جامعة سيدي محمد بن عبد الله بفاس
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ ⴱ ⴼⴰⵙ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم ظهر المهراز فاس
ⵜⴰⵖⵢⵍⵓⵜ ⵏ ⵜⵣⵔⴼⵜ ⵎⴰⵀⵔⴰⵣ ⴼⴰⵙ
FACULTE DES SCIENCES DHAR EL MAHRAZ FES

N° d'Ordre : **37/2021**

Formation Doctorale: ***Sciences et Technologies de l'Information et de la Communication STIC***

Discipline : Informatique

Spécialité : Informatique

Laboratoire de LISAC

THESE DE DOCTORAT

Présentée par

Fadoua SABBANE

Transformations polynomiales : applications au tatouage des images médicales

Soutenue le 27 / 07 / 2021 devant le jury composé de :

Pr SATORI Khalid	***Faculté des Sciences Dhar El Mahraz -Fès***	***Président***
Pr EL OUADGHIRI Driss	***Faculté des Sciences de Meknès***	***Rapporteur***
Pr EL KINANI El Hassan	***Faculté des Sciences de Meknès***	***Rapporteur***
Pr QJIDAA Hassan	***Faculté des Sciences Dhar El Mahraz -Fès***	***Rapporteur***
Pr YAHYAOUI Ali	***Faculté des Sciences Dhar El Mahraz -Fès***	***Examinateur***
Pr MAHRAZ Mohamed Adnane	***Faculté des Sciences Dhar El Mahraz -Fès***	**Examinateur**
Pr RIFFI Jamal	***Faculté des Sciences Dhar El Mahraz -Fès***	**Examinateur**
Pr Tairi Hamid	***Faculté des Sciences Dhar El Mahraz -Fès***	**Directeur de thèse**

Résumé

De nos jours, les actes médicaux réalisés à distance connaissent une forte demande et plus particulièrement durant les périodes de crise telle que celle liée au Covid-19. En imagerie médicale, cet échange rencontre des problèmes de sécurité de données des systèmes d'informations. A travers le présent travail, on propose une technique qui permet d'attester l'authenticité des images médicales et contrôler l'intégrité de ces images. Dans ce contexte médicolégal, une technologie nommée le tatouage numérique s'est avérée être une des solutions : jeune, innovante et très prometteuse en termes de recherche. Cette technique consiste à incorporer une marque, d'une manière imperceptible à l'œil, dans un support d'origine. La marque est insérée de telle sorte que l'on puisse la récupérer à tout moment. L'extraction de cette marque doit être robuste, même après modifications du document tatoué. L'originalité de notre approche est basée sur des modèles mathématiques appelés les transformations polynomiales : des modèles aussi proche que possible du système visuel humain, qui permettent de décomposer l'image en plusieurs composantes. Lesdits modèles permettent aussi de distinguer les zones peu pertinentes pour l'interprétation du diagnostic, zones que nous choisirons pour supporter une marque. En fonction de l'application envisagée, cette marque peut se présenter sous forme d'une séquence aléatoire de bits ou encore un logo binaire. Dans le contexte médical, la marque peut contenir des informations du patient, du médecin ou du centre hospitalier. Le présent travail de recherche apporte cinq différentes contributions relatives au domaine du tatouage numérique. La première contribution est la proposition d'une solution pour le tatouage des images numériques basée sur la transformation polynomiale de Laguerre combinée avec la DCT. La deuxième contribution est la conception d'un algorithme de tatouage des images médicales basé sur la transformée de Chebychev. La troisième contribution est la proposition d'un algorithme de tatouage des images médicales basé sur la transformée d'Hermite combinée avec une technique de fenêtrage adaptatif. La quatrième contribution présente un tatouage robuste basé sur la transformée de Legendre. La cinquième et dernière contribution est la proposition d'une technique de tatouage des séquences de vidéos médicales. Le vrai challenge est de pouvoir maîtriser deux principales contraintes, à savoir : l'invisibilité de la marque insérée et sa robustesse face à différents types d'attaques volontaires et involontaires.

Mots clés : *tatouage des images médicales, transformations polynomiales, polynômes orthogonaux extraction de texture, télémédecine, sécurité des images médicales.*

Abstract

Nowadays, medical acts performed remotely are in a high demand especially during time of crisis such as the coronavirus pandemic (COVID-19). In medical imaging, this exchange faces various data security problems in the information system. Through this thesis, we propose a technique for attesting the authenticity of medical images and controlling their integrity. In this medical-legal context, a technology known as Watermarking has turned out to be one of the efficient solutions as it is young, innovative and very promising in terms of research. This technique consists of embedding a watermark in an original support invisibly. The watermark is embedded in such a way that it can be recovered at any time. The extraction of the watermark should be robust, even after modifying the watermarked document. The originality of our approach is based on mathematical models named polynomial transforms, which are as close as possible to the human visual system. These models are used to decompose an image into several components. Moreover, these models help to extract areas marginally relevant to the interpretation of the diagnosis. These areas will be chosen to embed the watermark. This watermark can be a random sequence of bits or a binary logo depending on the target application. In the medical context, the watermark may contain information about the patient, the doctor or the hospital. This thesis presents five different contributions pertaining to digital watermarking. The first contribution consists of presenting a new solution for image watermarking based on Laguerre polynomial transform combined with DCT. The second contribution is the design of medical image watermarking algorithm based on Chebychev polynomial transform. The third contribution is a new medical image watermarking technique based on Hermite transform combined with a sliding window technique. The fourth contribution focuses on developing a robust medical watermarking scheme based on Legendre Transform. The fifth contribution is a new medical video watermarking scheme based on Krawtchouk polynomial transform. The true challenge is how to control two principal constraints namely, the invisibility of embedded watermark and its robustness against various types of attacks whether they are voluntary or involuntary.

Key words: *Medical image watermarking, polynomial transforms, orthogonal polynomials, texture extraction, telemedicine, security of medical images.*

Remerciements

Je remercie **DIEU** le tout Puissant de m'avoir donné le courage et la volonté d'achever ce travail.

Je commence par présenter ma plus vive gratitude à mon directeur de thèse **Monsieur Le Professeur TAIRI Hamid,** d'avoir accepté de m'accueillir au sein du laboratoire LISAC. Vous avez accepté avec joie de m'encadrer tout au long de ce travail en mettant à ma disposition les moyens nécessaires ayant permis l'aboutissement de ce travail. Je ne vous remercierai jamais assez pour votre disponibilité, conseils et critiques constructives et judicieuses.

Je tiens à exprimer ma parfaite considération à Monsieur Le Professeur **SATORI Khalid** la Faculté des Sciences Dhar El Mahraz de Fès**,** Vous me faites l'honneur de présider mon jury de soutenance et de juger mon travail. Je vous témoigne ma profonde et respectueuse reconnaissance.

Monsieur Le Professeur **EL OUADGHIRI Driss**, Monsieur Le Professeur **EL KINANI El Hassan** de la Faculté des Sciences de Meknès**,** Monsieur Le Professeur **QJIDAA Hassan** de la Faculté des Sciences Dhar El Mahraz de Fès**,** vous me faites l'honneur d'apporter votre expérience à la critique de ce travail en votre qualité de rapporteurs. Vos remarques ont contribué aux nombreuses améliorations de ce manuscrit. Je vous prie de bien vouloir accepter ma respectueuse **c**onsidération.

Monsieur Le Professeur **YAHYAOUI Ali**, Monsieur Le Professeur **MAHRAZ Mohamed Adnane** et Monsieur Le Professeur **RIFFI Jamal** de la Faculté des Sciences Dhar El Mahraz de Fès**,** Je vous remercie d'avoir accepté d'examiner mon travail avec beaucoup d'enthousiasme. Veuillez accepter ma considération profonde envers vos conseils et orientations.

J'en profite pour remercier le corps professoral du département d'informatique pour les efforts déployés en vue de nous apporter une formation doctorale de qualité.

Bien évidemment je remercie mes parents et ma famille pour leur sacrifice et leur soutien inconditionnel tout au long du chemin parcouru. C'est grâce à vous si j'en suis là aujourd'hui**.**

Liste des abréviations

BER	bit error rate
CT	computerized tomography
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
FPD	False Positive Detection
HE	Histogram equalization
HVS	Human Visual System
JPEG	Joint Photographic Experts Group
LDM	Carte de dissimilarité locale
LSB	Least Significant Bit
MF	Moyennes fréquences
IRM	Imagerie par résonance magnétique
MSE	Erreur quadratique moyenne (*Mean square error*)
NC	Corrélation normalisée (*Normalized correlation*)
PET	Tomoscintigraphie par émission de positons
PSNR	Rapport signal à bruit (*Peak Signal to Noise Ratio*)
ROI	Région d'intérêt (*Region of Interest*)
RONI	Région de non intérêt (*Region of Non Interest*)
SSIM	Indice de similarité structurelle
TIC	Technologies de l'information et de la communication
TP	Transformation polynomiale
US	Ultrason

Liste des figures

Figure 1.1: Schéma illustrant les techniques de protection de données 19

Figure 1.2 Exemple de stéganographie en utilisant une encre sympathique.....21

Figure 1.3: Nombre annuel des articles publiés sur le tatouage numérique.....22

Figure 1.4 Modèle générique de tatouage numérique 23

Figure 1.5 Compromis du tatouage numérique 24

Figure 1.6 Classification des techniques du tatouage numérique 27

Figure 1.7 Schéma illustrant la différence entre le domaine spatial et le domaine fréquentiel.....28

Figure 1.8 Découpage de l'image testé « Lena » en 8 plans 29

Figure 1.9 Décomposition par la transformée DCT 31

Figure 1.10 Spectre de Fourier de l'image « Lena » 34

Figure 1.11 Exemple de décomposition d'une image en ondelettes à 3 niveaux.....35

Figure 1.12 Illustration des termes relevant de la santé connectée : e-santé, télésanté, la santé mobile (m-santé), Télémédecine 51

Figure 1.13 Caractéristiques de sécurité d'un système d'information médical.....53

Figure 2.1 phase d'insertion 72

Figure 2.2 Phase d'extraction.....74

Figure 2.3 Images de tests (a) lena, (b) barbara, (c) cameraman, (d) pirate, (e) lake, (f) hill, (g) boat, (h) butterfly.....75

Figure 2.4 Images de tests représentant le watermark du tatouage 75

Figure 2.5 Résultats visuels des principales étapes de l'algorithme proposé 76

Figure 3.1 Schéma représentant la phase d'insertion.....85

Figure 3.2 Schéma représentant la phase d'extraction.....87

Figure 3.3 Ensemble des images médicales de test de différentes modalités 88

Figure 3.4 Les watermarks de test.....88

Figure 3.5 Performances entropie / degré de décomposition polynomiale.....90

Figure 3.6 Courbes du PSNR en dB pour différentes images médicales de test : a. IRM et échographie, b. radiographie et CT, c. TEP et mammographie. 91

Figure 3.7 Courbes de la NC pour différentes images médicales de test : a. IRM et échographie, b. radiographie et CT, c. TEP et mammographie.....92

Figure 3.8 La LDM des images de tests.....97

Figure 4.1 Schéma général de l'approche de tatouage proposée.....112

Figure 4.2 Exemple d'images médicales et des watermarks utilisés pour faire les tests 115

Figure 4.3 Les images de tests: (a) et (b) la modalité IRM, (c) et (d) la modalité US, (e) le watermark.....131

Figure 4.4 Illustration des résultantes des étapes de notre méthode de touage.....132

Figure 5.1 Schéma de la méthode proposée du tatouage des vidéos médicales.....137

Figure 5.2 Supports de tests: a. ultrasons, b. x-ray, c. microscopie, d. watermark 1, e. watermark 2 142

Liste des tableaux

TABLE 2-1 Comparaison des performances des différentes techniques en termes de PSNR dans le cas sans attaques. 77

TABLE 2-2 Comparaison des performances des différentes techniques en termes de NC dans le cas sans attaques. 77

TABLE 2-3 Les valeurs NC des watermarks extraits après exposition aux attaques 78

TABLE 3-1 Résultats dans le cas sans attaques de la méthode proposée pour deux modalités d'images médicales : IRM et échographie 93

TABLE 3-2 Résultats dans le cas sans attaques de la méthode proposée pour deux modalités d'images médicales : X-ray et CT 94

TABLE 3-3 Résultats dans le cas sans attaques de la méthode proposée pour deux modalités d'images médicales : PET et Mammographie 95

TABLE 3-4 Comparaison du PSNR (dB) et de la valeur NC de la méthode proposée avec les méthodes existantes 96

TABLE 3-5 Watermarks extraits et leurs valeurs NC après diverses attaques 98

TABLE 3-6 Variation de la corrélation normalisée (NC) contre l'attaque de compression JPEG 99

TABLE 3-7 Variation de la corrélation normalisée (NC) contre l'attaque d'ajout de bruit 100

TABLE 3-8 Variation de la corrélation normalisée (NC) contre l'attaque de filtrage 101

TABLE 3-9 Variation de la corrélation normalisée (NC) contre l'attaque d'accentuation et égalisation d'histogramme 102

TABLE 3-10 Variation de la corrélation normalisée (NC) contre la rotation 103

TABLE 3-11 Performance de la technique de tatouage proposée en variant la taille du watermark 104

TABLE 3-12 Résultats des Faux Positifs de notre méthode de tatouage 105

TABLE 3-13 Résultats du temps d'exécution de notre méthode de tatouage 105

TABLE 4-1 Résultats visuels de l'exemple d'implémentation de notre algorithme sur différents modalités 117

TABLE 4-2 PSNR des images tatouées 118

TABLE 4-3 Comparaison des résultats en terme de PSNR et NC 118

TABLE 4-4 Comparaison des résultats en faisant varier la taille du Watermark. 119

TABLE 4-5 Résultats de notre méthode e termes de PSNR et NC de 160 images médicales 120

TABLE 4-6 Robustesse de la méthode proposée à la compression JPEG.....121

TABLE 4-7 Robustesse de la méthode proposée à l'ajout de bruit.....122

TABLE 4-8 Robustesse de la méthode proposée au filtrage 122

TABLE 4-9 Robustesse de la méthode proposée aux attaques géométriques 123

TABLE 4-10 Robustesse de la méthode proposée aux autres attaques 123

TABLE 4-11 Comparaison numérique des valeurs de SSIM des watermarks extraits 124

TABLE 4-12Comparaison numérique des valeurs de NC des watermarks extraits 125

TABLE 4-13 Comparaison numérique des valeurs de SSIM des watermarks extraits 126

TABLE 4-14 Résultats des Faux Positifs.....127

TABLE 4-15 performances en temps d'exécution de la méthode proposée 128

TABLE 4-16 Comparaison des résultats en terme de PSNR et SSIM.....133

TABLE 4-17 Comparaison des valeurs NC des watermarks extrait avec et sans attaques 134

TABLE 4-18 Comparaison en temps d'exécution.....135

TABLE 5-1 La représentation visuelle des principales composantes de notre méthode de tatouage 143

TABLE 5-2 Comparaison sommaire en termes des moyennes du PSNR et NC pour différentes tailles du watermark 144

TABLE 5-3 Watermarks extraits après les attaques en termes de NC.....145

TABLE 5-4 Comparaison de la robustesse de notre méthode avec d'autres techniques en termes de NC.....145

Sommaire

Résumé 1

Abstract 2

Remerciements 3

Liste des abréviations 4

Liste des figures 5

Liste des tableaux 7

Sommaire 9

Introduction générale 13

Chapitre 1. Etat de l'art 18

1.1 Introduction 19

1.2 Généralités sur le tatouage numérique 19

1.2.1 Historique et terminologies 19

1.2.2 Modèle générique du tatouage numérique 23

1.2.3 Propriétés du tatouage des images numériques 24

1.2.4 Classifications des techniques du tatouage numérique 27

1.2.5 Evaluation des algorithmes du tatouage 39

1.2.6 Applications du tatouage numérique 44

1.3 Tatouage des images médicales 47

1.3.1 Imagerie médicale 47

1.3.2 Médecine à distance: usages, bénéfices et limites 50

1.3.3 Sécurité des images médicales 53

1.3.4 Classification des méthodes de tatouage d'images médicales 53

1.3.5 Méthodes existantes de tatouage d'images médicales 54

1.4 Conclusion.....59

Chapitre 2. Tatouage des images numériques basé sur la transformée de Laguerre combinée avec la DCT 60

2.1 Introduction 61

2.2 Formalisme mathématique 62

2.2.1 Notion de bases sur les polynômes orthogonaux 63

2.2.2 Construction de la base polynomiale 67

2.2.3 Décomposition polynomiale d'une image.....70

2.3 Algorithme proposé pour la phase d'insertion 72

2.4 Algorithme proposé pour la phase d'extraction 73

2.5 Expérimentations et résultats 75

2.5.1 Sans attaques 75

2.5.2 Avec attaques 78

2.6 Conclusion.....79

Chapitre 3. Tatouage des images médicales basé sur la transformée de Chebychev.....80

3.1 Introduction 81

3.2 Formalise mathématique 81

3.3 Méthode proposée 84

3.3.1 Phase d'insertion 84

3.3.2 Phase d'extraction 86

3.4 Expérimentations et résultats 87

3.4.1 Mesures de performances.....89

3.4.2 Paramètres de l'algorithme....89
3.4.3 Analyse d'invisibilité....91
3.4.4 Analyse de robustesse....97
3.4.5 Analyse de capacité....103
3.4.6 Analyse des faux positifs....104
3.4.7 Analyse du temps d'exécution....104
3.5 Conclusion....105
Chapitre 4. Tatouage des images médicales basé sur les Transformées d'Hermite et de Legendre....106
4.1 Introduction....107
4.2 Tatouage sécurisé des images médicales basé sur la transformée d'Hermite....107
4.2.1 Prétraitement....108
4.2.2 Approche proposée....112
4.2.3 Expérimentations et résultats....114
4.3 Tatouage robuste basé sur la transformée de Legendre....128
4.3.1 Prétraitement....128
4.3.2 Approche proposée....129
4.3.3 Expérimentations et résultats....131
4.4 Conclusion....135
Chapitre 5. Tatouage des séquences vidéos médicales basé sur la Transformée de Krawtchouk136
5.1 Introduction....137
5.2 Méthode proposée....137
5.2.1 Prétraitement....138
5.2.2 Algorithme de la phase d'insertion....140

5.2.3 Algorithme de la phase d'extraction 141
5.3 Expérimentations et résultats 142
5.3.1 Sans attaques 143
5.3.2 Avec attaques 144
5.4 Conclusion 146
Conclusion générale 147
Publications de l'auteur 150
Bibliographie 151

Introduction générale

Mis en contexte et problématique

Grâce à la digitalisation, les nouvelles technologies de l'information et de la communication (**TIC**) ont fortement modifiées les habitudes de manipulation des données numériques (tels que l'image, la vidéo, l'audio ou le texte) en facilitant leurs distributions, duplications et modifications. Bien que l'intégration de cette digitalisation dans différents domaines, notamment le domaine médical (qui est au cœur du plan « **Ma santé 2022, un engagement collectif** »), progresse d'une manière révolutionnaire et offre des opportunités sans limites ou presque**.** À l'autre extrémité du spectre, une mauvaise mise en œuvre de la digitalisation recèle encore certaines embûches. En effet, cela peut alimenter le doute sur la fiabilité de l'information circulant à travers les médias numériques. Sans mettre en cause le progrès informatique, il serait plutôt incontournable d'explorer tous les moyens de sécurisation et du renforcement de sa fiabilité et de son authenticité. Pour autant, il ne faut pas tomber dans le piège qui consiste à réglementer la technologie, il faut plutôt faire attention aux usages qui ne bloquent pas l'innovation et le progrès.

L'application des TIC au domaine médical, ne doit pas être arbitrairement exploitée, surtout que les décisions critiques sont faites sur la base des informations contenues dans l'image médicale. En effet, l'image médicale, qui est un document à caractère sensible, est d'une grande importance et sa juste valeur ne peut être valorisée que par les dégâts intolérables que peut causer son usage illicite. En général, les cybers attaques touchant les services de santé sont largement évoqués à travers les médias et ne cessent d'alerter la communauté scientifique à travers le monde sur le danger que courent les dispositifs de santé. La **sécurité** de l'image médicale n'est pas moins importante que ces dispositifs eux-mêmes. Elle expose les patients et les organismes de prestations de soins de santé à d'importants risques qui sont de nature très variés et ne présentent pas toutes le même degré de gravité.

Ne pas agir reviendrait à augmenter le risque d'avoir d'ici quelques années une santé à deux vitesses : l'une publique, dépassée, plus ou moins gratuite, mais peu efficace. L'autre, privée, payante, et probablement la plus efficace. On parle donc, de la **santé connectée** (l'**e-santé**, la **télésanté** ou encore la **télémédecine**), qui est définie comme une forme de pratique médicale à distance utilisant les TIC. La télémédecine de sa part s'annonce bien fort à travers le monde et connait un essor spectaculaire avec la crise actuelle liée au **Covid-19.** Dans ce sens, de nombreuses plateformes de télémédecine se présentent par leurs services en ligne comme alternatives aux services habituels durant le confinement. Au **Maroc** par exemple, la plateforme **DabaDoc** a lancé sa téléconsultation au début de la crise du covid-19 qui a été accompagnée par **Axa Assurance Maroc**. Par conséquent, assurer la sécurité des données échangées par ces plateformes devient une tache extrêmement importante. Par ailleurs, l'intégrité et l'authenticité de ces données ne peuvent être garanties rien qu'en se basant sur leur aspect visuel. En effet, des modifications malveillantes peuvent tout le temps altérer l'information sans que les altérations soient visibles à l'utilisateur.

S'inspirant principalement de la cryptographie et la sténographie, le **tatouage numérique** ou bien « **watermarking** » se présente comme solution efficace permettant la protection des données numériques, à savoir la protection de la propriété intellectuelle, l'authenticité et l'intégrité du document, nécessaires pour un échange fiable de ces données. Le tatouage est effectué en insérant une **signature**, nommée aussi **marque** ou encore ***watermark*** en anglais, dans le document d'origine à protéger. Cette marque doit être imperceptible à l'œil humain et robuste à différentes manipulations du document tatoué. Depuis plus d'une décennie, les éléments fondamentaux et les applications des algorithmes de tatouage se développent en littérature comme un moyen de protection de l'authenticité des données multimédia [1]. Toutefois, d'autant plus que des nouvelles techniques soient proposées, des failles inattendues surgissent toujours et stimulent les chercheurs en quête de meilleurs compromis entres les données à protéger et les traitements de sécurisation à envisager. Notre objectif est de contribuer à la réalisation d'un processus qui peut servir d'un système de protection des images médicales. Pour se faire, nous présentant, à travers cette thèse, des techniques pour tatouer des images médicales avec une signature invisible et indétectable à l'œil humain.

La motivation de notre recherche s'explique par plusieurs points d'intérêt. L'image en tant que document numérique est, entre autres, une structure de données réparties selon une configuration propre à chaque image. Cela nous incite à approfondir nos connaissances sur cette structure et chercher en l'occurrence les meilleurs outils de sécurisation qui permettent de renforcer son immunité contre tout ce qui porte atteinte à sa valeur informationnelle. De nouvelles thématiques de recherche ont vu le jour, notamment concernant les techniques du prétraitement de l'image permettant l'extraction d'un ensemble de caractéristiques pertinentes de l'image comme la texture[2]. Cette étape de prétraitement nécessite l'utilisant des modèles proches du système visuel humain (SVH). Ces modèles, ayant une caractéristique intéressante, attirent les chercheurs à adapter ce concept pour plusieurs applications, y compris le tatouage. Un modèle basé sur les transformations polynomiales est un sujet de recherche très actif en vison par ordinateur qui a trouvé le succès dans différent domaines d'application. Pour cela, Nous développons un outil de décomposition d'images à bases de polynômes orthogonaux pour l'étape du prétraitement du tatouage des images médicales.

