) et l'énergie) de chaque image, une analyse statistique de la base de données d'images est effectuée pour étudier la variabilité de notre base de données et de choisir les fonctionnalités pertinentes pour l'identification des images. L'analyse statistique est basée sur la mesure de la dispersion. Premièrement, nous sélectionnons les entités qui ont les valeurs les plus élevées de la plage statistique et les valeurs les plus élevées du coefficient de variation, puis nous calculons le plus petit ensemble de caractéristiques $\{f_1, f_2, \ldots f_n\}$ tel que pour toutes les paires d'images I et J de la base de données $(f_1(I),\ f_2(I),\ \ldots,\ f_n(I)) \neq (\mathrm{f}_1(J),\ f_2(J),\ \ldots,\ f_n(J))$ où $f_i(I)$ pour $i = 1, \ldots, n$ est la

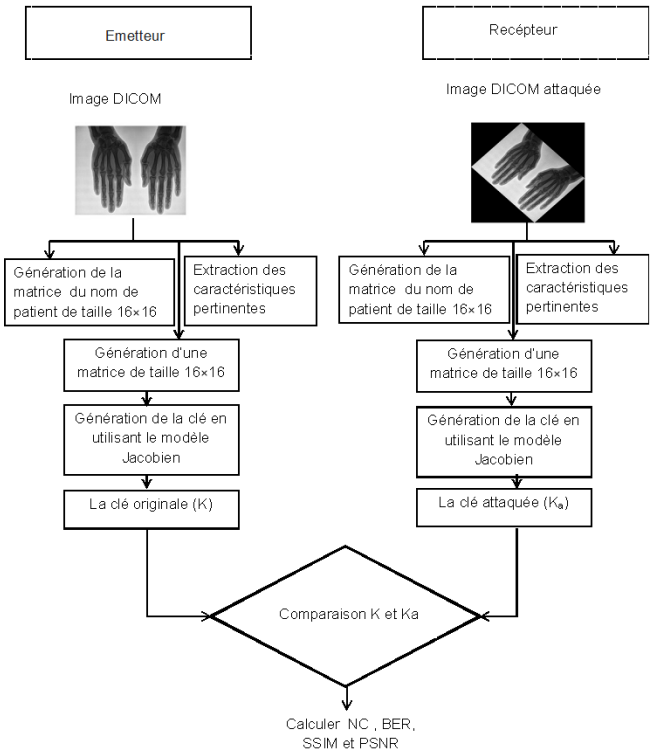


FIGURE 3.1 – L'organigramme de l'approche de zéro-tatouage proposée

valeur de la caractéristique f_i pour l'image I et $f_i(J)$ pour $i = 1, \ldots, n$ est la valeur de la caractéristique f_i pour l'image J. Ensuite, nous appliquons tout ce processus sur les images attaquées. La sélection finale des fonctionnalités est faite après l'application des attaques aux images de la base de données afin de prendre en compte la résistance des paramètres statistiques aux attaques. L'algorithme d'analyse statistique pour la sélection des caractéristiques peut être résumé comme suit :

1. Calculer les paramètres statistiques suivants : moyenne, maximum, minimum, asymétrie, entropie, plage, coefficient d'aplatissement (kurtosis), variance, médiane, moyenne quadratique (RMS) et énergie.
2. Analyser la dispersion des valeurs de chaque paramètre statistique sur l'ensemble de la base de données. Cette dispersion est mesurée à l'aide de la plage et du coefficient de variation.
3. Sélectionner le plus petit ensemble de paramètres ayant les valeurs de dispersion les plus élevées, et permettant d'identifier de manière unique chaque image de la base de données.
4. Appliquer différentes attaques géométriques et non géométriques sur les images de la base de données.
5. Répéter les étapes 1 et 2 ci-dessus sur les images attaquées pour sélectionner les caractéristiques pertinentes qui résistent le plus aux attaques.

Les éléments de l'ensemble sélectionné de caractéristiques sont des paramètres statistiques utilisés comme entrée dans le modèle Jacobien afin de construire la clé envoyée au récepteur pour l'authentification d'image. L'application de l'analyse statistique ci-dessus sur notre base de données de 100 images médicales conduit à sélectionner les trois paramètres suivants : l'asymétrie, l'entropie et la médiane

3.3.2 Étape 1. Extraction des caractéristiques pertinentes de l'image DICOM pour un zéro-tatouage

Cette étape consiste à calculer les valeurs des paramètres statistiques sélectionnés à l'issue de l'étape de prétraitement, à savoir l'asymétrie, l'entropie et la médiane.

3.3.3 Étape 2. Extraction du nom du patient et transformation des initiales en image logo binaire

Après avoir analysé l'en-tête de l'image DICOM, nous extrayons la première lettre du nom de famille et la première lettre du prénom pour construire la marque. L'extraction du nom du patient est décrite en détail dans l'algorithme 1 :

Algorithm 1 Extraction du nom et du prénom du patient de l'en-tête DICOM

Résultat : le nom et le prénom du patient sous forme de matrice binaire 16×16 (logo binaire)
Entrée : image originale I
Début : Ouvrir l'image DICOM
Lire l'en-tête de l'image DICOM
Lire le nom du patient (prénom et nom de famille)
Prendre la première lettre du prénom et la première lettre du nom de famille
Concaténer la première lettre du prénom et la première lettre de nom de famille
Convertir les deux caractères du nom du patient en un logo en niveaux de gris au format 16×16
Convertir le logo en niveaux de gris en un logo binaire de taille 16×16 par le processus de binarisation
Fin

Dans la figure 3.2, nous présentons l'extraction du nom du patient pour quatre images DICOM.

3.3.4 Étape 3. Génération d'une matrice de taille 16×16 à partir de l'image hôte

Dans le processus de génération de la marque, l'image originale est partitionnée en blocs non superposés de taille 16×16, chaque bloc est considéré comme une entrée dans un processus de soustraction cumulative dont le résultat est une matrice de taille 16×16. Le processus de soustraction commence en définissant une matrice nulle appelée add_{mat} de taille 16×16 et en soustrayant le premier bloc 16×16 de l'image originale et le bloc 16×16 de la matrice add_{mat}. L'algorithme 2 fournit le pseudo-code de ce processus.

La figure 3.3 montre un exemple de la matrice add_{mat} générée à partir de l'image originale de la figure 3.2.

FIGURE 3.2 – Extraction des noms des patients à partir de l'image DICOM

Algorithm 2 Génération d'une matrice de taille 16 × 16 à partir de l'image originale

Résultat : add_{mat} matrice de taille 16 × 16
Entrée : l'image originale I de taille $n \times m$
Initialisation : $add_{mat} = zéros(16\times16)$,i = 1,j = 1 ;
Début
Partitionnement de l'image I en blocs de 16 × 16
tant que $i < 256$ faire
    tant que $j < 256$ faire
        $add_{mat} = I(i : i + 15; j : j + 15) - add_{mat}$;
$j\leftarrow$ j + 16 ;
fin tant que
$i\leftarrow$ i + 16 ;
j ← 1;
    fin tant que
//Normalisation des valeurs matricielles entre [0,255].
$min_{Val} \leftarrow min(\text{add}_{mat}(\text{i,j}))$
$max_{Val} \leftarrow max(\text{add}_{mat}(\text{i,j}))$.
$add_{mat}(\text{i,j}) \leftarrow floor(((\text{add}_{mat}(\text{i,j}) - min_{Val}\ ) / (max_{Val} - min_{Val})) \times 255)$
Fin

$add_{mat}(x_1, ..., x_{16})$=

$$\begin{pmatrix}
146 & 135 & 162 & 127 & 55 & 62 & 97 & 167 & 161 & 112 & 133 & 198 & 191 & 111 & 101 & 73 \\
196 & 204 & 173 & 178 & 39 & 83 & 107 & 199 & 205 & 70 & 247 & 211 & 197 & 123 & 83 & 79 \\
137 & 156 & 92 & 146 & 40 & 146 & 90 & 97 & 183 & 123 & 198 & 211 & 181 & 104 & 131 & 0 \\
176 & 124 & 148 & 52 & 54 & 30 & 112 & 132 & 127 & 173 & 139 & 205 & 156 & 139 & 4 & 45 \\
88 & 145 & 123 & 133 & 123 & 77 & 126 & 102 & 117 & 115 & 224 & 122 & 117 & 144 & 76 & 156 \\
55 & 163 & 162 & 211 & 166 & 102 & 182 & 130 & 178 & 137 & 202 & 112 & 144 & 147 & 168 & 71 \\
51 & 62 & 148 & 135 & 113 & 111 & 182 & 253 & 148 & 150 & 106 & 106 & 68 & 184 & 177 & 138 \\
20 & 103 & 59 & 112 & 193 & 113 & 145 & 246 & 150 & 109 & 148 & 42 & 74 & 176 & 235 & 200 \\
109 & 82 & 80 & 85 & 107 & 145 & 134 & 186 & 173 & 110 & 183 & 112 & 147 & 121 & 172 & 148 \\
139 & 59 & 148 & 149 & 89 & 145 & 203 & 175 & 184 & 78 & 156 & 156 & 131 & 148 & 90 & 171 \\
93 & 119 & 229 & 138 & 148 & 104 & 111 & 137 & 102 & 216 & 125 & 81 & 174 & 103 & 90 & 125 \\
169 & 100 & 99 & 198 & 198 & 180 & 158 & 198 & 132 & 185 & 188 & 133 & 87 & 181 & 94 & 80 \\
133 & 117 & 211 & 146 & 190 & 190 & 39 & 111 & 154 & 110 & 193 & 240 & 122 & 121 & 66 & 104 \\
140 & 102 & 199 & 206 & 211 & 74 & 160 & 191 & 148 & 110 & 138 & 110 & 126 & 111 & 176 & 114 \\
96 & 214 & 156 & 255 & 229 & 149 & 187 & 206 & 136 & 165 & 88 & 51 & 144 & 140 & 198 & 96 \\
102 & 142 & 145 & 214 & 90 & 155 & 223 & 157 & 153 & 102 & 69 & 43 & 122 & 222 & 130 & 222
\end{pmatrix}$$

FIGURE 3.3 – La matrice add_{mat} de taille 16 × 16 générée à partir de l'image originale

3.3.5 Étape 4. Génération des clés à l'aide du modèle Jacobien

Sur la base du modèle Jacobien présenté dans la sous-section 3.1, 16 fonctions avec 16 paramètres sont utilisées pour générer une matrice de taille 16×16 qui est utilisée pour construire une clé en tant qu'image significative. Ces fonctions sont construites en utilisant la matrice de logo binaire générée à l'étape 2, les trois caractéristiques pertinentes (asymétrie, entropie et médiane) extraites de l'image hôte à l'étape 1 et la matrice add_{mat} générée à partir de l'image hôte à l'étape 3. Le modèle Jacobien proposé se compose de 16 fonctions :

$$Y_i : R^{16} \rightarrow R^{16}, i = 1, 2, \ldots, 16 \tag{3.16}$$

Ces fonctions $Y_1, Y_2, \cdots, Y_{16}$ sont définies par

$$Y_i(x_1, x_2, \ldots, x_{16}) = \sum_{j=1}^{16} \frac{add\_mat(i,j)}{f\_val_i} \frac{x_j^2}{2}, j = 1, \ldots, 16 \tag{3.17}$$

Où f_val_i est défini comme suit :

$$f_{val_i} = \begin{cases} lavaleurdel'asymetrie & si \quad 1 \leq i \leq 5 \\ lavaleurdel'entropie & si \quad 6 \leq i \leq 10 \\ lavaleurdemediane & si \quad 11 \leq i \leq 16 \end{cases} \tag{3.18}$$

La matrice Jacobienne J de Y en (x_1, x_2,..., x_{16}) est une matrice de taille 16×16 donnée par

$J_Y(x_1, \ldots, x_{1_6})$=

$$\begin{bmatrix} \frac{add\_mat(1,1)}{f\_val_1}x_1 & \cdots & \frac{add\_mat(1,16)}{f\_val_1}x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(5,1)}{f\_val_1}x_1 & \cdots & \frac{add\_mat(5,16)}{f\_val_1}x_{16} \\ \frac{add\_mat(6,1)}{f\_val_2}x_1 & \cdots & \frac{add\_mat(6,16)}{f\_val_2}x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(10,1)}{f\_val_2}x_1 & \cdots & \frac{add\_mat(10,16)}{f\_val_2}x_{16} \\ \frac{add\_mat(11,1)}{f\_val_3}x_1 & \cdots & \frac{add\_mat(11,16)}{f\_val_3}x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(16,1)}{f\_val_3}x_1 & \cdots & \frac{add\_mat(16,16)}{f\_val_3}x_{16} \end{bmatrix}$$

Cette matrice Jacobienne de taille 16×16 est une matrice d'image utilisée comme clé pour le zéro-tatouage. Par exemple, la matrice Jacobienne de l'image "Hands" (première image originale) de la figure 3.2 obtenue au point (1, 1,. . ., 1) est :

$J_f(1, 1, \ldots, 1)=$

$$\begin{bmatrix}
14 & 13 & 16 & 12 & 5 & 4 & 7 & 12 & 11 & 8 & 5 & 8 & 8 & 4 & 4 & 3 \\
19 & 20 & 17 & 18 & 3 & 6 & 7 & 14 & 14 & 5 & 10 & 8 & 8 & 5 & 3 & 3 \\
13 & 15 & 9 & 14 & 4 & 10 & 6 & 7 & 13 & 8 & 8 & 8 & 7 & 4 & 5 & 0 \\
17 & 12 & 14 & 5 & 5 & 2 & 8 & 9 & 9 & 12 & 5 & 8 & 6 & 5 & 0 & 1 \\
8 & 14 & 12 & 13 & 12 & 5 & 9 & 7 & 8 & 8 & 9 & 5 & 4 & 6 & 3 & 6 \\
5 & 16 & 0 & 21 & 16 & 7 & 0 & 9 & 12 & 9 & 8 & 4 & 6 & 6 & 7 & 2 \\
5 & 0 & 0 & 13 & 11 & 8 & 0 & 18 & 10 & 10 & 4 & 4 & 2 & 7 & 7 & 5 \\
2 & 0 & 0 & 11 & 19 & 8 & 0 & 17 & 10 & 7 & 6 & 0 & 3 & 7 & 0 & 8 \\
11 & 8 & 0 & 0 & 0 & 0 & 0 & 13 & 12 & 7 & 7 & 0 & 6 & 5 & 0 & 6 \\
14 & 5 & 0 & 0 & 0 & 0 & 0 & 12 & 13 & 5 & 6 & 0 & 5 & 6 & 0 & 7 \\
9 & 0 & 0 & 13 & 14 & 7 & 0 & 9 & 7 & 15 & 5 & 0 & 7 & 4 & 0 & 5 \\
17 & 0 & 0 & 20 & 20 & 13 & 0 & 14 & 9 & 13 & 7 & 0 & 3 & 7 & 0 & 3 \\
13 & 0 & 0 & 14 & 19 & 13 & 0 & 8 & 11 & 7 & 8 & 0 & 5 & 0 & 0 & 4 \\
14 & 10 & 0 & 20 & 21 & 5 & 0 & 13 & 10 & 7 & 5 & 4 & 0 & 4 & 0 & 4 \\
9 & 21 & 15 & 25 & 23 & 10 & 13 & 14 & 9 & 11 & 3 & 2 & 6 & 5 & 8 & 4 \\
10 & 14 & 14 & 21 & 9 & 11 & 16 & 11 & 11 & 7 & 2 & 1 & 5 & 9 & 5 & 9
\end{bmatrix}.$$

L'image correspondant à cette matrice est représentée dans la figure 3.4. Après le processus de génération, la clé est envoyée au récepteur. La figure 3.5 résume le processus de génération de la clé côté émetteur.

Pendant son transfert vers le récepteur, l'image originale peut être attaquée avec diverses attaques géométriques et non géométriques. On suppose que la clé générée côté émetteur n'est pas attaquée lors de son transfert vers le récepteur. Le récepteur peut générer la clé à partir de l'image attaquée en appliquant les mêmes étapes que l'expéditeur. Après l'extraction de la clé, le récepteur la compare à la clé originale reçue de l'expéditeur à l'aide des paramètres tel que le NC, le BER, le SSIM et le PSNR. Les clés sont considérées comme similaires lorsque les valeurs de NC et de SSIM sont supérieures à des seuils donnés et que les valeurs de BER sont inférieures à un seuil donné. La figure 3.6 présente le processus d'extraction et de comparaison de la clé côté récepteur. La mise en œuvre de la méthode proposée a été effectuée sur un ordinateur doté d'un processeur Intel (R) core

FIGURE 3.4 – La clé générée à partir de l'image originale "Hands" de la figure 3.2

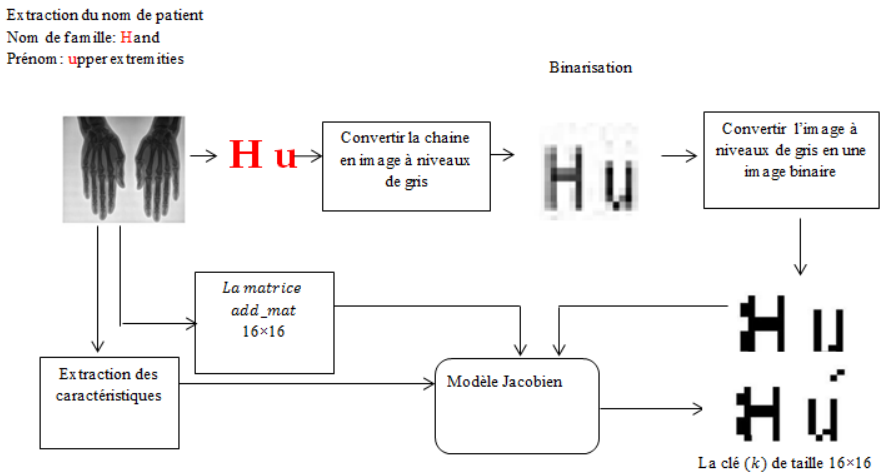


FIGURE 3.5 – Le processus de la génération de la clé côté émetteur

(TM) i7-3770 à 3,40 GHz et de 8 Go de RAM à l'aide du logiciel MATLAB R2016a. La méthode a été exclusivement testée sur une base de données DICOM.

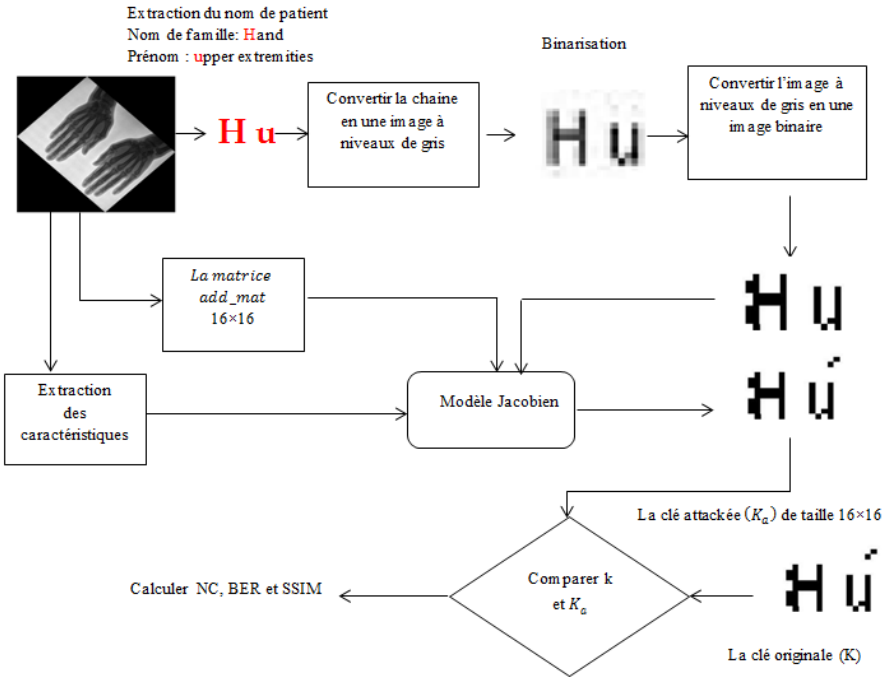


FIGURE 3.6 – Le processus d'extraction et de comparaison de la clé originale avec la clé extraite côté récepteur

3.4 Expérimentation et analyse des résultats

Dans cette section, nous présentons les expérimentations effectuées afin d'évaluer les performances de l'approche de zéro-tatouage proposée, puis nous discutons les résultats obtenus.

Les expérimentations se font en trois étapes, la première étape consiste à appliquer l'approche de zéro-tatouage à un ensemble d'images originales sans attaques et à vérifier si la clé est bien reconstruite côté récepteur. La seconde étape consiste à appliquer l'approche de zéro-tatouage sur le même ensemble d'images tout en considérant les attaques sur les images lors de leur transfert vers le récepteur.

La troisième étape permet d'évaluer les performances de l'approche proposée contre les attaques.

La figure 3.8 illustre l'effet des attaques sur toutes les images hôtes, ainsi que la clé attaquée extraite dans chaque cas. Nous pouvons remarquer visuellement l'effet de différents types d'attaques sur l'image originale. Nous pouvons observer la variation des images attaquées et la variation des clés attaquées extraites à partir de différentes images attaquées.

3.4.1 Les résultats expérimentaux

Les performances de l'approche proposée sont testées sur une large base de données de 100 images médicales. Nous présentons ici un échantillon d'images DICOM utilisées dans l'expérimentation. Les images originales utilisées pour étudier les performances de l'algorithme proposé de zéro tatouage, les clés générées et les valeurs pondérées des caractéristiques pertinentes (asymétrie, entropie et médiane) sont présentées dans la figure 3.7.

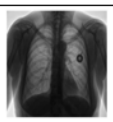
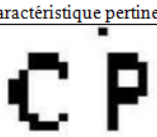
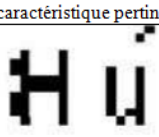
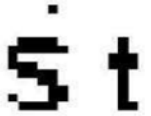
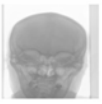
Image originale (i)	Clé originale (k) et caractéristique pertinentes	Image originale (i)	Clé originale (k) et caractéristique pertinentes
 Chest	 (11.2918, 13.2109, 8.75)	 Hands	 (9.8825, 13.7971, 23.78)
 Tspine	 (11.3533, 13.3749, 13.07)	 Skull	 (10.4331,12.8666, 28.11)

FIGURE 3.7 – Les images originales, les clés générées correspondantes (K) et les valeurs des caractéristiques pondérées

Le tableau 3.2 présente les valeurs de NC, de BER et de SSIM entre les clés originales et extraites en l'absence d'attaques pour les images originales présentées dans la figure 3.7.

Selon le tableau 3.2 , lorsque l'image originale n'est pas attaquée, la valeur de NC est égale à 1, la valeur de BER est égale à 0 et la valeur du SSIM est égale à 1 donc la clé reconstruite par le récepteur est exactement identique à la clé originale crée par l'expéditeur.

TABLE 3.1 – Les valeurs de NC, BER et SSIM entre les clés originales et les clés extraites

Images	NC	BER	SSIM
Hands	1	0	1
Chest	1	0	1
Skull	1	0	1
Tspine	1	0	1

Les performances sous les attaques

Afin d'évaluer les performances de notre modèle, nous considérons certaines attaques géométriques et non géométriques dans nos expériences. Ces attaques incluent le filtrage médian, le bruit du sel et du poivre, le filtrage moyen, le recadrage, le bruit Gaussien, l'égalisation d'histogramme, la rotation, l'affûtage et la translation. La Figure 3.8 montre les images attaquées, les clés attaquées extraites correspondantes et les valeurs pondérées des caractéristiques pertinentes extraites (asymétrie, entropie et médiane).
À partir de la figure 3.8, nous pouvons voir l'effet des attaques sur toutes les images originales, ainsi que la variation des clés attaquées extraites et les valeurs des caractéristiques pertinentes extraites qui sont l'asymétrie, l'entropie et la médiane dans chaque cas.

Afin de quantifier les résultats du système de tatouage proposé, nous calculons le taux d'erreur sur les bits (BER), le coefficient de corrélation normalisé (NC), la métrique d'indice de similarité de structure (SSIM), le rapport signal sur bruit - Peak Signal to Noise Ratio (PSNR) et le temps d'exécution.
Les tableaux **??**, 3.3, 3.4 et tableau 3.5 présente les valeurs de NC, de SSIM, de BER et de PSNR calculées entre la clé construite à partir de l'image originale et la clé construite à partir de l'image tatouée attaquée, ainsi que leurs valeurs moyennes respectives pour les différentes attaques.
Les tableaux 3.6 et 3.7 présentent le temps d'exécution en secondes pour générer les clés à partir des images originales ainsi que le temps d'exécution en secondes pour extraire les clés des images attaquées.