Contributions et organisation

Nous proposons dans le présent travail de nouvelles approches de tatouage numérique pour renforcer la sécurité des images médicales. L'originalité de notre approche se base sur les transformations polynomiales permettant d'extraire les zones de l'image les plus appropriées à l'insertion du *watermark* du tatouage. Le choix de cette approche est justifié par le besoin de trouver le meilleur compromis entre l'invisibilité et la robustesse de la marque à toutes modifications. Dans **le premier chapitre**, nous présentons un état de l'art de l'aspect général du tatouage numérique. Ce chapitre est divisé en deux grandes sections : la première décrit les aspects principaux et les terminologies liés aux méthodes de tatouage numérique, en introduisant les différents critères sur lesquels ces méthodes peuvent être classifiées. Nous citons aussi les différentes attaques que peut subir une image tatouée afin de détruire la marque insérée. La deuxième section aborde le tatouage d'images médicales, en introduisant les critères de sécurités et leurs importances pour la protection des ces images. Premièrement, nous visant à introduire les principales modalités d'imagerie médicale existantes ainsi que les différents critères du partage des images médicales et les risques et besoins en matière de sécurité qui y en découlent. Ensuite,

nous présentons les différents critères selon lesquels ces méthodes sont classées. Nous donnons aussi un aperçu des méthodes existantes dans la littérature et leurs limitations.

C'est ainsi que nous proposes dans **le second chapitre** notre première contribution de tatouage basé sur la transformation polynomiale de Laguerre combinée avec la DCT. Cette première approche est dédiée à la protection des la propriété intellectuelle des images classiques. Dans ce chapitre, nous expliquons tout d'abord, les formalismes de base utilisés pour réaliser une décomposition polynomiale à base de polynômes orthogonaux d'une image. Ensuite nous détaillons les différentes étapes du schéma de tatouage proposé ainsi que les résultats obtenus.

Le troisième chapitre est dédié à la protection des images médicales, en effectuant un tatouage robuste basé sur une transformation polynomiale discrète. En effet, dans ce chapitre on a testé une autre famille de polynômes orthogonaux (Chebychev) pour l'étape du prétraitement de l'image médicale. De ce fait, nous présentant, d'abord les outils de base de ce modèle mathématique pour l'extraction de la composante de texture de l'image ; ensuite nous détaillons l'algorithme proposé, et nous présentons les résultats expérimentaux évaluant les performances de notre méthode.

Dans l'objectif de la protection complète de l'image, nous proposons dans **le quatrième chapitre** deux techniques de tatouage des images médicales. La première technique de tatouage se base la transformée d'Hermite combinée avec une technique de fenêtrage adaptatif. Dans cette technique nous utilisant la transformée d'Arnold pour chiffrer le watermark, et ce afin de renforcer la sécurité du schéma du tatouage. Tandis que la deuxième technique se base sur la transformée de Legendre. Les formalismes mathématiques et les techniques utilisées pour les algorithmes proposés sont aussi détaillés. Enfin, nous présentant des expérimentations permettant de montrer la pertinence de nos deux méthodes.

Le cinquième chapitre est consacré au tatouage des séquences vidéos médicales basé la transformée de Krawtchouk combinée avec une technique de sélections d'images clés « *Key frames* » de cette séquence. De la même manière, les fondements de base sont présentés en premier. Ensuite, les algorithmes des phases d'insertion et d'extraction du *watermark* sont élaborés. Enfin, nous présentons les résultats expérimentaux évaluant les performances de notre approche.

La dernière partie de ce mémoire contient des conclusions générales dans lesquelles nous résumons notre recherche. Nous évoquant aussi, dans cette partie, les perspectives de notre travail et lignes possibles de recherche à partir des transformations polynomiales et leurs applications dans le tatouage des images médicales.

Chapitre 1. Etat de l'art

Sommaire

1.1 Introduction 19

1.2 Généralités sur le tatouage numérique 19

1.3 Tatouage des images médicales 47

1.4 Conclusion 59

1.1 Introduction

Dans ce chapitre, nous définissons le cadre général et les notions nécessaires à la compréhension de notre problématique de recherche : le tatouage des images médicales. Ce chapitre est organisé en deux sections principales : la première section regroupe les notions de bases des techniques de tatouage des images numériques. La deuxième section présente le tatouage des images médicales. Dans la première section, nous présentons les principales propriétés des techniques de tatouage numérique, leurs classifications, leurs méthodes d'évaluations et les différentes attaques que peut subir une image tatouée, ainsi que les différentes applications du tatouage. Dans la seconde section, nous décrivons d'abord les principales propriétés de l'imagerie médicale, ensuite nous distinguons les différents usages, bénéfices et limites de la médecine à distance et enfin nous présentons une classification pour le tatouage des images médicales ainsi qu'un état de l'art sur les techniques existantes dans la littérature.

1.2 Généralités sur le tatouage numérique

1.2.1 Historique et terminologies

Tout au long de l'histoire, l'humanité essaye d'échanger des informations appartenant à tous les domaines d'une manière sécurisée, le cas des données secrètes échangées pour des stratégies militaires par exemple. Afin d'éviter toute confusion relative à notre contexte de la transmission sécurisée des informations, on distingue principalement deux grandes catégories : la **cryptographie** et la **dissimulation d'informations**[3]**,** comme illustré sur la figure 1.1.

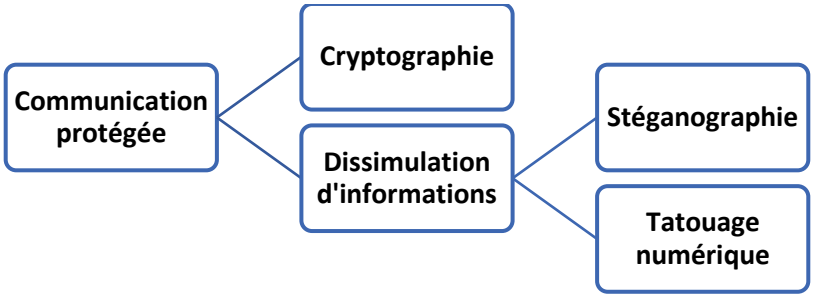


Figure 1.1: Schéma illustrant les techniques de protection de données

La cryptographie est l'art des codes secrets, elle permet de rendre indéchiffrable l'information que l'on désire transmettre, et ce à toute personne ne possédant pas la clé de son décodage. Cette technique permet de protéger l'information depuis sa création jusqu'à son utilisation mais, une fois décryptée, cette information n'est plus protégée et il n'y a plus de contrôle sur sa diffusion[4]. Ce mécanisme est un outil très important mais ne résout pas tous les problèmes de protection des données numériques. La deuxième catégorie regroupe des techniques qui permettent de cacher un message significatif dans un message d'origine. Cette dernière constitue une solution prometteuse dans ce contexte de protection, on distingue deux familles de dissimulation de données: La **stéganographie** et le **tatouage** numérique. La **stéganographie** est l'art de dissimuler une information au sein d'un contenu, et ce, afin qu'elle soit indiscernable et difficilement identifiable. Cette dissimulation se fait de sorte qu'elle soit difficile pour un observateur extérieur de se rendre compte qu'il y a eu dissimulation. Quant au **tatouage** numérique, compte tenu du principe de camouflage, c'est l'art d'altérer un média (une image, un son, une vidéo ...) de sorte qu'il contienne un message le plus souvent de manière imperceptible afin de faire face aux différents problèmes de protection des droits et de copie.

L'utilisation classique de la **stéganographie** prend place il y a plus de deux mille ans. On peut citer comme exemple, concernant la dissimulation d'information, celui de *Histiée*[1] : il sélectionne son plus fidèle esclave, lui fait raser la tête et tatouer un ordre de révolte sur le crâne; Dès que les cheveux eurent repoussé, l'esclave pouvait traverser les territoires ennemis sans éveiller les soupçons. Une fois arrivée à destination, *Aristagoras*[2] se permet de raser à nouveau le crâne de l'esclave pour récupérer le message[5]. Tout au long de l'histoire, les méthodes ont évoluées sans cesse vers de nouvelles techniques plus efficaces. A titre d'exemple les encres sympathiques (encres invisibles), qui compte parmi les méthodes les plus utilisées au cours des siècles. Le cas des textes écrits à l'encre, on en écrit au milieu, un message à l'aide de lait, de jus de citron ou de certains produits chimiques. Comme il est invisible à l'œil humain, pour le révéler on utilise soit une source de chaleur, soit un révélateur chimique (figure 1.2).

[1] Le tyran (individu disposant d'un pouvoir absolu) de la ville de Milet (une ancienne cité grecque) sous la suzeraineté de l'empire du roi perse Darius Ier à la vie siècle.

[2] Gouverneur de Millet. Le beau-fils et neveu de Histiée

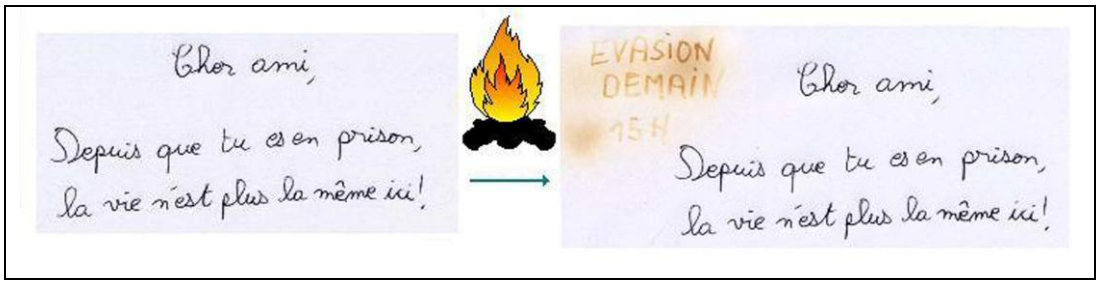


Figure 1.2 Exemple de stéganographie en utilisant une encre sympathique

Cependant, l'art du **tatouage** a aussi connu sa petite histoire et a été inventé en Chine depuis plus de mille ans pour tatouer le papier. Même si le but principal des premiers tatouages était incertain, mais ils ont été utilisés pour des fonctionnalités pratiques. Le plus ancien document tatoué trouvé dans les archives remonte à *1292* et qui a pour origine la ville de *« Fabriano »* en Italie qui a joué un rôle important dans l'évolution de l'industrie papetière afin d'éviter tout type de confusion. Le tatouage s'est rapidement étendu en Italie, en Europe et en Amérique au $18^{ème}$ siècle, initialement pour identifier un fabricant ou une usine de papeterie. Par la suite, Il a servi pour indiquer le format et la qualité du papier, et aussi comme base d'authentification du papier et une mesure anti-contrefaçon pour la monnaie et autres documents. L'analogie entre le tatouage du papier et le tatouage numérique est évidente puisque la première utilisation du terme «Marque d'eau» (*watermark* en anglais) dans le contexte de données numériques s'est inspirée du tatouage du papier des billets de banque et de timbres. Le tatouage numérique est une discipline très récente, qui a débuté en *1990* avec l'article de « *Tanaka et al* » en présentant une technique qui permet de cacher secrètement de l'information dans une image ainsi qu'à assurer les droits de propriété[6]. La fin des années *1990* a favorisé l'essor d'une nouvelle discipline, qui s'est caractérisée par une effervescence médiatique et scientifique, le plus souvent liée à des préoccupations de type sécurité. Cet axe recherche a été élaboré dans les publications en langue anglaise par le terme « **watermarking** », a été baptisé en français tatouage, filigrane ou encore aquamarquage. Ce dernier a pour but de parer le piratage des documents multimédia. Cette technique a rencontré un intérêt croissant de la part des chercheurs et des industriels à partir de l'année 1996. La figure 1.3 visualise le nombre de publications en utilisant le mot clé « watermarking » sur la base de données bibliographique INSPEC**.** En outre, à cette époque plusieurs organisations ont commencé à considérer le tatouage numérique pour l'inclure dans

leurs normes. Le *Copy Protection Technical Working Group* a testé des systèmes de tatouage numérique pour la protection de vidéos dans des disques DVD. Dans le domaine de l'imagerie, la société Adobe en collaboration avec la compagnie *Digimarc* [3] a utilisé cette technique dans son logiciel *Adobe Photoshop*. Ainsi, la véritable explosion du tatouage numérique s'est manifestée par l'explosion des connexions Internet, et du libre échange des fichiers. En bref, cette science si on peut la nommer ainsi est en pleine explosion actuellement en raison de la croissante demande des services en lignes partout dans le monde.

D'une manière générale et abstraite, la cryptographie consiste en une écriture secrète et indéchiffrable, la stéganographie consiste en une écriture discrète avec une indiscernabilité de nature statistique, tandis que le tatouage consiste en une écriture discrète avec une indiscernabilité de nature perceptuelle. En d'autres termes, la stéganographie permet d'assurer qu'aucun test statistique ne puisse discerner de différence entre le support avant et après insertion du message caché, tandis que le tatouage vise le système visuel humain quant au discernement. De plus en cryptographie si l'information originale est modifiée, il sera impossible de la recouvrer, tandis qu'en stéganographie, le message caché (secondaire) est supposé rester accessible et ce même après de multiples recopies et manipulations diverses de l'information originale. Il est à noter que les trois principes n'on jamais été concurrents, mais sont plutôt complémentaires.

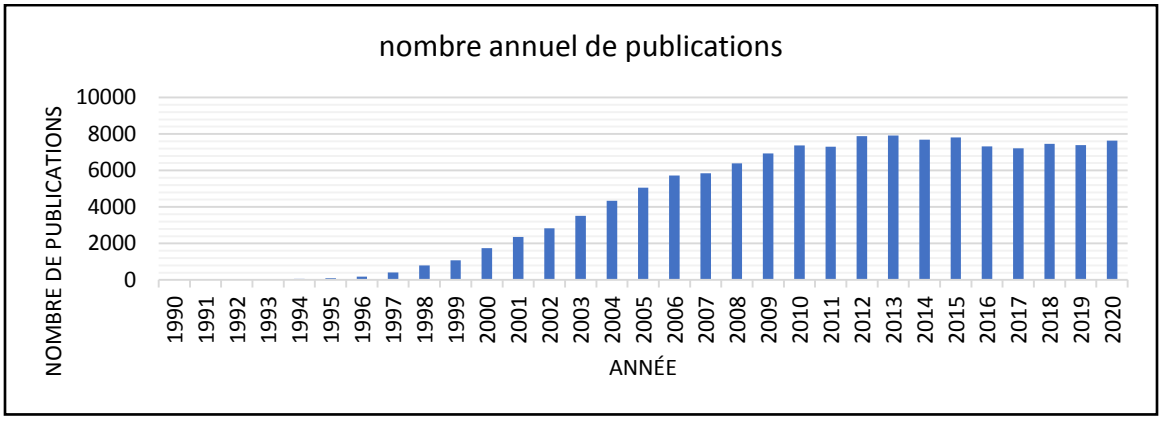


Figure 1.3: Nombre annuel des articles publiés sur le tatouage numérique

[3] Un fournisseur de technologies du tatouage numérique

1.2.2 Modèle générique du tatouage numérique

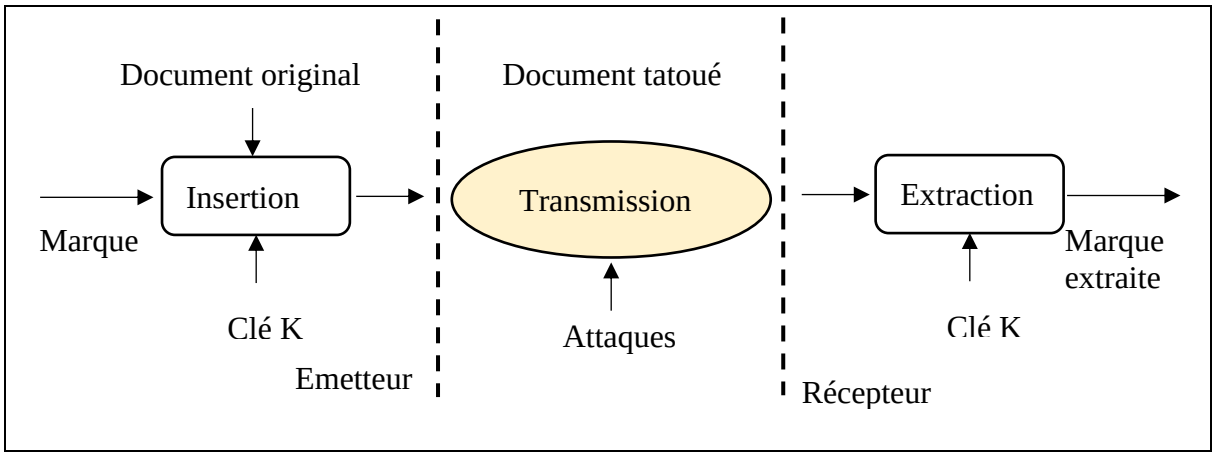


Figure 1.4 Modèle générique de tatouage numérique

Le processus du tatouage numérique est par deux phases fondamentales : l'insertion et l'extraction. On peut ajouter, cependant, une phase intermédiaire concernant la transmission du document tatoué. La figure 2.4 illustre cet enchaînement.

1.2.2.1 *Phase d'insertion*

La phase d'insertion (Embedding en anglais*)* consiste à insérer une marque dans un document original en vue de créer un document tatoué. Le paramètre facultatif « clé K » est une clé cryptographique spécifique à l'émetteur, qui permet de renforcer le niveau de sécurité du système du tatouage entier. A titre d'exemple, le tatouage d'une image numérique I en utilisant une marque W et une clé secrète K , résultant ainsi en une image tatouée I_ω. La résultante est par la suite transmise au récepteur et peut être soumise à différent types d'attaques. Cette phase est modélisée par la fonction suivante :

$$I_\omega = Embedding(I, W, K) \quad (1)$$

L'insertion se fait en utilisant différentes techniques qu'on a présentée dans la section 2.3 qui donne de plus amples détails.

1.2.2.2 *Phase d'extraction*

La phase d'extraction (Extraction en anglais) consiste à extraire la marque insérée sur le document d'origine, depuis le document tatoué en utilisant la clé K. Citant le même exemple présenté dans la phase d'insertion, le récepteur reçoit la version modifiée de l'image tatouée I_{ω}^{*}. Cette phase permet d'extraire la marque W^{*} depuis l'image tatouée I_{ω}^{*} en utilisant la même clé K et éventuellement d'autres paramètres dépendant de la technique utilisée (voir section 2.4 pour plus de détails). Cette phase est modélisée par la fonction suivante :

$$W^{*} = Extraction(I_{\omega}^{*}, K, ..) \quad (2)$$

La technique d'extraction d'un modèle de tatouage typique doit satisfaire les conditions suivantes :

- La détection de la marque W^{*} depuis I_{ω}^{*} est établie avec/ou sans l'utilisation explicite de l'image originale I.
- Si l'image tatouée I_{ω} n'a pas été altérée (attaquée), alors dans ce cas, la marque extraite W^{*} correspond exactement à la marque originale W.

1.2.3 Propriétés du tatouage des images numériques

Dans le but de concevoir un algorithme de tatouage performant, un compromis optimal entre les propriétés suivantes: invisibilité, robustesse, et d'autres propriétés dépendant de l'application envisagée, doit être atteint. Dans la suite nous présentons les propriétés principales du tatouage numérique.

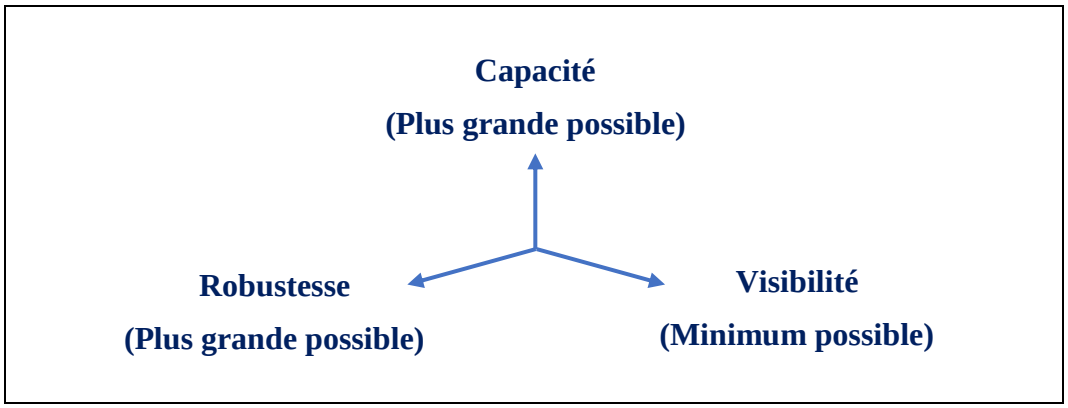


Figure 1.5 Compromis du tatouage numérique

• **Visibilité :** Le tatouage numérique ne devrait en aucun cas affecter la qualité visuelle de l'image originale après insertion de la marque. L'imperceptibilité est définie en tant que similitude visuelle entre l'image originale et l'image tatouée [3]. En d'autres termes, l'impact visuel du tatouage doit être le plus faible possible (i.e. modifications imperceptibles) et la marque insérée ne peut être extraite que par un algorithme. Ce facteur est une exigence importante pour le tatouage numérique en général et pour le tatouage des images médicales en particulier.

• **Robustesse :** Un tatouage est dit robuste s'il est capable d'extraire la marque insérée même si l'image tatoué est soumise à des modifications. Il est nécessaire de distinguer plusieurs types d'attaques selon qu'elles sont considérées comme étant licites ou illicites (en termes de dégradations visibles inacceptables et/ou d'utilisation commerciale rendue impossible). Les attaques bienveillantes regroupent les manipulations effectuées par un utilisateur de bonne foi. On trouve dans cette catégorie la compression JPEG, les conversions de format en général, les changements de résolution (zoom), etc. Il n'est pas possible d'énumérer l'ensemble des attaques bien ou malveillantes ne dégradant pas l'image de façon significative mais qui néanmoins sont capables de « lessiver » l'image marquée afin de retirer la marque, ou plus simplement d'empêcher de l'extraire correctement.

• **La capacité (payload) ou ratio** : c'est la quantité d'informations que l'on espère cacher par rapport à la quantité d'informations associée au support audio, image ou vidéo utilisé. Ordinairement Cette quantité varie selon l'application. En général, quelques bits suffisent pour assurer le service de la protection du droit d'auteurs à l'aide d'un identifiant, mais pas pour cacher des informations explicites comme un logo de société, assurer des services d'intégrité ou de non répudiation. On peut distinguer les signatures qui représentent seulement un pointeur vers une information stockée à l'extérieur de l'image, de celles qui s'auto-suffisent pour fournir une information significative (une chaîne de caractères, un logo visuel, etc.). Plus que la capacité est grande plus la déformation est grande. En général, La taille de la marque est généralement fixée et elle est la même à la phase de l'insertion et l'extraction.

De ce fait, on remarque que ces trois critères sont contradictoires (voir Figure 1.5). Si l'on augmente par exemple la force du tatouage dans le but de le rendre plus robuste, cela aura en

contrepartie pour effet de rendre ce dernier également plus visible. De la même manière, si l'on augmente la taille du message à cacher cela se fera au détriment de la robustesse. Il est donc nécessaire de trouver le meilleur compromis possible entre ces trois paramètres en fonction de l'application visée. Il serait, par exemple, absurde de mettre au point un algorithme de tatouage de grande capacité si seulement quelques messages différents sont cachés en pratique. Ce qui est typiquement le cas pour le contrôle de copies où deux bits suffisent pour coder les trois messages e même, certaines applications ne requièrent pas l'usage d'un tatouage robuste ; la fragilité du tatouage peut être alors exploitée afin d'assurer par exemple l'intégrité des images. D'où, si la marque est altérée, l'image n'est plus considérée comme intègre.

En plus des contraintes précédentes, d'autres critères sont aussi à considérer :

- **Sécurité :** cette propriété permet d'assurer que le *watermark* après extraction n'est accessible que par les utilisateurs autorisés disposant d'une clé secrète. La sécurité d'un algorithme de tatouage numérique ne repose pas seulement sur le fait que les algorithmes d'insertion et d'extraction ne sont pas publics. C'est pour cela que beaucoup d'algorithmes de tatouage numérique sont conçus pour utiliser une clé cryptographique. Dans un tel système, la méthode par laquelle la marque est insérée dépend de cette clé qui sera utile par la suite pour sa détection.

- **Fausse alarme :** c'est la détection d'une marque dans une image alors que l'image n'a pas été tatouée ou bien qu'elle ait été tatouée avec une autre marque. Cette contrainte est mesurée par la probabilité de fausse alarme. Le seuil requis de cette probabilité dépend de l'application : pour la protection du droit d'auteur, elle est typiquement de l'ordre de 10-6. Par contre, dans une application de contrôle de copies, des milliers de détecteurs de marque sont en cours d'exécution sur des milliers d'images. Si une image non tatouée génère constamment de fausses alarmes, cela pourrait causer de graves problèmes. Donc, pour une application, la probabilité de fausse alarme doit être très faible.

- **Coût algorithmique :** Certaines applications, comme le contrôle de diffusion, doivent utiliser des algorithmes de tatouage numérique peu coûteux en temps de calcul pour permettre une implémentation en temps réel.

- **Détection informée ou non informée :** Dans certaines applications, l'image originale et celle tatouée sont indispensables pour l'opération d'extraction : ce type de schéma est appelé informé. Dans le cas contraire, il est référé comme non informé : dans ce cas le processus d'extraction sera plus complexe.

- **Réversibilité :** ce facteur fait référence à la capacité du système à récupérer le contenu d'origine depuis la version tatouée. En effet, un tel facteur est très important en tatouage numérique et très recommandé en ce qui est le cas des images médicales et les applications militaires. En imagerie médical par exemple, toute petite dégradation visuelle du contenu original et qui ne peut être récupérée pourrait conduire à un mauvais diagnostic qui pourrait être fatal et entraîner d'éventuelles poursuites judiciaires[7].

1.2.4 Classifications des techniques du tatouage numérique

En raison du grand nombre des techniques du tatouage numérique, plusieurs schémas de classification ont été proposés dans la littérature selon différents critères, pour diverses applications [1], [3], [5], [8]. Dans cette section, on présente un organigramme de classification des principales catégories (Figure 1.6). Il est important de noter que le tatouage numérique dépend du document envisagé : image, vidéo, audio, texte, etc. Dans le présent travail on s'est focalisé sur les images numériques comme type de support.

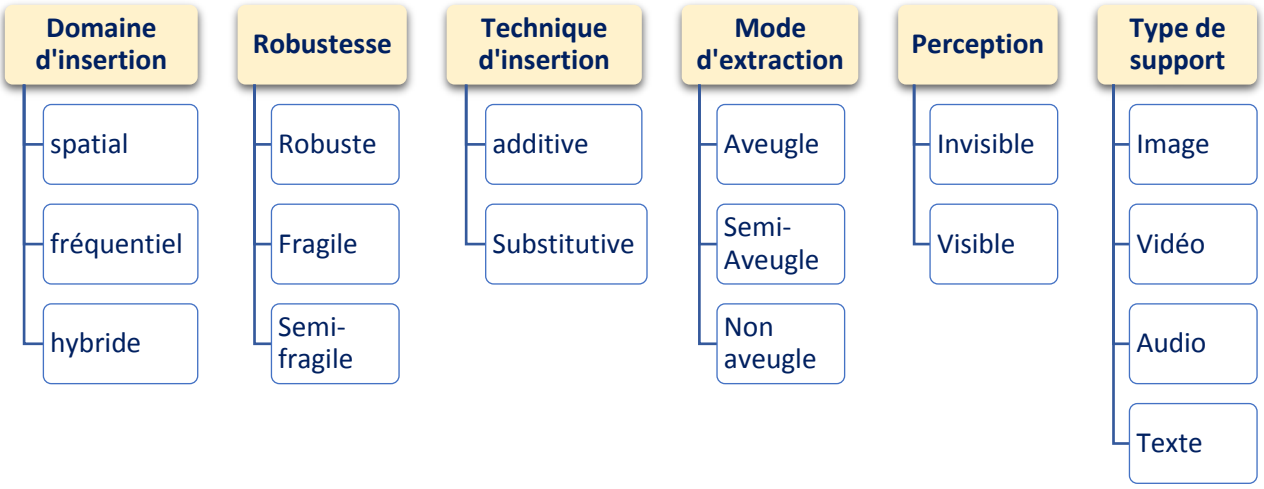


Figure 1.6 Classification des techniques du tatouage numérique

1.2.4.1 *Domaine d'insertion*

La conception d'un système de tatouage numérique, nécessite le choix d'un domaine d'insertion axé sur deux principales classes : spatial et fréquentiel. On peut distinguer aussi des algorithmes utilisant les deux domaines, on parle alors d'algorithmes hybrides, qu'on en parle que rarement. Cependant, ce domaine n'est pas aléatoirement choisi, différents critères interviennent à cette étape afin d'optimiser les performances du système. Premièrement, le domaine choisi doit être capable de décorréler le signal hôte (exemple l'image originale) du signal de tatouage (image tatouée). Deuxièmement, prendre en considération le fait que la distorsion et la déformation du document en phase d'insertion soit le moins faible possible. C'est-à-dire, permettre une altération importante de certaines composantes du document sans modifier sa perception, ce qui facilitera par la suite la détection de la marque du tatouage. Troisièmement, le domaine doit être invariant à certaines perturbations subies par le document; ce critère est fréquemment utilisé lorsque les perturbations désynchronisantes sont considérées. Cette invariance facilite la conception de systèmes robustes aux différents types de perturbations. De ce fait, La littérature propose les différents domaines respectant au moins l'un de ces critères (mais jamais les trois). Nous présentons dans ce qui suit les domaines d'insertion les plus utilisés (comme illustré sur la figure 1.7). Ainsi, nous présentons quelques exemples des méthodes de tatouage pour chaque domaine :

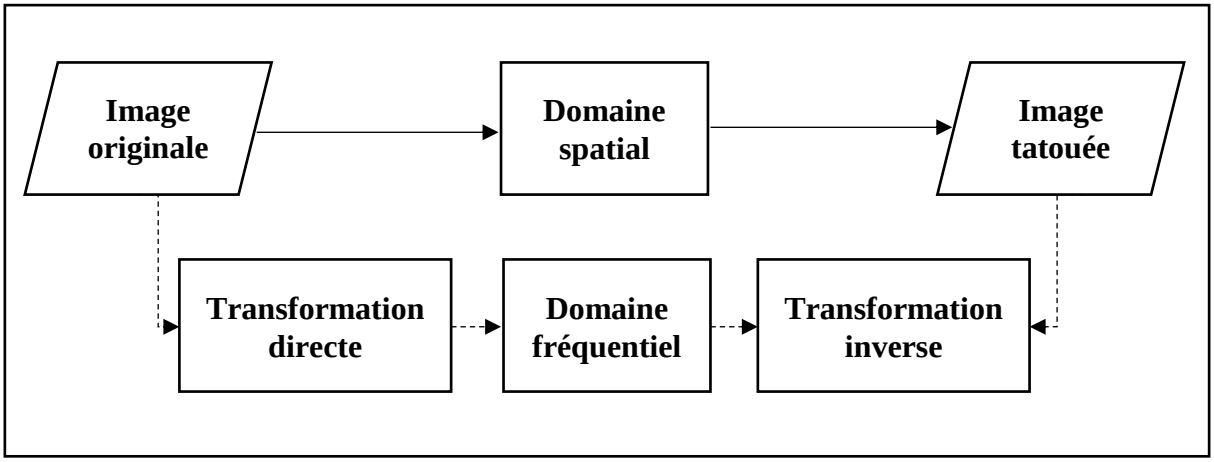


Figure 1.7 Schéma illustrant la différence entre le domaine spatial et le domaine fréquentiel

a. Domaine spatial

Les algorithmes opérant sur le domaine **spatial** ont été les premiers à être utilisé dans le domaine du tatouage numérique en général et du tatouage des images en particulier. En ce qui est le cas des images, le principe de cet algorithme dépend de l'espace colorimétrique de l'image et consiste à insérer la marque en modifient l'intensité lumineuse d'un nombre donné de pixels, dans le cas d'une image niveau de gris, ou on modifiant une ou plusieurs composantes d'un espace colorimétrique quelconque, dans le cas d'image couleurs[9]. Pour plus d'exemples de méthodes de tatouage fonctionnant sur ce domaine on peut ce référer à [10]–[13].

La méthode la plus utilisée dans ce domaine est : les bits les moins significatifs (**LSB** : *Least Significant Bit*)[14]. Il s'agit certainement de la méthode la plus basique du "data embedding". En effet les valeurs des pixels de l'image sont codées sur 8 bits, et chaque pixel d'une image à niveaux de gris peut être représenté par un vecteur binaire $v = (b^0, b^1, b^2, b^3, b^4, b^5, b^6, b^7)$. Ce qui permet de découper l'image en 8 plans comme illustré dans la Figure 1.8. La **marque** est insérée dans le bit le moins significatif c'est à dire le bit $\mathbf{b^7}$ de chaque pixel. La méthode de tatouage du LSB consiste donc à forcer le poids faible de chaque pixel à 0 ou 1, suivant la valeur du bit de la séquence contenue dans le watermark. Cette technique a été présentée initialement par *Tanaka et al* [6].

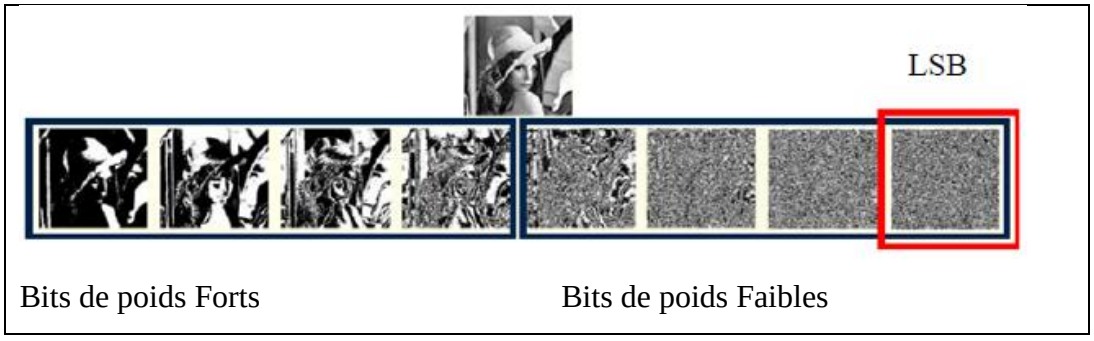


Figure 1.8 Découpage de l'image testé « Lena » en 8 plans

La technique présentée dans [15], consiste à établir une approche statistique nommée Patchwork afin d'optimiser les performances au niveau de la robustesse. Cette approche repose sur la différence de luminance observée entre deux ensembles de pixels, déterminés à l'aide d'une clé

pour insérer la marque. L'extraction de la marque est établie par un calcul de la somme des différences entre les positions des bits donnés par la clé. Cette approche résiste mieux que LSB à certaines altérations de l'image mais, elle n'est toujours pas satisfaisante face à une compression JPEG.

L'avantage principal des techniques du tatouage des images basées sur le domaine spatial est le faible coût, ce qui permet de l'utiliser dans les applications du tatouage en temps réel. Néanmoins, cette technique souffre de plusieurs limitations, dont on cite les principales:

- ***Robustesse :*** cette technique résiste très mal à tout type d'attaques, géométrique ou fréquentiel. Il est très simple d'enlever la marque insérée en mettant par exemple à 0 tous les bits de poids faible. Entre autres la compression JPEG ne laisse à ce schéma quasiment aucune chance. Le simple fait d'appliquer une rotation corrompt la plupart du temps la marque insérée.
- ***Visibilité :*** Contrairement, a ce que l'on peut penser, l'œil humain est très sensible aux contrastes dans les gris de faibles intensités et beaucoup moins dans les teintes proche du blanc. Ainsi, certaines méthodes profitent de cela en adaptant le nombre de bits de poids faible à coder en fonction de la teinte en cours et de la teinte adjacente (tout en se référant à des données physiologiques sur les couleurs).

A cause de cette faible robustesse, les méthodes de tatouage qui se basent sur le domaine spatial sont de moins en moins utilisées. Cet inconvénient a dirigé les chercheurs vers l'utilisation d'un autre domaine plus robuste à différents d'attaques.

b. Domaine fréquentiel

Les algorithmes de tatouage opérant sur le domaine fréquentiel consiste à transformer le signal d'origine appartenant au domaine spatial/temporel vers un autre domaine propose à la transformée utilisée. En d'autres termes, ces algorithmes incluent le *watermark* non pas directement dans l'image, mais dans les coefficients de la transformée de l'image. Ainsi, une transformation inverse est établie afin d'extraire la marque insérée et revenir au domaine d'origine. A cet égard, ces approches seront plus robustes, plus complexes et largement utilisées.

De plus, elles permettent en plus de choisir les régions de l'image qui seront plus résistants à certains types d'attaques. Parmi les transformées les plus utilisées dans les algorithmes du tatouage numérique des images on peut citer : la Transformée en Cosinus Discrète (**DCT**), la Transformée en Ondelettes Discrète (**DWT**), la Transformée de Fourier Discrète (**DFT**), sont les domaines transformées les plus fréquemment exploités pour les applications de tatouage d'image. la Transformée de Hadamard Discrète (**DHT**), la Transformée Ridgelet (**RIT**), la Transformée de Radon (**RAT**), la Transformée en Curvelets (**CUT**), la Transformée en Contourlets (**COT**) et la Transformée Slant (**SLT**)[16]–[24]

- Domaine de la transformée en cosinus discrète (DCT) :

La DCT (Discret Cosinus Transform) est une transformée qui prend un ensemble de points d'un domaine spatial et les transforment en une représentation équivalente dans le domaine fréquentiel sous forme de coefficients DCT. La DCT permet de segmenter l'image en blocs de taille 8*8 et ainsi appliquer la DCT pour chacun des blocs. Ses coefficients sont répartis en basses fréquences (BF), moyennes fréquences (MF), et hautes fréquences (HF) comme illustré dans la figure 1.9. Chaque bande de fréquence représente une information spécifique, telle que les coefficients BFs qui contiennent l'information la plus importante dans l'image, et les coefficients HFs représentent les détails exacts de l'image. La marque est insérée en modifiant les coefficients des bandes MFs de sorte que la visibilité de l'image ne soit pas affectée et que la marque résiste à la compression.

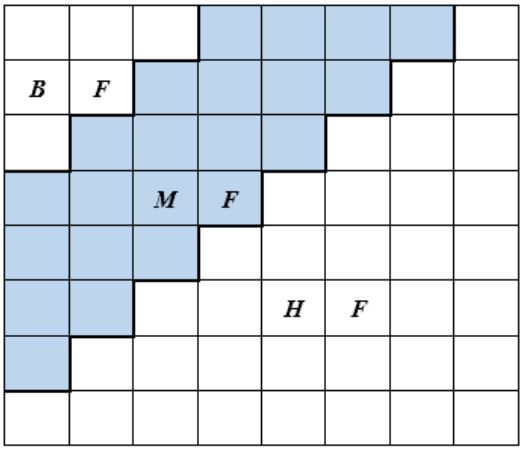


Figure 1.9 Décomposition par la transformée DCT

En effet, la DCT représente une image comme une somme de sinusoïdes de magnitudes et de fréquences variables. La DCT d'une image I de taille N, notée par F_{DCT} , est donnée par :

$$F_{DCT}(u,v) = \frac{2}{N} c(u)c(v) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} I(x,y) . \cos\left[\frac{\pi}{N} u(x+\frac{1}{2})\right] . \cos\left[\frac{\pi}{N} v(y+\frac{1}{2})\right] \qquad (2)$$

Avec

$$c(w) = \begin{cases} 1 \ pour\ w = 1,2,\dots,N-1 \\ 2^{-1/2} \end{cases} \qquad (3)$$

La transformée en cosinus discrète inverse, notée par $F_{DCT}^{-1}(x,y) = I(x,y)$, connue aussi sous IDCT est donnée par :

$$I(x,y) = \frac{2}{N} \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} c(u)c(v).F_{DCT}(u,v).\cos\left[\frac{\pi}{N} u(x+\frac{1}{2})\right] . \cos\left[\frac{\pi}{N} v(y+\frac{1}{2})\right] \qquad (4)$$

De nombreuses méthodes ont été développées dans ce domaine. Parmi les premières approches du tatouage des images basé sur cette transformée, une technique développée par Koch et al.[25]. Ces derniers proposent d'incorporer une marque binaire dans deux coefficients de chaque bloc des moyennes fréquences. Le choix des coefficients se fait d'une manière aléatoire. Par la suite chaque bloc est quantifié en utilisant la matrice de quantification correspondant à la compression JPEG. On constate que cette technique est bien adaptée pour une compression JPEG, mais la marque s'avère facilement détectable. Cox et al.[26] Suggèrent d'effectuer la transformée DCT sur l'image entière en sélectionnant les 1000 coefficients disposant une plus grande amplitude de manière à ce que la marque soit insérée dans une composante de l'image perceptuellement significative. La marque utilisée représente une séquence gaussienne de nombres réels pseudo-aléatoires d'une longueur 1000. Ensuite, cette dernière est incorporée en utilisant une loi normale afin de résister à des attaques de collusion. L'extraction de la marque est établie en soustrayant l'image originale à l'image tatouée.

La DCT permet entre autres de réduire la corrélation spatiale entre les pixels d'une image. Un autre avantage en faveur de l'utilisation de DCT est la possibilité de bénéficier des études psycho visuelles déjà menées en codage de source. En effet, elles se proposent de prendre en compte les phénomènes connus comme la représentation de la couleur, la sensibilité au contraste et les effets de masquage. La propriété essentielle de la DCT est la décroissance rapide de l'amplitude des coefficients lorsque la fréquence augmente, ce qui la rend utile pour la compression d'images. De plus, elle offre une bonne robustesse à des attaques telles que l'ajustement de brillance et de contraste, filtrage, lissage et compression.

- Domaine de la transformée de Fourier discrète (DFT) :

La transformée de Fourier permet de décomposer une image en une série de sinusoïdes à différentes fréquences. Les hautes fréquences contiennent moins d'informations que les basses fréquences qui sont localisées dans le centre de l'image résultante. Cette transformée permet donc de rendre visible les composantes en fréquence de l'image. L'équation ci-dessous donne la décomposition d'une image I_0 de taille en $M * N$ utilisant la transformée de Fourier :

$$F(p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I_0(m,n) e^{-j\left(\frac{2\pi}{M}\right)pm}\ e^{-j\left(\frac{2\pi}{N}\right)qn} \tag{5}$$

Avec j $= \sqrt{-1}, p\ = 1, 2, \ldots, N$ et $2\ q\ = 1, 2, \ldots, N$

$$I_0(m,n) = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} P(p,q) e^{j\left(\frac{2\pi}{M}\right)pm}\ e^{j\left(\frac{2\pi}{N}\right)qn} \tag{6}$$

L'équation peut être représentée aussi sous la forme :

$$F(p,q) = |F(p,q)|\ e^{-j\phi qn} \tag{7}$$

Tel que, la fonction $|F(p,q)|$ représente le spectre de la transformée de Fourier de I_0 tandis que ϕ représente sa phase. La Figure 1.10 représente l'image de test Lena et le spectre de sa transformée de Fourier.

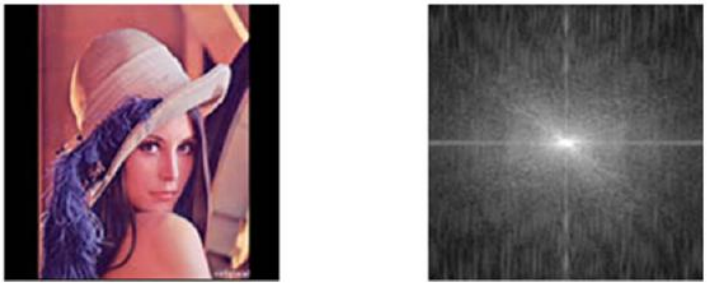


Figure 1.10 Spectre de Fourier de l'image « Lena »

Piva et al.[27] ont présenté une approche de tatouage d'images basée sur la transformée de Fourier discrète (DFT). Malgré sa faible robustesse, elle est intéressante pour la compréhension du tatouage d'image dans le domaine de Fourier. Cette méthode a été améliorée par Solachidis [28]. La marque est générée d'une manière pseudo aléatoire à moyenne nulle. Son incorporation se fait dans les bandes de moyennes fréquences. Un masque psycho visuels est utilisé pour remédier au problème de la difficulté de maîtriser le résultat au niveau local sur l'image finale.

Cette transformation permet de contrôler les fréquences du signal et permet aussi de choisir les zones adéquates à l'incorporation de la marque, de telles sortes à obtenir un bon compromis robustesse-invisibilité. Aussi, le principal avantage de ce domaine est qu'il est robuste à différents attaques géométriques, tels que la translation, rotation, et au changement d'échelle.

- Domaine de la transformée en Ondelette discrète (DWT)

La transformée en ondelettes discrète permet de décomposer une image en sous bandes fréquentielles à l'aide des bancs des filtres par convolution ou avec des algorithmes rapides basés sur le schéma du « lifting scheme ». Les bandes qu'ils en résultent sont classés en une sous-bande basses fréquences LL et trois sous-bandes hautes fréquences : LH, HH et HL, qui correspondent aux orientations spatiales verticales, diagonales et horizontales respectivement, comme illustré dans la figure 1.11. Cette décomposition permet de développer facilement des masques psycho visuels.

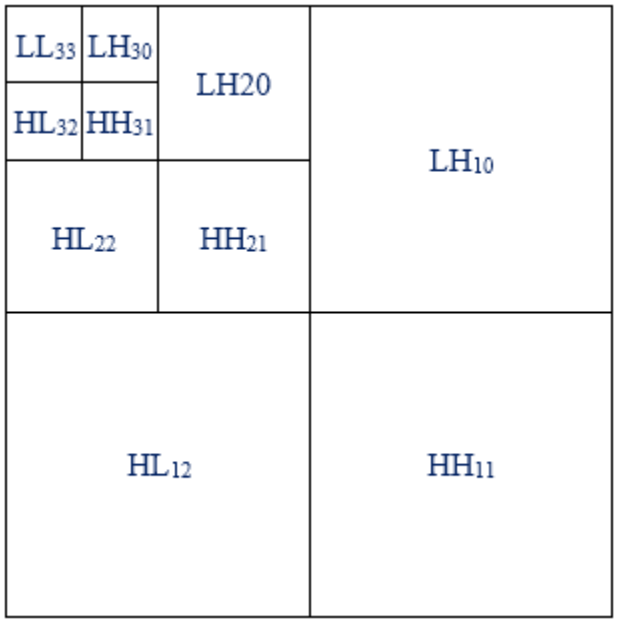


Figure 1.11 Exemple de décomposition d'une image en ondelettes à 3 niveaux.

En plus de la robustesse commune avec la DCT, le tatouage dans le domaine d'ondelettes est robuste face à un changement d'échelle de facteur. De plus, les masques perceptuels sont plus fins et il y a moins d'effets de blocs. Le principal inconvénient de cette transformée est la sensibilité aux transformations géométriques (attaques de désynchronisation).

1.2.4.2 *Robustesse*

- Robuste

Un tatouage robuste envisage la préservation de la marque insérée face aux attaques bienveillantes ou malveillantes afin qu'elle soit, toujours identifiable. Il est évident de souligner qu'il n'existe pas un algorithme de tatouage capable de résister à tous les types d'attaques, et ce quelle que soit leur gravité. Donc, à travers ce facteur, on désigne un sous ensemble d'attaques auxquels résiste l'algorithme concerné. Ce facteur a été abordé en détails dans la section précédente.

- Fragile

Un tatouage fragile est conçu pour être vulnérable à toutes les altérations. Les premières méthodes proposées pour assurer un service d'intégrité étaient basées sur l'utilisation d'un tatouage fragile, par opposition au tatouage robuste classiquement utilisé pour la protection des droits d'auteur. Dans ce cas, la marque est insérée de telle sorte que les moindres changements apportés à l'image se répercutent également sur la marque insérée. Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence de cette marque. Un algorithme de tatouage fragile est plus facile à concevoir qu'un tatouage robuste et est généralement appliqué dans des scénarios d'authentification[29], [30].

- Semi-fragile

Le tatouage semi-fragile combine les propriétés du tatouage robuste et fragile afin détecter les modifications volontaires tout en demeurant robuste face aux attaques involontaires ou de nature légitimes. Ce type de tatouage rend l'algorithme plus robuste face à certaines manipulations autorisées. Leurs applications sont surtout réservées à l'authentification d'images (par exemple les photos d'identité (cartes d'identité, passeport, permis de conduire), les images médicales (scanner, IRM, ...)). En pratique, tous les algorithmes de tatouage robustes sont semi fragile, seulement dans le premier cas, cette propriété n'est pas imposée par le système mais ne peut être négligée.

1.2.4.3 *Techniques d'insertion*

Les techniques d'insertion peuvent être distinguées selon la modulation de tatouage utilisée. On distingue généralement deux types de modulations : additives et substitutives. Nous présentons dans ce qui suit en détails chacune des modulations.