3.4.2 Analyse des résultats

Les résultats expérimentaux dans le tableau 3.2 prouvent que la clé originale est précisément récupérée en absence d'attaques, ce qui illustre que l'approche proposée réus-

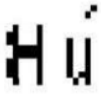
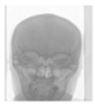
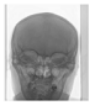
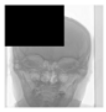
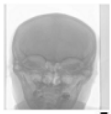
Nom de l'image	Type d'attaque				
	Le filtre median 3 × 3	Le bruit du sel et du poivre (0.01)	Le filtrage moyen 3 × 3	Recadrage 25%	Le filtre Gaussian 3 × 3
Hands					
Les clés					
Les caractéristiques	(9.8696, 13.7334, 23.81)	(22.6706,13.8498, 23.78)	(9.8705, 13.7189, 23.75)	(10.1388,13.5990, 16.34)	(9.8702, 13.7234, 23.77)
Chest					
Les clés					
Les caractéristiques	(11.2952,1 3.2063, 8.75)	(23.4828, 13.2670, 8.75)	(11.2945,1 3.2048, 8.74)	(11.5786,1 2.8399, 6)	(11.2939,1 3.2056, 8.74)
Tspine					
Les clés					
Les caractéristiques	(10.3695,1 3.3625, 13.05)	(33.3774, 11.6402, 0)	(11.3666,1 3.3609, 13.06)	(11.1534,13.1673, 10.41)	(11.3659,1 3.3616, 13.06)
Skull					
Les clés					
Les caractéristiques	(10.4354,1 2.8627, 28.11)	(23.5436, 12.9286,28.11)	(10.4377,1 2.8647, 28.08)	(9.393, 12.9873, 25.49)	(10.4386, 12.8639, 28.08)

FIGURE 3.8 – Les images tatouées attaquées, leurs clés attaquées extraites et leurs valeurs de caractéristiques pertinentes extraites correspondantes

TABLE 3.2 – Les valeurs de NC entre la clé originale et la clé attaquée

Les attaques	Les valeurs de NC				la moyenne de NC
	Hands	Chest	Tspine	Skull	
Le filtrage median 3×3	0.9462	1	0.8368	0.9881	0.9427
Le filtrage median 5×5	0.3014	0.9732	0.8215	0.9881	0.7710
Le bruit du sel et du poivre (0.01)	0.9560	0.9315	0.9574	0.7948	0.9099
Le bruit du sel et du poivre (0.03)	0.9563	0.9706	0.9562	0.8087	0.9229
Le filtrage moyen 3×3	0.9603	0.9857	0.8290	0.9881	0.9407
Recadrage du coin supérieur gauche 25%	0.9731	1	0.7748	0.6301	0.8445
Filtre passe bas Gaussien 3×3	0.9612	1	0.8461	0.9881	0.9488
L'égalisation d'histogramme	0.4746	0.4870	0.4132	0.5968	0.4929
Le bruit Gaussien (0.0001)	0.9583	0.9717	0.9414	0.8011	0.9181
Le bruit Gaussien (0.01)	0.9426	0.9854	0.9311	0.7868	0.9114
Le bruit Gaussien (0.05)	0.9596	0.9303	0.8687	0.8335	0.8980
Le bruit Gaussian (20)	0.9452	0.9189	0.9419	0.8095	0.9038
La rotation 5°	0.9447	0.9718	0.9556	0.8322	0.9260
La rotation 10°	0.9580	0.9707	0.9407	0.8211	0.9226
La rotation 45°	0.3047	0.9711	0.9561	0.8205	0.7631
La rotation 90°	0.9245	0.9595	0.9575	0.8222	0.9159
L'affûtage	1	1	0.9847	0.9561	0.9852
La translation (10)	0.9068	0.9182	0.9143	0.9758	0.9287

TABLE 3.3 – Les valeurs de SSIM entre entre la clé originale et la clé attaquée

Les attaques	Les valeurs de SSIM				La moyenne de SSIM
	Hands	Chest	Tspine	Skull	
Le filtrage median 3×3	0.9784	0.9829	0.8211	0.9961	0.9446
Le filtrage median 5×5	0.9748	0.9760	0.7985	0.9961	0.9363
Le bruit du sel et du poivre (0.01)	0.9420	0.9668	0.9404	0.9219	0.9427
Le bruit du sel et du poivre (0.03)	0.9624	0.9810	0.9455	0.9377	0.9566
Le filtrage moyen 3×3	0.9741	0.9895	0.7999	0.9961	0.9399
Recadrage du coin supérieur gauche 25%	0.9844	1	0.8574	0.8463	0.9220
Filtre passe bas Gaussien 3×3	0.9874	1	0.8101	0.9961	0.9484
L'égalisation d'histogramme	0.5833	0.6342	0.5108	0.6093	0.5844
Le bruit Gaussien (0.0001)	0.9620	0.9829	0.9430	0.9397	0.9569
Le bruit Gaussien (0.01)	0.9677	0.9867	0.9450	0.9219	0.9553
Le bruit Gaussien (0.05)	0.9779	0.9131	0.8819	0.9487	0.9304
Le bruit Gaussien (20)	0.9606	0.9185	0.9351	0.9351	0.9373
La rotation 5°	0.9782	0.9846	0.9510	0.9304	0.9610
La rotation 10°	0.9854	0.9622	0.9273	0.9588	0.9584
La rotation 45°	0.9838	0.9755	0.9456	0.9555	0.9651
La rotation 90°	0.9574	0.9383	0.9517	0.9575	0.9512
L'affûtage	1	1	0.9724	0.9880	0.9901
La translation (10)	0.9107	0.9572	0.8838	0.9904	0.9355

TABLE 3.4 – Les valeurs de BER entre entre la clé originale et la clé attaquée

Les attaques	Les valeurs de BER				la moyenne de BER
	Hands	Chest	Tspine	Skull	
Le filtrage median 3×3	0.0162	0.0082	0.0569	0.0045	0.0214
Le filtrage median 5×5	0.0191	0.0073	0.0645	0.0045	0.0238
Le bruit du sel et du poivre (0.01)	0.0197	0.0197	0.0233	0.0706	0.0333
Le bruit du sel et du poivre (0.03)	0.0115	0.0081	0.0116	0.0674	0.0246
Le filtrage moyen (3×3)	0.0113	0.0046	0.0609	0.0045	0.0203
Le filtrage moyen (2×2)	0.0114	0.0073	0.0368	0.0045	0.015
Recadrage du coin supérieur gauche	0.0082	0	0.0804	0.1415	0.0575
Le filtre passe bas Gaussien (3×3)	0.0113	0	0.0532	0.0045	0.0172
L'egalisation d'histogramme	0.3087	0.2883	0.3401	0.2302	0.2918
Le bruit Gaussien (0.0001)	0.0118	0.0073	0.0155	0.0701	0.0261
Le bruit Gaussien (0.01)	0.0162	0.0037	0.0187	0.0750	0.0284
Le bruit Gaussien (0.05)	0.0118	0.0190	0.0387	0.0596	0.0322
Le bruit Gaussien (20)	0.0153	0.0247	0.0157	0.0596	0.0288
La rotation 5°	0.0170	0.0072	0.0110	0.0588	0.0235
La rotation 10°	0.0120	0.0071	0.0151	0.0632	0.0243
La rotation 45°	0.0118	0.0076	0.0118	0.0645	0.0239
La rotation 90°	0.0231	0.0106	0.0115	0.0637	0.0272
L'affûtage	0	0	0.0039	0.0151	0.0047
La translation (10)	0.0268	0.0220	0.0238	0.0085	0.0202

TABLE 3.5 – Les valeurs de PSNR entre entre la clé originale et la clé attaquée

Les attaques	Les valeurs de PSNR				la moyenne de PSNR
	Hands	Chest	Tspine	Skull	
Le filtrage median 3×3	51	42	50	52	49
Le filtrage median 5×5	53	42	51	53	50
Le bruit du sel et du poivre (0.01)	35	30	27	35	32
Le bruit du sel et du poivre (0.03)	40	38	42	45	41
Le filtrage moyen (3×3)	60	60	50	44	54
Le filtrage moyen (2×2)	58	60	48	44	53
Recadrage du coin supérieur gauche	44	40	49	50	46
Le filtre passe bas Gaussien (3×3)	61	50	50	60	55
L'egalisation d'histogramme	50	44	55	61	53
Le bruit Gaussien (0.0001)	31	27	42	45	36
Le bruit Gaussien (0.01)	31	27	42	46	37
Le bruit Gaussien (0.05)	31	28	42	46	37
Le bruit Gaussien (20)	32	30	50	46	40
La rotation 5°	29	31	27	30	29
La rotation 10°	30	33	30	35	32
La rotation 45°	40	39	35	41	39
La rotation 90°	51	44	44	48	47
L'affûtage	55	50	56	60	55
La translation (10)	42	44	53	52	48

TABLE 3.6 – Performances de la clé générée à partir des images originales en termes de temps d'exécution en secondes

Nom de l'image	Temps d'éxecution de l'algorithme proposé en secondes
Hands	8.5194
Chest	8.6325
Skull	8.2947
Tspine	8.9225

TABLE 3.7 – Performances de la clé extraites à partir des images attaquées en termes de temps d'exécution en secondes.

Nom de l'image	Le filtre median 5×5	Le filtre median 3×3	Le bruit du sel et du poivre (0.01)	Le bruit du sel et du poivre(0.03)
Hands	8.5079	8.5490	8.7899	8.8855
Chest	8.0677	8.6827	8.0196	8.6445
Tspine	7.9039	8.3507	7.8502	8.2975
Skull	8.0359	8.5701	8.1359	8.4539

Nom de l'image	Le filtre moyen 3×3	Recadrage du coin supérieur gauche 25%	Filtre passe bas Gaussien 3×3
Hands	8.9479	9.1983	8.7678
Chest	8.6813	8.7617	8.7302
Tspine	8.2868	8.3097	8.8353
Skull	8.4765	8.5413	8.3802

Nom de l'image	L'égalisation d'histogramme	Le bruit_0.01	Le bruit_20	Le bruit_ 0.05
Hands	8.7435	8.2790	8.2460	8.8823
Chest	8.5898	8.1559	8.3320	8.5605
Tspine	8.3389	7.8672	8.0827	8.2170
Skull	8.4600	8.3016	8.2757	8.4985

Nom de l'image	La rotation 45°	La rotation 10°	La rotation 5°	L'affûtage
Hands	13.3256	9.5312	8.6055	8.6149
Chest	12.1990	9.5060	8.5886	8.6220
Tspine	13.2390	9.6250	8.9531	8.2093
Skull	13.7535	9.7366	9.0588	8.6939

Nom de l'image	La translation (10)	la valeur moyenne du temps d'éxecution
Hands	8.7742	9.0405
Chest	8.7876	8.8080
Tspine	8.3248	8.6681
Skull	8.3591	8.8582

sit dans le but d'identification et d'authentification. Les valeurs de NC du tableau 3.3 montrent que l'algorithme proposé est robuste contre différentes attaques géométriques et non géométriques telles que le filtrage médian, le filtrage moyen, le filtrage Gaussien, le bruit de sel et de poivre, le recadrage, l'égalisation d'histogramme, le bruit Gaussien, la rotation, la translation et l'affûtage.

En effet, il ressort du tableau 3.3 que les valeurs moyennes de NC sont proches ou supérieures à 0,8 pour la plupart des attaques (filtrage médian, bruit sel et poivre, filtrage moyen, recadrage, bruit Gaussien, rotation et translation). De plus, il existe une excellente valeur NC (NC = 1) dans le cas du filtrage médian (3×3), du recadrage du coin supérieur gauche, du filtrage gaussien (3×3) et de l'affûtage appliqué à l'image « Chest ». Dans ces cas, la clé originale et la clé extraite sont absolument identiques. L'attaque qui a en moyenne le pire impact sur la qualité de la clé extraite est l'égalisation d'histogramme (la valeur moyenne de NC la plus basse est égale à 0,49). Le pire résultat pas en moyenne est obtenu dans le cas de l'image « Hands » lors de l'application de l'attaque du filtrage médian 5×5 ou de l'attaque rotation 45 (valeur NC autour de 0,30). Le tableau 3.3 montre que la valeur moyenne de SSIM entre la clé générée à partir de l'image originale et la clé extraite de l'image attaquée est proche de $0,92$. Il montre que la méthode proposée assure une bonne robustesse contre les attaques. Néanmoins, on note que toutes les images médicales testées sont influencées par l'attaque d'égalisation d'histogramme (le SSIM moyen est égal à 0,58). En revanche, nous notons que lors de l'application du recadrage dans le coin supérieur gauche (25%), du filtrage Gaussien (3×3) et des attaques de l'affûtage sur l'image « Chest » et de l'attaque de l'affûtage sur l'image « Hands », nous avons des valeurs de SSIM égales à 1 ce qui signifie que la clé originale et la clé extraite sont visuellement assez identiques. Concernant les valeurs de PSNR dans le tableau 3.5, on peut conclure que dans le cas de certaines attaques telles que le filtre passe-bas Gaussien, l'affûtage, l'égalisation d'histogramme et le filtrage moyen, la méthode proposée a des valeurs de PSNR supérieures à 50 dB. La valeur moyenne du PSNR est égale à 44 dB. En analysant les valeurs de BER du tableau 3.4, nous pouvons voir que les valeurs moyennes de BER du schéma proposé ne dépassaient pas 0,06 sauf pour l'attaque d'égalisation d'histogramme dont la valeur moyenne de BER est élevée (0,2918). Cela signifie que l'approche proposée présente en général une bonne robustesse contre les attaques.
Les résultats du BER sont particulièrement bons dans le cas de l'application d'attaques de recadrage en haut à gauche et de filtrage Gaussien (3×3) sur l'image « Chest » et en

cas d'application d'attaque de l'affûtage sur les images « Hands », « Chest » et «Tspine » (la valeur du BER est égale à 0).
En analysant le tableau 3.6, nous notons que le temps d'exécution moyen pour générer une clé à partir de l'image hôte est de 8,6 secondes. De plus, le temps d'exécution requis pour extraire la clé attaquée à partir des images tatouées attaquées ne dépassait pas 9 secondes en moyenne (la moyenne sur toutes les attaques). En balayant le temps d'exécution de toutes les images contre les différents types d'attaques, on peut conclure que les pires résultats sont obtenus dans le cas de l'attaque rotation à 45°, où les temps d'exécution sont proches de 13 secondes. Les résultats mentionnés dans le tableau 3.7 prouvent l'applicabilité de l'approche de zéro-tatouage proposée dans les applications de soins de santé en temps réel. En effet, la durée des interventions médicales (chirurgie, consultation,...) est le plus souvent de plusieurs minutes. Un temps d'exécution inférieur à une minute est donc tout à fait acceptable dans un tel contexte. Enfin, les résultats expérimentaux montrent que les valeurs moyennes de BER, NC, SSIM et PSNR pour toutes les attaques sont respectivement de 3%, 88%, 92% et 44 dB. Ces résultats prouvent que l'approche proposée est robuste face aux attaques géométriques et non géométriques

3.5 Étude comparative du schéma proposé avec les schémas de zéro-tatouage existants

Les performances du schéma de zéro-tatouage proposé sont comparées aux schémas de zéro-tatouage proposés dans [50], [162], [142], [46]. La robustesse contre différents types d'attaques et le temps d'exécution sont pris en compte dans l'étude comparative.

3.5.1 Comparaison du BER du modèle proposé avec les modèles de zéro-tatouage existants

Le tableau 3.8 montre les résultats du BER de notre approche proposée et les résultats du BER des approches proposées dans [50], [162], [142], [46] pour des images médicales sous les attaques géométriques et non géométriques. L'approche proposée a donné de meilleures valeurs de BER par rapport à l'approche proposée dans [50]. En comparant les résultats de la méthode proposée avec la méthode de [142], les résultats du BER mentionnés montrent que l'approche proposée permet d'obtenir de meilleurs résultats contre les attaques d'affutage (en moyenne, le BER est égal à 0,0047 dans l'approche

proposée, tandis que le BER dans l'approche [142] est égal à 0,0261). Inversement, le schéma de [142] a de meilleurs résultats que l'approche proposée sous les attaques de filtrage médian 5×5, translate (10) et l'égalisation d'histogramme. La méthode de [142] n'est pas testée sous les attaques rotation, bruit, recadrage, filtrage Gaussien, filtrage médian, filtrage moyen et le bruit de sel et de poivre. Le BER de l'approche proposée est meilleur que le BER de l'approche [162], dans le cas d'un filtrage médian 3×3 (le BER de l'approche proposée est égal à 0,0214 et le BER de l'approche [162] est égal à 0,0342). À l'inverse, l'approche [162] a de meilleurs résultats que l'approche proposée sous les attaques filtrage Gaussien, filtrage moyen 3×3, le bruit Gaussien (0,001), le bruit Gaussien (0,01), le bruit Gaussien (0,05), le bruit Gaussien (20), le bruit de sel et de poivre (0,01), le bruit de sel et poivre (0,03) et la rotation 5°. Les résultats BER de [50], [162], [142], [46] sous les attaques de recadrage en haut à gauche (25%), le filtrage moyen 2×2, le filtrage gaussien 3×3, la rotation 10°, la rotation 45° ne sont malheureusement pas disponibles. L'approche de [46] a obtenu de meilleures valeurs de BER contre la translation (10), le bruit Gaussien (0,01) et la rotation de 5° que l'approche proposée, mais les résultats pour d'autres attaques ne sont malheureusement pas disponibles.

3.5.2 Comparaison de la valeur du NC du modèle proposé avec les modèles de zéro-tatouage existants

Une comparaison de la qualité d'image de l'approche proposée avec les approches de [[50],[162]] sur la base de NC est présentée dans le tableau 3.9. Dans le cas de l'affûtage, l'égalisation d'histogramme, le bruit Gaussien (0,01), le filtrage médian 2×2 , le bruit de sel et de poivre (0,1), le recadrage de coin supérieur gauche (25%), le filtrage moyen (2×2), la rotation à 90°, l'approche de [6] a atteint des valeurs de NC plus élevées que l'approche proposée. En comparant les valeurs de NC entre l'approche proposée et l'approche de [162], nous pouvons voir que l'approche proposée permet d'obtenir un meilleur rapport de NC contre l'attaque de l'affutage que l'approche de [162], mais elle obtient de moins bons résultats que cette dernière contre l'égalisation d'histogramme, le filtrage Gaussien et le filtrage médian. Dans [50] et [162] les auteurs ne fournissent pas les valeurs de NC pour les attaques sel et poivre (0,01), sel et poivre (0,03), filtrage moyen 3×3, le bruit Gaussien (0,05), le bruit Gausien (20), la rotation 45°, la rotation 10°, la rotation 5° et la translation (10).

TABLE 3.8 – Comparaison du BER du modèle proposé avec les modèles de zéro-tatouage existants [[50], [162], [142] et [46]

Les attaques	L'approche proposée	[50]	[142]	[162]	[46]
Rotation 10°	0.0243	0.22	-	-	-
Noise_ 20	0.0288	0.26	-	-	-
Filtrage médian 5×5	0.0238	0.19	0.0028	-	-
Recadrage (50)	0.0575	0.22	-	-	-
Translation (10)	0.0202	0.26	0.0120	-	0
L'affûtage	0.0047	-	0.0261	-	-
Egalisation d'histogramme	0.0172	-	0.0060	-	-
] Filtre Gaussien	0.0172	-	-	0.0127	-
Filtrage médian 3×3	0.0214	-	-	0.0342	-
Filtrage moyen 3×3 0.0203	-	-	0.0078	-	
Bruit Gaussien (0.01)	0.0284	-	-	0.0039	0.0142
Bruit Gaussien (0.001)	0.0261	-	-	0.0049	-
Bruit Gaussien (0.05)	0.0322	-	-	0.0078	-
Bruit Gaussien (20)	0.0288	-	-	0.0059	-
Bruit du sel et du poivre (0.01)	0.0333	-	-	0.0068	-
Bruit du sel et du poivre (0.03)	0.0246	-	-	0	-
Rotation 5°	-	-	-	0.0732	0.0897

TABLE 3.9 – Comparaison de la valeur de NC du modèle proposé avec les modèles de zéro-tatouage existants [[50] et [162]]

Les attaques	L'approche proposée	[50]	[162]
L'affutage	0.9852	1	0.9357
Egalisation d'histogramme	0.4929	0.86	0.8577
Le bruit Gaussien (0.01)	0.9114	0.99	-
Le filtrage median 2×2	0.9500	1	-
Le filtrage median 3×3	0.9427	-	0.9838
Le bruit du sel et du poivre (0.1)	0.9099	0.93	-
Le recadrage du coin superieur gauche 25%	0.8445	1	-
Le filtrage moyen 2×2	0.9407	0.99	-
La rotation 90°	0.9159	0.96	-
Le filtre Gaussien 3×3	0.9488	-	0.9593

TABLE 3.10 – Comparaison des valeurs de PSNR entre l'algorithme proposé et les algorithmes proposés dans [50]

Les attaques	L'approche proposée	[50]
La rotation 10°	31.97	27.3
Filtre median 5×5	49.67	50.2
La translation (10)	47.81	50.4
Le bruit (20) 2×2	39.70	26

3.5.3 Comparaison des valeurs de PSNR entre l'algorithme proposé et l'algorithme proposé dans [50]

Une étude comparative entre le PSNR de la méthode proposée et le PSNR d'une autre méthode de zéro-tatouage [50] est présentée dans le tableau 3.10. On note que la méthode proposée a des valeurs de PSNR plus élevées que la méthode présentée dans [50] en cas d'attaque de rotation de 10° et dans le cas du bruit (20). Par contre, dans le cas du filtrage médian 5×5 et de la translation (10) la méthode de [50] a des valeurs de PSNR plus élevées que la méthode proposée.

D'après le tableau 3.10, la valeur moyenne du PSNR de l'approche proposée est meilleure que celle de [50] (la valeur moyenne est de 42 dB pour l'approche proposée et de 38 dB pour [50]).

3.5.4 Comparaison du SSIM du modèle proposé avec les modèles de zéro-tatouage existants

Le tableau 3.11 montre une comparaison du SSIM de l'approche proposée avec une autre approche de zéro-tatouage. Selon les résultats présentés dans le tableau 43, l'approche proposée permet d'obtenir une meilleure valeur SSIM dans le cas de la rotation 2°, du bruit Gaussien (0,01) et des attaques de l'affutage que l'approche de Chunpeng et al. [142].

3.5.5 Comparaison du temps d'exécution avec les méthodes de zéro-tatouage existantes

Le tableau 3.12 montre une comparaison du temps d'exécution en secondes pour générer une marque entre l'approche proposée et les approches de [[50] , [142], [162]]. La

TABLE 3.11 – Comparaison du SSIM du modèle proposé avec les modèles de zéro-tatouage existants [142]

Les attaques	L'approche proposée	[142]
La rotation 2°	0.9652	0.4748
Bruit Gaussien (0.01)	0.9553	0.3347
L'affûtage	0.9901	0.7676

TABLE 3.12 – Comparaison du temps d'exécution en secondes de l'algorithme de génération de la marque entre le modèle proposé et d'autres schémas de zéro-tatouage [[50], [142] et [162]]

	L'approche proposée	[50]	[162]	[142]
Le temps d'exécution	8.5922	4.5	8.5961	10.9474

valeur du temps d'exécution de l'algorithme de génération de zéro-tatouage dans l'approche proposée est quasiment la même que celle de l'approche de [162] et est inférieure à celle de l'approche de [142]. Cependant, le temps d'exécution de [50] est meilleur que celui de l'approche proposée. La différence de temps d'exécution entre l'approche proposée et l'approche de [50] est égale à 4,0922 secondes. Cette différence pourrait être due au calcul des fonctionnalités extraites des images originales. En comparant notre approche avec les approches de [[142], [162]], notre approche est exécutée en moins de temps pour l'extraction de la marque que celle de Chunpeng et al. [142], mais, a un temps d'exécution plus élevé du côté de l'extraction de la marque par rapport à [50] et [162].

Pour résumer, nous pouvons souligner les remarques suivantes :

— L'approche proposée est conçue dans le domaine spatial et la marque est une image en niveaux de gris. Elle fournit toujours de bons rapports de robustesse par rapport à d'autres approches apparentées en termes de coefficient de corrélation normalisé (NC), de taux d'erreur sur les bits (BER) et d'indice de structure de similarité

TABLE 3.13 – Comparaison du temps d'exécution de l'extraction de la marque avec le temps d'exécution des méthodes de zéro-tatouage existantes [[50], [162] et [142]]

	L'approche proposée	[50]	[162]	[142]
Le temps d'exécution	9.0588	4.184	8.5961	10.9046

(SSIM).

— Le NC dans l'approche proposée varie de 0,87-1, alors qu'il variait respectivement de 0,68-1, 0,85-1, 0,81-1 en [[50], [139], [55]]. La seule approche ayant un BER plus petit en moyenne est celle proposée dans [162].

— Le BER dans l'approche proposée est égal en moyenne à 3%, alors qu'il est égal en moyenne à 18,5%, 13%, 5%, 19%, 3%, 3,7%, 21,1% dans [[50], [142], [139], [138],[161], [46], [41]] respectivement.

— Le SSIM dans l'approche proposée est égal en moyenne à 92%, alors que dans [142] il est égal en moyenne à 70%.

— Le PSNR moyen dans l'approche proposée est égal à 42 dB tandis que dans [50] il est égal à 38 dB.

— Pour le temps d'exécution, l'approche proposée est exécutée en moins de temps par rapport aux approches de [142], [161]]. Cependant, le temps d'exécution de l'approche de [50] est meilleur que celui de l'approche proposée.

3.6 Conclusion

Une approche de zéro-tatouage pour l'authentification et l'identification des images DICOM est proposée dans ce chapitre qui utilise stratégiquement une analyse statistique pour sélectionner des caractéristiques pertinentes à partir de l'image DICOM pour la génération de la clé transmise au récepteur. Le processus proposé extrait le nom du patient de l'en-tête de l'image DICOM, génère une matrice à partir de l'image hôte en utilisant un processus de soustractions cumulées et exploite tout cela comme une entrée du modèle matriciel Jacobien pour générer une clé envoyée au récepteur pour l'authentification et l'identification de l'image. La robustesse de la méthode proposée a été testée en l'absence d'attaques d'une part et, pour différents types d'attaques, d'autre part. Ses performances ont été évaluées à l'aide du coefficient de corrélation normalisé (NC), de l'indice de similarité de structure (SSIM) et du taux d'erreur sur les bits (BER). Les résultats montrent que le BER est de 3% en moyenne, la valeur NC de 87% en moyenne et la valeur SSIM de 92% en moyenne. Ainsi, la méthode proposée est robuste contre les attaques telles que le filtrage médian, le bruit Gaussien, le filtrage moyen, l'égalisation d'histogramme, l'affutage, le recadrage, la translation et les attaques de sel et poivre. En outre, l'approche proposée a été mise en œuvre avec un temps d'exécution de 8,7 secondes, ce qui est assez satisfai-

sant pour les applications médicales. Ces résultats sont très encourageants par rapport à d'autres approches connexes de zéro-tatouage et garantissent que l'approche proposée peut être une solution pratique pour résoudre les problèmes de sécurité, d'identification et d'authentification de l'image médicale dans les applications de télémédecine. L'originalité de cette approche réside dans le fait que les fonctionnalités pertinentes utilisées pour générer la clé sont choisies à partir d'une analyse statistique approfondie de toute une base de données d'images. Un avantage est que si le zéro-tatouage est appliqué à toutes les images de la base de données, seuls les résultats de l'analyse statistique unique sont nécessaires. Un autre avantage est que ces caractéristiques pertinentes sélectionnées par une analyse statistique sont des caractéristiques robustes des images médicales et peuvent aider à améliorer d'autres schémas de tatouage destinés aux applications médicales.
Dans le chapitre suivant, nous présentons la deuxième contribution de ce travail de thèse. Il s'agit d'une approche hybride qui utilise l'analyse statistique précédemment proposée pour réaliser un zéro-tatouage dans la région d'intérêt (ROI), et met en œuvre un tatouage par insertion de marque dans la région de non-intérêt (RONI).

Chapitre 4

Une approche de tatouage double des images DICOM

4.1 Introduction

Dans ce chapitre nous présentons une technique de tatouage numérique combinant une technique de zéro-tatouage dans la partie anatomique de l'image et une technique de tatouage par insertion de marque dans la partie du fond noir de l'image pour l'authentification et l'identification des images DICOM, ainsi que la confidentialité des informations des patients. En effet, le stockage et la transmission des images médicales nécessitent une forte confidentialité, authentification et intégrité. Dans l'approche proposée, des caractéristiques pertinentes extraites de l'image DICOM sont utilisées, d'une part, pour le zéro-tatouage basé sur le modèle Jacobien, et d'autre part, pour construire la marque insérée dans la région du fond noir de l'image en utilisant la technique d'interpolation linéaire. La marque est insérée uniquement dans la zone du fond noir afin d'éviter d'affecter la partie anatomique dont la modification peut provoquer un diagnostic erroné.
Nous commençons ce chapitre par la présentation du schéma général de l'approche proposée, ensuite nous détaillons le processus de séparation de la partie anatomique et de la partie du fond noir de l'image, puis nous présentons le processus de génération de la marque et son utilisation pour le zéro-tatouage de la partie anatomique. Par la suite, nous expliquons le processus d'insertion de la marque en utilisant la technique d'interpolation linéaire, ainsi que le processus d'extraction de la marque qui est basé sur l'inverse du processus d'insertion de la marque. Enfin, nous évaluons les résultats obtenus et réalisons une étude comparative avec les travaux existants.

4.2 L'approche de tatouage proposée

L'approche proposée est composée de 4 étapes : la séparation de l'objet anatomique et du fond noir de l'image, la génération de la marque en utilisant la technique de zéro-tatouage et l'insertion et l'extraction de la marque. Ces étapes sont utilisées à la fois du côté expéditeur et récepteur. L'insertion de la marque est utilisée uniquement du côté expéditeur et l'extraction de la marque est utilisée uniquement du côté récepteur. La Figure 4.1 montre le schéma général de l'approche proposée.

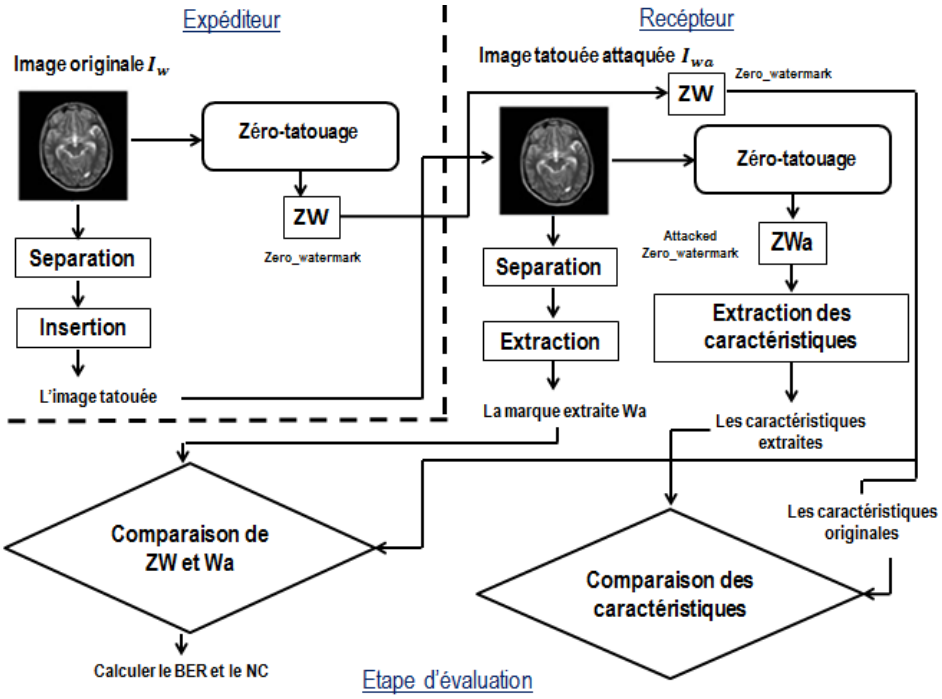


FIGURE 4.1 – Schéma général de la méthode du tatouage proposée

4.2.1 Séparation de la partie anatomique et la partie du fond noir

Une image médicale contient deux parties principales appelées respectivement ROI (région d'intérêt) et RONI (région de non intérêt). La ROI est la partie diagnostic [140] qui est sélectionnée soit par un médecin ou un spécialiste, soit par un processus automatisé. La RONI est la partie qui ne contient pas d'informations importantes pour le diagnostic. Les

parties ROI et RONI peuvent être séparées automatiquement en utilisant un algorithme [126] ou manuellement [78]. Dans cette approche, un processus automatisé est utilisé pour la séparation entre la partie ROI et la partie RONI. La ROI est la partie anatomique de l'image et la RONI correspond au reste qui est la zone du fond noir de l'image. Cette séparation est importante afin d'éviter de modifier la ROI de manière à préserver la qualité du diagnostic médical. La figure 4.2 montre un exemple de séparation de la partie de l'objet anatomique et la partie du fond noir de l'image en utilisant la méthode de séparation proposée. Dans cette approche nous sommes intéressées par les images médicales qui ont un fond noir. Notre méthode de séparation est basée sur un seuil. Nous avons choisi ce seuil

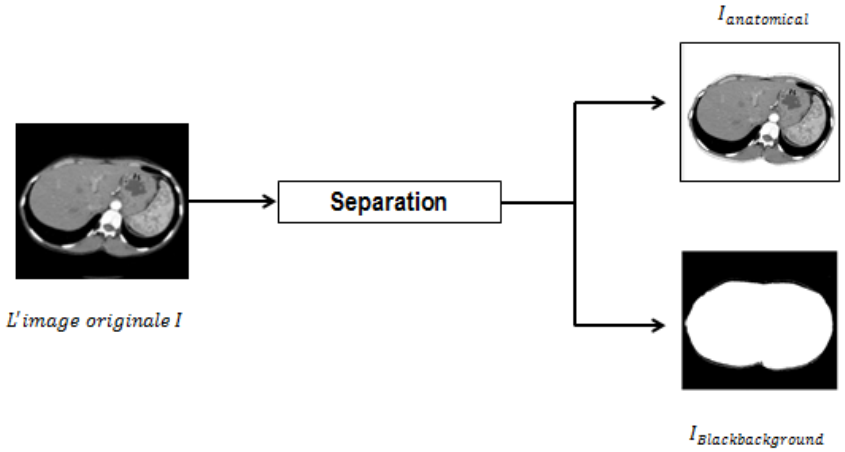


FIGURE 4.2 – Séparation de l'objet anatomique et de la partie du fond noir de l'image

Thr de telle sorte que tous les pixels dont les valeurs sont inférieures au seuil appartiennent à l'objet anatomique ($I_{Antomical}$) tandis que tous les pixels dont les valeurs sont supérieures au seuil appartiennent à la région du fond noir ($I_{Blackbackgroud}$). L'algorithme (3) présente le pseudo-code simplifié de la méthode de séparation.

4.2.2 Génération de la marque en utilisant la technique le zéro-tatouage

La génération de la marque est basée sur l'extraction des caractéristiques pertinentes appelées asymétrie, entropie et médiane [92] de l'objet anatomique de l'image originale, ainsi que sur l'extraction des informations du patient (nom de famille et prénom) de

Algorithm 3 Pseudo-code simplifié de la méthode de séparation

Entrée : l'image originale I de taille $n \times m$, $I_{Blackbackground}$, $I_{Antomical}$
Sortie : l'image de l'objet anatomique et l'image du fond noir de taille $n \times m$
Debut
Sélectionner un seuil Thr
Pour $i = 1$ to n
    Pour $j = 1$ to m
        si $I(i, j) <= Thr$
        $I_{Blackbackground}$ (i,j) ←I(i,j);
        sinon
        $I_{Antomical}$ (i,j) ←I(i,j);
        Finsi
    Fin pour
Fin pour
Fin

FIGURE 4.3 – Exemple de transformation de la clé en une marque appelée Zero-Watermark *ZW*

l'en-tête de l'image DICOM. Ces informations permettent de confirmer l'authenticité et l'intégrité de l'image. La première lettre du prénom et la première lettre du nom de famille du patient sont transformées et présentées comme une matrice de taille 16×16 pixels. Les trois caractéristiques pertinentes et la matrice représentant le nom du patient sont utilisées comme entrée dans le modèle Jacobien afin de construire l'image clé de taille 16×16 pixels. La définition du modèle Jacobien est présentée dans le chapitre 3. Après la génération, l'image clé est insérée dans une image noire de taille 32×32 pixels pour obtenir la marque comme illustré par l'exemple présenté dans la Figure 4.3. La Figure 4.4 montre le processus de la génération de la marque en utilisant la technique de zéro-tatouage.

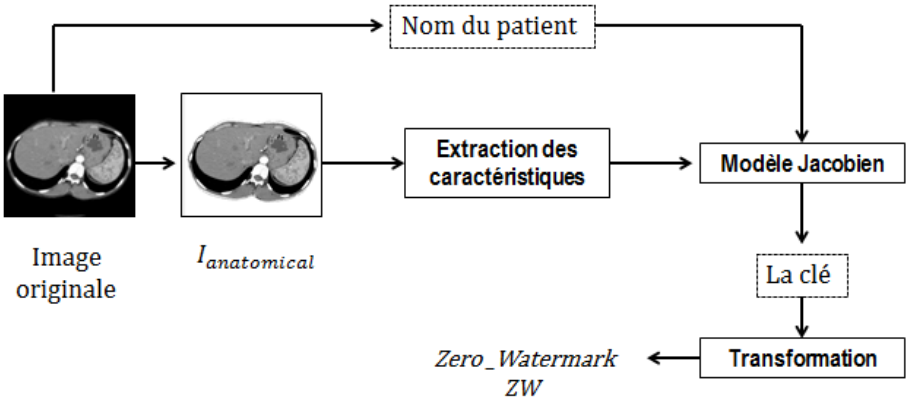


FIGURE 4.4 – Le processus de la génération de la marque en utilisant la technique de zéro-tatouage.

4.2.3 Processus d'insertion de la marque

La marque générée en utilisant l'approche de zéro-tatouage est insérée dans la partie du fond noir de l'image obtenue à l'étape de séparation. Dans notre modèle, nous divisons la partie du fond noir de l'image en régions de taille 8×8 pixels $(R1, R2, \cdot, Rn)$. Le zero-watermark ZW est divisé en quatre blocs de taille 8×8 pixels nommés $w1$, $w2$, $w3$ et $w4$, puis ces blocs sont insérés dans les 4 régions sélectionnées parmi les régions d'arrière-plan $(R1, R2, \cdot, Rn)$ en utilisant la technique d'interpolation linéaire. Cette technique permet de gérer un bon équilibre entre l'imperceptibilité et la robustesse en sélectionnant le bon facteur d'interpolation [49]. Ensuite, l'image de l'objet anatomique $I_{Anatomical}$ et l'image de fond noir tatouée $I_{WBlackbackground}$ sont combinées pour obtenir l'image tatouée I_w. La figure 4.5 illustre le processus d'insertion de la marque côté expéditeur. L'algorithme (4) présente le pseudo-code du processus d'insertion de la marque du côté expéditeur.

4.2.4 Le processus d'extraction de la marque

Après le processus d'insertion, la marque générée par le processus de zéro-tatouage est envoyée comme clé au récepteur via un canal sécurisé. L'image tatouée obtenue I_w sera envoyée au récepteur via des réseaux publics non sécurisés et elle sera exposée à différents types d'attaques. L'opération inverse du processus d'insertion est effectuée.
Par conséquent, l'image reçue est une image tatouée attaquée I_{wa} et le processus d'ex-

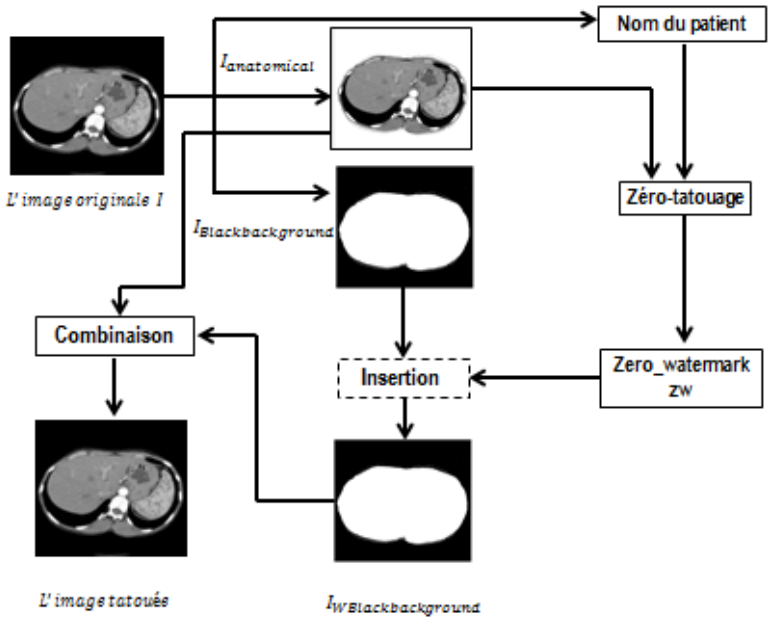


FIGURE 4.5 – Le processus d'insertion de la marque du côté expéditeur.

Algorithm 4 le pseudo code d'insertion de la marque

Entrée : l'object anatomique et la région de fond noir de l'image originale I, l'image originale de zero-watermark ZW de taille 8×8 pixels et le facteur d'interpolation linéaire t ($t \in]0,1[$)
Diviser la région de fond noir en blocs de taille 8×8 pixels ($block_1$, $block_2$,$\cdots$,block$_k$)
Pour i=1 à 4 faire
    $block_{iw} \leftarrow (1-t)ZW + t\times$block$_i$;
Fin pour
Combiner l'image de l'objet anatomique et l'image de fond noir tatouée
Sortie : l'image tatouée (I_w)
Fin

traction doit être appliqué pour prouver l'origine de l'image en extrayant l'ensemble de marques attaquées W_a de I_{wa}. La forme inverse de la technique d'interpolation linéaire est appliquée. D'une part, la marque attaquée extraite W_a est comparée à la marque originale appelée zero-watermark ZW en utilisant les métriques d'évaluation de robustesse et d'imperceptibilité BER et NC. S'ils sont similaires, l'image est authentifiée et peut être utilisée pour le diagnostic, sinon l'image est ignorée. D'autre part, une comparaison des caractéristiques originales extraites de la marque originale ZW et les caractéristiques extraites de la marque attaquée Z_{Wa} est effectuée pour l'authentification et l'identification de l'image médicale. L'image est considérée comme authentique si la différence entre les valeurs des caractéristiques initiales et extraites est inférieure à un seuil donné. La figure 4.6 montre le schéma du processus d'extraction de la marque du côté du récepteur. L'algorithme (5) montre le pseudo code du processus d'extraction de la marque.

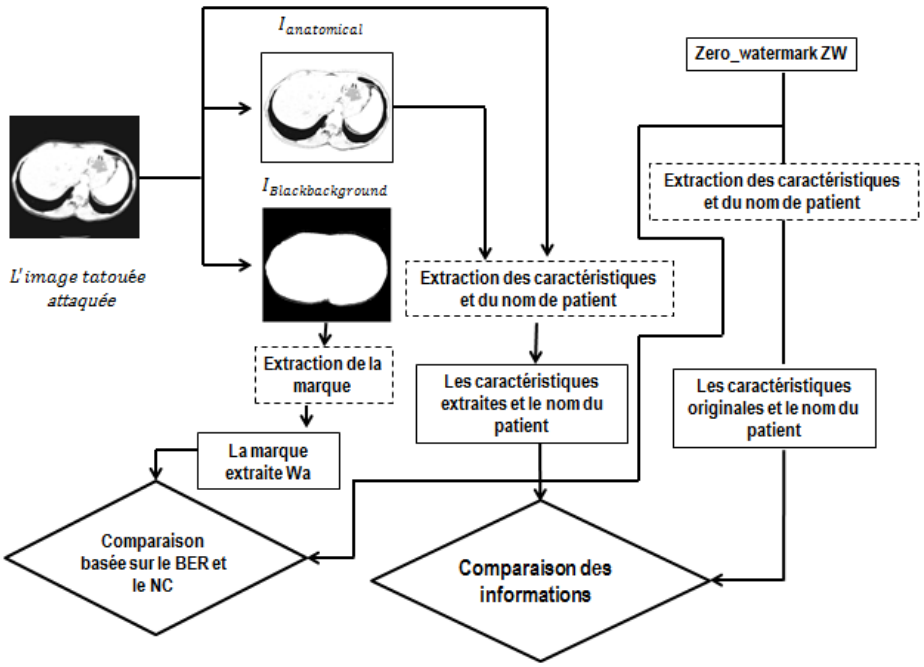


FIGURE 4.6 – Le processus d'extraction de la marque côté récepteur.

Algorithm 5 le pseudo code du processus d'extraction

Entrée : l'image de fond noir et l'image de l'objet anatomique de l'image tatouée attaquée I_{wa} , la marque originale ZW de taille 8×8 pixels et le facteur de l'interpolation t (t $\in]0,1[$)

Diviser l'image de fond noir en blocks de taille 8×8 pixels ($block_1$, $block_2$,$\cdots$,block$_k$)

Pour i=1 à 4 faire

W_a=(1/t)ZW+((1-t)/t)×$block_i$

Fin pour

Sortie : Ensemble des marques attaquées (W_a)

Fin

4.3 Les résultats expérimentaux

Dans cette section, nous présentons les résultats de la méthode proposée et nous les analysons et les comparons avec des travaux similaires. Le système de tatouage proposé est implémenté à l'aide de MATLAB et exécuté sur une machine Windows avec les caractéristiques suivantes : processeur Intel R Core i7, 4 GHz, 4 Go de RAM et plate-forme de système d'exploitation Microsoft Windows 8 Professional. Dans nos expériences, nous avons utilisé des images DICOM de taille 512×512 pixels comme indiqué sur la figure 4.7. La marque générée à l'aide de l'approche proposée est présentée dans la figure 4.8. Les

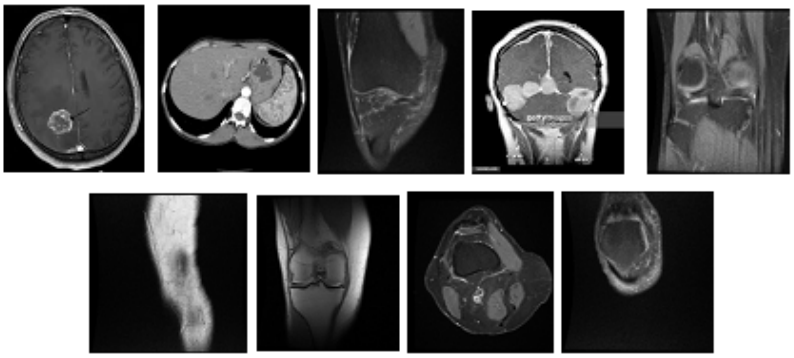


FIGURE 4.7 – Exemples des images DICOM utilisées dans l'expérimentation.

résultats montrent qu'il n'y a pas de différence visuelle entre l'image originale et l'image

FIGURE 4.8 – L'image originale et l'image tatouée correspondante.

tatouée. La figure 4.8 montre un exemple de l'image originale et de son image tatouée correspondante.

4.3.1 Les paramètres d'évaluation

Analyse de l'imperceptibilité

Pour évaluer la force de l'imperceptibilité de la méthode de tatouage proposée après l'insertion de la marque, une analyse qualitative a été réalisée. Pour quantifier la distorsion causée aux images DICOM, le rapport signal / bruit (PSNR) [78] et la mesure d'indice de similarité structurelle (SSIM) [[78],[142]] sont calculés. Le Tableau 4.1 présente les valeurs de SSIM entre l'image originale et l'image tatouée sous différentes attaques ainsi que leur valeur moyenne. Les résultats du tableau 4.1 montrent que l'approche proposée présente un bon niveau d'imperceptibilité, les valeurs SSIM sont supérieures à 0,9 ce qui indique la similitude entre l'image originale et l'image tatouée.
Le tableau 4.2 présente les valeurs du PSNR entre l'image originale et l'image tatouée sous différentes attaques.

On remarque dans le tableau 4.2 que les valeurs de PSNR entre l'image originale et l'image tatouée sont supérieures à 71 dB.

Analyse de la robustesse

Pour évaluer la robustesse de la marque insérée contre les différentes attaques, le taux d'erreur sur les bits (BER) [142] et le coefficient de corrélation normalisée (NC) [142] ont été utilisés.

Les valeurs de BER présentées dans le tableau 4.4 montrent une grande robustesse de la marque insérée contre les différentes attaques. Les valeurs de BER en moyenne égales à 0,0110 indiquent que la méthode proposée est robuste contre ces différentes attaques. De plus, les valeurs NC du tableau 4.3 montrent que la marque insérée a également résisté

Les attaques	Les valeurs de SSIM				Les valeurs moyennes
	Hands	Chest	Tspine	Skull	
Filtrage median 3×3	0.9887	0.9829	0.8789	0.9981	0.9621
Filtrage median 5×5	0.9850	0.9630	0.9983	0.9953	0.9854
Bruit de sel et de poivre (0.01)	0.9735	0.9870	0.9618	0.9789	0.9753
Bruit de sel et de poivre (0.03)	0.9920	0.9912	0.9678	0.9579	0.9772
Filtrage moyen (3×3)	0.9858	0.9798	0.9989	0.9980	0.9906
Recadrage de coin supérieur gauche (25%)	0.9866	0.9989	0.9986	0.8770	0.9652
Filtrage Gaussien (3×3)	0.9880	0.9978	0.8101	0.9976	0.9483
Egalisation d'histogramme	0.9033	0.9352	0.8999	0.8789	0.9043
Bruit Gaussian (0.05)	0.9789	0.9512	0.8898	0.9789	0.9497
Bruit Gaussian (0.01)	0.9877	0.9889	0.9725	0.9819	0.9827
Bruit Gaussian (20)	0.9789	0.9886	0.9789	0.9849	0.9828
Rotation 5	0.9782	0.9846	0.9510	0.9304	0.9610
Rotation 10	0.9854	0.9622	0.9273	0.9588	0.9584
Rotation 45	0.9878	0.9850	0.9613	0.9578	0.9729
L'affûtage	0.9997	0.9968	0.9826	0.9888	0.9919
Translation (10)	0.9804	0.9778	0.9915	0.9914	0.9852

TABLE 4.1 – Les values de SSIM entre l'image originale et l'image tatouée.