- Additive

Lors de la phase d'insertion, une technique additive consiste principalement à insérer les bits de la marque dans l'image originale ou une transformée de celle-ci. La première étape est la génération de la marque. La seconde étape est la pondération de cette marque par un paramètre α

représentant la force du tatouage (paramètre de robustesse) par la marque w_i , par la suite et comme troisième étape, ajouter la marque résultante à l'image originale. Il est important de noter que l'insertion d'un message de grande taille résulte en une marque particulièrement visible. L'insertion selon la règle additive peut être définie mathématiquement par l'équation suivante :

$$I^* = I + \alpha\, w_i \tag{8}$$

Avec I^* représente l'image tatouée, I l'image originale, et α un facteur représentant la force d'insertion.

- Substitutive

A l'inverse des méthodes additives, une technique d'insertion substitutive consiste à substituer des composantes de l'image originale par d'autres de la marque. Ces composantes peuvent désigner des pixels de l'image, des coefficients issus de blocs de transformées de l'image ou encore des propriétés géométriques de l'image. Les techniques du tatouage substitutif les plus connus sont : la technique de substitution de bits de poids faible « Least Significant Bit » (LSB) et la technique de modulation d'indice de quantification « Quantized Index Modulation » (QIM)[31]–[34]. La technique de LSB consiste à remplacer le bit de poids faible du niveau de gris de chaque pixel de l'image par un bit de la marque à insérer. Cette technique dispose d'une forte capacité d'insertion 1 bit par pixel (bpp) qui résulte en une faible dégradation de l'image originale. Cependant, elle est fragile à toute altération de l'image, i.e. la marque est perdu ou définitivement modifiée si l'image a subi des modifications. La deuxième technique du QIM est une généralisation de la technique précédente (LSB). La QIM se base sur la quantification des composantes de l'image en fonction d'un ensemble de quantificateurs à base de dictionnaires pour insérer la marque. Quant à la détection, il suffit d'identifier à quel dictionnaire appartient la composante tatouée de l'image pour déterminer le message transmis.

1.2.4.4 ***Mode d'extraction***

On distingue trois principaux types de détection d'un schéma de tatouage:

- Schéma non aveugle :

Dans le cas d'une extraction non aveugle ou encore informée, on dispose à la fois de l'image originale, l'image tatouée et la marque insérée. La présence de l'image originale permet de faciliter le procédé d'extraction.

- Schéma aveugle :

Une extraction aveugle ou encore non informée (blind en anglais) consiste à extraire la marque insérée depuis l'image tatouée sans avoir recours à l'image originale.

- Schéma semi-aveugle :

Dans une extraction semi-aveugle, on dispose de l'image tatouée et de la marque sans image originale. On cherche dans ce cas à confirmer la présence de la marque dans l'image tatouée.

1.2.4.5 *Perception*

- Visible:

Pour quelques applications, un tatouage visible peut être envisagé. Dans un tel cas, le procédé d'insertion altère l'image originale. C'est un exemple fréquent pour le cas du logo des sociétés dans les programmes télévisuels et aussi le cas des agences de photos qui incorporent une marque visible sous forme de copyright. En effet, ce type de tatouage constitue un sujet de controverse, vu qu'un ensemble de chercheurs estiment que si la marque est visible, alors elle est facilement attaquée. En pratique, l'intérêt d'un *watermark* efficace réside dans son invisibilité. Dans cette catégorie, on distingue les travaux récents : [35]–[38]

- invisible :

Dans cette catégorie de tatouage invisible, l'image tatouée est très similaire à l'image originale et il est presque impossible de faire la distinction entre elles. Aussi, il est difficile d'enlever ou de détruire le *watermark* en plus de la préservation de la qualité visuelle de l'image

originale. Il convient de souligner que ce concept est très complexe vu que la modification de l'image originale doit se faire de la manière la plus fidèle possible et d'une manière transparente pour l'utilisateur. A titre d'exemple, l'agence de photos dispose d'un *watermark* invisible utile pour la détection d'une éventuelle source de vol ainsi qu'éviter son utilisation de manière non autorisée.

1.2.4.6 *Type de support*

Un algorithme de tatouage numérique dépend aussi du type de support de l'application envisagée : image, vidéo, audio, texte, etc. Le tatouage des images est le document envisagé dans le présent rapport, qui consiste à incorporer le *watermark* dans une image. Un support de type vidéo est une extension du type précédent[39]–[44]. Tandis qu'un tatouage du texte consiste à insérer le *watermark* dans un PDF, DOC et d'autres fichier texte dans la forme de la police, l'espace entre les caractères et les interlignes[45]–[47]. Quant au tatouage audio c'est un sujet d'actualité en raison de la musique disponible sur internet et MP3[1], [24], [48], [49].

1.2.5 Evaluation des algorithmes du tatouage

1.2.5.1 *Attaques*

Un des points forts d'un système de tatouage réside dans sa robustesse. Un tatouage robuste se caractérise par la capacité du *watermark* à résister à différentes attaques. Ces attaques tiennent une place très intéressante dans le cahier des charges d'un système de tatouage puisqu'elles déterminent la robustesse d'un système. En effet, une attaque peut effacer le *watermark* ou du moins les altérer. Cependant, plusieurs algorithmes ont été développés pour valider ce cahier de charges et répondre à une ou à un ensemble d'attaques. Cela signifie qu'il est impossible de développer un algorithme général pour l'ensemble des attaques. Dans cette section, nous présentons une liste non exhaustive des attaques les plus courantes que peut subir une image. Dans la littérature, plusieurs classifications ont été proposées concernant les attaques du tatouage numérique [5] [50], [51]. On propose de regrouper ces attaques en deux grandes familles : attaques géométriques et attaques d'effacement.

a. Attaques d'effacement

Ce sont des attaques liées à l'image (ou au signal du watermark), elles ne sont pas forcément volontaires. En effet, sans le savoir, l'image peut être dégradée suffisamment pour que le tatouage soit effacé. Un algorithme de tatouage robuste est sensé résister de manière efficace à ce type de transformations, ou du moins tant que l'image reste utilisable. Nous citons:

- *Attaques par Compression JPEG*

La compression avec perte a pour but de simplifier le codage du document, en supprimant l'information peu significative. Plus on compresse l'image tatouée, plus on va supprimer une gamme de fréquences importante, plus l'image tatouée va être dégradée. En effet, les algorithmes dans le domaine spatial souffrent de ce genre d'attaques e dans le but d'augmenter la robustesse face à la compression, une solution parmi d'autres consiste à concevoir des algorithmes de tatouage adaptés au contenue des images dans le domaine fréquentiel.

- *Attaques par filtrage*

Le filtrage correspond à l'augmentation (resp. la diminution) des composantes hautes fréquences. En effet, L'ajout d'un bruit gaussien ou un filtre moyen permet de désynchroniser la phase de l'insertion et la détection. Un exemple simple, si le marquage est effectué en modifiant la luminance de certains pixels. Il suffit alors d'effectuer un filtre.

- *transformations volumétriques :*

Le principe de ce type d'attaques est de changer la luminance de l'image par une fonction non-linéaire afin d'améliorer l'image. En effet, ce changement de luminance améliore l'image mais, en revanche il désynchronise l'image tatouée. On distingue dans ce type d'attaques l'étalement d'histogramme, égalisation d'histogramme, transformation Gamma, etc.

- Bruitage

Ce type d'attaques consiste à altérer l'image tatouée de manière à ce que toute

l'information importante de l'image ne soit pas facilement accessible. Or, la marque insérée dans l'image correspond généralement à du bruit, il est par conséquent naturel que l'attaquant utilise une technique de débruitage pour estimer la marque (les filtres de Hanning, Butterworth, Metz et Wiener en sont des exemples).

Des exemples de bruits peuvent être de type :

- bruit « Poivre et Sel » qui consiste à transformer l'image en pixels noirs ou blancs.
- bruit Gaussien consiste en l'ajout successif de valeurs aléatoires à chaque pixel de l'image.
- bruit Poisson.
- Bruit Speckle.

b. Attaques géométriques

- *Recadrement :*

Le recadrage est un processus qui consiste à supprimer certains pixels d'une image numérique. Il s'agit d'une attaque très courante puisque, dans de nombreux cas, l'attaquant est intéressé par une petite partie de l'image tatouée seulement. Dans cette optique, pour survivre, le *watermark* doit être réparti sur l'image en entier. Ce type d'attaques concerne surtout la mise en page de diverses images scannées. Cela peut correspondre à une simple rotation de quelque degré, ou bien un découpage brutal d'une partie de l'image.

- *Rotation :*

Dans ce type d'attaques, l'image est pivotée par un angle d'un certain degré. Des petites angles de rotation, n'ont pas l'habitude de changer la valeur commerciale de l'image, mais peuvent rendre le *watermark* non détectable.

1.2.5.2 *Mesures de distorsions*

La performance d'un système de tatouage est évaluée généralement en fonction de son imperceptibilité et sa robustesse face aux attaques. Le rapport signal-bruit de pointe (PSNR), l'indice de similarité structurelle (SSIM), la corrélation normalisée (NC) et le taux d'erreur binaire (BER) sont les plus utilisés. Plus le PSNR, la NC, le SSIM et le BER sont élevés, plus l'algorithme du tatouage est performant. Ces indicateurs sont décrits comme suit :

- **Erreur quadratique moyenne (MSE)**

Le MSE (*Mean square error*) représente l'erreur quadratique moyenne entre l'image tatouée et celle originale. Afin de permettre d'évaluer l'influence de la marque sur l'image cette mesure évalue l'influence de la marque sur l'image. Il est définit comme suit :

$$\mathrm{MSE} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(\frac{(I_w(i,j) - I(i,j))^2}{MxN} \right) \tag{9}$$

Tel que $I(i,j)$ est l'intensité de l'image originale de taille MxN.

$I_w(i,j)$ Est l'intensité de l'image tatouée.

- **Rapport signal à bruit (PSNR)**

La mesure de distorsion la plus utilisée en traitement d'images est le rapport signal à bruit (PSNR, *Peak Signal to Noise Ratio*), il exprime le rapport entre la puissance maximale d'un signal et la puissance du bruit de corruption affectant la fidélité de la représentation. Ce dernier permet de déterminer l'imperceptibilité de la signature. En d'autres termes, il permet d'évaluer la dégradation en dB de l'image originale provoquée par l'insertion de la marque, et éventuellement par d'autres attaques, qui est défini comme suit :

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{MSE} \tag{10}$$

Dans le domaine du traitement du signal, lorsque le PSNR est élevé, la distorsion devient moins importante. On estime qu'un bon PSNR se situe au-dessus de 35dB. Par exemple, le tatouage proposé dans le présent rapport permet d'obtenir un PSNR d'environ 48dB.

- **Corrélation normalisée (NC)**

La corrélation normale (NC), entre la marque extraite et l'originale, est aussi utilisée pour évaluer la qualité de l'extraction de la marque cachée. Cette corrélation est calculée par la formule (1.13) suivante :

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)xW'(i,j)}{\left(\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)\text{^}2}\right)\left(\sqrt{\sum_{i=}^{M}\sum_{j=1}^{N} W'(i,j)\text{^}2}\right)} \quad (11)$$

Cette valeur est comprise entre 0 et 1. La valeur idéale est 1.

- **Indice de similarité structurelle (SSIM)**

Le SSIM évalue la similarité structurelle entre l'image originale et l'image tatouée en considérant trois paramètres : la luminance, le contraste et la structure [52]. La valeur de cette mesure doit être proche de l'unité. Mathématiquement, elle s'énonce comme suit

$$SSIM(I, I_w) = l(I, I_w)c(I, I_w)s(I, I_w) \quad (12)$$

Tel que I_w et I réprésentent l'image tatouée et l'image originale respectivement.

- **Le taux d'erreur binaire (BER)**

Le BER (*Bit Error Rate*) c'est un indicateur qui permet d'évaluer la qualité du *watermark* extrait. Il est défini comme étant un rapport entre le nombre de bits extraits incorrectement e le nombre total de bits transmis. Ce paramètre est adapté à une *watermark* de séquence binaire aléatoire. Idéalement, la valeur de BER devrait être égale à 0. Il est définit comme suit :

$$\mathrm{BER} = \left(\sum_{i=1}^{N_w} \sum_{j=0}^{N_w} \mathrm{XOR}(w(i,j), w'(i,j)) \right) / N_w^2 \qquad (13)$$

Les valeurs prises par cet indicateur appartiennent au domaine [0-1]. Il est évident que plus le BER est faible plus l'algorithme du tatouage est robuste.

1.2.6 Applications du tatouage numérique

Les applications du tatouage numérique sont nombreuses, elles permettent de distinguer différents usages selon l'application envisagée et l'information à insérer. Parmi celle-ci on peut citer :

1.2.6.1 *Protection des droits d'auteur*

Une des premières applications étudiée en tatouage d'image est la protection de la propriété intellectuelle (ou droit d'auteur, qui se distingue sensiblement du *copyright* anglo-saxon). Ce service reste cependant toujours d'actualité et concerne encore la majorité des publications. L'objectif est d'offrir, en cas de besoin, la possibilité à l'auteur ou au propriétaire d'une image d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce même si l'image concernée a subi des dégradations par rapport à la version originale. La mise en place d'un tel service doit respecter les trois contraintes suivantes :

- **Préserver la qualité de l'image :** minimiser la distorsion liée à l'insertion de la marque sur l'image, de manière à ce que la qualité visuelle de l'image tatouée soit quasi identique à l'originale. Malheureusement cette notion d'invisibilité est très subjective et difficile à modéliser. D'autant plus qu'elle dépend de nombreux facteurs, tels que : la nature de l'image à tatouer (peinture, image médicale, photo satellite, etc.), la qualité du document original (plus une image est de bonne qualité, plus il est difficile de garantir l'invisibilité de la marque) et des conditions de visualisation (problème bien connu en codage de source avec pertes).
- **Garantir la non-ambiguïté de la preuve :** le tatouage doit constituer une preuve solide. permettant d'assurer l'unicité (éviter les problèmes de collision) et de

l'authenticité de l'identifiant, mais également de dater le dépôt (au cas où l'image aurait été tatouée plusieurs fois avec des marques différentes).

- Assurer la robustesse des éléments de preuve (tatouage) : l'algorithme utilisé doit être capable d'extraire correctement la marque insérée, même si l'image subit des modifications.

1.2.6.2 *Vérification de l'intégrité du contenu d'une image*

L'idée de base consiste à utiliser les techniques de tatouage d'image afin de cacher dans certaines zones de l'image des informations sur d'autres zones. Ces informations servent à alerter l'utilisateur face à une éventuelle modification ou découpe de l'image par une personne non autorisée et à localiser précisément les régions manipulées, voire éventuellement à les restaurer.

1.2.6.3 *Gestion du nombre de copies d'une image :*

Contrairement aux données de nature analogique pour lesquelles une succession de reproductions entraîne rapidement une perte significative de la qualité, les données numériques peuvent être dupliquées quasiment à l'infini. Dans ce contexte, une personne ayant accès à ce type de données et au matériel adéquat, est potentiellement capable de les reproduire bit à bit à l'identique. Il est évident que cette personne, si elle est malintentionnée, peut ensuite redistribuer d'une manière illégale des copies avec une qualité égale au document d'origine. Face à cette nouvelle situation, d'où l'intérêt d'utiliser des techniques de tatouage afin de limiter l'ampleur de ce phénomène et indiquer que le contenu ne peut pas être répliqué illégalement.

1.2.6.4 *Non répudiation d'accès et suivi de copies*

Cette application constitue une bonne illustration de la complémentarité entre les techniques de cryptographie et le tatouage d'image. Soit une image diffusée sous forme chiffrée, empêchant qu'un utilisateur puisse avoir accès à son contenu lors de la transmission de celle-ci. Au niveau du destinataire, on procède simultanément au décryptage et au tatouage de l'image de façon à ce que l'utilisateur remet illégalement en circulation cette image, il sera alors possible de remonter à l'origine du délit grâce à l'identifiant du destinataire (ou « fingerprint ») caché dans

l'image. Ce type d'application ne va pas sans poser de sérieux problème en matière de sécurité, du fait qu'il existe plusieurs copies d'une même image contenant des tatouages différents.

1.2.6.5 *Contrôle d'accès*

L'objectif est d'ôter tout intérêt commercial à l'image en y superposant un tatouage (voir Seules les personnes ayant les droits d'accès sont en mesure d'inverser le processus de marquage de manière à reconstituer l'image originale. L'avantage de cette méthode par rapport à un système de cryptage classique où l'image est totalement inintelligible, réside dans le fait que le tatouage peut être porteur d'informations relatives à l'image. On peut, par exemple, y faire figurer l'adresse où commander l'image en clair, le nom de la société, etc.

1.2.6.6 *Applications médicales*

Ce service est très complexe vu la sensibilité de l'image médicale et du contenu qu'elle contient. Pour de plus amples détails, voir section suivante.

1.2.6.7 *Autres services*

Bien évidemment il existe d'autres applications possibles en dehors de celles décrites précédemment, et dans des domaines autres que des services de sécurité. On peut imaginer utiliser une technique de tatouage d'image pour faciliter la recherche dans une base de données multimédia en cachant par exemple dans le document des informations textuelles sur son contenu. Le tatouage d'image trouverait également sa place dans un système de montage vidéo où il pourrait servir par exemple à étiqueter les différentes séquences. Un des avantages de cette technique par rapport à des méthodes traditionnelles, est qu'elle offre la possibilité de retrouver facilement l'origine d'un extrait à partir d'un enregistrement quelconque. D'une manière générale, le principal avantage du tatouage d'image par rapport à d'autres formes de marquage, réside dans son indépendance vis-à-vis du support de l'image et des manipulations éventuelles.

1.3 Tatouage des images médicales

Après avoir introduit, dans la première section, les généralités du tatouage des images numériques, nous allons élaborer, dans cette section, plus particulièrement du tatouage des images médicales, ainsi qu'un état de l'art sur les différentes méthodes existantes dans la littérature et leurs limitations.

1.3.1 Imagerie médicale

L'imagerie médicale joue un rôle important et vital dans l'aide au diagnostic et la prise des décisions. A ce propos, une grande variété de technologie s'est développée depuis le début du 20ème siècle grâce aux découvertes de la physique moderne. Dans ce sens, nous distinguons plusieurs types d'images.

1.3.1.1 *La radiographie*

La radiographie est la forme la plus ancienne des images médicales. Elle utilise les rayons X comme ondes électromagnétiques. Ces derniers sont très puissants et peuvent traverser les tissus en fonction de leur densité. Pratiquement, l'objet est placé entre une source de rayon X et un récepteur sensible à ces rayons notamment le cliché. Généralement, ce type d'image est très utile lorsque les objets à photographier sont cachés comme le cas des os dans un corps.

1.3.1.2 *Le scanner*

Le scanner est de la radiographie améliorée. Il utilise une source de rayons X et d'un détecteur de part et d'autre du corps étudié. De même, grâce à la rotation simultanée de la source émettrice et du détecteur autour du corps, l'information collectée peut générer une représentation 3D du corps étudié après les traitements appropriés.

1.3.1.3 *La scintigraphie mono-photonique*

La photographie par la scintigraphie mono-photonique se base sur un traceur radio actif injecté dans le tissu à étudier et une caméra sensible au rayon gamma comme récepteur. La

source émet alors des rayons gamma dans toutes les directions de l'intérieur de la région à photographier tandis que la caméra capte les rayons utiles pour former la photo.

1.3.1.4 *La tomographie*

La tomographie par émission de positons (TEP) utilise un traceur marqué par des atomes radioactifs qui émettent des positons (le Fluor 18 ou le Carbone 11). Le traceur s'associe à sa cible biologique par l'interaction des positons avec les électrons environnant en émettant deux photons dans des directions diamétralement opposées. Les détecteurs sont placées autour du corps cible permet de capter les photons de part et d'autre de la région pointée. Le traitement convenable des données captées conduira à la reconstitution des images 3D de la zone étudiée.

1.3.1.5 *L'échographie ultrasonore*

Comme son nom l'indique, cette technologie utilise les ondes ultrasons. De ce fait, le système se compose d'un écran de visualisation et de la sonde émettrice et réceptrice des ondes ultrasonores appelée transducteur. Pratiquement, les ondes émises traversent les tissus visés et font écho selon la densité et la nature du tissu. Les ondes réfléchies sont alors collectées par le transducteur. Les données collectés subissent le traitement convenable afin de les afficher à l'écran de visualisation ou destinés à d'autre sorties. Tous les appareils actuels d'échographie sont dotés de mémoire numérique pour stocker les images. Elles peuvent être ainsi partagées, transmises à travers le net ou subir des traitements supplémentaires.

1.3.1.6 *La magnétoencéphalographie*

La magnétoencéphalographie est une technologie d'imagerie « passive » du cerveau, tout comme l'électroencéphalographie, car elle repose sur la captation du champ magnétique résultant de l'activité du cerveau. La circulation de l'influx nerveux le long des neurones équivaut à la circulation d'un signal électrique le long d'un fil conducteur, ici les axones. Un courant électrique induit un champ magnétique perpendiculaire au sens de sa circulation. C'est ce très faible champ magnétique, plus d'un million de fois plus faible que le champ magnétique terrestre, qui va être mesuré grâce à des capteurs appelés SQUID (Superconducting QUantum Interference Device).

Appliquant le principe inverse, un champ magnétique induit un courant dans une bobine, ce courant est ensuite analysé pour visualiser les zones d'activité du cerveau.

1.3.1.7 *L'imagerie par résonance magnétique*

L'imagerie par résonance magnétique repose sur les propriétés magnétiques des molécules d'eau qui composent à plus de 80% le corps humain. Les molécules d'eau, plus précisément ses atomes d'hydrogène, possèdent un "moment magnétique", ou spin, qui agit comme un aimant. L'appareil IRM consiste à créer un champ magnétique puissant (B0) grâce à une bobine. Le patient est placé au centre de ce champ magnétique, et toutes les molécules d'eau présentes dans le corps vont s'orienter suivant B0. Une antenne placée sur la partie du corps étudiée (ici la tête) va permettre d'émettre et de réceptionner certaines fréquences. A l'émission, la fréquence induite va faire basculer les molécules dans un plan perpendiculaire à B0. Lorsque l'antenne arrête d'émettre, les molécules reviennent à leur position d'origine en émettant à leur tour une fréquence captée par l'antenne. Celle-ci est ensuite traitée comme un signal électrique et analysée par des logiciels. Le signal diffère selon que les tissus observés contiennent plus ou moins d'eau.

1.3.1.8 *L'IRM de diffusion*

L'IRM ou MRI de diffusion repose sur les principes de base de l'IRM tout en se focalisant sur le déplacement des molécules d'eau présentes à l'intérieur des fibres nerveuses (ou axones). Ces fibres sont gainées de myéline, principalement constituée de lipide, qui va, en partie, retenir les molécules d'eau à l'intérieur de l'axone. C'est pourquoi, dans un temps donné, les molécules d'eau, qui bougent de manière aléatoire, vont parcourir une plus grande distance lorsque leur déplacement se fera dans le sens de la fibre. L'analyse IRM va ensuite permettre de visualiser le parcours de chacune des molécules et ainsi de reconstituer le réseau de fibres nerveuses à l'intérieur du cerveau.

1.3.1.9 *L'IRM fonctionnelle*

L'IRM fonctionnelle permet de visualiser les zones du cerveau activées par un stimulus présenté ou appliqué au sujet. Par exemple, lorsque l'on demande à la personne de regarder une image, les zones activées dans le cerveau vont recevoir un apport d'oxygène par voie sanguine plus important qu'en l'absence du stimulus. Les échanges d'oxygène entre le sang et les neurones modifient le signal IRM. Cette différence de signal IRM entre les états de repos et de stimulation est analysée par informatique. Les images IRM dont le signal est rehaussé correspondent à la zone du cerveau impliquée dans la réponse au stimulus.