Les attaques	Les valeurs de PSNR				Les valeurs moyennes
	Hands	Chest	Tspine	Skull	
Filtrage median 3×3	63.80	70.29	72.89	87.91	73.72
Filtrage median 5×5	66.58	69.63	69.83	77.53	70.89
Bruit de sel et de poivre (0.01)	79.35	78.70	76.18	77.89	78.03
Bruit de sel et de poivre (0.03)	71.22	79.82	76.33	72.86	75.05
Filtrage moyen (3×3)	66.57	68.89	70.78	77.85	71.02
Recadrage de coin supérieur gauche (25%)	78.66	79.92	78.86	70.77	77.05
Filtrage Gaussien (3×3)	65.86	77.78	81.56	87.53	78.18
Egalisation d'histogramme	61.23	80.35	79.99	87.42	77.24
Bruit Gaussien (0.05)	68.26	70.36	77.23	80.98	74.20
Bruit Gaussien (0.01)	70.58	82.60	85.39	79.85	79.60
Bruit Gaussien (20)	66.32	77.25	80.78	82.24	76.64
Rotation 5	77.21	82.79	77.25	88.17	81.35
Rotation 10	68.56	81.56	72.23	78.98	75.33
Rotation 45	72.26	72.98	85.11	75.16	76.37
L'affûtage	69.32	79.02	80.21	78.96	76.87
Translation (10)	70.14	80.26	85.16	86.75	80.57

TABLE 4.2 – Les valeurs de PSNR entre l'image originale et l'image tatouée

Les attaques	Les valeurs de NC				Les valeurs moyennes
	Hands	Chest	Tspine	Skull	
Filtrage median 3×3	0.9462	0.9995	0.9368	0.9881	0.9676
Bruit de sel et de poivre (0.01)	0.9560	0.9315	0.9574	0.9603	0.9513
Bruit de sel et de poivre (0.03)	0.9663	0.9806	0.9862	0.9089	0.9605
Filtrage moyen (3×3)	0.9603	0.9857	0.9892	0.9887	0.9809
Recadrage de coin supérieur gauche (25%)	0.9870	0.9968	0.8898	0.8945	0.9420
Filtrage Gaussien (3×3)	0.9775	0.9997	0.9461 0.9881	0.9778	
Egalisation d'histogramme	0.8752	0.8870	0.9512	0.9612	0.9186
Bruit Gaussien (0.05)	0.9796	0.9588	0.9687	0.8999	0.9517
Bruit Gaussien (0.01)	0.9740	0.9877	0.9685	0.8957	0.9564
Bruit Gaussien (20)	0.9783	0.9895	0.9878	0.9095	0.9662
Rotation 5	0.9447	0.9925	0.9787	0.9321	0.9620
Rotation 10	0.9580	0.9807	0.9883	0.9214	0.9621
Rotation 45	72.26	72.98	85.11	75.16	76.37
L'affûtage	0.9999	0.9992	0.9950	0.9968	0.9977
Translation (10)	0.9468	0.9292	0.9642	0.9859	0.9565

TABLE 4.3 – Les valeurs de NC entre l'image originale et l'image tatouée sous différentes attaques

Les attaques	Les valeurs de BER				Les valeurs moyennes
	Hands	Chest	Tspine	Skull	
Filtrage median 3×3	0.0078	0.0092	0.0067	0.0025	0.0065
Bruit de sel et de poivre (0.01)	0.0071	0.0088	0.0065	0.0055	0.0069
Bruit de sel et de poivre (0.03)	0.0035	0.0038	0.0040	0.0045	0.0039
Filtrage moyen (3×3)	0.0112	0.0056	0.0106	0.0023	0.0074
Recadrage de coin supérieur gauche (25%)	0.0112	0.0083	0.0115	0.0045	0.0088
Filtrage Gaussien (3×3)	0.0085	0	0.0502	0.0089	0.0169
Egalisation d'histogramme	0.0114	0.0099	0.0302	0.0078	0.0148
Bruit Gaussien (0.05)	0.0018	0.0025	0.0030	0.0089	0.0040
Bruit Gaussien (0.01)	0.0152	0.0024	0.0185	0.0602	0.0240
Bruit Gaussien (20)	0.0152	0.0202	0.0100	0.0010	0.0116
Rotation 5	0.0056	0.0072	0.0088	0.0132	0.0087
Rotation 10	0.0100	0.0089	0.0111	0.0205	0.0126
Rotation 45	0.0112	0.008	0.0116	0.0301	0.0154
L'affûtage	0	0	0	0.0003	0
Translation (10)	0.0165	0.0202	0.0080	0.0089	0.0134

TABLE 4.4 – Les valeurs de BER entre l'image originale et l'image tatouée sous différentes attaques

Image	Temps d'exécution de l'insertion (sec)	Temps d'exécution de l'extraction (sec)
1	9.9760	10.9880
2	10.9878	11.0150
3	9.9845	9.9982
4	9.9924	10.0085

TABLE 4.5 – Le temps d'exécution d'insertion et d'extraction de la marque

aux différentes attaques, la valeur de NC en moyenne entre la marque attaquée extraite et la marque originale est égale à 0,9588.

Analyse du temps d'exécution de l'insertion et de l'extraction de la marque

Le tableau 4.5 présente le temps d'exécution en secondes pour l'insertion et l'extraction de la marque de la région du fond noir de l'image (RONI) après le test des attaques.

Comme le montre le tableau 4.5, le temps d'exécution d'insertion de la marque est égal en moyenne à 10,2351 secondes et le temps d'exécution d'extraction de la marque est égal à 10,5024 en moyenne.

4.3.2 Étude comparative

Pour mieux situer la performance de la méthode de tatouage proposée, une analyse comparative avec plusieurs travaux connexes a été effectuée.

Les auteurs	L'objectif	La marque	La région d'insertion	La technique d'insertion	La robustesse	Les résultats
Wei Pan et al. [114]	Authentication, integrité, diagnostic	Message binaire 0 ou 1	ROI et RONI	Modification d'histogramm, Bruit quantium	Robuste contre les attaques de compression	SSIM égale à 0.99 et PSNR égale à 76.5
Afef Tareef et al. [150]	Authentication	EPR+ROI	RONI	SVD (Singular Value Decomposition)	Robuste contre le bruit Gaussien et la compression JPEG	PSNR égale 49.82 dB et NC égale à 0.80
Ales Rocek et al. [132]	Securité, authentication	Secret share et public share	ROI et RONI	DT-CWT et LSB	Fragile	SSIM égale à 0.99 et PSNR égale à 81 dB
Nisar Ahmed Memon et al. [96]	Securité, integrité, confidentialité, diagnostic, imperceptibilité, droits d'auteur, et détection de sabotage	Electronic Patient Record (EPR), (Doctor's Identification et Code (DIC)) et Le 1er bit-plane de la ROI	ROI et RONI	IWT, LSB et (Cohen-Daubechies-Fauraue (CDF))	Robuste contre le bruit Gaussian, le filtrage median, la compression JPEG et l'attaque de copie	PSNR égale à 59.89 dB
La méthode proposée	Authentication, integrité et diagnostic	Le nom du patient et les caractéristiques pertinentes	RONI	L'interpolation linéaire	Robuste contre le filtre median, le bruit du sel et du poivre, le filtre moyen, le recadrage du coin supérieur gauche, le filtrage Gaussien, l'égalisation d'histogramme, le bruit Gaussien, la rotation, l'affûtage et la translation	SSIM égale à 0.9683, PSNR égale à 71 dB, BER égale à 0.0110 et NC égale à 0.9588

TABLE 4.6 – Comparaison des approches de tatouage existantes

Le tableau 4.6 présente une comparaison entre l'approche proposée et d'autres approches existantes dans [114], [150], [132] et [132]. Les objectifs de chaque approche, les types d'images testées, le type de la marque générée, la technique d'insertion utilisée, la robustesse face aux différentes attaques et les résultats obtenus en terme de BER, NC, SSIM et le temps d'exécution sont un ensemble d'aspects utilisés dans le processus de comparaison. Comme le montre le tableau la plupart des approches ont comme objectif l'authentification et l'intégrité des images médicales. Les types de marques générées dans les approches dans [114], [150], [132] et [132] sont différents d'une approche à une autre. Dans l'approche [114] la marque générée est un message binaire, alors qu'il s'agit d'une marque générée à partir des informations extraites de la partie ROI de l'image et l'EPR du patient et représentée sous forme d'une image au niveau de gris dans l'approche de [150]. Une marque construite à partir de l'EPR du patient, du code d'identification du médecin et du 1er bit de la ROI de l'image est utilisée dans l'approche de Nizar Ahmed et

al. [96]. Dans l'approche de Ales Rocek et al [132] deux marques appelées « secret share » et « public share » sont générées à partir des informations extraites de l'image originale. En terme de méthode d'insertion de la marque, nous remarquons d'après le tableau que les approches [Nisar Ahmed et al, [132], Wei Pan et al] insèrent la marque dans les deux régions de l'image ROI et RONI. Tandis que l'approche de Afef et al [150] et notre approche insèrent la marque dans la région RONI. L'approche de Wei Pan et al [114] utilise par ailleurs une méthode d'insertion réversible qui est la méthode de modification d'histogramme. L'approche de Traeef et al [150] insère la marque en utilisant la technique SVD. Les approches de [[96],[132]] ont utilisé des méthodes d'insertion dans le domaine fréquentiel tel que IWT et DT-CWT alors que notre méthode utilise une technique d'insertion de la marque dans le domaine spatial qui est la technique d'interpolation linéaire. Afin de comparer l'imperceptibilité de notre méthode par rapport à d'autres, nous comparons les valeurs de SSIM des méthodes existantes avec nos valeurs de SSIM. Nous pouvons voir que les méthodes de [[114], [132]] ont une valeur de SSIM égale à 0,99, ce qui est supérieur à la valeur SSIM de notre méthode qui est égale à 0,96. En termes de PSNR, la méthode proposée atteint une valeur PSNR en moyenne égale à 71 dB qui est meilleure que la valeur PSNR de Afef et al [150] qui est égale à 49,82 dB, mais inférieure au PSNR de [132] (76,5 dB) et le PSNR de la méthode en [114] (81 dB).
En comparant la robustesse de la méthode proposée avec celle des autres méthodes, nous pouvons voir que le BER de l'approche proposée a atteint 0,0110, alors que dans l'approche de [140] le BER en moyenne est égal à 0,0281, ce qui est supérieur à notre BER. En comparant les valeurs de NC, on peut voir que notre méthode a une meilleure valeur (0,9588) que la méthode de [150] dont la valeur NC est égal à 0,80.

4.4 Conclusion

Ce chapitre décrit une méthode de tatouage numérique combinant une approche de zéro-tatouage dans la région de l'objet anatomique et une approche de tatouage par insertion de marque dans la région du fond noir de l'image pour l'authentification et l'identification des images médicales. La marque a été insérée uniquement dans le fond noir de l'image afin d'éviter de modifier la partie anatomique dont le changement peut affecter le diagnostic médical. La méthode proposée fournit une solution d'authentification forte. En effet, cette méthode propose deux façons d'authentifier l'image : soit par l'extraction de la marque insérée dans le fond noir soit par les caractéristiques extraites de la partie

anatomique de l'image. De plus, elle permet d'authentifier l'image même en cas de dommage sur le fond noir rendant la marque insérée inutilisable. L'analyse des résultats de la méthode proposée montre sa robustesse contre l'attaque de filtrage médian, le bruit du sel et du poivre, le filtrage moyen, le recadrage du coin supérieur gauche, le filtrage gaussien, l'égalisation d'histogramme, le bruit gaussien, la rotation, l'affûtage et la traduction des attaques. La comparaison avec des méthodes existantes montre également que notre méthode offre de bonnes performances. Dans le chapitre suivant nous proposons une approche de tatouage forte et résistante aux clones pour la sécurité des images médicales, c'est une solution originale pour répondre aux objectifs de sécurité qui permet de tirer avantage de la complémentarité qui existe entre les mécanismes de tatouage et les mécanismes de cryptographie.

Chapitre 5

Une approche d'authentification forte et résistante aux clones pour le système d'images médicales

5.1 Introduction

Les applications de télémédecine sont de plus en plus utilisées en raison du développement rapide de l'imagerie numérique et des technologies de l'information et de la communication. Les informations médicales qui comprennent des images médicales numériques et les informations des patients sont extraites et transmises sur des réseaux non sécurisés pour le diagnostic clinique et les traitements. Le tatouage numérique est l'une des principales approches utilisées pour garantir la sécurité des images médicales. Néanmoins, dans certains cas, la seule utilisation du tatouage numérique n'est pas suffisante pour atteindre un haut niveau de sécurité. En effet, la marque pourrait contenir des informations essentielles sur le patient et doit être protégée. Dans de tels cas, la cryptographie peut être utilisée pour protéger la marque et améliorer la gestion sécurisée globale dans l'environnement médical. Dans ce chapitre, nous proposons une approche de tatouage résistante aux clones combinant une technique de tatouage à expansion de différence avec une technique cryptographique basée sur des clés secrètes générées par un dispositif résistant aux clones appelé Secret Unknown Ciphers (SUCs). L'utilisation de SUC pour signer la marque renforce la sécurité des images médicales pendant leur transfert et leur stockage. Les résultats expérimentaux montrent que le système offre un haut niveau de sécurité contre diverses formes d'attaques.
La première partie de ce chapitre décrit la motivation de la méthode proposée. La deuxième partie exprime l'avantage de combiner le tatouage avec des primitives cryptographiques.

Sous certaines contraintes, nous verrons que ces deux méthodes peuvent être combinées pour vérifier la fiabilité de l'image, sa traçabilité et la non-répudiation. La troisième partie de ce chapitre présente le concept de SUC et son contexte technologique. La quatrième partie de ce chapitre porte sur la description d'un nouveau système de tatouage résistant au clonage dans cette partie nous présentons le processus de la génération de la marque, le processus d'insertion de la marque et le processus d'extraction de la marque.
Ce chapitre se termine par l'évaluation des résultats expérimentaux et la comparaison avec les travaux existants.

5.2 Motivation et état de l'art

Il existe deux approches principales pour garantir un niveau de sécurité élevé des systèmes de transmission d'images médicales [70] : Premièrement, le tatouage numérique qui est défini comme une technique d'insertion de certaines informations dans une image médicale [159]. Les cibles de tatouage numérique sont le masquage des données, le contrôle d'intégrité et l'authenticité [28]. Deuxièmement, les métadonnées sont définies dans ce contexte comme les données jointes à une image médicale. Ici, la signature numérique est l'une des fameuses techniques de métadonnées qui garantissent l'intégrité et l'authenticité des images médicales.

La figure 5.1 illustre l'utilisation des deux techniques précédentes (tatouage et signature) pour fournir des systèmes de transmission d'images médicales avec un haut niveau de sécurité. Sur la figure 5.1-(a), une signature numérique est générée à partir d'une valeur hachée de l'image médicale originale puis elle est cryptée par un algorithme de cryptage asymétrique. L'image médicale originale et la signature numérique sont ensuite concaténées pour générer une image signée. Côté récepteur, la vérification de la validité de l'image signée résultante nécessite que la clé publique correspondante soit utilisée pour récupérer la valeur hachée reçue et la comparer à nouveau avec la valeur hachée calculée à partir de l'image médicale originale. Le schéma de signature numérique présenté déploie une fonction de hachage et un cryptage asymétrique. Cependant, la plupart des fonctions de hachage sont vulnérables aux collisions de sortie et aux modifications accidentelles. De plus, la plupart des algorithmes de chiffrement asymétriques sont considérés comme des techniques de calcul intensif, relativement lents, et une autorité de certification est requise pour gérer les clés publiques et privées [110].

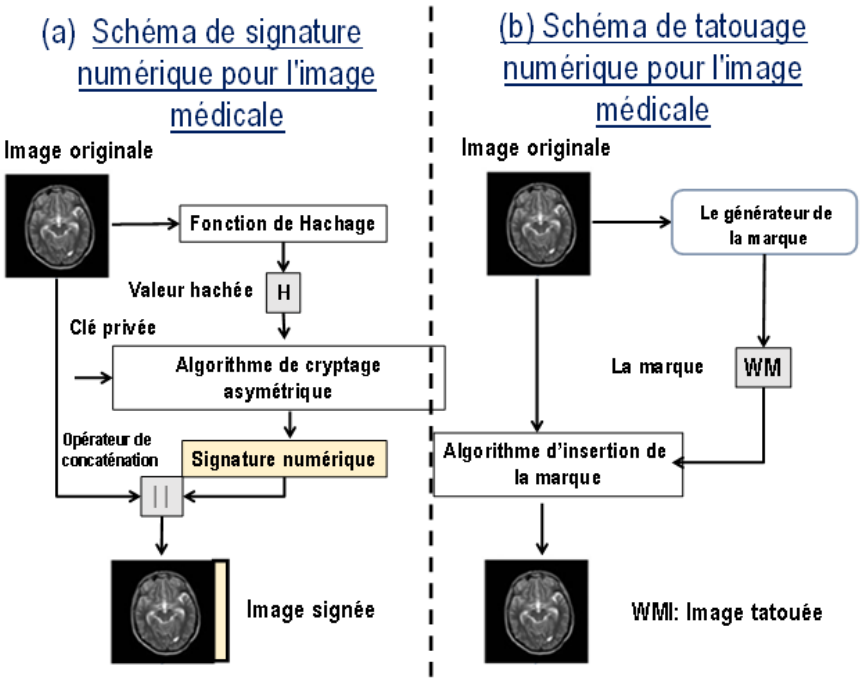


FIGURE 5.1 – Deux propositions de systèmes sécurisés de transmission d'images médicales

Sur la figure 5.1-(b), un système de tatouage est présenté. La marque (WM) est notamment extraite de l'image médicale originale par un générateur de marque. Ensuite, la marque extraite est insérée dans l'image médicale originale. En outre, les informations médicales telles que les informations du patient, le logo de l'hôpital, l'ID du médecin peuvent être intégrées dans l'image originale sous forme d'une marque pour l'authentification, l'inviolabilité et la protection des droits d'auteur [33],[94]. Dans [110], une discussion technique sur le tatouage pour les images médicales et d'autres techniques de sécurité a été passée en revue. Les résultats ont montré que les techniques de tatouage ne sont pas encore acceptées pour les applications modernes, où les techniques de tatouage actuelles souffrent de certaines faiblesses ; par exemple, la sensibilité de l'erreur sur les bits est très faible et la possibilité de détecter une image de marque valide en tant qu'image de marque non valide ou vice versa est très élevée [110]. Comme solution à ces vulnérabilités, plusieurs approches de sécurité des images médicales qui fusionnent les techniques de tatouage et de cryptographie pour les systèmes d'images médicales ont été proposées dans la littérature comme [16], [98], [18]. Dans ce qui suit, nous présentons brièvement quelques notions préliminaires utiles à compréhension de l'approche de tatouage résistante au clonage proposée.

Il s'agit dans un premier temps de la notion de PUF (Physically Unclonable Function), puis de la notion de SUC (Secret Unknown Cypher) proposée comme alternative à la notion de PUF, consistante avec cette dernière et palliant à ses inconvénients.

5.3 Système de transmission d'images médicales non clonable : PUF et non « clonabilité »

Dans [157], le mécanisme PUF (Physically Unclonable Function) a été proposé pour fournir au système d'image médicale, Medical Image System (MIS) en anglais, des empreintes électroniques intrinsèques aux dispositifs médicaux. Ici, chaque appareil / générateur d'images médicales a un PUF. La figure 5.2 illustre le système d'image médicale (MIS) conçu dans [157].

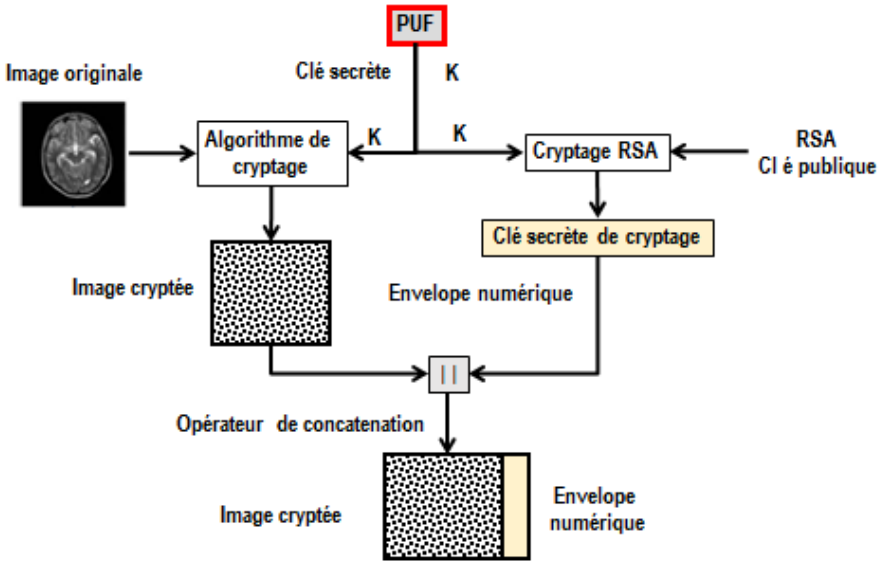


FIGURE 5.2 – Système d'imagerie médicale déployant un PUF avec un algorithme de chiffrement et un système RSA

En particulier, PUF génère une clé secrète K pour un algorithme de chiffrement. La clé secrète générée K est utilisée pour crypter l'image originale. Ici, le système RSA en tant qu'algorithme asymétrique protège la clé secrète générée K et génère une enveloppe

numérique sous forme de K chiffré par la clé publique RSA du récepteur. Un dispositif / générateur d'images médicales en tant qu'expéditeur transmet l'image cryptée résultante avec l'enveloppe numérique du côté réception. Côté récepteur, le récepteur récupère la clé secrète K de l'enveloppe numérique en utilisant sa clé secrète RSA. Ensuite, le récepteur utilise K pour déchiffrer l'image chiffrée reçue. Semblable au mécanisme Pretty Good Privacy (PGP) pour la communication de données [172], le MIS proposé dans la figure 5.2 fournit une confidentialité cryptographique et une authentification pour les images médicales numériques. La seule différence entre eux est que le MIS proposé utilise un PUF pour générer une clé secrète K au lieu d'un générateur de nombres pseudo-aléatoires dans le cas de PGP. Toutefois, le MIS proposé est un mécanisme de calcul intensif, relativement lent, et nécessite une autorité de certification pour gérer les clés publiques et privées RSA. D'autre part, plusieurs travaux de recherche ont été publiés sur les PUFs au cours des deux dernières décennies, tels que les PUF à oscillateur en anneau [48], TERO-PUF [88], les PUF arbitres [80], les PUF basés sur le chaos [102], etc. Malheureusement, les réponses bruitées et incohérentes ainsi qu'un nombre limité de paires PUF-défi-réponse sont considérées comme les principales vulnérabilités des PUF [40].
Toute tentative pour contrer ces vulnérabilités rend l'implémentation du PUF plus coûteuse et compliquée. Pour surmonter de telles faiblesses, une technique appelée SUC a été proposée comme une identité résistante aux clones définie dans [4] et [5]. Le SUC proposé fournit à chaque appareil électronique du MIS une signature numérique unique imprévisible et résistante aux clones. Ces modules physiques SUC, comparés aux PUF, sont hautement cohérents en tant que structures numériques pures. Les SUCs sont auto-créés et intégrés dans des dispositifs FPGA (Field Programmable Gate Arrays) standard dans un processus de post-fabrication où le fabricant du dispositif peut être exclu du processus de sécurité.

5.4 Le concept SUC et le contexte technologique

L'objectif de cette section est d'exprimer le concept et le principe de fonctionnement de SUC, qui n'est pas largement connu dans la littérature publique.

Le concept de chiffrement inconnu est un paradigme de sécurité entièrement nouveau dans la littérature publique. Le chiffrement inconnu ici ne traite pas de la protection des communications ou des liens entre au moins deux parties, en tant qu'émetteur et récepteur, qui nécessite que le chiffrement soit communément connu des deux parties

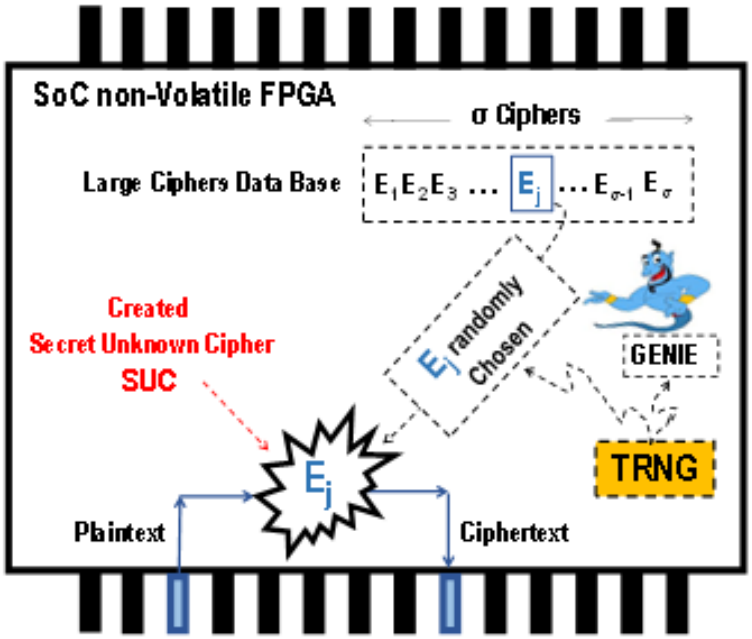


FIGURE 5.3 – Le concept de SUC (Secret Unckown Ciphers)

(principe de Kerckhoffs). En particulier, le SUC est fondamentalement conçu pour que le processus d'identification puisse servir d'identité résistante aux clones [4], [5]. La conception du SUC part du principe suivant lequel la «non clonabilité» n'est possible que si des structures inconnues sont créées. Par conséquent, un chiffrement conçu pour être intégré comme une structure inconnue de quiconque (y compris son concepteur) ne viole pas le principe de Kerckhoff. D'un autre côté, le SUC ne doit pas être confondu avec la «sécurité par obscurité», où le chiffrement est conçu par un cryptographe, connu du fabricant, puis gardé secret et obscur.

La création de SUC est une tâche très difficile. La figure 5.3 illustre un concept de création de SUC possible dans un dispositif FPGA non volatile (NV) ayant une capacité d'auto-reconfiguration interne. Une grande classe de chiffres $\{E1, E2 \ldots E\}$ sont d'abord créés tels que $\sigma \rightarrow \infty$ et proposés à la sélection. Ensuite, un processus à événement unique déclenche le générateur de nombres aléatoires vrais (TRNG) interne au FPGA, ce qui conduit à sélectionner au hasard un chiffre inconnu Ej parmi le nombre infini des chiffres distincts créés. Un module matériel TRNG est proposé dans tous les appareils FPGA modernes répondant aux exigences cryptographiques standard de l'état de l'art NIST (voir les spécifications du module TRNG dans le FPGA utilisé dans l'article [89]). Après ce

processus, toutes les entités en pointillés de la figure 5.3 sont ensuite supprimées de manière irréversible de la puce.
Le chiffre résultant est un chiffre secret mais inconnu et il est une sélection non répétable. C'est même un choix inconnu pour le concepteur / créateur de chiffrement lui-même. Le «Secret Unknown Cipher» (SUC) est réalisable dans un dispositif VLSI émergent qui permet l'auto-création de structures secrètes utilisables inconnues permanentes comme «une mutation électronique», comme indiqué dans [3]. Notez que pour la fonctionnalité du concept, il n'est pas nécessaire de publier la procédure / le programme de création SUC de la classe de chiffrement, qui est désormais désigné comme le «GENIE» en tant que concepteur de chiffrement intelligent. Cependant, pour l'analyse de sécurité la plus défavorable, nous supposons que le chiffrement créant «GENIE» est publié.