1.3.2 Médecine à distance: usages, bénéfices et limites

Le développement des TIC dans le domaine médical s'est accompagné de bouleversements importants avec la crise actuelle liée au COVID-19. Cette crise nous a montré l'importance d'investir dans le secteur de l'e-santé comme étant un ensemble de moyens permettant d'améliorer l'accès aux soins, la qualité des prises en charge ainsi que l'autonomie des patients. Afin d'éviter toute confusion, la figure 1.12 ci-dessous regroupe les différents termes utilisés dans le domaine de la santé connectée. On distingue, l'**e-santé** (*e-Health*) ce terme est défini pour signifier le déploiement des TIC dans la santé, la **télésanté** (télématique de santé) qui est définie par l'utilisation des outils de production, de transmission, de gestion et de partage d'informations numérisées au bénéfice des pratiques tant médicales que médico-sociales. On parle aussi de la **m-santé** (santé mobile) qui signifie l'utilisation des communications mobiles émergentes en santé publique, et de la **Télémédecine** qui représente une forme de pratique médicale à distance. Récemment, un grand nombre de portails électroniques sont publiés sur le web offrant des services de partage de l'image médicale. Ces services, bien qu'ils soient encore limités comparés aux services conventionnels, prévoit un usage élargie dans l'avenir proche. La récente pandémie en est témoins. Cependant, le flux d'information médicale sous forme d'image ou de vidéo s'accroitra de plus en plus, et sans doute il deviendra l'élément fondamental dans la prise de décision. A cet égard, l'un des problèmes à résoudre d'une telle propagation serait le problème de sécurité et d'authenticité des médias partagés. D'une part, le partage de ces documents va les mettre entre les mains d'un large public dont on ne connait pas nécessairement

leurs intentions. D'autre part, il serait très difficile à différentier les faux des vrais documents surtout avec les outils numériques de manipulation des ressources. Ceci ouvre un large domaine d'exploration et de développement devant la recherche, il parait qu'il est à la charge de la communauté scientifique de planifier un usage sûr et sécurisé de toute la documentation médicale en particulier l'image ou la vidéo.

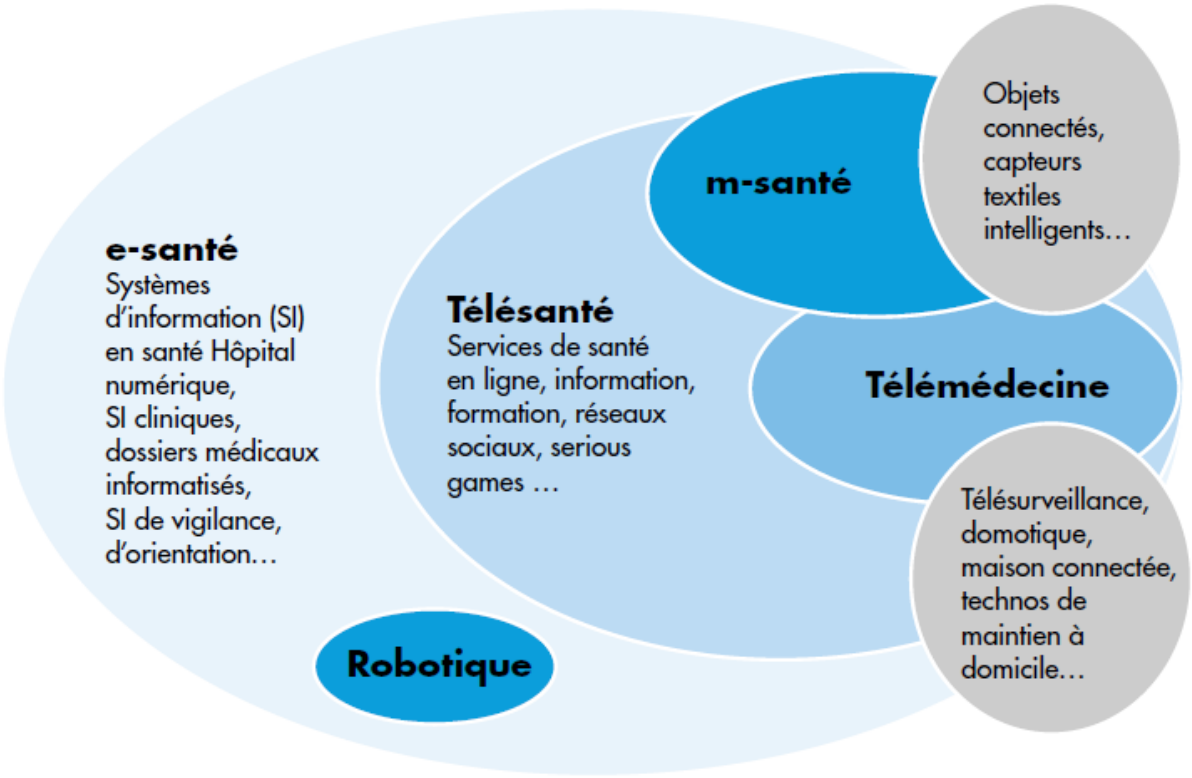


Figure 1.12 Illustration des termes relevant de la santé connectée : e-santé, télésanté, la santé mobile (m-santé), Télémédecine

Les bénéfices apportés par l'utilisation de la médecine à distance sont nombreuse, on cite plus particulièrement qu'elle pourrait aider à améliorer les systèmes de santés, à faciliter l'accès aux soins dans les déserts médicaux, à libérer du temps aux professionnels de santé et même, à faciliter la consultation de bases de données et la communication entre professionnels de santé et à assurer un suivi médical permanent. En effet, durant la crise du covid-19, les patients ne pouvaient pas se déplacer. Cependant, la téléconsultation ou consultations à distance (C.à.d. les patients peuvent consulter leurs médecins traitants sans contrainte de lieux de disponibilité), a

connu une forte demande et beaucoup de médecins affirment qu'avec la télémédecine ils ont pu facilement entrer en contact avec le patient et améliorer sa qualité de vie même en l'absence d'un contact physique. En réalité, ces services sont souvent concentrés dans les grandes métropoles tandis que les zones rurales ou même les petits patelins restent privés de services médicaux de qualité. A cet égard, le développement de télémédecine ne serait en aucun cas du prestige mais plutôt le seul moyen pour une couverture médicale équitable à toute la société. Naturellement, la télémédecine ne se substitue pas à la consultation en présentielle. Elle serait plutôt son compagnon pour procurer aux citoyens de meilleurs services médicaux et éviter toutes sortes discrimination.

Les usages naissants de l'e-santé ont déjà fait apparaître de sincères menaces quant à la diffusion de l'information médicale. En effet, le déploiement d'une telle technologie doit être fondé sur une stratégie partagée par différents acteur afin de soutenir les principes fondamentaux attachés à ce déploiement, notamment les impératifs éthiques d'informations médicales, du respect de la confidentialité du patient et de son consentement au partage de ses données personnelles. De ce fait, la protection de l'information médicale dérive des règles législatives et des éthiques strictes selon le pays. Le cas des règlements directifs comme HIPAA CE 95/46 des Etats-Unis et de l'Europe sont l'expression d'une telle contrainte qui classe les données de santé parmi les données les plus sensibles. Ces règlements visent à sécuriser les dossiers d'informations médicales se présentant sous la forme d'un dossier électronique du patient (EPR - Electronic Patient Records). L'importance de la sécurité des images médicales est due aux graves conséquences que peuvent causer les altérations et les attaques bienveillantes ou malveillants, à savoir les diagnostics erronés, possibilité de tremper les agences d'assurances médicales, l'invalidité des données informatisées dans la médico-légale etc. Par ailleurs, Mettre à jour les lois de cette pratique n'est pas suffisant pour ne pas bloquer l'innovation et le progrès dans ce domaine. En d'autres termes Il ne faut pas tomber dans le piège de vouloir réglementer la technologie. Il faut plutôt faire attention aux différentes utilisations des données médicales et donc penser à assurer un environnement de confiance afin d'ancrer durablement ces pratiques médicales.

1.3.3 Sécurité des images médicales

La sécurité des images médicales est d'une grande importance et sa juste valeur ne peut être valorisée que par les dégâts intolérables que peut causer son usage illicite permettant ainsi un diagnostic erroné. D'après Coatrieux[53], cette sécurité dépend de trois principes fondamentaux : fiabilité, confidentialité et disponibilité (Figure 1.13 ci-dessous) :

- La fiabilité : est composée en deux caractéristiques :
  - **L'intégrité :** garantie que les images transmises n'ont pas été altérées par erreur ou frauduleusement par des personnes non autorisées.
  - **L'authenticité :** garantie que l'image médicale a été émise par des utilisateurs autorisés et appartient au bon patient.
- La confidentialité : garantie que seuls les utilisateurs autorisés peuvent accéder aux informations médicales transmises par les réseaux ou stockées pour l'archivage.

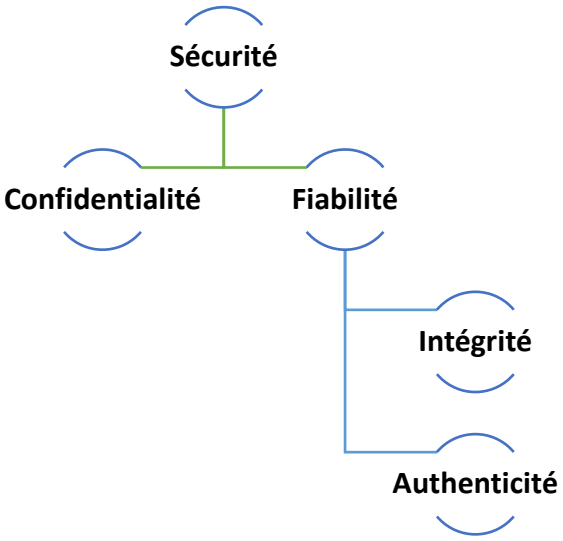


Figure 1.13 Caractéristiques de sécurité d'un système d'information médical

1.3.4 Classification des méthodes de tatouage d'images médicales

En plus des différentes classifications présentés dans la section précédente, nous distinguons trois grandes catégories de tatouage des images médicales : les méthodes ROI

(Region of Interest) et RONI (Region of Non Interest), réversibles et les méthodes classiques[5], [53].

1.3.4.1 *Méthodes ROI et RONI*

Cette catégorie permet de séparer l'image en deux régions : ROI et RONI[54]–[56]. La ROI est une partie de l'image médicale contenant des informations cruciales et importantes pour le diagnostic, qui est généralement définit par un médecin. Tandis que la RONI est le reste de l'image. Le tatouage basé l'insertion du *watermark* dans la ROI cause une grande limitation au niveau de la capacité d'insertion et nécessite l'accord du médecin pour éviter les erreurs de diagnostic d'une part. D'une autre part, le tatouage basé sur l'insertion du *watermark* dans la RONI assure que l'information du diagnostic ne soit pas modifiée et donc une bonne invisibilité de la marque ; cependant cela peut entrainer un effet de bruit à la RONI et ce qui peut gêner le médecin.

1.3.4.2 *Méthodes réversibles*

La seconde catégorie regroupe des méthodes qui permettent d'insérer le *watermark* de manière invisible et réversible, ce qui signifie que la version originale de l'image médicale est complètement restaurée[29], [44], [44], [48], [57]–[61].

1.3.4.3 *Méthodes classiques*

La troisième catégorie consiste à utiliser des méthodes de tatouage classiques permettant de minimiser la distorsion de l'image médicale[17], [18], [31].

1.3.5 Méthodes existantes de tatouage d'images médicales

Durant les deux dernières décennies, la communauté des chercheurs a montré un grand intérêt pour les techniques de tatouage numérique dans les applications médicales. A cet égard, de nombreux travaux ont présenté différentes méthodes pour tatouer les images médicales. Par la suite, nous illustrons brièvement ces techniques.

Thanki et al. [62], ont suggéré une technique de tatouage d'image médicale basée sur la transformation de courbe discrète rapide (FDCuT) et la DCT. Tout d'abord, les coefficients de courbes hautes fréquences sont sélectionnés. Ensuite, le bloc DCT est appliqué dessus et des coefficients de fréquence moyenne sont choisis pour l'insertion du *watermark* à l'aide du bruit blanc gaussien. Cette méthode permet une récupération aveugle des images médicales. La limitation de ce schéma est que du bruit est toujours présent dans l'image médicale tatouée extraite, ce qui peut conduire à un diagnostic erroné.

Parah et al.[57], [58] ont proposé une approche de masquage de données réversible pour un système de e-santé à haute capacité d'intégration. Dans ce schéma, la technique de conversion de pixel en bloc est appliquée d'abord à l'image originale. Ensuite, l'image tatouée est obtenue en incorporant un dossier électronique du patient (EPR) (Electronic Patients Record), un *watermark* fragile et un Block Checksum en utilisant la technique intermédiaire de substitution de bits significatifs. Le schéma signalé est capable de faciliter la détection et la localisation des falsifications contre diverses attaques. En utilisant cette méthode, une bonne invisibilité a été obtenue au prix d'une charge utile réduite. Une autre technique a été proposée par les mêmes auteurs dans le même contexte. Le nouvel algorithme consiste à diviser d'abord l'image de couverture en blocs ne se chevauchant pas, puis l'EPR est intégré dans les pixels non amorces de chaque bloc pour faciliter la réversibilité.

Ramly et al. [63] ont mené une étude utilisant des techniques de machine à vecteur de support (SVM) et de spectre étalé (SS) pour l'algorithme de tatouage d'images médicales. Dans cette étude, le SVM est utilisé pour classer les régions d'intérêt (ROI) et les régions de non-intérêt (RONI) de l'image médicale hôte, tandis que SS est appliqué dans les processus d'intégration/extraction dans/à partir des pixels de l'image d'origine situés dans la partie RONI. Cette partie est transformée par DCT et le watermark, qui contient les informations médicales du patient, est utilisé pour l'intégration sur les coefficients DCT souhaités. De plus, la robustesse de ce schéma n'a été réalisée contre aucun type d'attaque.

Rai et al. [64] ont conçu un système de *watermark* hybride pour une sécurité améliorée des images médicales à l'aide de SVM. Les données intégrées sont initialement brouillées à l'aide

d'une clé unique. L'image hôte est classée en zones ROI/RONI à l'aide de SVM. La partie RONI, qui est sélectionnée pour incorporer les données brouillées, est transformée à l'aide de DWT, puis les coefficients sélectionnés sont soumis à SVD. Ce travail assure la robustesse contre diverses attaques et permet d'obtenir une bonne imperceptibilité. Cet article propose un algorithme de tatouage qui est très robuste aux modifications et préserve également la qualité de l'image avec une bonne capacité d'intégration. Cependant, la complexité de calcul de ce schéma doit être améliorée.

Shehab et al. [30] ont suggéré une approche de tatouage fragile basée sur SVD et la transformée d'Arnold pour sécuriser la transmission d'images médicales. L'image originale est d'abord décomposée en blocs et le LSB de ces blocs est établi à zéro. Après SVD est appliquée pour chaque bloc afin de faciliter la détection des zones attaquées de l'image tatouée. Le *watermark* est intégré dans deux LSB de chaque bloc sélectionné de l'image de couverture. La transformation d'Arnold est utilisée pour trouver l'emplacement d'intégration approprié et, par conséquent, fournir un moyen plus fiable et sécurisé pour masquer les informations d'image. Les expériences montrent que ce schéma est efficace contre plusieurs attaques : attaque par copie/coller, ajout de texte, suppression de contenu et attaques VQ.

Rahman et al. [29] ont proposé une méthode de tatouage réversible et aveugle pour les images médicales. Dans ce schéma, une clé chaotique est utilisée pour déterminer l'emplacement des pixels, à partir de l'image hôte d'origine, devant être tatoués par un *watermark* généré de manière chaotique. Le *Residue Number System* (RNS) est utilisé pour transformer le reste des pixels en résidus. Un polynôme est utilisé pour représenter les pixels sélectionnés de manière chaotique et un polynôme primitif de degré quatre est utilisé pour diviser ces pixels et obtenir le reste qui est ajouté au message de tatouage. Cette technique atteint un haut niveau d'imperceptibilité mais la capacité d'enfouissement et la robustesse contre les attaques n'ont pas été mesurées. De plus, cette méthode ne prend pas en charge la stratégie de tatouage médical basée sur le ROI.

Chauhan et al.[65] ont proposé une technique sécurisée de tatouage d'images médicales utilisant le concept d'étalement du spectre dans le domaine de la transformée en ondelettes. Tout d'abord, l'image de couverture est décomposée en quatre sous-bandes de fréquences en utilisant la

transformée en ondelettes discrète (DWT) et le chapeau mexicain comme ondelette mère. Un *watermark* binaire 50×9 est intégré dans la sous-bande horizontale (HL) et verticale (LH). Ce *watermark* est extrait à l'aide d'un profil statistique de coefficients DWT de l'image tatouée. La technique proposée a atteint une forte robustesse contre différentes attaques au prix d'une capacité réduite. Les expériences ont été testées sur une seule modalité d'imagerie médicale (CT scan), où d'autres telles que les rayons X, l'IRM et l'échographie n'ont pas été rapportées.

Bamal et al.[66] a présenté une méthode de tatouage médical hybride basée sur le SVD combiné avec Fast Walsh Transform (FWT) et Slantlet Transform (SLT). Dans leur travail, les réseaux de neurones artificiels (ANN) sont utilisés pour la détection de régions d'intérêt (ROI), et deux *watermarks* sont générés. La sécurité de leur schéma est renforcée par l'utilisation d'une technique cryptographique. Ce schéma maintient une qualité visuelle élevée de l'image tatouée tout en augmentant simultanément les facteurs de robustesse et de capacité.

Pan et al. [59] ont développé un algorithme réversible pour le tatouage utilisant le bruit dominant dans les images médicales, en particulier pour les images radiographiques. Dans un premier temps, l'image médicale radiographique est décomposée en deux composants, l'image de fond noir et l'image de l'objet anatomique, en utilisant une technique de classification de région invariante. Ensuite, le processus d'intégration de *watermark* est appliqué aux deux composants dans une deuxième étape. Le *watermark* est incrusté dans l'image de fond en modifiant les valeurs de gris des pixels de l'histogramme Shifting modulation. De même, l'objet anatomique est tatoué en appliquant le décalage d'histogramme aux coefficients d'ondelettes du bruit quantique de l'image. Cette technique assure la réversibilité du processus de tatouage et préserve la valeur diagnostic de l'image radiographique. Néanmoins, la capacité de camouflage reste très faible.

Gangadhar et al. [67] ont proposé un algorithme de tatouage d'images médicales en transformation en ondelettes (IDWT) utilisant la décomposition en valeurs singulières (SVD) et l'optimisation par essaim de particules (PSO). Le DWT amélioré est appliqué à l'image médicale pour récupérer le domaine d'ondelettes invariant. Le *watermark* est inséré dans la région sélectionnée en modifiant les valeurs des coefficients dans l'image à l'aide de la fonction de seuil. Il a été constaté que ce schéma est efficace et robuste contre les attaques passives et actives.

Gomez et al. [18] ont proposé une méthode de tatouage basée sur la transformée d'Hermite pour les images cardiaques de tomodensitométrie. La transformée d'Hermite, qui intègre un schéma de normalisation, a été utilisée pour améliorer la robustesse contre les attaques géométriques. Alors qu'une seule modalité d'imagerie médicale a été testée. Là où d'autres tels que l'IRM, la radiographie et l'échographie n'ont pas été signalés. De plus, le stratagème n'a pas été exécuté contre différents types d'attaques.

Vellaisami et al. [68] ont utilisé le domaine composite CT-SVD, la fonction de génération de nombres triangulaires et les moments invariants de Hu pour l'authentification des images médicales. Ils ont présenté un schéma de marquage zéro pour résister aux attaques par inversion. L'utilisation de la transformation de Hu préserve la fidélité de l'image hôte et offre une robustesse suffisante contre les attaques courantes, ce qui la rend appropriée pour protéger les images médicales.

Khare et al. [69] ont conçu un schéma de tatouage d'image médicale efficace basé sur une transformation homomorphe (HT), une transformation en ondelettes discrète redondante (RDWT) et une décomposition en valeur singulière (SVD). La transformation d'Arnold est utilisée pour fournir plus de sécurité à l'algorithme proposé. La composante de réflectance de l'image originale est obtenue en utilisant HT, sur laquelle SVD et RDWT sont appliqués. De même, le *watermark* est transformé à l'aide de RDWT et SVD et ses valeurs singulières sont choisies pour le processus d'intégration. En outre, une transformation d'Arnold chaotique (AT) 2D est utilisée pour brouiller l'image du *watermark* et, par conséquent, augmenter le niveau de sécurité du schéma. Enfin, les expériences montrent que ce schéma est à la fois robuste et imperceptible avec la capacité de résister à la variation de la taille du *watermark.*

Après avoir examiné ces articles, nous sommes parvenus à la conclusion que trouver le meilleur schéma de tatouage dépend de l'obtention du compromis optimal entre la robustesse, l'invisibilité et la capacité d'intégration du tatouage. La plupart des schémas de tatouage existants présentés ci-dessus ne sont pas adaptés à diverses modalités d'images médicales, ce qui les rend inefficace pour tous les types d’applications médicales. Ces techniques améliorent un ou un sous-ensemble des paramètres de compromis, mais elles compromettent les autres paramètres restants. Par

conséquent, il est nécessaire de développer une méthode de tatouage efficace qui gère la plupart des modalités d'imagerie médicale et offre un compromis optimal entre ces paramètres pour les applications de cyber santé. Cette perspective est l'une des fortes motivations du présent travail.

1.4 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur le tatouage en général et d'images numériques en particulier. Nous nous sommes intéressés aux terminologies et aux notions liées aux techniques du tatouage numérique. Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle. Nous avons aussi abordé les différentes phases de la conception d'une méthode de tatouage. Nous avons présenté aussi une classification des techniques du tatouage selon différents critères : les champs d'application, les types d'algorithmes et les domaines d'insertion. Selon le dernier critère les techniques du tatouage peuvent utiliser le domaine spatial où l'insertion modifie directement les valeurs des pixels, mais la plupart des techniques de tatouage passent souvent par une transformée. Les plus populaires sont la transformée de Fourier, la DCT (la transformée qu'on a utilisé par la suite pour implémenter notre algorithme de tatouage).

Chapitre 2. Tatouage des images numériques basé sur la transformée de Laguerre combinée avec la DCT

Sommaire

2.1 Introduction. 61

2.2 Formalise mathématique 62

2.3 Algorithme proposé pour la phase d'insertion 72

2.4 Algorithme proposé pour la phase d'extraction 73

2.5 Expérimentations et résultats 75

2.6 Conclusion 79

2.1 Introduction

Comme l'indique le chapitre précédent, il existe une grande diversité des techniques de tatouage dans la littérature. Cependant, aucune de ces techniques n'est à la fois totalement robuste face aux attaques et totalement invisible. En effet, le but de la présente méthode n'est pas de trouver une méthode de tatouage qui répond à tous les problèmes soulevés, mais d'apporter une contribution pertinente en ce qui concerne le choix de la meilleure zone d'insertion du *watermark* permettant de trouver le compromis optimal entre robustesse et invisibilité du watermark. En nous appuyant sur l'état de l'art du chapitre précédent, nous avons développé une méthode de tatouage robuste dédiée aux images numériques basée sur une transformation polynomiale combinée avec la DCT. Pour se faire, une transformation polynomiale basée sur le polynôme de Laguerre est utilisée afin de décomposer l'image originale en deux composantes : structure et texture. La composante texture est choisie pour insérer le *watermark* en raison de l'insensibilité des yeux humains au bruit présent dans les régions texturées par rapport aux régions lisses. La DCT est utilisée pour extraire les moyennes fréquences de la composante texture, et ce, afin d'améliorer la robustesse de notre technique de tatouage sans dégrader la qualité visuelle de l'image. L'objectif de cette combinaison étant de sélectionner la meilleure zone d'insertion du *watermark* permettant d'atteindre un compromis optimal entre l'invisibilité et la robustesse du *watermark* [70].

Puisque les transformations polynomiales servent de base théorique de notre étude de recherche au cours de la présente thèse, nous présentons dans ce chapitre, un rappel sur lesdites transformées. Pour se faire, nous allons présenter différentes transformations qui peuvent être effectuées sur une image à partir des projections sur des bases de polynômes. Nous définissons dans un premier temps la notion de base polynomiale, sa construction et les techniques d'orthogonalisation. Puis, nous montrons comment il est possible d'utiliser une base de polynômes pour réaliser des approximations d'une image par projection sur cette base polynomiale. Dans un deuxième temps, nous présentons les différentes étapes de notre algorithme proposé. Finalement, et afin d'évaluer la robustesse de notre méthode et sa pertinence par rapport aux autres méthodes existantes, des résultats expérimentaux seront présentés dans la dernière section

2.2 Formalisme mathématique

Dans cette section, nous rappelons d'abord le concept d'une transformation polynomiale. D'une manière générale, une transformée polynomiale est une transformation locale qui permet de décomposer un signal localisé en l'observant par morceaux à travers une fonction de poids[4], dite aussi fenêtre d'analyse, que l'on positionne successivement en différents endroits du signal. Cette fonction, qui sert à localiser le signal pour ensuite faire l'analyse (la décomposition), est une fonction de l'argument x et elle représente les poids donnés aux polynômes orthogonaux dans la décomposition. La décomposition se fait par projection du signal d'origine à travers la fonction de poids sur une base de polynômes orthogonaux par rapport à la fonction en question. La décomposition de tout le signal peut se réaliser en faisant glisser la fenêtre d'analyse sur différentes positions régulièrement espacées. Afin de garantir la reconstruction, il faut un recouvrement non nul des fenêtres, entre deux positions adjacentes. En effet, les polynômes orthogonaux, introduits formellement par Szego [71], fournissent un outil qui convient à l'approximation locale de fonctions réelles d'une ou plusieurs variables. Ils interviennent notamment dans plusieurs domaines de l'analyse d'images à savoir la reconstruction, la compression, la reconnaissance de forme et la classification des objets[2], [72]–[75]. L'intérêt principal de l'utilisation de ces transformations, est le fait qu'elles correspondent à un bon modèle du système visuel humain. Nous allons donc utiliser ce modèle mathématique afin d'extraire certaines caractéristiques de l'image. Notre décomposition consiste à décomposer l'image en deux composantes. La première contient les informations géométriques, intitulée "composante structure". La seconde correspond aux variations à petite échelle, intitulée "composante texture". Pour se faire, on explique dans ce qui suit les principales étapes qui permettent de décomposer une image en utilisant une transformée polynomiale.

[4] Nous utilisons tout au long de ce rapport de manière équivalente les termes suivants: "fenêtre d'analyse", "fonction de poids" ou "fonction de pondération".

2.2.1 Notion de bases sur les polynômes orthogonaux

2.2.1.1 *Notion d'orthogonalité*

On considère que la notion d'orthogonalité est définie au sens de la mesure de Lebesgue-Stieltjes dans un intervalle. On dits qu'une séquence de polynômes $\{p_n\}_{n\in N}$, tel que p_n un polynôme de degré n en x, est orthogonale par rapport à la mesure Lebesgue-Stieltjes $d\mu(x)$ sur l'intervalle [a, b] si :

$$\int_a^b p_n(x)\, p_m(x) d\mu(x) = 0 \text{ , n} \neq \text{ m} \tag{14}$$

Si la mesure μ est bornée et absolument continue sur [a,b] tel que $d\mu(x) = w(x)dx$, on dit que les polynômes orthogonaux $\{p_n\}_{n\in N}$ sont d'une variable continue et la relation d'orthogonalité définie en (15) devient [76] :

$$\int_a^b p_n(x)\, p_m(x) w(x) \text{dx} = 0 \text{ , n} \neq \text{ m} \tag{15}$$

Si la mesure μ est une fonction en escalier à des sauts w_j au point $x = x_j$, $j = 0,1,2,..$ nous dirons que les polynômes orthogonaux $\{p_n\}_{n\in N}$ sont d'une variable discrète et la relation d'orthogonalité définie en (15) se présente sous la forme suivante [76] :

$$\sum_{j=0}^{\infty} p_n(x_j) p_m(x_j) w_j(x_j) = 0 \text{ , n} \neq \text{ m} \tag{16}$$

2.2.1.2 *Procédé d'orthogonalisation*

L'orthogonalisation de Gram-Schmidt, également appelé le processus de Gram-Schmidt, est une procédure qui prend un ensemble non orthogonal de fonctions linéairement indépendantes et le transforme en un ensemble fini de polynômes orthogonaux $p_0, p_1, .., p_{n-1}$. Donc pour chaque $m \in N$, le polynôme p_m est orthogonal à tous les polynômes de degré $k < m$ en particulier,

$$\int_a^b p_n(x)\, x^k d\mu(x) = 0 \text{ , pour tout k} = 0,1,..,\text{n} - 1 \qquad (17)$$

En effet, cette condition détermine le polynôme p_n à une constante près. Si on considère que les coefficients du polynôme p_n comme des variables, l'équation (18) détermine un système linéaire avec n équations et $\text{n} + 1$ variables. Si on fixe la constante de normalisation, on ajoute une équation de plus à ce système et donc, lors de la résolution de ce système, on obtient une solution unique en termes de la mesure μ.

2.2.1.3 *Formules de récurrences*

La propriété d'orthogonalité implique une série de propriétés importantes pour les polynômes telles les relations de récurrence par rapport à l'ordre n . Il existe deux types de relations de récurrences selon la nature de la base des polynômes : orthogonale ou orthonormée[77].

a. Base orthogonale

On considère un système de trois polynômes orthogonaux consécutifs $p_{n-1}(x), p_n(x), p_{n+1}(x)$ la relation de récurrence est définie dans ce cas par :

$$p_{n+1}(x) = (A_n\text{x} + B_n)\, p_n(x) - C_n p_{n-1}(x) \text{ ; n} = 1,2,3,\ldots \qquad (18)$$

Tel que $A_n, B_n \, et \, C_n$ sont des constantes définies par :

$$A_n = \frac{a_{n+1}}{a_n}, \qquad C_n = \frac{a_{n+1} a_{n-1} h_n}{a_n^2 h_{n-1}}, \qquad B_n = \frac{a_{n+1}}{a_n h_n} \int_a^b x\, p_n^2(x)\, d\mu(x), \quad h_n = \int_a^b p_n^2(x)\, d\mu(x)$$

Et a_n est le principal coefficient du polynôme p_n.

Afin de simplifier encore une fois cette formule on exige, en plus de la condition de normalisation, que chaque polynôme doit être unitaire ou bien que le terme constant du polynôme soit égal à un. En effet, en considérant le cas particulier où les polynômes orthogonaux sont

unitaires, la relation de récurrence des trois termes définie par l'équation précédente pout s'écrire sous la forme :

$$p_{n+1}(x) = (\mathrm{x} + B_n)\, p_n(x) - C_n p_{n-1}(x)\ ;\ \mathrm{n} = 1,2,3,\ldots \tag{19}$$

Où $B_n\ et\ C_n$ sont des constantes définies par :

$$C_n = \frac{h_n}{h_{n-1}},\quad B_n = -\frac{1}{h_n}\int_a^b x\, p_n^2(x)\, d\mu(x)$$

b. Base orthonormée

En vue d'obtenir la relation de récurrence à trois termes pour une base de polynômes orthonormés $\{p_n\}_{n\in N}$, il suffit de diviser les polynômes $\{p_n\}_{n\in N}$ par leurs normes carrées. On obtient ainsi une famille de polynômes orthonormés $\tilde{p}_n = {p_n}/{\|p_n\|}$ tel que $\|p_n\| = \int_a^b p_n^2(x)\, d\mu(x)$ est la norme associée au produit scalaire. Cette famille vérifie alors la relation de récurrence suivante :

$$xp_n(x) = A_n p_{n+1}(x) + B_n p_n(x) - A_{n-1} p_{n-1}(x)\ ;\ \mathrm{n} = 2,3,\ldots \tag{20}$$

Avec

$$A_n = \frac{a_n}{a_{n+1}},\quad B_n = \int_a^b x\, p_n^2(x)\, d\mu(x)$$

2.2.1.4 *Types de polynômes orthogonaux*

D'après les relations d'orthogonalité des polynômes, le choix de la fonction de poids $w(x)$ permet d'obtenir plusieurs ensembles de polynômes orthogonaux. Ils satisfont, selon la nature de la variable (continu ou discrète), les équations différentielles du second ordre ou les équations de différence à coefficients polynomiales[78].

a. Polynômes orthogonaux d'une variable continue

Les polynômes orthogonaux d'une variable continue satisfont l'équation différentielle du second ordre suivante :

$$\sigma(x)\frac{d^2}{dx^2}\mathrm{y(x)} + \tau(\mathrm{x})\frac{d}{dx}y(x) + \lambda_n y(x) = 0 \qquad (21)$$

Avec σ et τ sont des polynômes de 2ème degré et du premier degré respectivement. λ_n est une constante qui dépend des fonctions σ et τ et défini par : $\lambda_n = -n\,\tau'^{(\mathrm{x})} - 1/2n(n-1)\,\sigma"(x)$

Les polynômes solutions de cette équation sont les polynômes de Jacobi, Laguerre, Hermite et Bessel.

b. Polynômes orthogonaux d'une variable discrète

On distingue principalement deux catégories de polynômes orthogonaux d'une variable discrète, selon le type de la variable discrète x :

- **Variable discrète sur un intervalle linéaire**

Les polynômes orthogonaux d'une variable discrète sur un intervalle linéaire de la forme : $x_j = j, j = 0,1,\ldots$ sont des solutions de l'équation de différence de second ordre suivante :

$$\sigma(x)\,\Delta\nabla\,\mathrm{y(x)} + \tau(\mathrm{x})\nabla y(x) + \lambda_n y(x) = 0 \qquad (22)$$

Où σ et τ sont des polynômes de 2ème degré et du premier degré, respectivement. λ_n est une constante appropriée. Les opérateurs Δ et ∇ indiquent respectivement, l'opérateur de différence en avance et l'opérateur de différence en arrière. Ces derniers sont définis comme suit : $\Delta\,\mathrm{y(x)} = y(x+1) - y(x)$; $\nabla\,\mathrm{y(x)} = y(x) - y(x-1)$

Les polynômes solutions de l'équation (23) sont principalement les polynômes de Tchebichef, Hahn, Krawtchouk, Charlier et Meixner.

- **Variable discrète sur un intervalle q-linéaire**

Les polynômes orthogonaux d'une variable discrète sur un intervalle q-linéaire de la forme : $x_j = q^j, j = 0,1, \ldots$ ou $j = \cdots, -1,0,1, \ldots$ sont des solutions de l'équation de q-différence du second ordre suivante :

$$\sigma(x)\, D_q D_{1/q}\, \mathrm{y(x)} + \tau(\mathrm{x}) D_q y(x) + \lambda_n y(x) = 0 \tag{23}$$

Où D_q est l'opérateur de différence de Hahn défini par :

$$D_q f(\mathrm{s}) = \frac{f(qs) - f(s)}{(q-1)s}\ pour\ s \neq 0;\ D_q f(0) = f'(0) \tag{24}$$

Les polynômes solutions de l'équation (24) sont les q-analogues des solutions des équations (22) et (23) [79]. On cite à titre d'exemple : les polynômes de q-Jacobi, q-Krawtchouk, etc.

2.2.2 Construction de la base polynomiale

L'objectif étant d'effectuer des transformations sur une image I à partir de bases orthogonales de fonctions polynomiales. Pour cela, nous définissons une image I en niveau de gris comme suit :

$$\begin{cases} I : \Omega \subset \mathbb{R}^2 \rightarrow \mathbb{R} \\ x : (x_1, x_2) \mapsto I(x) \end{cases} \tag{25}$$

Où Ω est le domaine de définition de l'image.

Les transformations par des fonctions polynomiales utilisent des polynômes à deux variables sont définies dans $\mathbb{R}[x_1, x_2]$ de la manière suivante :

$$P_D(x) = P_D(x_1, x_2) = \sum_{\substack{(i,j)\in[0;D]^2 \\ (i+j)\leq D}} a_{i,j} x_1^i\, x_2^j \tag{26}$$

Tel que $i \in \mathbb{N}^+$ et $j \in \mathbb{N}^+$ représentent les degrés respectivement des variables x_1 et x_2. $a_{i,j}$ représente l'ensemble des coefficients réels du polynôme. $D = \sup\{i + j\}$ est le degré global du polynôme.

On considère $\mathcal{E}_d$ l'ensemble des polynômes bivariables de degré inférieur ou égal à D.

$$\mathcal{E}_d = \{P(x) | \deg(P) \leq D\} \tag{27}$$

Une base polynomiale finie est une famille $\mathcal{E}_d$ qui est à la fois libre et génératrice de cet espace. Une famille F est dite libre ou linéairement indépendante si pour toute combinaison linéaire d'éléments de F nulle, alors tous les coefficients de cette combinaison linéaire sont nuls. Cela revient à dire qu'aucun des vecteurs de la famille n'est combinaison linéaire des autres. Par ailleurs, une famille F est un système générateur (ou une famille génératrice), si tout autre élément de $\mathcal{E}_d$ peut s'exprimer comme étant une combinaison linéaire d'éléments de F. Dans l'anneau des polynômes sur un ensemble $\mathcal{E}_d$, la base canonique est la famille des monômes définie par :

$$K_D = \{ K_{i,j}(x) = x_1^i \, x_2^j \}_{(i,j) \in D} \tag{28}$$

Tel que D représente un ensemble fini de degrés des monômes $D = \{(i, j)\} \subset \mathbb{N}^2$ et $\mathcal{E}_d$ l'espace de tous les polynômes réels bivariables tels que $a_{i,j} \equiv 0$ si $(i, j) \notin D$

On considère une famille $\mathbb{B}_D$:

$$\mathbb{B}_D = \{\mathbb{B}_{i,j}(x) \}_{(i,j) \in D} \tag{29}$$

Composée des polynômes $B_{i,j}$ de degré $i + j$:

$$B_{i,j}(x) = \sum_{\substack{k \in [0;i] \\ l \in [0;j]}} b_{k,l} \, x_1^k \, x_2^l \tag{30}$$

Parmi toutes les bases polynômiales finies possibles, il existe une classe particulière, celle de bases orthogonales. Cette orthogonalité fait référence à un produit scalaire et implique que l'on a :

$$\langle B_{i,j} | B_{m,n} \rangle_{\omega} = \begin{cases} 0 \; si \; i,j \neq m,n \\ |B_{i,j}|^2 \; si \; i,j = m,n \end{cases} \tag{31}$$

Avec une norme induite par ledit produit scalaire. De plus, on dira que la base est normée si l'on a $|B_{i,j}|^2 = 1$. On désigne par $\langle . | . \rangle_{\omega}$ le produit scalaire applicable à deux fonctions F et G de Ω dans $\mathbb{R}$ et définit par :

$$\langle F | G \rangle_{\omega} = \iint_{x \epsilon \Omega} F(x) G(x) \omega(x) \, dx \tag{32}$$

Ce dernier est relatif à une fonction de pondération ω (ou fonction de poids) qui permet de déterminer le type de la base et qui doit vérifier :

$$\omega(x) \geq 0, \forall x \in \Omega \tag{33}$$

Afin de calculer ce produit scalaire, nous devons calculer une approximation de ces intégrales. Plusieurs solutions existent : Newton, trapèzes, intégration de Gauss, dans notre cas, nous avons choisi d'utiliser la transposition élémentaire définie par :

$$\langle F | G \rangle_{\omega} = \sum_{x \epsilon \Omega} F(x) G(x) \omega(x) \tag{34}$$

Il reste cependant à choisir une fonction de pondération afin de pondérer la qualité de l'approximation. Dans ce chapitre on a opté d'utiliser le polynôme de Laguerre qui est définit dans l'intervalle 0 à ∞ comme suit :

$$\omega(x) = \omega(x_1, x_2) = exp^{-(x_1 - x_2)} \tag{35}$$

Arrivons à cette étape, il est important d'utiliser un procédé d'orthogonalisation afin de générer une base orthogonale. Pour cela, on utilise l'orthogonalisation de Gram-Schmidt, également appelé le processus de Gram-Schmidt, présentée dans la section précédente, qui est une procédure qui prend un ensemble non orthogonal de fonctions linéairement indépendantes et le transforme

en un ensemble orthogonal. Pour cela, nous devons définir un ordre sur les indices des polynômes. Cet ordre est défini par la relation :

$$(i,j) \prec_2 (m,n) \; si \begin{cases} i + j < m + n \\ i > j \; si \; i + j = m + n \end{cases} \tag{36}$$

On considère le procédé d'orthogonalisation suivant :

$$T_{i,j}(x) = K_{i,j}(x) - \sum_{(m,n) \prec_2 (i,j)} \langle K_{i,j} | B_{m,n} \rangle_{\omega} B_{m,n}(x) \tag{37}$$

C'est ainsi qu'on obtient la base bidimensionnelle $\mathbb{B}_D = \{\mathbb{B}_{i,j}(x)\}_{(i,j)\in D}$ qui est composée de $n = \frac{(i+1)(j+1)}{2}$ polynômes orthogonaux triés par ordre lexicographique croissant. Le degré D de cette base est le degré le plus élevé des polynômes qui la composent. Cette base est générée par récurrence sur i, j par :

$$B_{i,j} = \frac{T_{i,j}(x)}{|T_{i,j}|_{\omega}} \tag{38}$$

2.2.3 Décomposition polynomiale d'une image

Après avoir présenté les fondements de base sur les transformations polynomiales, nous allons appliquer ce principe pour approximer n'importe quelle fonction bivariable. En effet cette transformation permet de décomposer l'image originale en deux composantes significatives : structure et texture. La première concerne les informations géométriques de l'image tandis que la deuxième composante concerne les variations à petite échelle. Mathématiquement, la composante structure peut être décrite par une fonction lissage (ou une fonction constante) par morceaux, tandis que la composante texture est communément oscillante. En raison de leurs caractéristiques de nature différentes, il est plus efficace de les séparer pour le traitement et l'analyse d'images. Généralement, l'analyse de ces composants joue un rôle particulièrement important dans quatre grands enjeux à savoir en matière d'analyse de la texture. Premièrement, c'est l'extraction de caractéristiques pour calculer une signature d'une image numérique en mesure de décrire numériquement ses propriétés de texture. Deuxièmement, la discrimination de la texture pour partitionner une image texturée en régions, où chacune correspond à une texture perceptuellement homogène (mène à la segmentation d'images). Ensuite, on parle aussi de la classification de textures dont le but est d'affecter un échantillon d'image inconnu à l'un des ensembles de classe

connue de texture. Finalement, on peut parler de l'extraction de la forme d'objets à partir de leur texture, dans ce cas, l'image 2D est considérée comme une projection d'une scène 3D et les distorsions de texture apparente dans l'image en 2D sont utilisées pour estimer les orientations de surface dans la scène 3D. L'extraction de caractéristiques est la première phase d'analyse de texture d'image. Les résultats obtenus à partir de cette étape sont employés dans nos contributions de la présente thèse notamment dans le cadre de l'extraction des zones optimales pour l'insertion du watermark.

On rappel l'objectif de cette technique de décomposition d'images permet d'obtenir une représentation mathématique de chacune des composantes d'une image. Pour cela, on propose de garder la même formule de base pour la décomposition d'images comme cela est défini dans les modèles variationnels :

$$I = I^T + \tilde{I} \tag{39}$$

Tel que I est l'image originale à décomposer, I^T représente la composante texture et $\tilde{I}$ représente la composante structure.

Étant donnée une base orthogonale de B_D, l'approximation polynomiale $\tilde{I}$ d'une image numérique ou sa modélisation s'obtient par projection de chacun des pixels dans la base de référence. L'approximation de l'image I sera donc, relative à la base choisie est définie comme suit :

$$\begin{cases} \tilde{I} = \sum_{i=0}^{D} \sum_{j=0}^{D-i} \tilde{\imath}_{i,j} \, B_{i,j} \\ \tilde{\imath}_{i,j} = \dfrac{\langle I | B_{i,j} \rangle_{\omega}}{\langle B_{i,j} | B_{i,j} \rangle_{\omega}} \end{cases} \tag{40}$$

Tel que $\tilde{\imath}_{i,j}$ représentent les coefficients de cette projection.

La reconstruction de l'image se fait simplement en réévaluant, à partir des coefficients $\tilde{\imath}_{i,j}$ et de la base B, l'équation (40) pour tous les sites (x_1, x_2) du domaine Ω de l'image.

Enfin, la composante texture est déduire de la reconstruction partielle en considérant que c'est la partie résiduelle de l'image :

$$I^T = I - \tilde{I} \tag{41}$$

2.3 Algorithme proposé pour la phase d'insertion

La technique proposée pour sécuriser les images numériques par le biais du tatouage, permet d'insérer le *watermark* dans la composante texture de l'image, car les yeux humains ne sont pas si sensibles au bruit dans les régions les plus texturées par rapport aux régions lisses. Cette composante est générée par modèle mathématique présenté précédemment concernant la décomposition de l'image en utilisant les transformations polynomiales. Le domaine de la DCT est utilisé afin d'améliorer la robustesse sans dégrader la qualité visuelle de l'image. La raison principale de ce choix est que le domaine DCT tend à avoir plus d'énergie concentrée dans moins de coefficients. Ainsi, l'image originale est partitionnée en blocs de taille 8x8. Ce choix représente un compromis entre performance et qualité : en effet, en augmentant la taille des blocs, la complexité temporelle de l'algorithme devient de plus en plus coûteuse. Les moyennes fréquences sont choisies pour l'insertion du watermark, afin de préserver l'imperceptibilité du *watermark* et le protéger contre la suppression lorsque l'image tatouée est soumis à différents attaques.

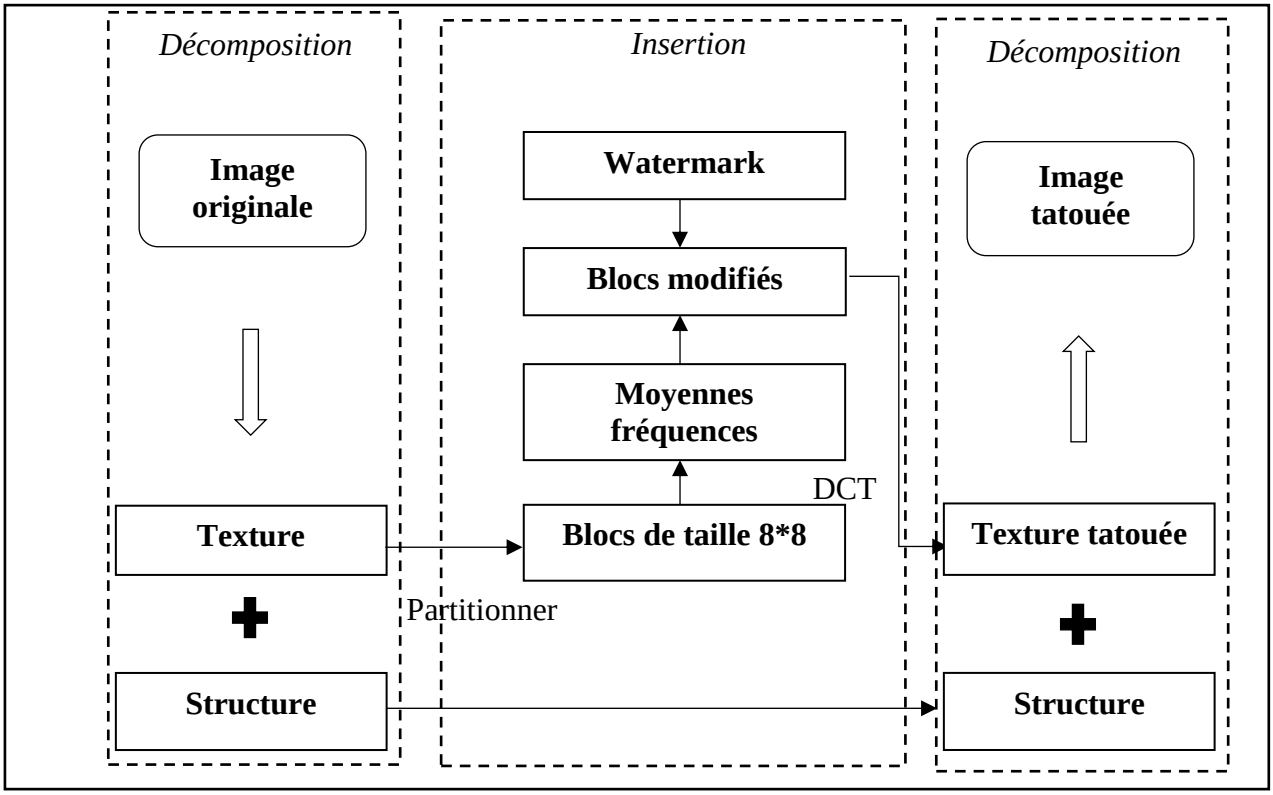


Figure 2.1 phase d'insertion

Le processus d'insertion est présenté dans la figure 2.1 ci-dessus et comprend les étapes suivantes :

Etape 1. Convertir l'image originale en niveau de gris et convertir le *watermark* choisi en binaire.