5.4.1 Le concept de création de chiffres inconnus en tant qu'entités / modules résistants aux clones

Pour construire une approche de tatouage résistante aux clones, il est nécessaire que chaque dispositif médical insère son identité unique non clonable ou résistante aux clones. L'idée clé consistant à générer une fonction câblée SUC pour servir l'identité résistante aux clones est illustrée à la figure 5.14.
Cette identité est basée sur le déclenchement d'un processus aléatoire à événement unique qui injecte dans un dispositif System-on-Chip (SoC) un système irréversible, le module de chiffrement irremplaçable et difficile à prévoir. D'un point de vue pratique, si le créateur du chiffrement lui-même ne peut pas prédire exactement le chiffrement créé, alors le chiffrement est considéré comme inconnu lorsque la taille de la classe de chiffrement $\sigma \to \infty$.
La figure 5.14 illustre la phase de création de SUC dans un environnement sécurisé. Le processus peut se décrire comme suit :
***Phase de création du SUC* :**
Une autorité de confiance (TA) injecte une fois dans un dispositif SoC le progiciel «GENIE» en tant que créateur de SUC pendant une courte période (autant de temps que nécessaire pour créer un chiffre inconnu, généralement quelques millisecondes). Ensuite, le «GENIE» est déclenché en interne pour générer / sélectionner un chiffrement sécurisé permanent et imprévisible à l'aide d'un flux binaire interne, non répétable, imprévisible et inconnu à partir du TRNG intégré. Après avoir créé un SUC, le «GENIE» est complètement et irréversiblement supprimé. Ce qui reste est un chiffrement opérationnel non

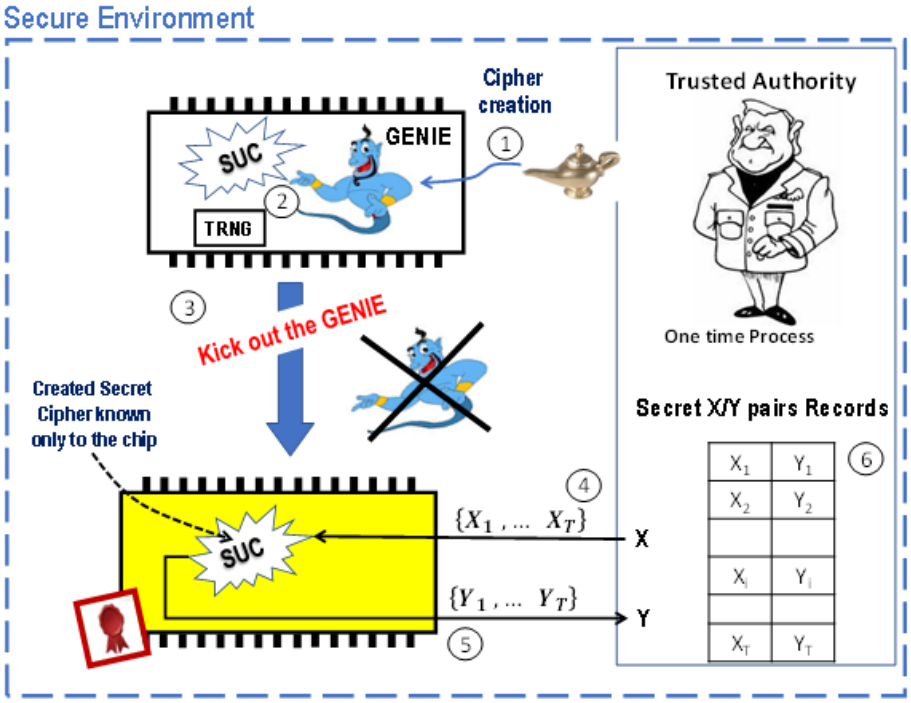


FIGURE 5.4 – Mutation d'un chiffre secret inconnu (SUC) en un dispositif système sur puce (SoC) [101]

amovible et inchangeable (un SUC) que personne ne connaît.

Phase d'authentification du SUC :

TA sélectionne de manière aléatoire un ensemble $\{x_1, \dots x_T\}$ en texte clair parmi les 2^n combinaisons possibles, où n est la taille de l'espace d'entrée / sortie SUC en bits. TA stimule le dispositif SoC pour chiffrer les vecteurs en texte clair dans les textes chiffrés $\{y_1, \dots y_T\}$ en utilisant son SUC dans le dispositif. Les T paires (x_i, y_i) résultantes sont stockées sous forme de paires secrètes dans les enregistrements individuels (personnels) de l'appareil par le TA. Les enregistrements doivent être gardés secrets pour une utilisation ultérieure. Comme les bits TRNG créés sont entièrement et exclusivement responsables de la création du SUC, et comme les bits TRNG sont imprévisibles, non répétables et inconnus, le SUC créé résultant dans le dispositif SoC est également inconnu et imprévisible, ainsi pour chaque $t > 0$:

$$SUC = GENIE(TRNG_t) \tag{5.1}$$

Cela implique que,

$$SUC_t : \{0,1\}^n \times \{0,1\}^{k_t} \rightarrow \{0,1\}^n \tag{5.2}$$

où n et k_t sont respectivement la taille en bits de l'espace d'entrée/sortie SUC et la taille en bits de la clé secrète du chiffrement.

Ainsi, le nombre maximum de permutations différentes est $\sigma = 2^n!$ tout comme le nombre de toutes les permutations possibles de $\{0,1\}^n$ à $\{0,1\}^n$. Par conséquent, dans ce cas, le nombre de blocs de chiffrements sélectionnables possibles de taille n est

$$\sigma = 2^n! \tag{5.3}$$

Le SUC a donc la propriété de pouvoir générer un grand nombre de paires défi-réponse (CRP – Challenge Response Pair) distinctes sous forme de paires texte clair - texte chiffré, qui peut aller jusqu'à $2^n!$. Cela compense le manque d'espace CRP dans le cas des PUF analogiques traditionnels. Comme Le chiffrement généré SUC_t est le résultat de la séquence du flux de bits aléatoires $TRNG_t$ qui n'est connue de personne, il est très probable que pour deux points de temps $t1$ et $t2$.

$$TRNG_{t1} \neq TRNG_{t2} \rightarrow SUC_{t1} \neq SUC_{t2} \tag{5.4}$$

Par conséquent, chaque dispositif SoC résultant a donc son SUC personnel avec une

probabilité de

$$(1 - \frac{1}{\sigma}) \to 1 \tag{5.5}$$

Comment utiliser un SUC ?

La figure 5.15 montre un protocole d'identification bidirectionnel générique utilisant de

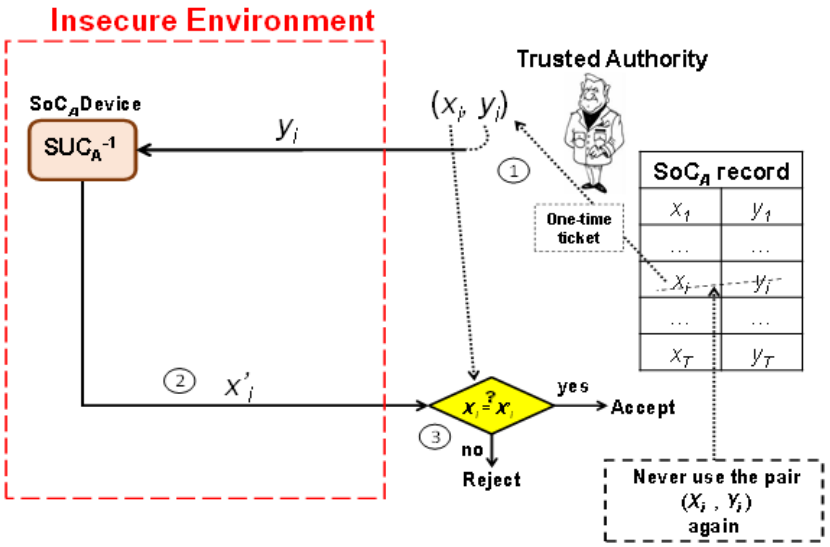


FIGURE 5.5 – Protocole d'identification bidirectionnel sur un canal non sécurisé [101]

tels SUC pour authentifier un dispositif SoC_A personnalisé.
Un protocole d'identification basé sur SUC peut procéder comme suit :

1. Une paire secrète (x_i, y_i) est choisie au hasard parmi les enregistrements secrets de SoC_A du TA. Ensuite, le TA teste le dispositif SoC_A en lui demandant la source correspondant à la valeur cryptée y_i sur un canal non sécurisé.
2. L'appareil SoC_A répond en envoyant le texte clair décrypté x'_i.
3. Si $x'_i = x_i$, le périphérique SoC_A est réputé authentique et la paire (x_i, y_i) est alors marquée comme paire utilisée et n'est plus jamais utilisée en évitant une attaque de relecture pour une sécurité maximale.

Des versions raffinées de ce protocole sont développées comme indiqué dans [103]. Il est démontré qu'une gestion des CRP beaucoup plus efficace et à faible coût est possible en raison de la propriété d'invisibilité du SUC par rapport aux propriétés sujettes aux collisions de tous les mappages basés sur les PUFs (comme un hachage inconnu).

5.5 Proposition d'un nouveau système de tatouage médical sécurisé non clonable

L'idée clé de l'approche proposée est d'intégrer le SUC dans chaque dispositif d'imagerie médicale. Un générateur d'images médicales avec un SUC intégré, en particulier, devient un générateur d'images médicales résistant aux clones. La figure 5.16 illustre une comparaison entre un dispositif médical traditionnel sans identité et un dispositif médical avec un SUC intégré.

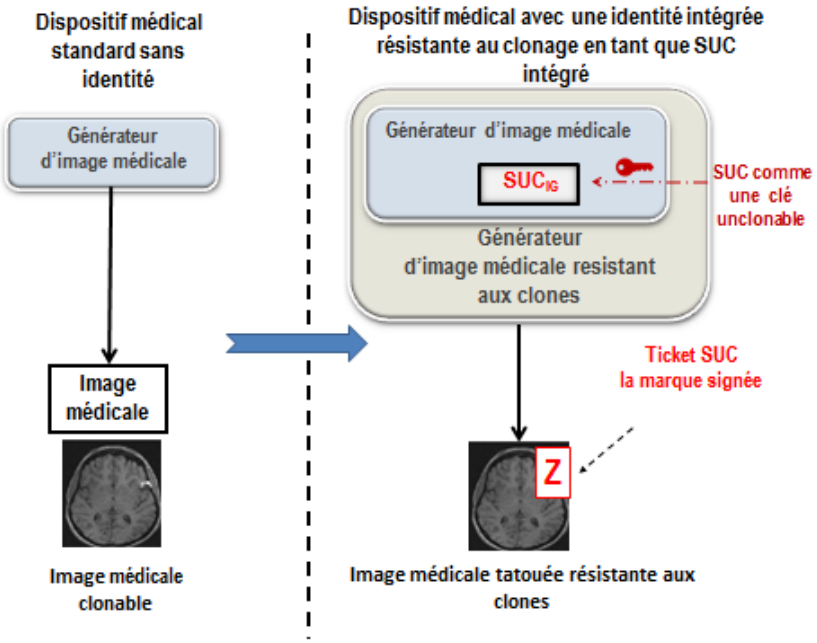


FIGURE 5.6 – Le concept proposé d'une image médicale résistante aux clones en utilisant la technique SUC

Le générateur d'images médicales proposé résistant aux clones (CRMIG) produit une image tatouée résistante aux clones comme suit :

— Après avoir généré une image dite image originale, une marque WM est générée, puis elle est signée à l'aide d'une paire d'entrée-sortie SUC également appelée ticket. La marque signée résultante (Z) est intégrée dans l'image originale en tant que signature de la marque unique.

— Le CRMIG proposé est robuste contre toutes les attaques de traitement d'image et

de clonage attendues car SUC fournit un générateur d'images médicales avec une signature unique qui est non répétable et non clonable.

5.5.1 L'architecture proposée du système d'images médicales

Le MIS proposé permet à un médecin / utilisateur de recevoir en toute sécurité une image médicale via un serveur TA. Le médecin ne communique pas directement avec le générateur d'images médicales. La Figure 5.7 montre le scénario de fonctionnement du système proposé.

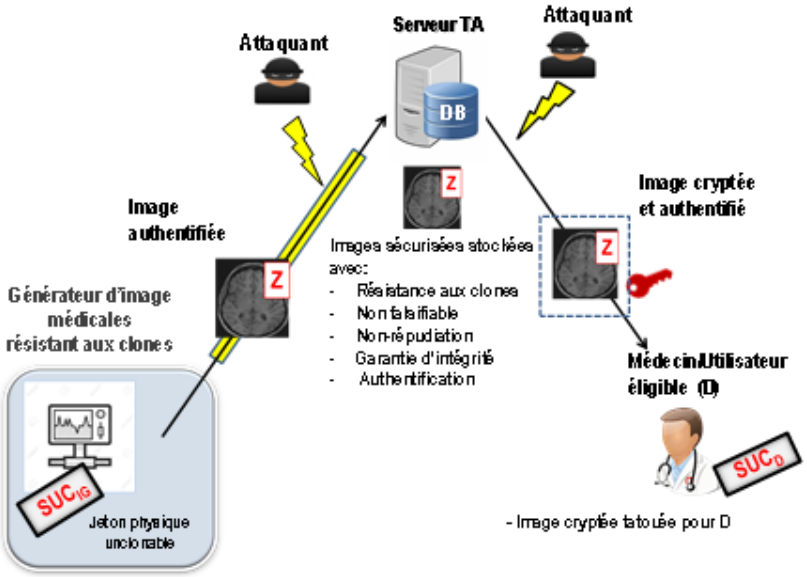


FIGURE 5.7 – Scénario de fonctionnement du système proposé

Ici, le serveur TA joue un rôle de médiateur dans le système proposé.
Dans la figure 5.7, l'architecture de système proposée est composée de trois composants principaux.
Premièrement : le serveur TA héberge une base de données sécurisée (DB).
Deuxièmement : un dispositif médical comme exemple de générateur médical résistant aux clones et un médecin en tant qu'utilisateur éligible avec un SUC intégré dans un dispositif tel qu'un ordinateur ou un mobile / jeton.
Tous les dispositifs médicaux doivent être enregistrés dans TA DB. Le MIS proposé atteint les caractéristiques de sécurité suivantes :

— Les images médicales ne sont pas reproductibles et ne sont pas remplaçables.

— Unicité prouvable de l'image médicale.

— Privilège d'authentification sélective.

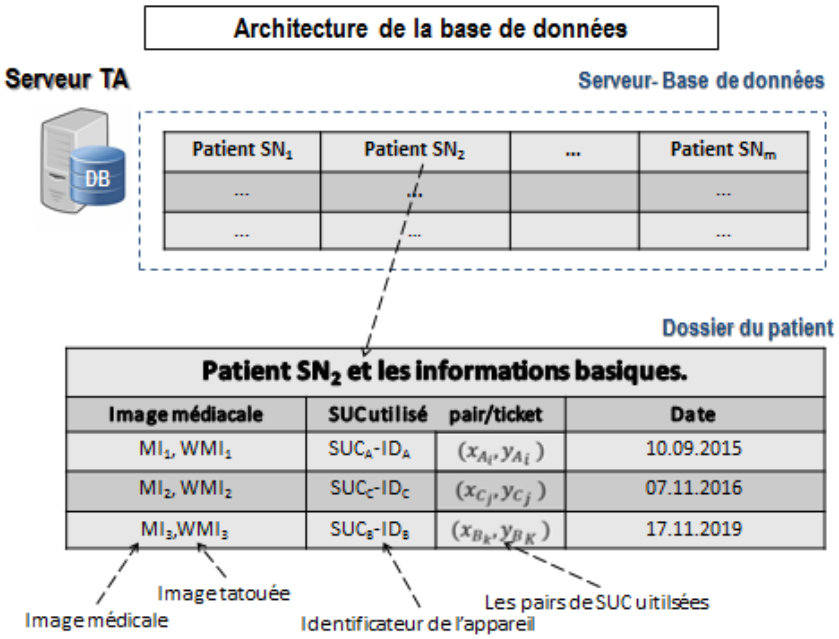


FIGURE 5.8 – Un exemple de dossier d'un patient dans la base de données DB

La figure 5.8 illustre la conception de la base de données du TA (TA DB) qui stocke les dossiers des patients. Chaque dossier de patient contient des images médicales du patient et quelques informations sur leurs images tatouées. La figure 5.8 montre un exemple concernant le dossier d'un patient composé des informations de base du patient, des images tatouées du patient, des ID des dispositifs médicaux et des tickets utilisés pour la signature des marques, et des données. Notez que l'image tatouée résistante aux clones est transmise et stockée dans TA DB. Par conséquent, chaque utilisateur / médecin doit envoyer une demande au serveur d'assistance technique pour obtenir l'image médicale d'un patient. Dans cette architecture de système proposée, l'utilisateur / médecin ne peut pas communiquer directement avec le dispositif médical. La communication se fait uniquement via le serveur TA et la communication avec le serveur TA s'effectue sur des canaux non sécurisés.

5.5.2 L'approche de tatouage résistante aux clones proposée : insertion et extraction

Le système proposé comporte deux phases principales. Premièrement, générer et insérer une marque signée dans l'image originale. Deuxièmement, extraire la marque pour vérifier l'authenticité et l'intégrité de l'image tatouée. Ces deux phases sont décrites comme suit :

— **Phase de la génération et d'insertion de la marque (signature d'une marque unique) :**
Les caractéristiques pertinentes à savoir l'asymétrie, l'entropie et la médiane sont extraites de l'image originale [43]. Le nom du patient est extrait de l'en-tête de l'image DICOM et les initiales correspondantes (première lettre du prénom et nom de famille) sont transformées en une matrice binaire de taille 16×16. Une matrice de taille 16×16 est ensuite générée à partir de l'image originale par un processus de soustraction cumulative. Toutes ces informations sont utilisées pour construire une marque significative basée sur le modèle Jacobien [50].

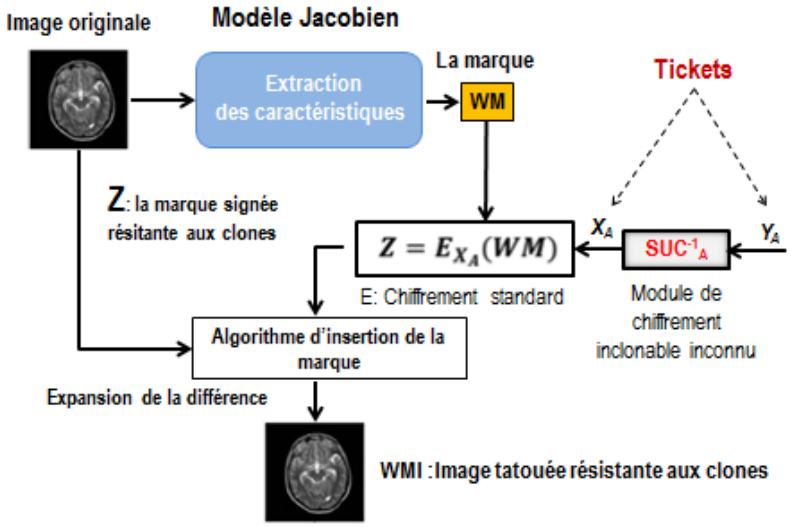


FIGURE 5.9 – Le processus de génération et d'insertion de la marque résistante aux clones

Le processus d'insertion de la marque est illustré sur la figure 5.9. Un chiffrement standard est déployé pour signer la marque extraite en utilisant un ticket unique (x_A, y_A) généré par le SUC_A de l'appareil. Ici, un chiffrement standard peut être perçu comme un outil pour le mécanisme de signature. La marque signée résultante peut être considérée comme une signature de marque unique résistante aux clones Z. Après cela, Z est insérée dans l'image originale à l'aide de la technique d'extension de différence pour obtenir l'image tatouée résistante aux clones (WMI).

— **Phase d'extraction et de vérification de la marque :**
La procédure d'extraction et de vérification de la marque est l'inverse de la phase d'insertion et de signature de la marque. Un tel processus est illustré à la figure 5.10. Le processus commence par l'extraction de la marque signée Z et la récupération de la marque.

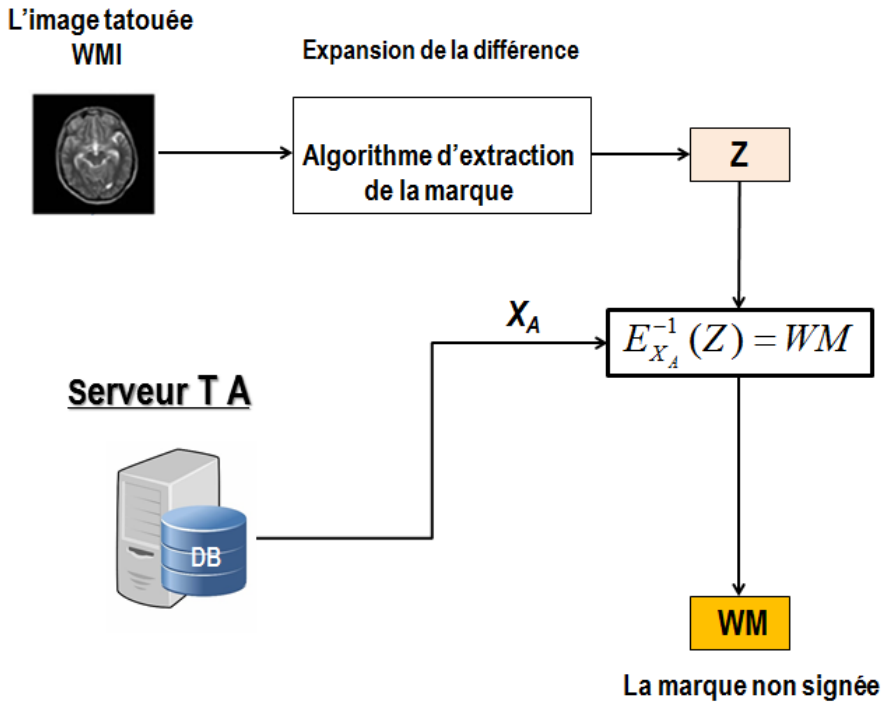


FIGURE 5.10 – Le processus d'extraction de la marque

Au cours de ce processus, le texte en clair (plaintext) stocké X_A obtenu à partir du serveur TA est utilisé pour terminer le processus de vérification. Le récepteur

doit à nouveau comparer le WM non signé avec le WM extrait. La vérification (la comparaison) peut être effectuée avant les procédures cliniques et le diagnostic.

5.5.3 Analyse du système : avantages de combiner le SUC et le tatouage

L'objectif principal de cette section est de montrer les procédures de tatouage particulières et efficaces lorsque la technique SUC est impliqué. Dans ce but, deux protocoles primitifs génériques proposés pour générer et vérifier les images tatouées résistantes aux clones sont présentés.

Protocole 1 : enregistrement sécurisé d'une transaction d'image médicale

Le premier protocole générique proposé est conçu pour illustrer le processus de génération d'une image médicale tatouée résistante aux clones. Le dispositif médical A génère une image tatouée et l'envoie au serveur TA. Ensuite, le serveur TA vérifie l'image tatouée et la stocke dans la base de données. Dans ce qui suit, le protocole proposé peut procéder comme indiqué dans la figure 5.11 :

1. Le dispositif médical A demande au serveur TA de démarrer le processus de génération d'une image tatouée.
2. Le serveur TA sélectionne au hasard un ticket (x_{Ai}, y_{Ai}) dans le dossier secret du dispositif médical A dans DB.
3. Le serveur TA répond avec y_{Ai}.
4. Le dispositif médical A calcule x_{Ai} en utilisant son SUC comme SUC_A^-1 (y_{Ai})=x_{Ai}
5. Le dispositif médical A génère ou sélectionne une image médicale MI_1.
6. Le dispositif médical A génère une marque WM_1 à partir de MI_1
7. Le dispositif médical A chiffre la marque générée WM_1 en utilisant un chiffrement standard E avec la clé secrète x_{Ai} comme : $Z = E_{xAi}(WM_1)$.
8. Le dispositif médical A insère la marque signée Z dans l'image originale MI_1 pour générer l'image médicale tatouée résistante aux clones WMI_1.
9. Le dispositif médical A envoie WMI_1 au serveur TA.
10. Le serveur TA inverse l'algorithme d'insertion pour extraire Z et récupérer l'image médicale MI_1 de l'image tatouée reçue WMI_1 puis utilise x_{Ai} pour récupérer la marque WM_1'

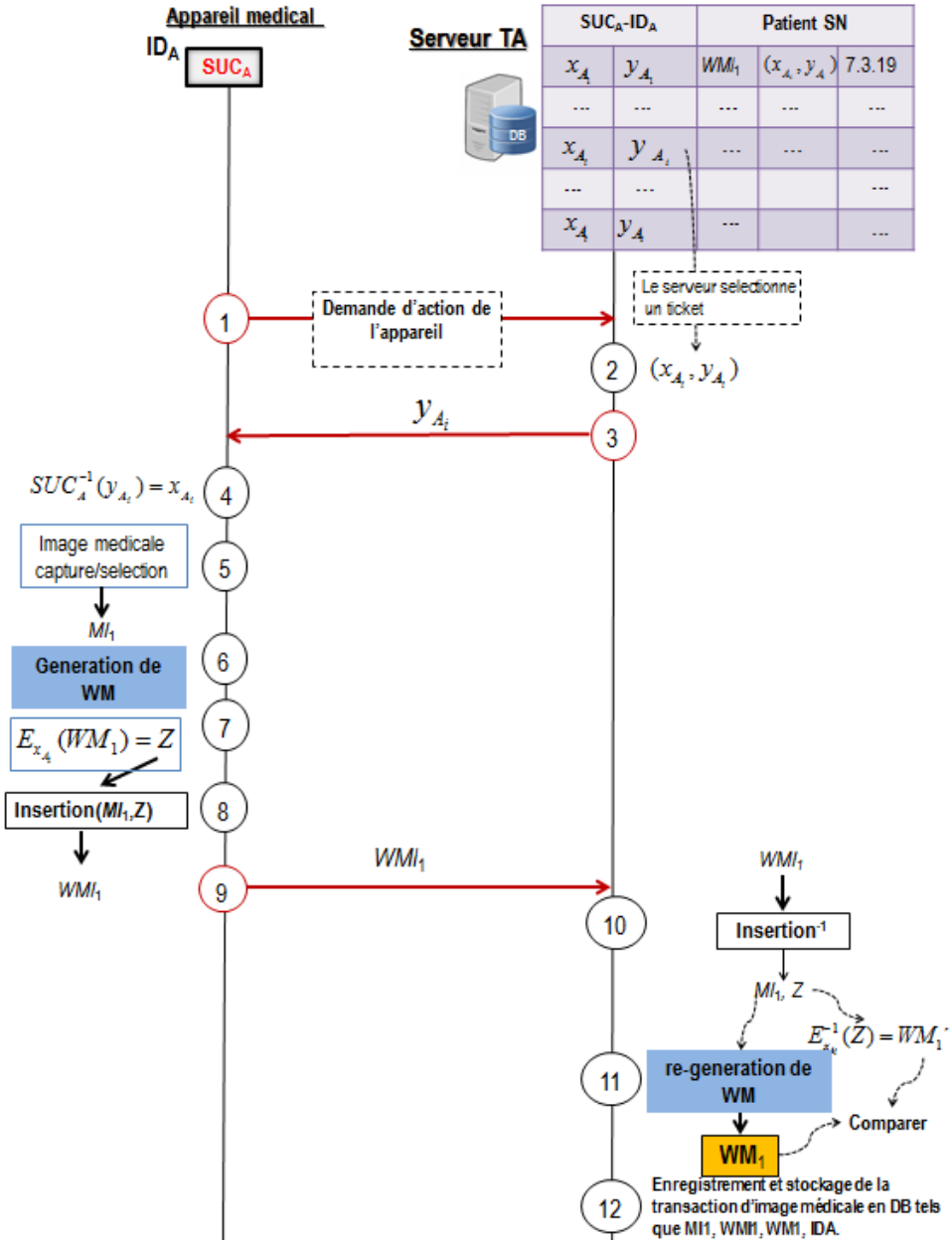


FIGURE 5.11 – Le protocole d'enregistrement sécurisé d'une transaction d'image médicale

11. Le serveur TA génère WM_1 à partir de l'image médicale récupérée MI_1 et rejette si $WM_1 \neq WM_1'$
12. Le serveur TA stocke la transaction d'image médicale MI_1, WMI_1,WM_1,et ID_A, ainsi que le ticket utilisé (x_{Ai}, y_{Ai}) dans DB pour une utilisation ultérieure.