Etape 2. Décomposer l'image originale en deux composantes : structure et texture, et ce en utilisant une transformation polynomiale pondérée par le polynôme de Laguerre.

Etape 3. Diviser la composante texture en blocs de taille 8 * 8.

Etape 4. Appliquer la transformation DCT sur chaque bloc $B_i(B_1, \dots, B_k)$.

Etape 5. Extraire les moyennes fréquences de chaque bloc.

Etape 6. Insérer les bits du *watermark* w_i dans les coefficients DCT sélectionnés a_i de chaque bloc en utilisant la formule suivante :

$$B_i^* = B_i(a_i + w_i * S) \quad (42)$$

Tel que le facteur S représente la force du tatouage

Etape 7. Effectuer la transformée inverse de la DCT (IDCT) en vue d'obtenir les blocs tatoués. Ces blocs sont utilisés afin de construire la partie texture tatouée.

Etape 8. Combiner la composante texture tatouée et la composante structure non modifiée pour obtenir l'image tatouée I_w.

2.4 Algorithme proposé pour la phase d'extraction

Dans la phase d'extraction, nous devons extraire le *watermark* depuis l'image tatouée même en cas de modifications.

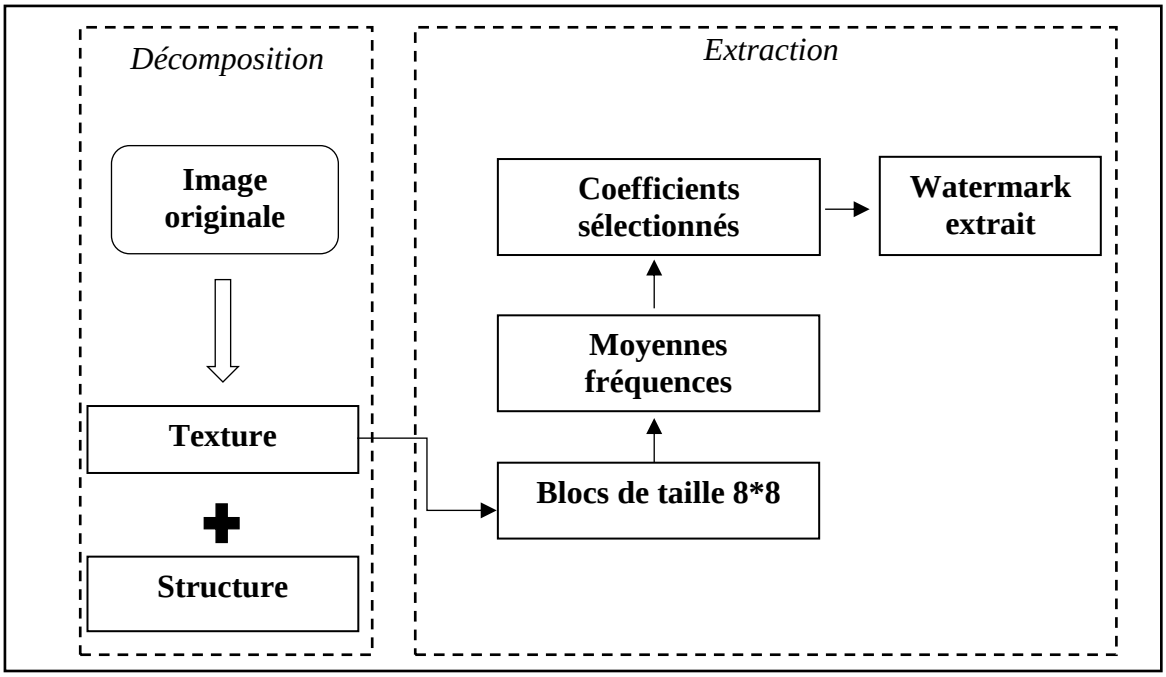


Figure 2.2 Phase d'extraction

Cette phase est présentée dans la figure 2.2 et comprend les étapes suivantes :

Etape 1. Partitionner l'image tatouée I_w en composantes structure et texture en utilisant le procédé de décomposition décrit précédemment.

Etape 2. Diviser la composante texture en blocs de tailles 8 * 8.

Etape 3. Appliquer la transformation DCT pour chaque bloc $B_i^*(B_1^*, \dots, B_k^*)$ et sélectionner leurs moyennes fréquences a_i^*.

Etape 4. Extraire les bits du *watermark* à partir des coefficients DCT sélectionnés de chaque bloc comme suit :

$$a_i^* = \frac{B_i^*}{B_i} - w_i * S \tag{43}$$

Etape 5. Reconstruire le *watermark* en utilisant les coefficients modifiés

SI $a_i^* < 0$ alors $watermark_i = 0$

Sinon $watermark_i = 1$

2.5 Expérimentations et résultats

Dans cette section, plusieurs expérimentations ont été réalisées pour vérifier l'efficacité de l'approche proposée en termes d'invisibilité et robustesse du watermark. Les images des tests choisis sont des images niveau de gris de tailles 512 x 512. Cet ensemble d'images se compose de huit images classiques en traitement d'images, dont les noms sont : Lena, Barbara, Cameraman, Pirate, Lake, Hill, Boat, Butterfly (voir figure 2.3). Le choix de ces images a été basé sur leur diversification en termes de texture et d'uniformité. Ainsi que des images binaires de tailles 64 x 64 ont été choisi comme *watermark* (comme illustré sur la figure 2.4).

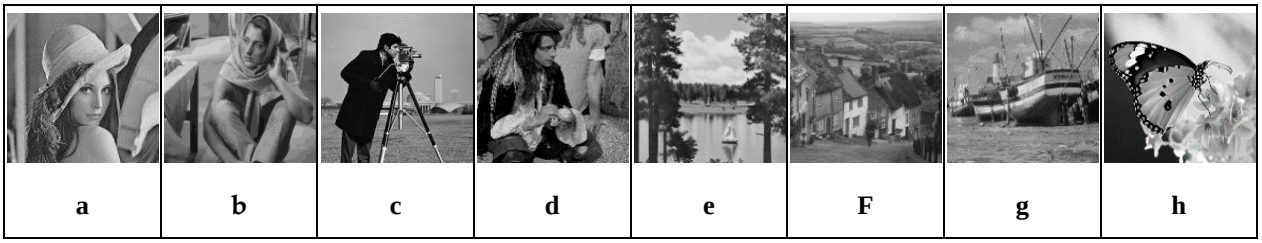


Figure 2.3 Images de tests (a) lena, (b) barbara, (c) cameraman, (d) pirate, (e) lake, (f) hill, (g) boat, (h) butterfly.



Figure 2.4 Images de tests représentant le watermark du tatouage

2.5.1 Sans attaques

Afin de démontrer l'efficacité de notre technique de tatouage, nous proposons un exemple explicatif présentant les principales étapes du tatouage de différentes images de test.

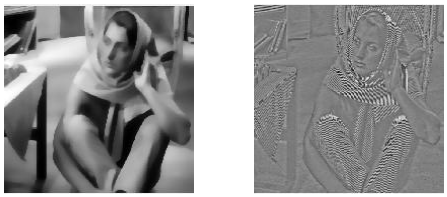
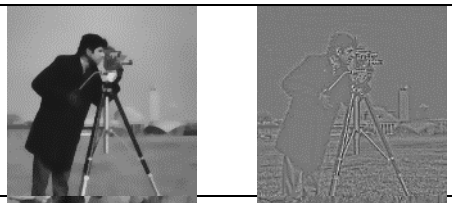
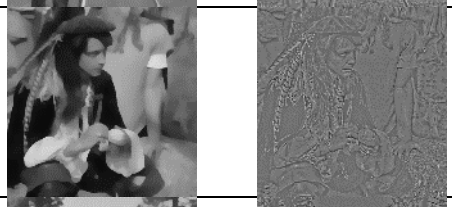
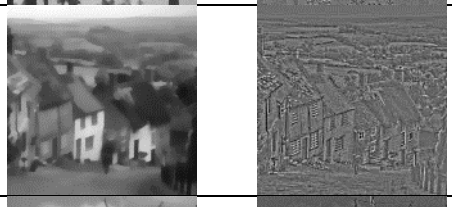
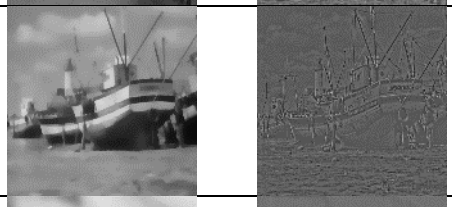
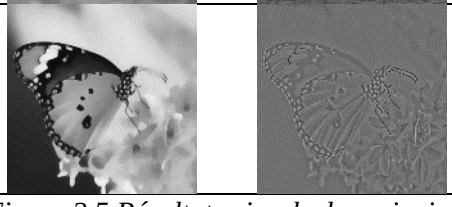
	Décomposition	Image tatouée	Watermark extrait
a			
b			
c			SABBANE
d			SABBANE
e			
f			
g			
h			

Figure 2.5 Résultats visuels des principales étapes de l'algorithme proposé

Dans la figure 2.5 ci-dessus, la première colonne illustre le résultat de la décomposition polynomiale de l'image en composantes structure et texture. La deuxième colonne est consacrée au résultat de l'image tatouée tandis que la dernière colonne représente le *watermark* extrait dans le cas sans attaques.

approche	***a***	***b***	***c***	***d***	***e***	***f***	***g***	***H***
[80]	40.69	NA	40.26	52.36	NA	NA	NA	NA
[81]	44.59	NA	44.52	NA	NA	NA	NA	NA
[82]	44.40	NA	NA	NA	NA	NA	NA	44.38
[83]	40.78	40.78	NA	40.78	40.78	40.78	40.79	NA
[84]	38.48	38.41	NA	38.45	38.47	38.41	38.42	NA
[85]	43.53	NA	NA	NA	NA	NA	NA	NA
proposée	**50.69**	**51.18**	**52.44**	**51.91**	**51.82**	**52.24**	**52.60**	**52.73**

TABLE 2-1 Comparaison des performances des différentes techniques en termes de PSNR dans le cas sans attaques.

L'évaluation de l'invisibilité du *watermark* dans l'image tatouée de notre méthode est comparée dans le tableau 2-1 avec les travaux précédents [80]–[85] dans le cas sans attaques en terme de du PSNR (Peak signal to noise ration). Une autre comparaison dans le cas sans attaques est présentée dans le tableau 2-2 en termes de NC (corrélation normalisée) avec [82]–[84]. D'après ces résultats, il est clair que notre méthode est plus prometteuse par rapport aux méthodes précédentes.

approche	***A***	***b***	***c***	***d***	***e***	***f***	***g***	***H***
[82]	0.9581	NA	NA	NA	NA	NA	NA	0.9400
[83]	0.9581	0.9987	NA	0.9986	0.9987	0.9988	0.9986	NA
[84]	0.9968	0.9967	NA	0.9968	0.9965	0.9966	0.9966	NA
proposée	**0.9999**	**1.0000**	**0.9998**	**0.9997**	**0.9995**	**0.9999**	**1.0000**	**0.9998**

TABLE 2-2 Comparaison des performances des différentes techniques en termes de NC dans le cas sans attaques.

2.5.2 Avec attaques

Afin d'évaluer la robustesse de l'approche proposée, l'image tatouée est testée selon deux types d'attaques : Compression JPEG et l'addition du bruit. Dans le tableau 2-3 ci dessous, QF fait référence au facteur de qualité de la compression JPEG et D à la densité du bruit poivre et sel.

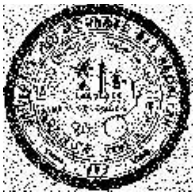
		Lena	**Barbara**	**Peppers**
JPEG Compression	QF=50	 NC = 0.99	 NC = 0.99	 NC = 0.99
	QF=25	 NC = 0.90	 NC = 0.90	 NC =0.91
	QF=10	 NC = 0.86	 NC =0.87	 NC =0.89
Salt & Pepper Noise	D= 0.02	 NC = 0.90	 NC = 0.95	 NC = 0.90
	D= 0.04	 NC = 0.81	 NC= 0.83	 NC = 0.82

TABLE 2-3 Les valeurs NC des watermarks extraits après exposition aux attaques

2.6 Conclusion

Dans ce chapitre, une nouvelle technique de tatouage des images basée sur la décomposition polynomiale combinée avec la DCT a été élaborée. Les résultats expérimentaux indiquent que notre algorithme est capable d'atteindre un bon compromis entre la robustesse et l'imperceptibilité du *watermark* selon deux types d'attaques, à savoir l'ajout du bruit et la compression JPEG, par rapport à différentes techniques existantes. La pertinence de la méthode d'extraction de la texture nous donne la possibilité de répandre l'information du *watermark* sur toute l'image, de sorte qu'il est difficile de détecter l'existence du watermark. En outre, la fidélité de la représentation de l'image est préservée. Ces résultats sont très encourageantes puisque l'objectif principal de cette contribution est tester l'efficacité de l'algorithme proposé avant de passer à un autre type de documents de nature très sensible et complexe : les images médicales.

Chapitre 3. Tatouage des images médicales basé sur la transformée de Chebychev

Sommaire

3.1 Introduction 81

3.2 Formalise mathématique..... 81

3.3 Méthode proposée 84

3.4 Expérimentations et résultats 87

3.5 Conclusion 105

3.1 Introduction

Nous avons présenté dans le chapitre précèdent notre méthode de tatouage consacrée aux images classiques dans le but de la protection des droits d'auteur de l'image. Nous avons vu que les transformations polynomiales comme étant une base théorique de prétraitement de l'image permettent d'extraire les régions pertinentes de l'image et de cacher la perception de la présence du *watermark*. Nous présentons ainsi, dans ce chapitre, une contribution qui a fait l'objet d'un article journal [86], dédiée aux tatouage des images à caractère sensible : tatouage des images médicales. Dans un premier temps, nous allons présenter le formalisme mathématique nécessaire pour effectuer cette méthode de tatouage. Par la suite, nous allons détailler les étapes d'insertion et d'extraction de la méthode proposée. Finalement, nous présentons des résultats expérimentaux évaluant les performances de notre méthode.

3.2 Formalise mathématique

Le modèle mathématique de la décomposition polynomiale proposé utilise les notions de bases définis dans la section 2.2 du chapitre 2, et qui est présenté comme suit. Notons I_M l'image médicale originale en niveaux de gris de taille M x N, définie sur le domaine Ω. Elle est représentée comme un ensemble de valeurs discrètes qui peuvent être considérées comme une partie d'une fonction continue $I_M : \Omega \rightarrow \mathbb{R}$.

$$\begin{cases} I_M : \Omega \subset \mathbb{R}^2 \rightarrow \mathbb{R} \\ x : (x_1, x_2) \mapsto I_M(x) \end{cases} \tag{44}$$

La construction de la base polynomiale est effectuée en utilisant la procédure de récurrence à trois termes (ou aussi la procédure de Stieljes lorsque le produit scalaire est approximé par discrétisation en calculant l'intégrale par une transposition élémentaire). Dans le cas où la base est constituée des polynômes bivariables, la base des polynômes orthogonaux est définie comme suit :

$$\begin{cases} \mathcal{B}_{-1,\mathrm{j}}(x_1, x_2) = 0 \\ \mathcal{B}_{i,-1}(x_1, x_2) = 0 \\ \mathcal{B}_{0,0}(x_1, x_2) = 1 \\ \mathcal{B}_{i+1,j}(x_1, x_2) = (x_1 - \lambda_{i+1,j})\mathcal{B}_{i,j}(x) - \mu_{i+1,1}\,\mathcal{B}_{i-1,j}(x) \\ \mathcal{B}_{i,j+1}(x_1, x_2) = (x_2 - \lambda_{i,j+1})\mathcal{B}_{i,j}(x) - \mu_{i,j+1}\,\mathcal{B}_{i-1,j}(x) \end{cases} \quad (45)$$

Avec des coefficients λ et μ donnés par :

$$\lambda_{i+1,j} = \frac{\langle x_1 \mathcal{B}_{i,j} | \mathcal{B}_{i,j} \rangle_\omega}{\langle \mathcal{B}_{i,j} | \mathcal{B}_{i,j} \rangle_\omega} \qquad \lambda_{i,j+1} = \frac{\langle x_2 \mathcal{B}_{i,j} | \mathcal{B}_{i,j} \rangle_\omega}{\langle \mathcal{B}_{i,j} | \mathcal{B}_{i,j} \rangle_\omega}$$

$$\mu_{i+1,j} = \frac{\langle \mathcal{B}_{i,j} | \mathcal{B}_{i,j} \rangle_\omega}{\langle \mathcal{B}_{i-1,j} | \mathcal{B}_{i-1,j} \rangle_\omega} \quad \mu_{i,j+1} = \frac{\langle \mathcal{B}_{i,j} | \mathcal{B}_{i,j} \rangle_\omega}{\langle \mathcal{B}_{i,j-1} | \mathcal{B}_{i,j-1} \rangle_\omega} \quad (46)$$

La base bidimensionnelle $\mathcal{B}_{OP} = \{P_{\mathrm{p,q}}\}_{\mathrm{p}\in\{0..\mathrm{P}\}, q\in\{0..\mathrm{Q}\}}$ est donc composée de $\mathrm{n} = \frac{(p+1)(q+1)}{2}$ polynômes orthogonaux triés par ordre lexicographique croissant. Le degré de cette base est le degré le plus élevé des polynômes qui la composent. Cette base est notée par :

$$\mathcal{B}_{OP} = \{P_{0,0}, .., P_{0,\mathrm{q}}, P_{-1,0}, .., P_{1,\mathrm{q}-1}, .. P_{p,0}\} \quad (47)$$

Les polynômes de Chebychev de première espèce $T_n(x)$ sont définis à partir de la formule suivante :

$$T_n(x) = \frac{n!}{(\frac{1}{2})_n} P_n^{(-\frac{1}{2},-\frac{1}{2})}(x) \quad (48)$$

Les polynômes orthogonaux de Chebychev de première espèce satisfont les relations de récurrences à trois termes suivantes :

$$2\,x\,T_n(x) = T_{n+1}(x) + T_{n-1}(x), T_0(x) = 1, T_1(x) = x \quad (49)$$

Ces polynômes sont orthogonaux relativement à la fonction de poids $\omega(x) = (1 - x^2)^{-1/2}$, sur l'intervalle $[-1,1]$ et vérifient la relation d'orthogonalité suivante :

$$\int_{-1}^{1}(1-x^2)^{-1/2}\;\; T_n(x)T_m(x)\,\mathrm{dx} = \begin{cases}\frac{\pi}{2}\delta_{n,m}\\ \pi\delta_{n,m}\end{cases} \tag{50}$$

Afin de discrétiser le domaine Ω, nous considérons par défaut que le domaine de définition est $\Omega = [-1,1]^2$, ce choix va nous ramener à une approximation de l'image. Pour se faire on utilise la collocation de Gauss-Tchebychev suivante: elle correspond aux zéros des polynômes de Tchebychev et est optimale au sens de la quadrature de Gauss. Il s'agit d'un échantillonnage non régulier de la forme :

$$x_i(k) = \cos\left(\frac{2k+1}{2N}Pi\right), k = 0..N \tag{51}$$

Avec N représente le nombre de points que comporte le domaine Ω.

Une fois la base est générée, l'image médicale est projetée sur cette base en utilisant :

$$I_p = \frac{\langle I_M | \mathcal{B}_{i,j}\rangle_\omega}{\langle \mathcal{B}_{i,j} | \mathcal{B}_{i,j}\rangle_\omega} \tag{52}$$

L'approximation de l'image médicale représentant la partie structure est décrite par :

$$\tilde{I} = \sum_{i=0}^{D}\sum_{j=0}^{D-i} I_p\,\mathcal{B}_{i,j} \tag{53}$$

Comme cette approximation représente les régions lisses de l'image originale, la composante texture est extraite de la manière suivante (comme détaillée dans la section 2.2):

$$T = I_M - \tilde{I} \tag{54}$$

La propriété d'orthogonalité de cette technique offre la possibilité d'extraire les informations pertinentes et les caractéristiques globales de l'image d'origine d'une part ; d'autre part, cet outil mathématique est choisi en raison de sa polyvalence et de son inspiration de la perception visuelle humaine qui représente le mieux les caractéristiques de l'image médicale[87].

3.3 Méthode proposée

Dans cette contribution, une nouvelle approche du tatouage des images médicales est proposée. Ces images, qui contiennent des informations critiques utilisées pour un e-diagnostic, nécessitent souvent un choix raisonnable de zones d'incorporation du watermark. Notre objectif principal est de trouver la zone d'incorporation la plus appropriée. Dans ce but, la partie texture, obtenue par la décomposition polynomiale décrite dans la section précédente, est considérée comme la zone la plus appropriée pour une intégration d'un *watermark* robuste. Cette stratégie est avant tout motivée par le fait que l'œil humain est moins sensible aux modifications dans les régions texturées que dans les régions lisses[33], [88], [89]. Par conséquent, l'amélioration de l'imperceptibilité du watermark.

Les principales étapes de notre méthode, sont expliquées dans les sous-sections suivantes.

3.3.1 Phase d'insertion

La méthode d'insertion du *watermark* proposée, illustrée dans la figure 3.1, peut être divisée en deux parties principales :

- Procédé de décomposition polynomiale : l'image orginale est d'abord projetée dans une base polynomiale orthogonale selon un facteur de degré polynomial donné. Cette projection transforme les intensités des pixels de l'image originale et donne, comme résultat, une autre image nommée "moments de l'image" qui contient les coefficients de cette projection. Ensuite, une transformée inverse est appliquée reconstruire l'image originale. La propriété d'orthogonalité de cette transformation permet de retrouver les intensités des pixels de l'image originale à partir de ces moments.
- Procédé de tatouage : Ce procédé commence par l'intégration du *watermark* dans la texture partitionnée, selon une force de tatouage donné, afin de construire la texture tatouée. Cette dernière remplace la texture originale dans l'image originale pour former l'image tatouée.

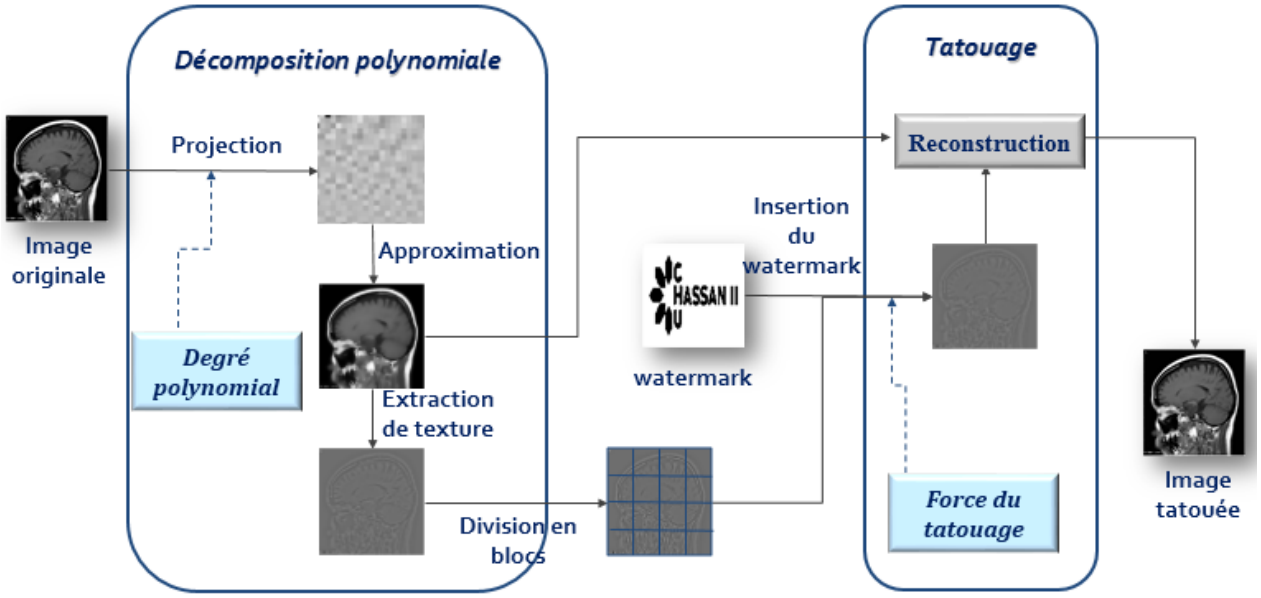


Figure 3.1 Schéma représentant la phase d'insertion

Algorithme : insertion du watermark

Entrées : Image médicale en niveau de gris de taille 960x960 I_M, *Watermark w*

Sorties : image médicale tatouée I_{MW}

Etape 1. Charger l'image médicale et convertir l'image du *watermark* en binaire.