Le protocole 1 atteint les fonctions de sécurité suivantes :

— Le dispositif médical A génère une image tatouée résistante aux clones en déployant son SUC_A.

— L'image tatouée résultante est inviolable.

— Le dispositif médical A ne peut nier avoir généré l'image tatouée.

Protocole 2 : protocole d'authentification utilisateur-serveur pour la vérification d'image

Le deuxième protocole proposé permet à un utilisateur tel qu'un médecin B de demander une image médicale d'un patient au serveur TA. Ensuite, le serveur TA répond avec l'image demandée comme le montre la figure 5.12.

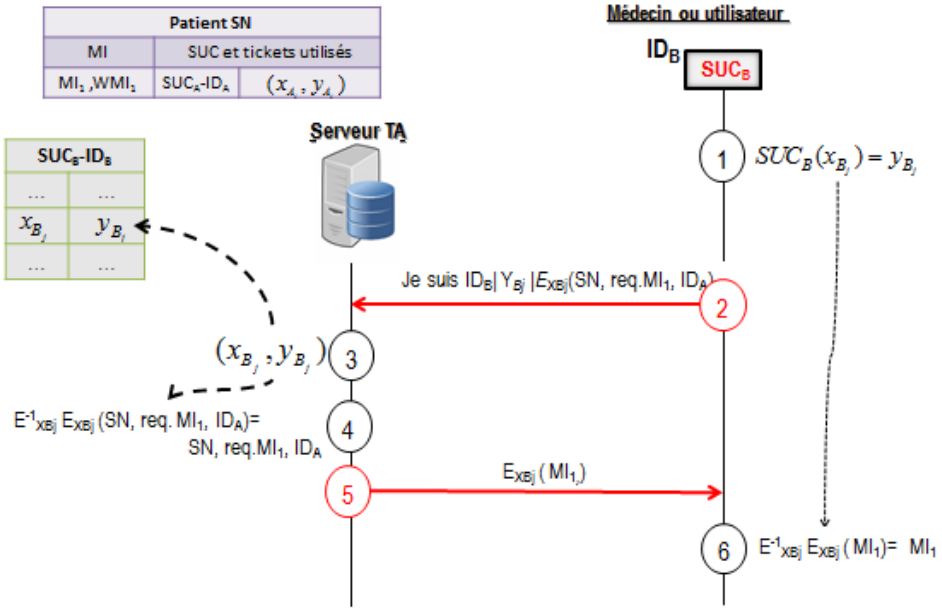


FIGURE 5.12 – Le protocole d'authentification utilisateur-serveur pour la vérification d'image

Le protocole 2 peut procéder comme suit :

1. Le docteur B sélectionne au hasard x_{Bj} et calcule la valeur chiffrée y_{Bj} correspondante en utilisant son SUC_B.
2. Le docteur B demande au serveur TA d'envoyer l'image médicale requise MI_1 du patient SN comme $y_{Bj} \mid E_{xBj}\ (SN, req.MI_1, ID_A)$, où, $req.MI_1$ est la demande de l'image médicale MI_1.
3. Le serveur TA utilise y_{Bj} pour déterminer x_{Bj} à partir de l'enregistrement secret du périphérique B dans DB.
4. Le serveur TA déchiffre le message $E_x^{-1}{}_{Bj} E_{xBj}(SN, req.MI_1, ID_A) = SN, req.MI_1, ID_A$
5. Le serveur TA répond $E_{xBj}(MI_1)$ où MI_1 est l'image tatouée demandée.
6. Le docteur B déchiffre le message reçu : $E_x^{-1} B_j E_{xBj}(MI_1) = MI_1$

Ce protocole proposé atteint les fonctions de sécurité suivantes :

— Le docteur B ne peut pas nier l'utilisation de l'image génerée par le dispositif médical A.

— Le docteur B ne peut nier avoir reçu l'image tatouée du serveur TA.

— L'image ne peut pas être modifiée ou truquée ultérieurement par un médecin B.

— Le serveur TA sait «qui et quand» un utilisateur tel qu'un médecin B utilisait l'image médicale.

5.5.4 Génération de la marque à l'aide d'un modèle Jacobien

Les caractéristiques pertinentes à savoir l'asymétrie, l'entropie et la médiane sont extraites de l'image originale. Le nom du patient est extrait de l'en-tête de l'image DICOM et les initiales correspondantes (première lettre du prénom et nom de famille) sont transformées en une matrice binaire de taille 16×16. Une matrice de taille 16×16 appelée add_{mat} est ensuite générée à partir de l'image originale par un processus de soustraction cumulative. Toutes les informations précédentes sont utilisées pour construire une marque WM significative basée sur le modèle Jacobien. Nous proposons 5.13 fonctions avec 16 paramètres pour générer une matrice 16×16 qui peut être exploitée pour construire la marque. Nous construisons toutes les fonctions en utilisant la matrice binaire du nom du patient, les trois caractéristiques pertinentes (asymétrie, entropie et médiane) extraites de l'image hôte et la matrice add_{mat} extraite de l'image hôte. Le modèle matriciel Jacobien proposé est basé sur un vecteur Y de 16 fonctions.

$$Y_i : R^{16} \rightarrow R^{16}, i = 1, 2, \ldots, 16 \tag{5.6}$$

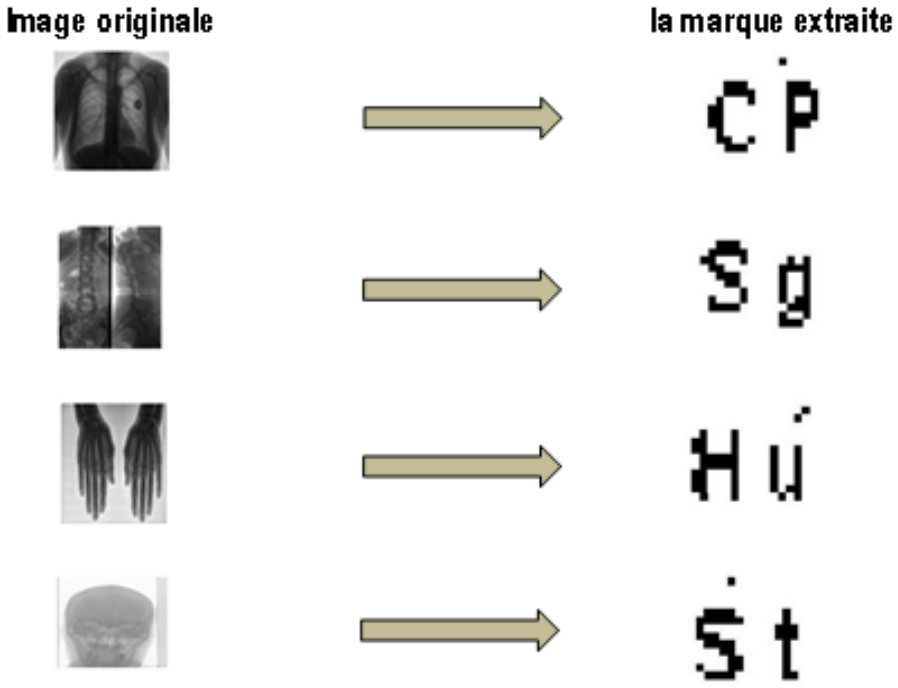


FIGURE 5.13 – Images originales et exemples de marques correspondants

Ces fonctions $Y_1, Y_2, \cdots, Y_{16}$ sont définies par

$$Y_i(x_1, x_2, \ldots, x_{16}) = \sum_{j=1}^{16} \frac{add\_mat(i,j)}{f\_val_i} \frac{x_j^2}{2}, j = 1, \ldots, 16 \tag{5.7}$$

Où f_val_i est défini comme suit :

$$f_{val_i} = \begin{cases} lavaleurdel'asymetrie & si \quad 1 \leq i \leq 5 \\ lavaleurdel'entropie & si \quad 6 \leq i \leq 10 \\ lavaleurdemediane & si \quad 11 \leq i \leq 16 \end{cases} \tag{5.8}$$

La matrice Jacobienne J de Y en $(x_(1,)x_(2,), \ldots, x_(1_6))$ est une matrice de taille 16×16 donnée par

$J_Y(x_1, \ldots, x_{1_6})$=

$$\begin{bmatrix} \frac{add\_mat(1,1)}{f\_val_1}x_1 & \cdots & \frac{add\_mat(1,16)}{f\_val_1}x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(5,1)}{f\_val_1}x_1 & \cdots & \frac{add\_mat(5,16)}{f\_val_1}x_{16} \\ \frac{add\_mat(6,1)}{f\_val_2}x_1 & \cdots & \frac{add\_mat(6,16)}{f\_val_2}x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(10,1)}{f\_val_2}x_1 & \cdots & \frac{add\_mat(10,16)}{f\_val_2}x_{16} \\ \frac{add\_mat(11,1)}{f\_val_3}x_1 & \cdots & \frac{add\_mat(11,16)}{f\_val_3}x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(16,1)}{f\_val_3}x_1 & \cdots & \frac{add\_mat(16,16)}{f\_val_3}x_{16} \end{bmatrix}$$

Cette matrice Jacobienne de taille 16×16 est une matrice d'image utilisée comme une marque à intégrer dans l'image originale. Des exemples de marques générées avec le modèle Jacobien sont présentés à la figure 5.13.

5.5.5 Analyse du tatouage numérique et évaluation de la sécurité

Dans la section suivante, les résultats expérimentaux et l'analyse de sécurité de la méthode proposée sont présentés. Ici, $AES-128$ avec la taille d'entrée 128 bits est déployé en tant que chiffrement standard. Par conséquent, les tickets générés par le SUC

ont la même taille, c'est-à-dire 128 bits.

Analyse de sécurité des protocoles proposés

Dans cette section, l'analyse de la sécurité des protocoles proposés déployant des SUCs est présentée. L'analyse de sécurité de tels protocoles nécessite tout d'abord de déterminer le modèle adversaire puis d'analyser les scénarios d'attaque possibles sur les protocoles proposés.

— **Le modèle adversaire**
L'objectif d'un adversaire est de profiter des failles du système de tatouage proposé. Par exemple, un adversaire tente d'envoyer à distance des instructions malveillantes pour falsifier et cloner un dispositif médical avec SUC intégré. Par conséquent, deux scénarios d'attaque possibles sont analysés : premièrement, l'attaque de l'homme au milieu (Man In the Middele (MIM)) et deuxièmement, altérer ou truquer un appareil avec un SUC intégré. Dans ce qui suit, l'adversaire Ψ a (oracle) accès au système SUC [103] :

  — Ψ peut exécuter un appareil avec SUC intégré.
  — Ψ peut connaître la conception des protocoles proposés et peut les exécuter.
  — Ψ connaît les messages transmis entre deux appareils.
  — Ψ peut envoyer un message à n'importe quel appareil et au serveur TA.
  — Ψ peut recevoir des réponses de l'appareil.
  — Ψ peut exécuter une expérience de sécurité pour usurper l'identité de n'importe quel appareil.

— **L'attaque de l'homme au milieu (MIMA)** :
Dans MIMA, un adversaire peut intercepter tous les messages pertinents entre un dispositif médical (ou un utilisateur) et un serveur TA. L'objectif de l'adversaire est d'écouter et plus tard de délivrer un faux message. Par conséquent, une MIMA réussie signifie qu'un adversaire peut tromper un serveur TA. Ici, nous supposons que même si l'adversaire écoute un message envoyé au dispositif médical par le serveur TA, il transmet ce message au dispositif médical.
Dans le protocole 1 proposé :

L'adversaire MIMA intercepte les messages des étapes 3 et 8. Dans ce cas, l'adversaire peut extraire la marque signée Z de l'étape 8 en utilisant l'inverse de l'algorithme d'insertion public. Pour délivrer un faux message au serveur $TA4$, un adversaire MIMA devrait être en mesure d'utiliser à nouveau / plus tard la marque signée Z, ce qui équivaut à ce qu'il y ait deux images marquées WM_1 et WM_2 ayant la même marque signée $Z_1 = Z_2$. La taille de l'espace clé est de 2^n, donc la probabilité d'une telle collision est de 2^{-n} . Par conséquent, le protocole 1 proposé de MIS est sécurisé contre MIMA. La même analyse peut être utilisée pour prouver que le protocole 2 proposé est sécurisé contre MIMA.

— **Les attaques de falsification**

Dans ce schéma proposé, les attaques de falsification se réfèrent à un adversaire qui essaie d'apporter des modifications à l'image médicale originale [99] et produit ensuite une marque signée Z valide. Par exemple, dans le protocole 1 proposé, une attaque de sabotage réussie équivaut à la prédiction réussie de x_{Ai} pour un WM_1 spécifique dans $E_{xAi}(WM_1) = Z$. Dans ce cas, l'adversaire peut produire une marque signée Z valide pour une WM falsifiée en utilisant le x_{Ai}. Le théorème suivant montre que l'adversaire a un avantage négligeable pour récupérer x_{Ai}. Cependant, la définition des fonctions pseudo-aléatoires (PRF) est requise pour la preuve du théorème. Dans [51], Goldreich et al. ont présenté le concept des PRF comme suit :
Définition 1 :
une PRF est une famille de fonctions F avec les propriétés suivantes :
Chaque fonction F_K peut être identifiée par une clé unique K.
Chaque adversaire de temps polynomial probabiliste (p.p.t.) a tout au plus un avantage négligeable pour distinguer entre la sortie de $F_K(.)$ et la valeur aléatoire.
Théorème.1 :
La probabilité de réussite d'une attaque falsifiée sur une WM générée par un dispositif A avec un SUC intégré est négligeable pour chaque adversaire. *Preuve* :
Supposons par contradiction qu'il existe un adversaire Ψ qui peut prédire x_{Ai}, pour chaque $i > 0$, avec une probabilité non négligeable dans le protocole 1, puis l'adversaire Ψ peut altérer l'image originale générée par un appareil A. Pour le protocole proposé, considérons un adversaire Ψ qui intéragit avec un challenger agissant comme suit :

— Le challenger choisit au hasard un bit $b \leftarrow^u \{0, 1\}$

— Le challenger renvoie $P \leftarrow^{u} \{0,1\}^{n}$ si $b = 1$ à Ψ ; sinon, elle renvoie $P \leftarrow E_{xAi}(.)$ dans le temps t.

— Après cela, l'adversaire Ψ soumet à un challenger un nombre polynomial de requêtes (q) telles que y_{Ai}, ou $i = 1, \cdots, q$. Ensuite, l'adversaire termine l'expérience en renvoyant b'. Dans ce cas, l'avantage de Ψ pour faire la distinction entre la sortie de $E_{xAi}(.)$, et une valeur aléatoire est défini comme :

$$adv_{PRF}^{E}(\Psi) = |Pr[b = b'] = 1| \tag{5.9}$$

Ici, Ψ est un algorithme de temps polynomial probabiliste, c'est-à-dire p.p.t. adversaire et l'avantage maximum sur tout Ψ est

(5.10)

Selon l'hypothèse ci-dessus, l'adversaire Ψ envoie y_{Ai} au dispositif médical A et recueille les $E_{xAi}(WM_1)$ correspondants pour $i = 0, 1, \cdots, q$ car Ψ a un accès complet aux étapes 3, 4, 6 et 7 dans le protocole.1. Après cela, l'adversaire récupère x_{Ai} avec une probabilité non négligeable. Cela signifie que l'adversaire Ψ a un avantage non négligeable pour distinguer entre la sortie de $E_{xAi}(.)$ et une valeur aléatoire. Apparemment, cela contredit le pseudo-aléatoire de E. Par conséquent, l'adversaire a un avantage négligeable pour récupérer x_{Ai} car

(5.11)

Où, 2^n est le nombre de tous les x_{Ai} possibles. Il s'avère que l'adversaire ne peut pas altérer une image médicale générée par un appareil avec un SUC intégré. Par conséquent, le SUC fournit un MIS avec une limite de sécurité de $O(2^n)$.

5.6 Résultats expérimentaux

Les performances de la méthode proposée ont été évaluées en utilisant quatre images médicales en niveaux de gris au format DICOM, «Chest», «T-spine», «Hands» et «Skull» de la taille de 512×512 pixels comme images hôtes. Une marque binaire de taille 16×16 est générée à partir des images hôtes à incorporer. L'expérience est réalisée sur un ordinateur avec Intel Core i5, CPU 2,6 GHz, 4 Go de mémoire, windows10 et MATLAB

2016b.
Les performances du système de tatouage proposé sont évaluées en termes d'imperceptibilité et de robustesse face aux différentes attaques. Pour mesurer l'imperceptibilité de la marque, l'indice de similitude structurelle (SSIM) et le rapport signal / bruit (PSNR) sont utilisés.
Pour mesurer la robustesse entre la marque extraite et la marque originale, le taux d'erreur sur les bits (BER) et la corrélation normalisée (NC) sont utilisés.
Les images originales utilisées pour étudier les performances de la méthode proposée sont présentées à la figure 5.14.

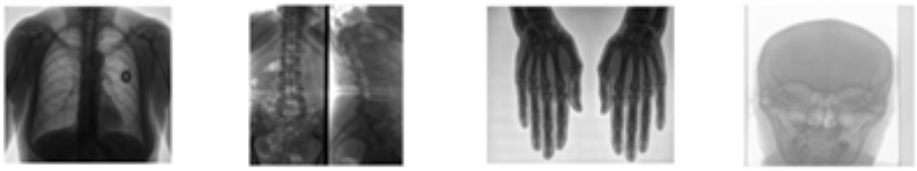


FIGURE 5.14 – Les images DICOM utilisées dans l'expérimentations.

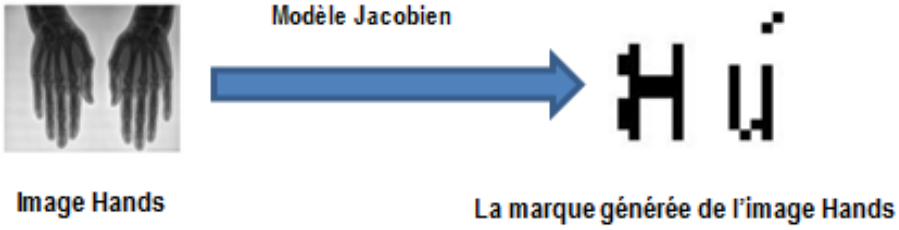


FIGURE 5.15 – L'image "Hands" et sa marque générée.

La figure 5.15 présente la marque générée à partir de l'image "Hands".

5.6.1 Analyse de l'imperceptibilité

Pour évaluer l'imperceptibilité de la marque, nous calculons le PSNR et le SSIM entre l'image originale et l'image tatouée.

D'après le tableau 5.1 , il est évident que les valeurs PSNR dépassent 37 dB et toutes les valeurs de SSIM sont très proches de la valeur idéale 1. La figure 5.16 montre un

Les images	SSIM	PSNR
Chest	0.9861	38.15
Tspine	0.9895	37.77
Hands	0.9997	49.52
Skull	0.9995	52.89

TABLE 5.1 – Les valeurs moyennes de SSIM et PSNR entre les images tatouées et originales

exemple d'image originale, la marque générée correspondant, la marque signée par un ticket unique généré par le SUC et l'image tatouée résultante. Pour le ticket généré par le SUC, AES-128 a été utilisé. Comme on peut le voir sur cette figure, il n'y a pas de différence perceptuelle significative entre les images originales et sa version tatouée.

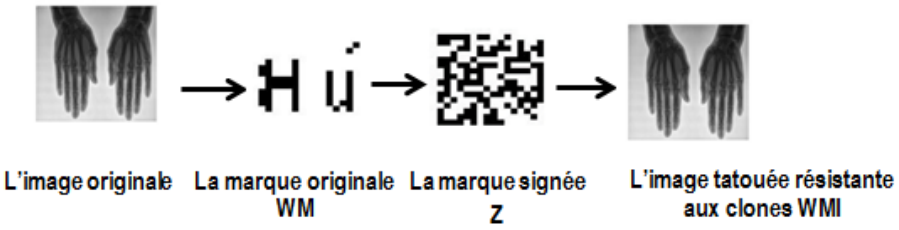


FIGURE 5.16 – Exemple d'image originale, ses marques générées et signées correspondantes et l'image tatouée résultante.)

5.6.2 Analyse de la robustesse

La marque doit être robuste contre les attaques (les distorsions dues aux attaques doivent rester minimes). Nous considérons quelques attaques géométriques et non géométriques dans nos expériences. Ces attaques incluent le filtrage médian, le bruit du sel et du poivre, le filtrage de Wiener, le recadrage du coin supérieur gauche, l'amélioration du contraste, la mise à l'échelle, le filtrage Gaussien, le filtrage passe-bas, l'égalisation d'histogramme, le bruit, la rotation, l'affûtage et les attaques de translation.
Les résultats détaillés du BER et du NC en moyenne pour toutes les images sont résumés dans le tableau 5.2.

Nous pouvons voir dans le tableau 5.2 que les valeurs moyennes de NC entre la marque originale et la marque extraite sont proches de 1 sauf dans un cas, et les valeurs moyennes de BER entre la marque originale et la marque extraite sont proches de 0, ce

Les attaques	La moyenne de BER	La moyenne de NC
Filtrage médian 2×2	0.0080	0.9494
Filtrage médian 3×3	0.0214	0.9427
Bruit de sel et de poivre (0.01)	0.0333	0.9099
Filtrage moyen (3×3)	0.0203	0.9407
Recadrage de coin supérieur gauche (25%)	0.0575	0.8445
Filtrage Gaussien (3×3)	0.0172	0.9488
Egalisation d'histogramme	0.0918	0.4929
Bruit Gaussian (0.01)	0.0284	0.8980
Rotation 1°	0.0221	0.9881
Rotation 5 °	0.0235	0.9260
Rotation 10 °	0.0243	0.9226
L'affûtage	0.0047	0.9852
Translation (10)	0.0202	0.9287
Flou (Blurring)	0.0847	0.9904
Amélioration de contraste	0.0126	0.9530
Mise à l'échelle	0.0112	0.9558
Le filtre Wiener	0.0536	0.9819

TABLE 5.2 – Les valeurs moyennes de NC et BER entre les marques originales et extraites attaquées.

qui montre que l'approche proposée est robuste contre différentes attaques de traitement. Pour démontrer l'efficacité de la méthode proposée, des comparaisons avec d'autres travaux sont présentées dans les tableaux 5.3 et 5.4.

D'après le tableau 5.3, nous pouvons voir que notre méthode a une meilleure valeur de BER pour l'attaque par le bruit du sel et du poivre et l'attaque par le bruit (0,01) que la méthode de J. Dagadu et al. [38], alors que la méthode de J. Dagadu et al. [38] a une meilleure valeur que la notre dans le cas d'un recadrage à 25% en haut à gauche avec une valeur BER égale à 0.
Comparons notre méthode avec celle de Chauhan et al. [29], on peut voir que notre méthode est plus robuste dans le cas d'attaques de netteté, de filtre gaussien et d'amélioration de contraste. Les résultats montrent que notre méthode fonctionne bien pour ces trois attaques car le BER est proche de 0. Mais quand on considère l'attaque d'égalisation d'histogramme, la méthode de Chauhan et al. [29] a une meilleure valeur de BER que l'approche proposée.
La méthode de S. A. Parah et al. [115] est plus robuste que l'approche proposée dans le cas du recadrage du coin supérieur gauche (25%), du bruit de sel et de poivre (0,01), de la netteté, de l'égalisation d'histogramme, du filtrage de Wiener et du bruit gaussien 0,0001, mais elle est moins robuste que notre méthode pour les autres attaques.
La méthode de Singh et al. [142] n'a été testée que pour les attaques suivantes : l'affûtage, le filtrage médian 2×2, le filtrage de Wiener, le bruit Gaussien 0,01 et la rotation 10°. Les valeurs moyennes de BER de l'affûtage, du filtrage de Wiener et du bruit Gaussien sont égales à 0. Ainsi, cette méthode est très robuste et fonctionne bien avec ces trois attaques alors que dans le cas du filtrage médian 2×2 notre méthode est plus robuste.
Une comparaison de la technique proposée avec [38], [115], [152] et [29] pour les valeurs moyennes de NC est présentée dans le tableau 4. La comparaison des résultats avec [38] prouve que la technique proposée par Joshua Dagadu et Al. [38] est plus robuste que l'approche proposée dans le cas du bruit et du sel et du poivre mais dans [38] les autres attaques n'ont pas été testées. En comparant nos résultats avec [29], nos valeurs de NC entre la marque originale et la marque extraite dans le cas des attaques de l'affûtage et du filtrage Gaussien sont meilleures que les résultats de [29].

En comparant les valeurs de NC de l'approche proposée avec les valeurs de NC de [115], on peut voir que dans le cas des filtrages de Wiener et moyen, du bruit Gaussien 0.0001 et de la rotation 1°, notre méthode est plus robuste que la méthode de [115]. Alors que dans le cas des autres attaques telles que le recadrage du coin supérieur gauche,

Les attaques	La méthode proposée	[38]	[29]	[115]	[142]
Recadrage du coin supérieur gauche 25%	0.0575	0	- 0.0566	-	
Bruit (0.01) 99	0.0284	0.1418	-	-	-
Bruit du sel et du poivre (0.01)	0.0333	0.4323	-	0.0175	-
L'affûtage	0.0047	-	0.0180	0.0026	0
Egalisation d'histogramme	0.0918	-	0.0259	0.0080	-
Filtre Gaussian (0.01)	0.0102	-	0.0117	-	-
Filtrage median 2×2	0.0080	-	0.0027	0.0596	0.0383
Le filtre Wiener	0.0536	-	-	0.0488	0
Filtrage moyen	0.0150	-	-	0.0654	-
Bruit Gaussien (0.0001)	0.0994	-	-	0.0800	-
Bruit Gaussien (0.01)	0.0284	-	-	-	0
Rotation 1°	0.0221	-	-	0.0259	-
Rotation 5 °	0.0235	-	-	0.0283	-
Rotation 10 °	0.0243 -	-	0.0330	0.0597	
Flou (Blurring)	0.0847	-	0.0738	-	-
Amélioration de contraste	0.0126	-	0.0131	-	-

TABLE 5.3 – Comparaison de la valeur de BER moyenne de la méthode proposée avec [38], [115], [29] et [142].

Les attaques	La méthode proposée	[38]	[29]	[115]	[152]
Recadrage du coin supérieur gauche 25%	0.8445	0.9997	-	1	0.9966
Bruit (0.01)	0.9114	0.9589	-	-	-
Bruit du sel et du poivre (0.01)	0.9099	0.9589	-	-	0.9758
L'affûtage	0.9852	-	0.9018	0.9977	0.8898
Egalisation d'histogramme	0.4929	-	0.8556	0.9921	0.6038
Filtre Gaussian (0.01)	0.9488	-	0.9322	-	-
Filtrage median 2×2	0.9494	-	-	-	0.6973
Filtrage median 3×3 0.9427	-	0.9845	0.9430	-	
Le filtre Wiener	0.9819	-	-	0.9539	-
Filtrage moyen	0.9407	-	-	0.9354	-
Bruit Gaussien (0.0001)	0.9856	-	-	0.9215	0.9979
Bruit Gaussien (0.01)	0.9114	-	-	-	0.9144
Rotation 1°	0.9881	-	-	0.9728	0.9460
Rotation 5 °	0.9260	-	-	0.9695	-
Rotation 10 °	0.9226	-	-	0.9653	-
Filtre passe bas Gaussien	0.9488	-	-	-	0.5406
Mise à l'échelle de l'image $\times 1.1$	0.9558	-	-	-	0.9309

TABLE 5.4 – Comparaison de la valeur moyenne de NC de la méthode proposée avec [[38], [29], [115] et [152]

]

l'affutage, l'égalisation d'histogramme, le filtrage médian, la rotation de 5° et la rotation de 10°, la méthode de S.A.Parah et al. [115] est plus robuste que notre méthode mais il n'y a pas de grande différence, sauf dans le cas de l'égalisation d'histogramme.
En comparant les résultats de notre méthode avec la méthode de S.Thakur et al. [152] en termes de NC, nous pouvons voir que les résultats obtenus après l'application des attaques de la netteté, du filtrage médian 2×2, la rotation 1°,le filtre passe-bas Gaussien et de la mise à l'échelle de l'image est meilleure avec notre méthode, tandis que en cas d'attaques telles que le recadrage, le sel et le poivre, l'égalisation d'histogramme la méthode de [152] est plus robuste que l'approche proposée.
Les résultats expérimentaux de notre méthode montrent qu'après toutes les attaques, les marques extraites sont visuellement reconnaissables et toutes les marques extraites sont similaires aux marques originales. La valeur de NC moyenne est égale à 0,9055, la valeur de BER en moyenne est égale à 0,0374 et la valeur de SSIM en moyenne est égale à 0,8162. Ainsi, notre méthode est robuste contre les différentes attaques.

5.7 Conclusion

Dans ce chapitre, nous avons proposé une approche de tatouage résistante aux clones pour les applications de télémédecine. Pour générer une marque nous avons extrait le nom du patient et les caractéristiques pertinentes de l'image originale à l'aide du modèle Jacobien. Un ticket unique est extrait des chiffres inconnus secrets (SUC) du dispositif médical pour signer la marque afin de générer une signature unique de la marque. La marque signée est ensuite intégrée dans l'image médicale du patient à l'aide d'une technique de tatouage réversible (Difference Expansion).
En combinant le tatouage et le SUC, l'approche proposée offre plusieurs avantages : résistance au clonage, confidentialité, authentification, non-répudiation et intégrité de l'image médicale. De plus, la réversibilité de la technique de tatouage utilisée dans l'approche proposée permet de récupérer non seulement la marque mais également l'image originale. Une telle récupération de l'image originale est une exigence critique pour les applications d'images médicales.
Les résultats expérimentaux montrent que le schéma proposé est robuste contre les attaques de tatouage (géométrique et non géométrique) et fournit de bonnes bases pour résister à d'autres attaques de sécurité telles que l'attaque de l'homme au milieu et les attaques de falsification.

Conclusion générale et futurs travaux

La télémedecine est de plus en plus utilisée en raison de la maturité des TIC (Technologies de l'Infomration et de Communication) et de son interêt pour des besoins tels que la consultation de personnes situées dans des zones sous-dotées en personnels médicaux, l'intervention de spécialistes situés à distance et ne peuvant pas se déplacer sur site.

Le télédiagnostic nécessite de plus en plus d'échanges d'images médicales de modalités numériques différentes (IRM, Scanner X, médecine nucléaire, etc.) entre les hopitaux et permettant à plusieurs médecins spécialistes distants d'émettre un avis pour une meilleure prise en charge du patient.
L'échange des informations médicales relatives aux patients ainsi que la collection et la diffusion des données médicales doivent se faire en complète sécurité à travers les réseaux. Dans ces conditions, de nouvelles méthodes ont été développées. Il s'agit notament de méthodes de tatouage et de cryptographie.

Dans ce contexte, cette thèse apporte des contributions qui permettent d'augmenter la sécurité du partage des données médicales en permettant de garder la confidentialité des données du patient et de vérifier l'intégrité et l'authenticité des images médicales en utilisant des techniques de tatouage avec une robustesse élevée, une faible complexité de calcul et une bonne imperceptibilité.
Dans cette thèse, nous nous sommes focalisés principalement sur le tatouage numérique et la combinaison du tatouage numérique et la cryptographie pour la sécurité des images médicales.
Nous avons étudié l'extraction des caractéristiques à partir de l'image originale en utilisant une analyse statistique appliquée à une base de données représentative d'images médicales pour sélectionner parmi les paramètres statistiques descriptifs classiques, les caractéristiques candidates les plus significatives fournissant les meilleurs niveaux d'identification des images médicales. Nous avons extrait des caractéristiques robustes de l'image médicale et nous les avons utilisées pour mettre en plaçe une approche de zéro-tatouage

dans laquelle une marque générée à partir des caractéristiques extraites, est transmise au récepteur et est utilisée par ce dernier pour vérifier l'authenticité de l'image reçue.

Nous avons aussi étudié l'impact de l'insertion de la marque dans la région de non interêt (RONI) de l'image afin d'éviter la modification de la zone d'interêt qui pourrait conduire à un diagnostic erroné. Suite à cette étude, nous avons proposé des solutions de tatouage qui donnent plus de robustesse et d'imperceptibilité que les solutions existantes et qui prennent en compte les contraintes de temps indispensables au bon fonctionnement de certaines applications médicales. Pour assurer un haut niveau de sécurité des images médicales, nous avons étudié et proposé une approche combinant le tatouage numérique et la cryptographie basée sur des composants physiques pour la marque. L'idée est de fournir à chaque appareil électronique du systeme médical une signature numérique unique imprévisible et résistante aux clones. L'utilisation d'une identité physiquement résistante aux clones permet de générer un système de tatouage résistant aux clones et d'empêcher la falsification des images du système médicale.

Résumé des contributions

Trois contributions principales ont ete apportées au cours de cette thèse pour améliorer la sécurité des images et des applications médicales.
La première est **une approche de zéro-tatouage pour l'authentification et l'identification d'images DICOM basée sur le modèle Jacobien**. Elle est présentée au chapitre 3. L'approche proposée comporte plusieurs phases. La première phase consiste à extraire des caractéristiques de l'image, appelées caractéristiques pertinentes. Ces caractéristiques sont sélectionnées à partir d'un large ensemble de caractéristiques d'image, en utilisant une approche d'analyse statistique qui vise à sélectionner l'ensemble minimal discriminant de caractéristiques ayant la plus grande résistance aux attaques.
La deuxième phase consiste à extraire le nom du patient de l'en-tête de l'image DICOM, à générer une matrice caractéristique à partir de l'image hôte et à utiliser les caratéristiques pertinentes, le nom du patient et la matrice caractéristique comme des entrées du modèle Jacobien pour générer une clé envoyée au récepteur pour l'authentification et l'identification de l'image.
Les avantages de l'approche proposée sont les suivants :

— L'approche de zéro-tatouage proposée n'apporte aucune modification à l'image ori-

ginale car la marque générée n'est pas insérée dans l'image.

— La séléction des caractéristiques utilisées pour la construction de la clé repose sur une analyse statistique appliquée à une base de données représentative d'images médicales permettant de sélectionner, parmi les paramètres statistiques descriptifs classiques, ceux fournissant les meilleurs niveaux d'identification des images médicales.

— Le modèle Jacobien utilisé pour la construction de la marque, offre un haut niveau de confidentialité tout en garantissant un temps de calcul réduit afin de satisfaire les contraintes de temps des applications médicales ciblées.

— Le modèle proposé est basé sur le domaine spatial et utilise des valeurs de pixels pour génerer la clé plutôt que des techniques du domaine fréquentiel, ce qui permet une complexité moins importante que les approches reposant sur le domaine fréquentiel.

D'autre part, l'approche proposée offre des durées de génération et d'extraction de clés satisfaisantes pour les applications médicales.

La deuxième contribution de cette thèse est **une approche de tatouage double des images DICOM**. Elle est décrite au chapitre 4. Il s'agit d'une approche combinant un système de zéro-tatouage dans la partie ROI de l'image et un système de tatouage dans lequel une marque est insérée dans la partie RONI de l'image. L'insertion de la marque dans cette région de l'image a un impact positif sur l'imperceptibilité, la robustesse et permet de ne pas modifier la partie de l'image utilisée pour le diagnostic. Dans l'approche proposée, des caractéristiques pertinentes extraites de l'image DICOM sont utilisées, d'une part, pour le zéro-tatouage basé sur le modèle jacobien, et d'autre part, pour construire la marque insérée dans la région du fond noir de l'image par la technique d'interpolation linéaire. Les avantages de l'approche proposée sont les suivants :

— La marque est insérée uniquement dans la zone du fond noir de l'image (RONI) afin d'éviter d'affecter la partie anatomique (ROI) dont la modification peut entraîner un diagnostic erroné.

— La méthode proposée fournit une solution d'authentification forte. En effet, elle offre deux manières d'authentifier l'image : soit par l'extraction de la marque inserée dans le fond noir de l'image, soit par les caractéristiques extraites de la partie anatomique de l'image.

— l'approche proposée permet d'authentifier l'image même en cas d'endommagement sur le fond noir rendant la marque insérée inutilisable.

L'approche proposée a une limitation : elle n'offre son plein potentiel d'authentification que pour les images qui ont un fond noir. En effet, pour les images sans fond noir, seul le zéro-tatouage reste applicable pour l'authentification.

La troisième contribution de cette thèse est **une approche d'authentification forte et résistante aux clones pour les systèmes d'images médicales**. Cette dernière est présentée au chapitre 5. Il s'agit d'un système de tatouage résistant aux clonages pour la sécurité des applications de télémédecine combinant une technique de tatouage réversible et une technique de cryptographie. L'idée clé de l'approche proposée est d'intégrer le SUC dans chaque dispositif d'imagerie médicale pour renforcer la sécurité des images médicales. Ce système de tatouage extrait le nom du patient et les caractéristiques pertinentes de l'image originale pour générer une marque en utilisant le modèle Jacobien. Un ticket unique est extrait à partir du SUC du dispositif médical pour signer la marque afin de générer une signature unique de la marque. La marque signée est ensuite intégrée dans l'image médicale du patient à l'aide d'une technique de tatouage réversible (Difference Expansion).
Les avantages de cette approches sont les suivants :

— Résistance au clonage.

— Confidentialité.

— Authentification.

— Non-répudiation et intégrité de l'image médicale.

— La réversibilité de la technique de tatouage utilisé dans l'approche proposée permet de récupérer non seulement la marque mais également l'image d'origine. Une telle récupération de l'image originale est une exigence critique pour les applications d'images médicales.

— L'utilisation du SUC pour signer la marque renforce la sécurité des images médicales lors de leur transfert et de leur stockage.

Après avoir parcouru une large gamme de travaux de recherche connexes, les résultats d'analyse ont montré que les approches proposées dans le cadre de cette thèse apportent des améliorations significatives par rapport aux méthodes existantes du point de vue de l'imperceptibilité, de la robustesse façe à diverses attaques et du temps d'exécution.

Travaux futurs

Le travail proposé dans cette thèse contribue à la résolution des problèmes liés à l'authentification des images médicales basée sur le tatouage numérique. Nous envisageons d'améliorer ce travail en recherchant des solutions à certaines limitations rencontrées. Concernant le tatouage double nous prévoyons d'étudier la division de la marque en un nombre de blocs plus important et l'insertion de plusieurs copies de la marque dans le fond noir de l'image afin d'augmenter la robustesse, l'imperceptibilité et la résistance aux attaques.

Nous envisageons également d'étudier l'utilisation des méthodes d'intelligence artificielle pour l'extraction des caractéristiques robustes à partir de l'image originale afin de générer une marque robuste. Cette étude nous permettra d'évaluer les avantages potentiels des approches d'intelligence artificielle pour une amélioration globale des systèmes de tatouage. Le travail pourrait aussi être élargi aux images médicales colorées ou 3D qui intègrent d'autres caractéristiques.

Une autre perspective est l'implémentation des approches de tatouage proposées sur des prototypes réels de laboratoire.

Bibliographie

[1] Rajendra Acharya et al., « Simultaneous storage of patient information with medical images in the frequency domain », in : *Computer methods and programs in biomedicine* 76.*1* (2004), p. 13-19.

[2] Wael Adi, « Clone-Resistant DNA-Like Secured Dynamic Identity », in : *Proceedings of the 2008 Bio-inspired, Learning and Intelligent Systems for Security, IEEE 4* (2008), p. 148-153.

[3] Wael Adi et Bassel Soudan, *Bio-inspired electronic-mutation with genetic properties for secured identification*, 2007, p. 133-136.

[4] Wael Adi et al., *Deploying FPGA self-configurable cell structure for micro crypto-functions*, 2009, p. 348-354.

[5] Wael Adi et al., *IP-core protection for a non-volatile self-reconfiguring SoC environment*, 2013, p. 252-255.

[6] Adnan M Alattar, *Reversible watermark using difference expansion of quads*, t. 3, 2004, p. iii-377.

[7] Adnan M Alattar, « Reversible watermark using the difference expansion of a generalized integer transform », in : *IEEE transactions on image processing* 13.*8* (2004), p. 1147-1156.

[8] A Albert et al., *Le défi de sécurité dans les réseaux informatiques de santé*, t. 10, Paris, France : dans Collection Informatique et santé : Santé et Réseaux informatiques, 1998, p. 185-191.

[9] Musrrat Ali et Chang Wook Ahn, « An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain », in : *Signal processing* 94 (2014), p. 545-556.

[10] Musrrat Ali, Chang Wook Ahn et Millie Pant, « A robust image watermarking technique using SVD and differential evolution in DCT domain », in : *Optik* 125.*1* (2014), p. 428-434.

[11] François-André Allaert, Liliane Dusserre et B Leclercq, *La sécurité des systèmes d'information médicohospitaliers*, t. 9, Paris : Informatique et Santé, 1997, p. 149-157.

[12] Muhammad Arsalan, Sana Ambreen Malik et Asifullah Khan, « Intelligent reversible watermarking in integer wavelet domain for medical images », in : *Journal of Systems and Software* 85 (2012), p. 883-894.

[13] Imane Assini et al., *Hybrid multiple watermarking technique for securing medical image using DWT-FWHT-SVD*, 2017, p. 1-6.

[14] Meryem Benyoussef et al., « ROBUST IMAGE WATERMARKING SCHEME USING VISUAL CRYPTOGRAPHY IN DUAL-TREE COMPLEX WAVELET DOMAIN. », in : *Journal of Theoretical & Applied Information Technology* 60.*2* (2014).

[15] Dalel Bouslimi et Gouenou Coatrieux, « A crypto-watermarking system for ensuring reliability control and traceability of medical images », in : *Signal Processing : Image Communication* 47 (2016), p. 160-169.

[16] Dalel Bouslimi et Gouenou Coatrieux, « A crypto-watermarking system for ensuring reliability control and traceability of medical images », in : *Signal Processing : Image Communication* 47 (2016), p. 160-169.

[17] Dalel Bouslimi, Gouenou Coatrieux et Ch Roux, *A joint watermarking/encryption algorithm for verifying medical image integrity and authenticity in both encrypted and spatial domains*, 2011, p. 8066-8069.

[18] Dalel Bouslimi, Gouenou Coatrieux et Christian Roux, « A joint encryption/watermarking algorithm for verifying the reliability of medical images : application to echographic images », in : *Computer methods and programs in biomedicine* 106.*1* (2012), p. 47-54.

[19] Dalel Bouslimi et al., « A joint encryption/watermarking system for verifying the reliability of medical images », in : *IEEE transactions on information technology in biomedicine* 16.*5* (2012), p. 891-899.

[20] Dalel Bouslimi et al., *Combination of watermarking and joint watermarking-decryption for reliability control and traceability of medical images*, 2014 36th Annual International Conference of the IEEE Engineering in Medicine et Biology Society, 2014, p. 4495-4498.

[21] Roberto Caldelli, Francesco Filippini et Rudy Becarelli, « Reversible watermarking techniques : An overview and a classification », in : *EURASIP Journal on Information Security* 2010 (2010), p. 1-19.

[22] Michela Cancellaro et al., « A commutative digital image watermarking and encryption method in the tree structured Haar transform domain », in : *Signal Processing : Image Communication* 26.*1* (2011), p. 1-12.

[23] Christine Cavaro-Ménard, Zhang Ge Lu et Patrick Le Callet, *QoE for telemedicine : Challenges and trends*, t. 8856, 2013, 88561A.

[24] Mehmet Utku Celik et al., « Lossless generalized-LSB data embedding », in : *IEEE transactions on image processing* 14 (2005), p. 253-266.

[25] Mehmet Utku Celik et al., « Secure embedding of spread spectrum watermarks using look-up-tables », in : *2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07. IEEE* 2 (2007), p. II-153-II-156.

[26] CEN, *Security categorisation and protection for healthcare information systems*, rapp. tech, 1997.

[27] Jun-Dong Chang, Bo-Hung Chen et Chwei-Shyong Tsai, « LBP-based fragile watermarking scheme for image tamper detection and recovery », in : *In 2013 International Symposium on Next-Generation Electronics* (2013), p. 173-176.

[28] Hui-Mei Chao, Chin-Ming Hsu et Shaou-Gang Miaou, « A data-hiding technique with authentication, integration, and confidentiality for electronic patient records », in : *IEEE Transactions on Information Technology in Biomedicine* 6.*1* (2002), p. 46-53.

[29] Digvijay Singh Chauhan et al., « Quantization based multiple medical information watermarking for secure e-health », in : *Multimedia tools and applications* 78.*4* (2019), p. 3911-3923.

[30] Yiu-ming Cheung et Hao-tian Wu, « A sequential quantization strategy for data embedding and integrity verification », in : *IEEE transactions on circuits and systems for video technology* 17.*8* (2007), p. 1007-1016.

[31] E Chrysochos et al., *Reversible image watermarking based on histogram modification*, 2007, p. 93-104.

[32] Gouenou Coatrieux et al., « A low distorsion and reversible watermark : Application to angiographic images of the retina », in : *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the* (2005), p. 2224-2227.

[33] Gouenou Coatrieux et al., *A review of image watermarking applications in healthcare*, 2006 International conference of the IEEE Engineering in Medicine et Biology Society, 2006, p. 4691-4694.

[34] Gouenou Coatrieux et al., « Mixed reversible and RONI watermarking for medical image reliability protection », in : *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE* (2007), p. 5653-5656.

[35] Dinu Coltuc et Jean-Marc Chassery, « Very fast watermarking by reversible contrast mapping », in : *IEEE Signal processing letters* 14.*4* (2007), p. 255-258.

[36] Ingemar J Cox et al., « Secure spread spectrum watermarking for multimedia », in : *IEEE transactions on image processing* 6.*12* (1997), p. 1673-1687.

[37] Scott Craver et al., « Resolving rightful ownerships with invisible watermarking techniques : Limitations, attacks, and implications », in : *IEEE Journal on Selected Areas in Communications* 16.*4* (1998), p. 573-586.

[38] Joshua C Dagadu et Jianping Li, « Context-based watermarking cum chaotic encryption for medical images in telemedicine applications », in : *Multimedia Tools and Applications* 77.*18* (2018), p. 24289-24312.

[39] Christophe De Vleeschouwer, JE Delaigle et Benoit Macq, « Circular interpretation of histogram for reversible watermarking », in : *2001 IEEE Fourth Workshop on Multimedia Signal Processing (Cat. No. 01TH8564)* (2001), p. 345-350.

[40] Jeroen Delvaux et al., « A survey on lightweight entity authentication with strong PUFs », in : *ACM Computing Surveys (CSUR)* 48.*2* (2015), p. 1-42.

[41] Chunhua Dong et al., *Robust zero-watermarking for medical image based on DCT*, 2011 6th International Conference on Computer Sciences et Convergence Information Technology (ICCIT), 2011, p. 900-904.

[42] Liliane Dusserre, Ducrot Henry et François-André ALLAËRT, *L'information médicale, l'ordinateur et la loi*, Editions médicales internationales, 1996.

[43] Shervan Fekri Ershad, « A review on image texture analysis methods », in : *CoRR, abs/1804.00494* (2018).

[44] Marco Fontani et al., « Reversible watermarking for image integrity verification in hierarchical pacs », in : *Proceedings of the 12th ACM workshop on Multimedia and security* (2010), p. 161-168.

[45] V Fotopoulos, Maria L Stavrinou et Athanassios N Skodras, *Medical image authentication and self-correction through an adaptive reversible watermarking technique*, 2008 8th IEEE International Conference on BioInformatics et BioEngineering, 2008.

[46] Guangyong Gao et Guoping Jiang, « Bessel-Fourier moment-based robust image zero-watermarking », in : *Multimedia Tools and Applications* 74.*3* (2015), p. 841-858.

[47] Xinbo Gao et al., « Reversibility improved lossless data hiding », in : *Signal Processing* 89 (2009), p. 2053-2065.

[49] Musab Ghadi et al., *A joint spatial texture analysis/watermarking system for digital image authentication*, 2017 IEEE International Workshop on Signal Processing Systems (SiPS), 2017, p. 1-6.

[50] Musab Ghadi et al., « A novel zero-watermarking approach of medical images based on Jacobian matrix model », in : *Security and communication networks* 9.*18* (2016), p. 5203-5218.

[51] Oded Goldreich, Shafi Goldwasser et Silvio Micali, 2019, p. 241-264.

[52] Clara Delpas Guy Frija et Bernard Mazoyer, *Imagerie médicale*, San Francisco : Fondation recherche médicale, 2002.

[53] Ahmed S Hadi, Baydaa M Mushgil et Heba M Fadhil, « Watermarking based Fresnel transform, wavelet transform, and chaotic sequence », in : *J. Appl. Sci. Res* 5.*10* (2009), p. 1463-1468.

[54] Ali Al-Haj et al., « Secured telemedicine using region-based watermarking with tamper localization », in : *Journal of digital imaging* 27.*6* (2014), p. 737-750.

[55] Baoru Han, Jingbing Li et Liang Zong, « A new robust zero-watermarking algorithm for medical volume data », in : *International Journal of Signal Processing, Image Processing and Pattern Recognition* 6.*6* (2013), p. 245-258.

[56] Kevin Heylen et Tim Dams, « An image watermark tutorial tool using Matlab », in : *Mathematics of Data/Image Pattern Recognition, Compression, and Encryption with Applications XI* 7075 (2008), p. 70750D.

[57] Yongjian Hu, Heung-Kyu Lee et Jianwei Li, « DE-based reversible data hiding with improved overflow location map », in : *IEEE Transactions on Circuits and Systems for Video Technology* 19 (2008), p. 250-260.

[58] Ahmed Al-Jaber et Mohammad K Yaqub, « Reversible watermarking using modified difference expansion », in : *International Journal of Computing & Information Sciences* 4.*3* (2006), p. 134-142.

[59] Wei Jin et al., *A wavelet-based method of zero-watermark utilizing visual cryptography*, 2010, p. 1-4.

[60] Ying-Shen Juang et al., « Histogram modification and wavelet transform for high performance watermarking », in : *Mathematical Problems in Engineering* (2012), p. 1-14.

[61] A Kannammal et S Subha Rani, « Two level security for medical images using watermarking/encryption algorithms », in : *International Journal of Imaging Systems and Technology* 24.*1* (2014), p. 111-120.

[62] Mandeep Kaur et Rupinder Kaur, « Reversible watermarking of medical images : Authentication and Recovery-A Survey », in : *Journal of Information and Operations Management* 3.*1* (2012), p. 241.

[63] Awanish Kr Kaushik, « A novel approach for digital watermarking of an image using DFT », in : *Int JElectronComp Sci Eng* 1.*1* (2012), p. 35-41.

[64] Awanish Kr Kaushik, « A novel approach for digital watermarking of an image using DFT », in : *Int JElectronComp Sci Eng* 1.*1* (2012), p. 35-41.

[65] Mehdi Khalili, « DCT-Arnold chaotic based watermarking using JPEG-YCbCr », in : *Optik* 126.*23* (2015), p. 4367-4371.

[66] Asifullah Khan et al., « A recent survey of reversible watermarking techniques », in : *Information sciences* (2014), p. 251-272.

[67] Asifullah Khan et al., « A recent survey of reversible watermarking techniques », in : *Information sciences* 279 (2014), p. 251-272.

[68] Kyung-Su Kim et al., « Reversible data hiding exploiting spatial correlation between sub-sampled images », in : *Pattern Recognition* 42 (2009), p. 3083-3096.

[69] Lu-Ting Ko et al., « Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems », in : *Computational and mathematical methods in medicine* 2012 (2012).

[70] Luiz Kobayashi et al., « Providing integrity and authenticity in DICOM images : a novel approach », in : *IEEE Transactions on Information Technology in Biomedicine* 13.*4* (2009), p. 582-589.

[71] Aleksey Koval, Frank Y Shih et Boris S Verkhovsky, « A pseudo-random pixel rearrangement algorithm based on Gaussian integers for image watermarking », in : *Journal of Information Hiding and Multimedia Signal Processing* 2.*1* (2011), p. 60-70.

[72] Hayet Lamine et Fatma Laribi, « Solution web pour l'imagerie médicale favorisant la télé-radiologie », in : ().

[73] Jiann-Der Lee, Yaw-Hwang Chiou et Jing-Ming Guo, « Reversible data hiding based on histogram modification of SMVQ indices », in : *IEEE Transactions on Information Forensics and Security* 5.*4* (2010), p. 638-648.

[74] Sang-Kwang Lee, Young-Ho Suh et Yo-Sung Ho, « Reversible image authentication based on watermarking », in : *2006 IEEE international conference on multimedia and Expo* (2006), p. 1321-1324.

[75] Xiaoxu Leng, Jun Xiao et Ying Wang, *A robust image zero-watermarking algorithm based on DWT and PCA*, Communications et Information Processing, 2012, p. 484-492.

[76] Xiaolong Li et al., « A novel reversible data hiding scheme based on two-dimensional difference-histogram modification », in : *IEEE Transactions on Information Forensics and Security* 8 (2013), p. 1091-1100.

[77] Xiaolong Li et al., « General framework to histogram-shifting-based reversible data hiding », in : *IEEE Transactions on image processing* 22 (2011), p. 2181-2191.

[78] Siau-Chuin Liew et Jasni Mohamad Zain, « Reversible medical image watermarking for tamper detection and recovery », in : *2010 3rd International Conference on Computer Science and Information Technology* 5 (2010), p. 417-420.

[79] Siau-Chuin Liew et Jasni Mohamad Zain, « Reversible medical image watermarking for tamper detection and recovery », in : *2010 3rd International Conference on Computer Science and Information Technology. IEEE* 5 (2010), p. 417-420.

[80] Daihyun Lim et al., « Extracting secret keys from integrated circuits », in : *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 13.*10* (2005), p. 1200-1205.

[81] Chia-Chen Lin, Wei-Liang Tai et Chin-Chen Chang, « Multilevel reversible data hiding based on histogram modification of difference images », in : *Pattern Recognition* 41 (2008), p. 3582-3591.

[82] Chia-Chen Lin, Wei-Liang Tai et Chin-Chen Chang, « Multilevel reversible data hiding based on histogram modification of difference images », in : *Pattern Recognition* 41.*12* (2008), p. 3582-3591.

[83] Jian Liu et Xiangjian He, « A review study on image digital watermarking », in : *The Tenth International Conference on Networks* 45 (2011), p. 24-28.

[84] Der-Chyuan Lou et Chia-Hung Sung, *Robust image watermarking based on hybrid transformation*, IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings., 2003, p. 394-399.

[85] Khaled Loukhaoukha, « Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain », in : *Journal of Optimization* (2013).

[86] M Loytynoja et al., « Audio encryption using fragile watermarking », in : *2005 5th International Conference on Information Communications Signal Processing. IEEE* 16.*5* (2005), p. 881-885.

[87] Fazal Malik et Baharum Baharudin, « The statistical quantized histogram texture features analysis for image retrieval based on median and laplacian filters in the dct domain », in : *The International Arab Journal of Information Technology* 10.*6* (2013), p. 1-9.

[88] Cédric Marchand et al., « Implementation and characterization of a physical unclonable function for IoT : a case study with the TERO-PUF », in : *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37.*1* (2017), p. 97-109.

[89] Ayoub Mars et al., *Random stream cipher as a PUF-like identity in FPGA environment*, 2017, p. 209-214.

[90] Jan Masek et al., « Evolutionary improved object detector for ultrasound images », in : *2013 36th international conference on telecommunications and signal processing (TSP). IEEE* (2013), p. 586-590.

[91] Ko Lu-Ting Chen Jwu-E Shieh Yaw-Shih Scalia Massimo et Tze-Yun Sung, « A novel fractional-discrete-cosine-transform-based reversible watermarking for healthcare information management systems », in : *Mathematical Problems in Engineering* 2012 (2012).

[92] Andrzej Materka, Michal Strzelecki et al., « Texture analysis methods–a review », in : *Technical university of lodz, institute of electronics, COST B11 report, Brussels* 10.*1.97* (1998), p. 4968.

[93] Nisar Ahmed Memon et Syed Asif Mahmood Gilani, « Watermarking of chest CT scan medical images for content authentication », in : *International Journal of Computer Mathematics* 88 (2011), p. 265-280.

[94] Nisar Ahmed Memon, Zulfiqar Ali Keerio et Fatima Abbasi, *Dual watermarking of CT scan medical images for content authentication and copyright protection*, International Multi Topic Conference, 2013, p. 173-183.

[95] Nisar Ahmed Memon et al., « Hybrid watermarking of medical images for ROI authentication and recovery », in : *International Journal of Computer Mathematics* 88 (2011), p. 2057-2071.

[96] Nisar Ahmed Memon et al., « Hybrid watermarking of medical images for ROI authentication and recovery », in : *International Journal of Computer Mathematics* 88.*10* (2011), p. 2057-2071.

[97] Nisar Ahmed Memon et al., « Reversible watermarking method based on adaptive thresholding and companding technique », in : *International Journal of Computer Mathematics* 88 (2011), p. 1573-1594.

[98] Shilpa P Metkar et Milind V Lichade, *Digital image security improvement by integrating watermarking and encryption technique*, 2013 IEEE international conference on signal processing, computing et control (ISPCC), 2013, p. 1-6.

[99] Minati Mishra et MC Adhikary, « Detection of clones in digital images », in : *arXiv preprint arXiv :1407.6879* (2014).

[100] Seyed Mojtaba Mousavi, Alireza Naghsh et SAR Abu-Bakar, « Watermarking techniques used in medical images : a survey », in : *Journal of digital imaging* 27 (2014), p. 714-729.

[101] Saleh Mulhem et Wael Adi, « New Mathblocks-Based Feistel-Like Ciphers for Creating Clone-Resistant FPGA Devices », in : *Cryptography* 3.*4* (2019), p. 28.

[102] Saleh Mulhem, Maen Mohammad et Wael Adi, *A New Low-Complexity Cipher Class for Clone-Resistant Identities*, 2019 42nd International Convention on Information, Communication Technology, Electronics et Microelectronics (MIPRO), 2019, p. 971-976.

[103] Saleh Mulhem, Randa Zarrouk et Wael Adi, « Security and Complexity Bounds of SUC-Based Physical Identity », in : *2018 NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*, IEEE, 2018, p. 317-322.

[104] MUHAMMAD AGUNG MULTAZAM, Muhammad Fachrurrozi et Osvari Arsalan, « PERBANDINGAN METODE INTERPOLASI BICUBIC DAN GABUNGAN METODE INTERPOLASI BICUBIC DENGAN DUAL TREE COMPLEX WAVELET TRANSFORM PADA PENINGKATAN KUALITAS CITRA MEDIS », thèse de doct., Sriwijaya University, 2020.

[105] Arash Ashtari Nakhaie et Shahriar B Shokouhi, *No reference medical image quality measurement based on spread spectrum and discrete wavelet transform using ROI processing*, 2011 24th Canadian Conference on Electrical et Computer Engineering (CCECE), 2011, p. 000121-000125.

[106] Zhicheng Ni et al., « Reversible data hiding », in : *IEEE Transactions on circuits and systems for video technology* 16 (2006), p. 354-362.

[107] Teresa G Norris, « Telemedicine and teleradiology », in : *Radiologic technology* 71.*2* (1999), p. 139-139.

[108] Hussain Nyeem, Wageeh Boles et Colin Boyd, « A review of medical image watermarking requirements for teleradiology », in : *Journal of Digital Imaging* 26 (2013), p. 326-343.

[109] Hussain Nyeem, Wageeh Boles et Colin Boyd, « A review of medical image watermarking requirements for teleradiology », in : *Journal of digital imaging* 26.*2* (2013), p. 326-343.

[110] Hussain Nyeem, Wageeh Boles et Colin Boyd, « A review of medical image watermarking requirements for teleradiology », in : *Journal of digital imaging* 26.*2* (2013), p. 326-343.

[111] T Ojala et inen M PIETIKÄINEN, « Texture classification, machine vision, and media processing unit », in : *University of Oulu, Finland* (2004).

[112] Wei Pan et al., « Comparison of some reversible watermarking methods in application to medical images », in : *In 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (2009), p. 2172-217.

[113] Wei Pan et al., « Imperceptible reversible watermarking of radiographic images based on quantum noise masking », in : *Computer methods and programs in biomedicine* 160 (2018), p. 119-128.

[114] Wei Pan et al., « Imperceptible reversible watermarking of radiographic images based on quantum noise masking », in : *Computer methods and programs in biomedicine* 160 (2018), p. 119-128.

[115] Shabir A Parah et al., « Information hiding in medical images : a robust medical image watermarking system for E-healthcare », in : *Multimedia Tools and Applications* 76.*8* (2017), p. 10599-10633.

[116] Fabien AP Petitcolas, Ross J Anderson et Markus G Kuhn, « Attacks on copyright marking systems », in : *International workshop on information hidin. Springer, Berlin, Heidelberg* (1998), p. 218-238.

[117] Fabien AP Petitcolas, Ross J Anderson et Markus G Kuhn, « Attacks on copyright marking systems », in : *International workshop on information hiding. Springer, Berlin, Heidelberg* (1998), p. 218-238.

[118] Kutter Andf Petitcolas, « A Fair Benchmark for Image Watermarking Systems », in : *Electronic Imaging : Security and Watermarking of Multimedia Content* 3657 (1999).

[119] William Puech et Jose M Rodrigues, *A new crypto-watermarking method for medical images safe transfer*, 2004 12th European Signal Processing Conference, 2004, p. 1481-1484.

[120] K Pushpala et R Nigudkar, « A novel watermarking technique for medical image authentication », in : *Computers in Cardiology, IEEE* (2005), p. 683-686.

[121] Asaad F Qasim, Farid Meziane et Rob Aspin, « Digital watermarking Applicability for developing trust in medical imaging workflows state of the art review », in : *Computer Science Review* 27 (2018), p. 45-60.

[122] Asaad F Qasim et al., « ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images », in : *Multimedia Tools and Applications* 78.*12* (2019), p. 16433-16463.

[123] Osamah M Al-Qershi et BE Khoo, « Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images », in : *Proceedings of international conference on medical systems engineering (ICMSE)* (2009), p. 829-834.

[124] Osamah M Al-Qershi et Bee Ee Khoo, « Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images », in : *Journal of digital imaging* 24.*1* (2011), p. 114-125.

[125] Min Qi, Bing-Zhao Li et Huafei Sun, « Image watermarking via fractional polar harmonic transforms », in : *Journal of Electronic Imaging* 24.*1* (2015), p. 013004.

[126] Farhad Rahimi et Hossein Rabbani, « A dual adaptive watermarking scheme in contourlet domain for DICOM images », in : *Biomedical engineering online* 10.*1* (2011), p. 1-18.

[127] Farhad Rahimi et Hossein Rabbani, « A dual adaptive watermarking scheme in contourlet domain for DICOM images », in : *Biomedical engineering online* 10.*1* (2011), p. 1-18.

[128] Hossein Rahmani, Reza Mortezaei et Mohsen Ebrahimi Moghaddam, *A new lossless watermarking scheme based on DCT coefficients*, 2010, p. 28-33.

[129] W Craig Revie et al., « Color management in digital pathology », in : *Analytical Cellular Pathologyg. Hindawi* (2014).

[130] Michael L Richardson, Mark S Frank et Eric J Stern, « Digital image manipulation : What constitutes acceptable alteration of a radiologic image ? », in : *AJR. Am. J. Roentgenol* 164 (1995), p. 228-229.

[131] Aleš Roček, Karel Slavíček, Michal Javornik et al., *RONI size and another attributes of representative sample of medical images in common hospital operation, related to securing by watermarking methods*, 2016.

[132] Aleš Roček et al., « A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters », in : *Biomedical Signal Processing and Control* 29 (2016), p. 44-52.

[133] Jose Marconi Rodrigues, William Puech et Christophe Fiorio, *Lossless cryptodata hiding in medical images without increasing the original image size*, MEDSIP'04 : 2nd Medical Image et Signal Processing, 2004, p. 358-365.

[134] Mohammad J Saberian, Mohammad A Akhaee et Farokh Marvasti, *An invertible quantization based watermarking approach*, 2008 IEEE International Conference on Acoustics, Speech et Signal Processing, 2008, p. 1677-1680.

[135] Bidyut Jyoti Saha, Kunal Kumar Kabi, Chittaranjan Pradhan et al., *Non blind watermarking technique using enhanced one time pad in DWT domain*, Fifth International Conference on Computing, Communications et Networking Technologies (ICCCNT), 2014, p. 1-6.

[136] Roland Schmitz et al., *A new approach to commutative watermarking-encryption*, 2012, p. 117-130.

[137] Roland Schmitz et al., *Towards more robust commutative watermarking-encryption of images*, 2013, p. 283-286.

[138] Vellaisamy Seenivasagam et Ramesh Velumani, « A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud », in : *Computational and mathematical methods in medicine* 2013 (2013).

[139] Ayesha Shaik et V Masilamani, « Zero-watermarking in transform domain and Quadtree decomposition for under water images captured by robot », in : *Procedia computer science* 133 (2018), p. 385-392.

[140] Manisha Sharma et al., « Medical image watermarking technique in the application of E-diagnosis using M-Ary modulation », in : *Procedia Computer Science* 85 (2016), p. 648-655.

[141] Frank Y Shih et Yi-Ta Wu, « Robust watermarking and compression for medical images based on genetic algorithms », in : *Information Sciences* 175 (2005), p. 200-216.

[142] Abhilasha Singh et Malay Kishore Dutta, « A robust zero-watermarking scheme for tele-ophthalmological applications », in : *Journal of King Saud University-Computer and Information Sciences* (2017).

[143] Abhilasha Singh et Malay Kishore Dutta, « A robust zero-watermarking scheme for tele-ophthalmological applications », in : *Journal of King Saud University-Computer and Information Sciences* 13 (2017), p. 1-14.

[144] Amit Kumar Singh, Mayank Dave et Anand Mohan, « Hybrid technique for robust and imperceptible multiple watermarking using medical images », in : *Multimedia Tools and Applications* 75.*14* (2016), p. 8381-8401.

[145] Neha Solanki, Sanjay Kumar Malik et Sonam Chhikara, « Roni medical image watermarking using dwt and rsa », in : *International Journal of Computer Applications* 96.*9* (2014).

[146] Karen Su, Deepa Kundur et Dimitrios Hatzinakos, « Novel approach to collusion-resistant video watermarking », in : *Security and Watermarking of Multimedia Contents IV. International Society for Optics and Photonics* 4675 (2002), p. 491-502.

[147] A Venkata Subramanyam, Sabu Emmanuel et Mohan S Kankanhalli, « Robust watermarking of compressed and encrypted JPEG2000 images », in : *IEEE Transactions on Multimedia* 14.*3* (2011), p. 703-716.

[148] Chun Kiat Tan et al., « Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability », in : *Journal of Digital Imaging* 24.*3* (2011), p. 528-540.

[149] Nidhi Taneja et al., « Joint watermarking and encryption for still visual data », in : *Multimedia tools and applications* 67.*3* (2013), p. 593-606.

[150] Afaf Tareef et al., « A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding », in : *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE* (2014), p. 5554-5557.

[151] Falgun N Thakkar et Vinay Kumar Srivastava, « A blind medical image watermarking : Dwt-svd based robust and secure approach for telemedicine applications », in : *Multimedia Tools and Applications* 76.*3* (2017), p. 3669-3697.

[152] Sriti Thakur et al., « Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications », in : *Multimedia tools and Applications* 78.*3* (2019), p. 3457-3470.

[153] N Thilagavathi et al., « A survey of reversible watermarking techniques, application and attacks », in : *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering Technology (ICARCSET 2015)* (2015), p. 1-7.

[154] Diljith M Thodi et Jeffrey J Rodriguez, « Expansion embedding techniques for reversible watermarking », in : *IEEE transactions on image processing* 16.*3* (2007), p. 721-730.

[155] Diljith M Thodi et Jeffrey J Rodriguez, *Prediction-error based reversible watermarking*, t. 3, 2004, p. 1549-1552.

[156] Joseph D Touch, « Performance analysis of MD5 », in : *ACM SIGCOMM Computer Communication Review* 25.*4* (1995), p. 77-86.

[157] Yueh-Shen Tu et Jenhui Chen, *A secure and unclonable medical image transmission system by using embedded physical uncloneable function*, 2016 International Conference On Communication Problem-Solving (ICCP), 2016, p. 1-3.

[158] A Umaamaheshvari et K Thanushkodi, « High performance and effective watermarking scheme for medical images », in : *European Journal of Scientific Research* 67.*2* (2012), p. 283-293.

[159] G Van Schyndel amd Ron, Andrew Z Tirkel et Charles F Osborne, *A digital watermark*, t. 2, Proceedings of 1st international conference on image processing, 1994, p. 86-90.

[160] Dandu Ravi Varma, « Managing DICOM images : Tips and tricks for the radiologist », in : *the Indian journal of radiology imaging* 22.*1* (2012), p. 1-4.

[161] Chun-peng Wang et al., « Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping », in : *Multimedia Tools and Applications* 76.*24* (2017), p. 26355-26376.

[162] Chunpeng Wang et al., « Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm », in : *Information Sciences* 470 (2019), p. 109-120.

[163] Xingyuan Wang et Chuanming Liu, « A novel and effective image encryption algorithm based on chaos and DNA encoding », in : *Multimedia Tools and Applications* 76.*5* (2017), p. 6229-6245.

[164] Bin Xiao, Jian-Feng Ma et Xuan Wang, « Image analysis by Bessel–Fourier moments », in : *Pattern Recognition* 43.*8* (2010), p. 2620-2629.

[165] Guorong Xuan et al., *Reversible data hiding using integer wavelet transform and companding technique*, International Workshop on Digital Watermarking, 2004, p. 115-124.

[166] Monika Yadav et Neeraj Jain, « An Invisible, Robust and Secure DWT-SVD Based Digital Image Watermarking Technique with Improved Noise Immunity », in : *IOSR Journal of Electronics and Communication Engineering* 12 (2017), p. 07-11.

[167] Bian Yang et al., « Reversible watermarking techniques : An overview and a classification », in : *Security, steganography, and watermarking of multimedia contents VI. International Society for Optics and Photonics* 2010 (5306), p. 405-415.

[168] Trache N Ahmed-Foitih Z et Benamrane N, « Artificial Immune System Optimization Technique For Robust and Secure Image Watermarking », in : *the International Journal of Imaging and Robotics, In press* (2018).

[169] Jasni M Zain, Lynne P Baldwin et Malcolm Clarke, « Reversible watermarking for authentication of DICOM images », in : *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* 2 (2004), p. 3237-3240.

[170] Aditi Zear, Amit Kumar Singh et Pardeep Kumar, « A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine », in : *Multimedia tools and applications* 77.*4* (2018), p. 4863-4882.

[171] Yanping Zhang et al., « Research on embedding capacity and efficiency of information hiding based on digital images », in : *International Journal of Intelligence Science* 2.*3* (2013), p. 77-85.

[172] Philip Zimmermann, « PGP User's Guide, Volume II : Special Topics », in : *Available on the WWW via ftp ://ftp. pegasus. esprit. ec. org/-pub/arne/pgpdoc2. ps. gz* (1994).

DOCTORAT BRETAGNE LOIRE MATHSTIC

Université de Bretagne Occidentale

Titre : Sécurité des images par tatouage numérique et cryptographie pour les applications médicales

Mot clés : Imagerie médicale, Sécurité, Tatouage numérique, Cryptographie, Authentification, Robustesse, Secret Unknown Ciphers (SUC)

Résumé : Le développement rapide des tech-nologies multimédia et de communication per-met de faciliter le partage et l'accès à dis-tance aux données des patients, notamment en télémédecine. La demande de sécurité des images médicales augmente. Pour les appli-cations de télémédecine, il ne s'agit pas seule-ment de garantir la confidentialité et la fiabi-lité (intégrité et authenticité) des images, mais aussi de fournir des preuves dans le cas où il y'a une modification illicite des données. Le tatouage numérique d'image est l'une des technologies cherchant à protéger les images médicales lors de la transmission sur un ré-seau public non sécurisé. Il permet d'insé-rer ou masquer une marque dans une image numérique de manière invisible sans dégra-der visuellement la qualité de l'image dans le but d'assurer l'intégrité, l'authentification et la confidentialité des images et des données des patients dans les applications d'imagerie médicale. Dans cette thèse, nous avons tra-vaillé sur la sécurité des images médicales en nous basant sur des solutions de tatouage nu-mérique ainsi que des solutions combinant le tatouage numérique et la cryptographie.

Une première contribution de ce travail concerne une approche de zéro-tatouage pour l'authen-tification des images DICOM. Une deuxième contribution est une approche qui combine une méthode de zéro-tatouage dans la partie ROI de l'image et une méthode d'insertion de marque dans la partie RONI de l'image pour l'authentification des images médicales. Une troisième contribution est une approche d'au-thentification forte et résistante aux clones pour le système d'images médicales combi-nant une technique de tatouage réversible et une technique de cryptographie physique ap-pelée SUC (Secret Unckown Ciphers) . Les approches proposées sont robustes et ré-sistantes à différents types d'attaques. Elles couvrent les caractéristiques de sécurité sui-vantes : intégrité, confidentialité, authentifica-tion. Elles permettent d'assurer la non modi-fication de la partie de l'image utilisée pour le diagnostic, et garantissent ainsi aux méde-cins un diagnostic non entaché d'erreur. De plus, la réversibilité du tatouage proposé dans la troisième approche garantit la récupération de l'image médicale originale lors de la phase d'extraction.

Title: Image security by digital watermarking and cryptography for medical applications

Keywords: Medical image, Security, Digital watermarking, Cryptography, Authentication, Ro-bustness, Secret Unknown Ciphers (SUC)

Abstract: The rapid development of multi-media and communication technologies facilitates remote sharing and access to patient data, particularly in telemedicine. The demand for the security of medical images is increas-ing. For telemedicine applications, it is not only a matter of ensuring the confidentiality and re-liability (integrity and authenticity) of the im-ages, but also of providing evidence in the event that there is an unlawful modification of the data. Digital image watermarking is one of the technologies seeking to protect medi-cal images while transmitting over an unse-cured public network. It allows to insert or hide a mark in a digital image invisibly without vi-sually degrading the quality of the image in order to ensure the integrity, the authentica-tion and the confidentiality of the images and the data of the patients in the medical imag-ing applications. In this thesis, we worked on the security of medical images based on digi-tal watermarking solutions as well as solutions combining digital watermarking and cryptogra-phy.

A first contribution of this work concerns a zero-watermarking approach for the authentication of DICOM images. A second contri-bution is an approach that combines a zero-watermarking method in the ROI part of the image and a watermark insertion method in the RONI part of the image for the authentica-tion of medical images. A third contribution is a strong and clone-resistant authentication ap-proach for the medical image system combin-ing a reversible watermarking technique and a physical cryptography technique called SUC (Secret Unckown Ciphers). The proposed ap-proaches are robust and resistant to differ-ent types of attacks. They cover the follow-ing security features: integrity, confidentiality, authentication and guarantee that the part of the image used for the medical diagnosis is unmodified. In addition, the reversibility of the proposed watermarking in the third approach guarantees the recovery of the original medi-cal image during the extraction phase.