Etape 2. Calculer la projection de l'image originale sur la base de polynôme orthogonaux selon un facteur représentant le degré du polynome.

Etape 3. Effectuer la transformée inverse afin d'obtenir l'image approximé permettant d'extraire la composante texture.

Etape 4. Partitionner la texture en bloc de tailles 8x8

Etape 5. Insérer les bits du *watermark* w_i dans les pixel X_k de chaque bloc $B_i(X_1, \dots, X_k)$ selon un certain facteur représentant la force du tatouage. L'équation suivante est utilisée pour obtenir les blocs tatouée $B_i^*(X_1^*, \dots, X_k^*)$:

$$B_i^* = B_i(1 + w_i * S)$$

$$X_i^* = X_i + w_i * S \quad (55)$$

Etape 6. Reconstruire l'image médicale dans sa version tatouée I_{MW} en combinant la partie texture tatouée et la partie structure non modifiée.

3.3.2 Phase d'extraction

Le processus d'extraction du *watermark* proposé, est illustré à la figure 3.2 ci-dessous, et peut être divisé en deux principales parties:

- Le processus de la décomposition polynomiale est appliqué de manière similaire à la procédure d'insertion du watermark.
- Le processus de tatouage : Ce processus extrait le *watermark* depuis la texture tatouée.

Algorithme : extraction du watermark

Entrées : Image médicale tatouée I_{MW}, *Watermark w*

Sorties : *watermark* extrait W

Etape 1. Charger l'image médicale tatouée et calculer sa projection sur la base de polynôme orthogonaux selon un facteur représentant le degré du polynome.

Etape 2. Effectuer la transformée inverse en vue d'obtenir l'approximation de l'image qui servira comme support pour extraire la partie texture de l'image.

Etape 3. Partitionner la texture en blocs de taille 8x8 et en extraire les bits du *watermark* par :

$$\widetilde{X_i} = \frac{B_i^*}{B_i} - 1 \tag{56}$$

Etape 4. former le *watermark* en regroupant les bits obtenus.

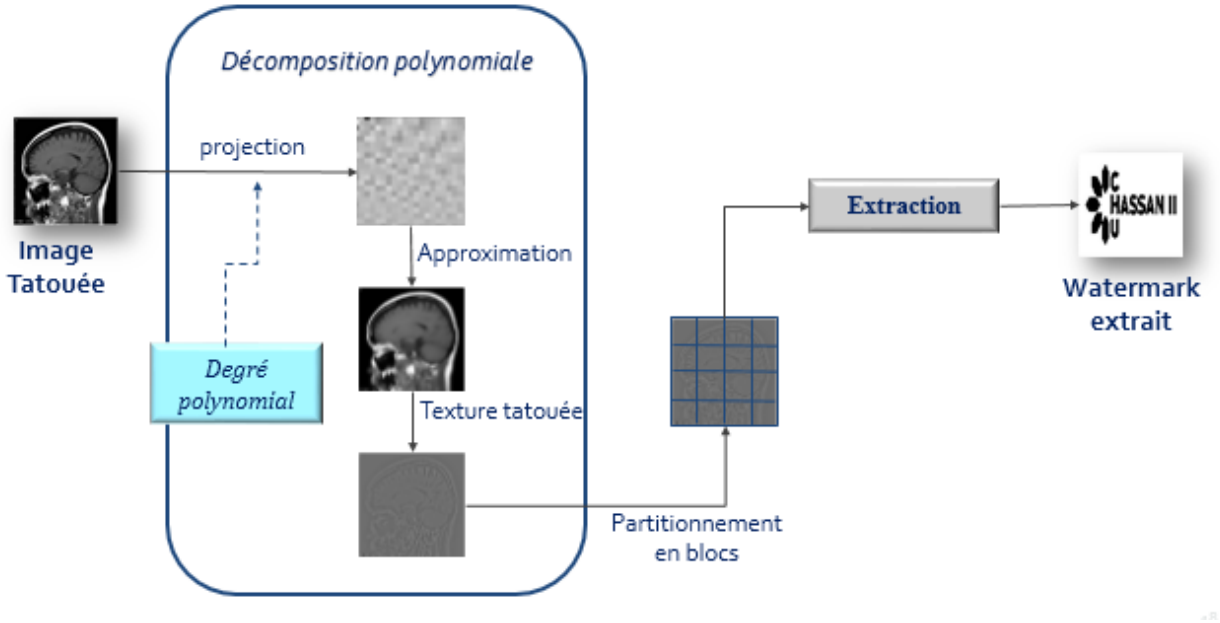


Figure 3.2 Schéma représentant la phase d'extraction

3.4 Expérimentations et résultats

Dans cette section, nous évaluons les performances de notre méthode. Pour ce faire, nous présentons d'abord les images médicales de test choisies ainsi que les paramètres et les mesures d'évaluations utilisées, ensuite nous introduisons les méthodes de comparaison, et enfin nous présentons les résultats expérimentaux évaluant la robustesse et l'invisibilité de de la méthode proposée comparés aux autres méthodes de la littérature.

Les expériences de tests ont réalisées sur des images médicales en niveaux de gris de taille 960 x 960 avec différentes modalités, à savoir les rayons X, les ultrasons, l'IRM, le CT, le PET et la mammographie. Ces images proviennent de la base de données d'images médicales MedPix (MedPixTM). Quelques échantillons de ces images sont présentés dans la figure 3.3 ci-dessous.

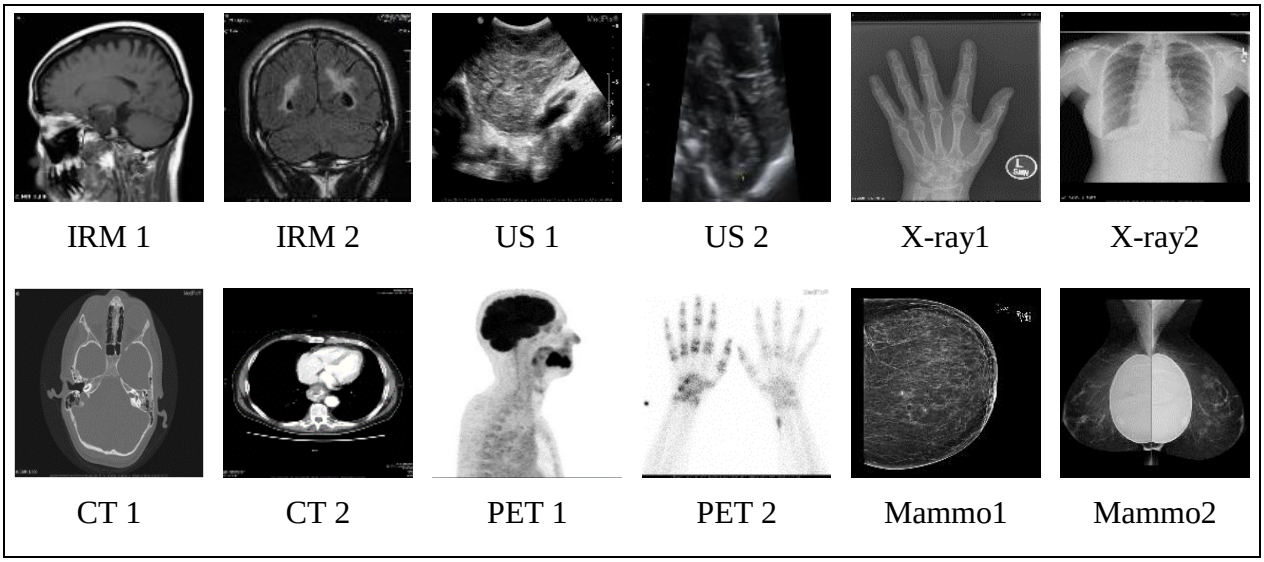


Figure 3.3 Ensemble des images médicales de test de différentes modalités

De plus, 3 images binaires avec des contenus différents sont utilisées comme *watermark* pour les tests (illustré à la Figure 3.4 ci-dessous). La première représente une image contenant des informations texturales. La deuxième représente un logo avec des détails plus nets. La troisième contient un logo avec des détails plus lisses. Les *watermark* sont des images binaires de 120 x 120. Nous remarquons que la taille de chaque image de *watermark* est choisie identique pour une meilleure comparaison des schémas et une meilleure visualisation des résultats des expériences. La mise en œuvre du système proposé est effectuée sur un ordinateur portable 2.20 GHz processeur Core i7 avec 2 Go de RAM.

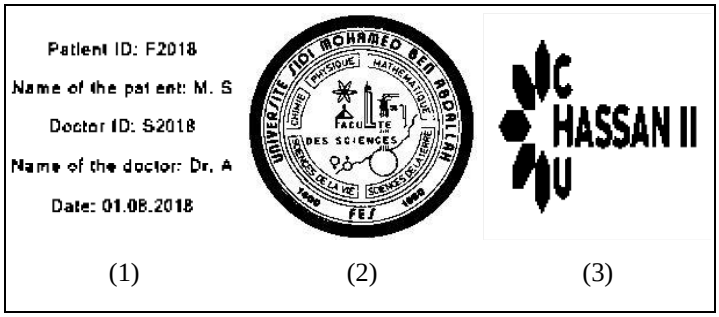


Figure 3.4 Les watermarks de test

3.4.1 Mesures de performances

Différentes mesures sont proposées pour évaluer la qualité visuelle (imperceptibilité) des images médicales tatouée, c'est-à-dire, mesurer la distorsion ou le niveau de dégradation perceptive introduit par toute modification appliquée à l'image originale. Les métriques utilisées dans ce chapitre sont : PSNR, NC et la carte de dissimilarité locale (LDM). Les deux premières métriques ont été détaillées dans le chapitre de l'état de l'art. Tandis que la Carte de dissimilarité locale est utilisée pour localiser et quantifier la différence entre deux images. L'algorithme utilisé est basé sur une transformée de distance. Cette métrique associe à chaque pixel une distance au pixel le plus proche. Sa définition mathématique pour le cas d'images binaires s'exprime par :

$$td(A) = min[d(A, X), X \in O] \tag{57}$$

Tel que d représente la distance euclidienne entre deux images et O représente l'ensemble des pixels appartenant à l'objet concerné.

La LDM est alors définit comme suit :

$$LDM\ (A, B) = |A - B| * max(td(A), td(B)) \tag{58}$$

Tel que td est la transformée de distance des images A et B.

3.4.2 Paramètres de l'algorithme

Un bon compromis (robustesse - invisibilité) du tatouage est le résultat d'une bonne sélection de régions d'insertion du watermark. Pour obtenir ce résultat, la technique qui a été mise en œuvre nécessite la définition de deux paramètres principaux : la force du processus du tatouage et le degré de décomposition des polynômes.

Tout d'abord, la force du tatouage est fixée à 0,01 pendant le processus de tatouage de l'image médicale. En effet, les valeurs les plus élevées de la force du tatouage fournissent une insertion du *watermark* plus robuste mais cela se fera au détriment de la qualité de l'image. Après

plusieurs expériences, il s'est avéré que la valeur fixée de la force du tatouage permet d'obtenir le compromis optimal entre robustesse et invisibilité de la marque.

Deuxièmement, afin de trouver le degré de décomposition optimal. L'entropie est utilisée pour approximer la quantité d'information contenue sur chaque composante de l'image originale. Elle est définie comme suit :

$$\text{Entropy} = -\sum_{i=0}^{N-1} P_i . \log_2(P_i) \tag{59}$$

Tel que P_i représente la probabilité d'occurrence du niveau i et N représente le niveau de couleur de l'image.

La figure 3.5 ci-dessous représente le comportement de l'entropie en faisant varier le degré de décomposition pour chaque composante : l'image originale, l'image tatouée, la partie structure et la partie texture. Comme on peut le remarquer, les images originales et tatouées sont confondues ce qui justifie qu'il n'y a pas de perte d'information médicale. De plus, la différence entre les courbes des images structure et originales est beaucoup plus faible une fois le degré 20 atteint. De plus, la partie texture est mieux visible à ce degré. C'est pourquoi le degré 20 est choisi pour la suite des tests de la méthode proposée.

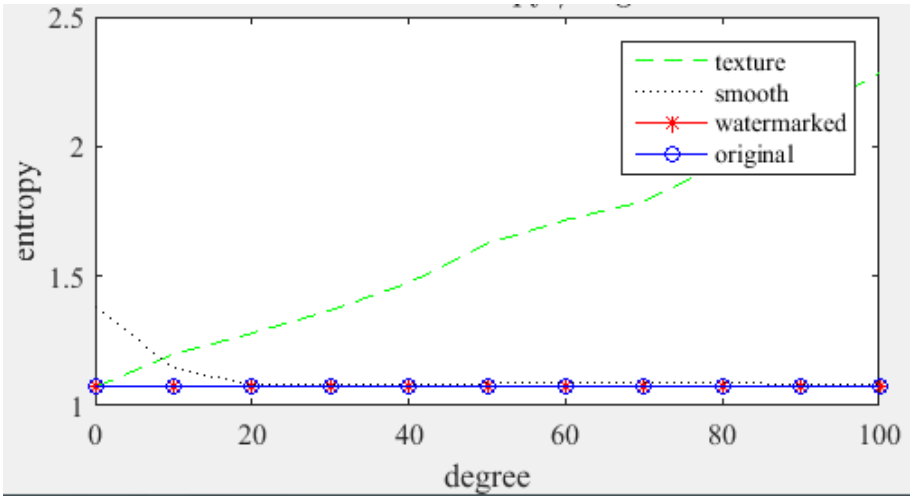


Figure 3.5 Performances entropie / degré de décomposition polynomiale

3.4.3 Analyse d'invisibilité

Les tests de transparence perceptive sont effectués pour vérifier comment la dégradation apparaît dans l'image médicale après l'insertion du watermark. L'algorithme proposé est testé sur différentes modalités d'images médicales (IRM, rayons X, échographie, CT, PET et mammographie). Afin de solidifier les résultats obtenus, nous avons aussi effectué des tests sur 120 images médicales de test et le *watermark* (3). La figure 3.6 montre les valeurs PSNR calculées entre les images médicales originales et les images médicales tatouée. La valeur de PSNR la plus élevée atteinte est de 70,7865 dB, tandis que la valeur 55,2436 dB représente la valeur la plus faible. La figure 3.7 illustre les mesures NC calculées des *watermark* extraits des images médicales tatouée. La plus haute valeur NC atteinte est égale à 1 tandis que la plus basse est égale à 0.9999.

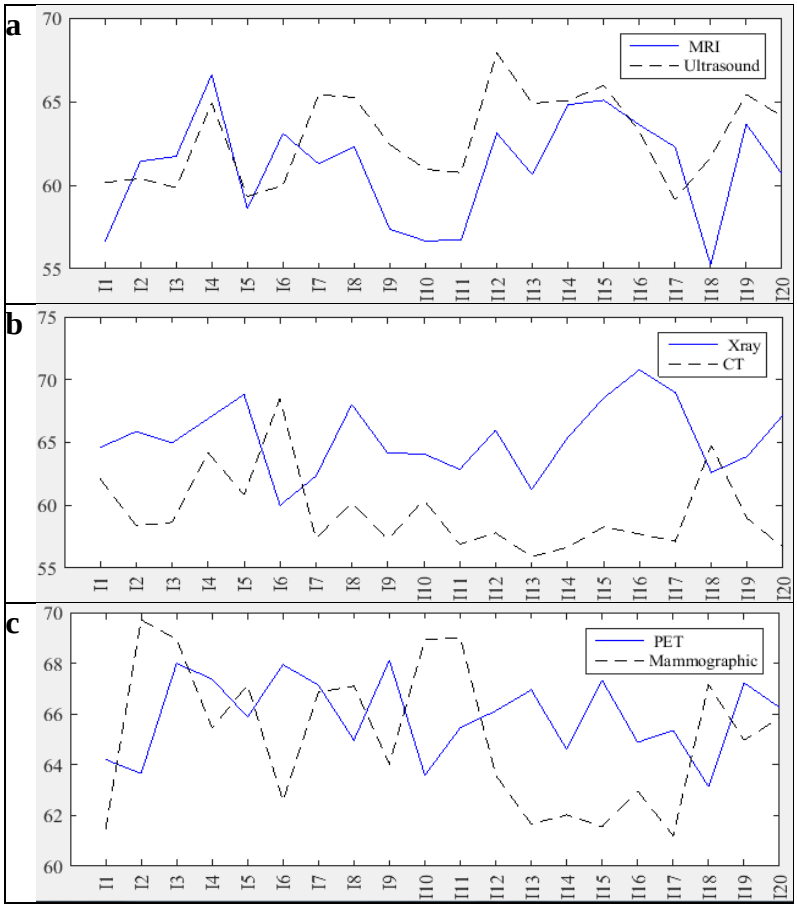


Figure 3.6 Courbes du PSNR en dB pour différentes images médicales de test : a. IRM et échographie, b. radiographie et CT, c. TEP et mammographie.

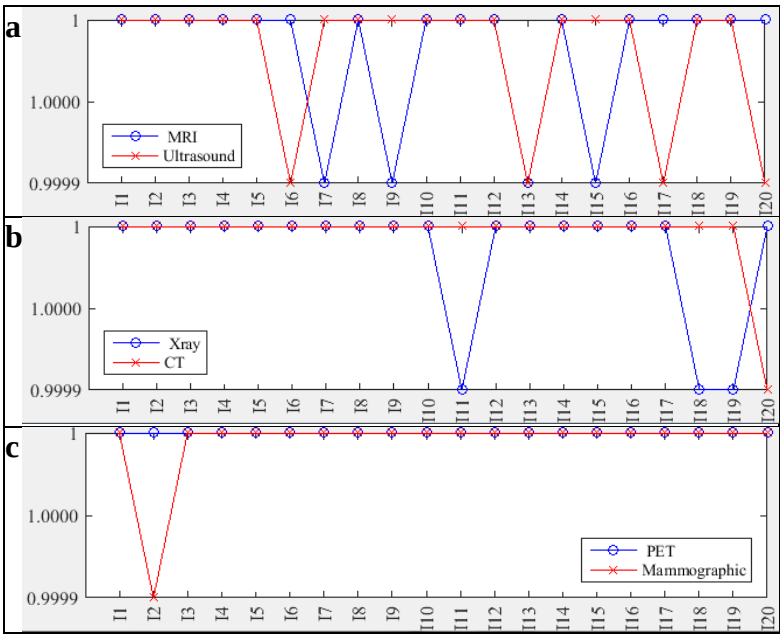


Figure 3.7 Courbes de la NC pour différentes images médicales de test : a. IRM et échographie, b. radiographie et CT, c. TEP et mammographie.

Pour illustrer les principales étapes de notre méthode, les tableaux suivants (3-1, 3-2, 3-3) montrent la décomposition de l'image médicale (composantes structure et texture), les images médicales tatouée avec les 6 modalités et les watermarks extraits. Un échantillon de 12 images médicales est utilisé pour cette illustration. De plus, comme on peut le voir dans les tableaux, les images médicales tatouées et les images originales sont similaires et le processus d'intégration du *watermark* ne présente aucune altération observable.

Les valeurs PSNR et NC du schéma proposé sont calculées pour 12 images médicales et comparées à 5 schémas existants dans un cas sans attaque [57], [58], [62], [67], [90]. Le tableau 3-4 montre que la moyenne des valeurs PSNR obtenues (61,7769 dB) est modérée et que la moyenne des valeurs NC est très proche de la valeur idéale. Les résultats obtenus sont beaucoup plus élevés que les méthodes rapportées. Ainsi, notre schéma est plus efficace en fonction du facteur d'imperceptibilité.

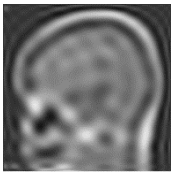
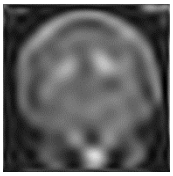
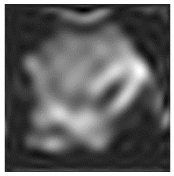
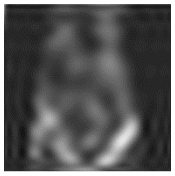
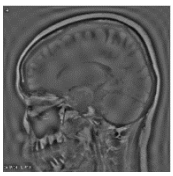
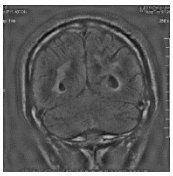
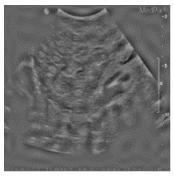
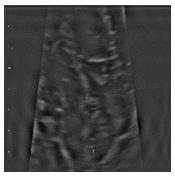
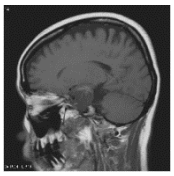
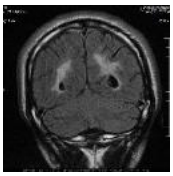
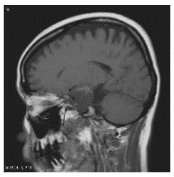
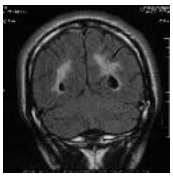
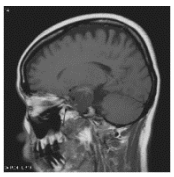
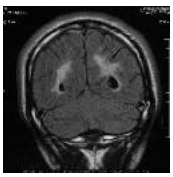
décomposition d'image	structure				
	texture				
Image tatouée **1**					
watermark extrait **1**		Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018
image taouée **2**					
Watermark extrait **2**					
image tatouée **3**					
watermark extrait **3**					

TABLE 3-1 Résultats dans le cas sans attaques de la méthode proposée pour deux modalités d'images médicales : IRM et échographie

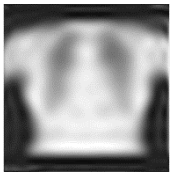
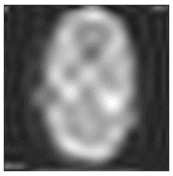
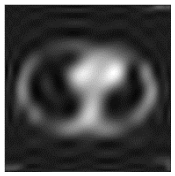
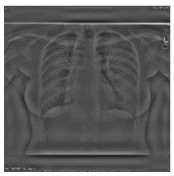
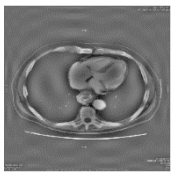
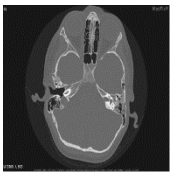
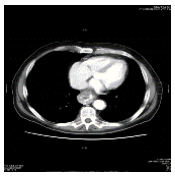
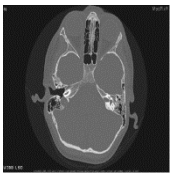
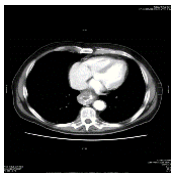
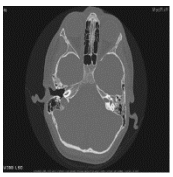
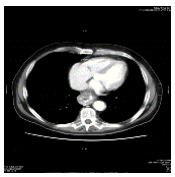
décomposition d'image	structure				
	Texture				
Image tatouée **1**					
watermark extrait **1**		Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018
image taouée **2**					
Watermark extrait **2**					
image tatouée **3**					
watermark extrait **3**					

TABLE 3-2 Résultats dans le cas sans attaques de la méthode proposée pour deux modalités d'images médicales : X-ray et CT

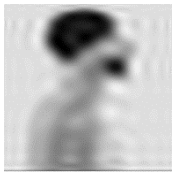
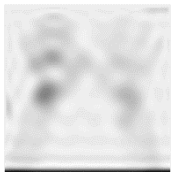
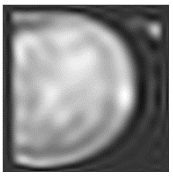
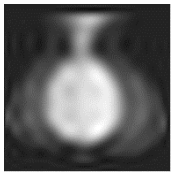
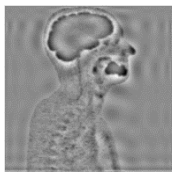
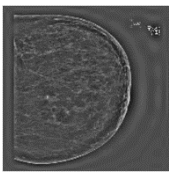
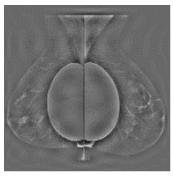
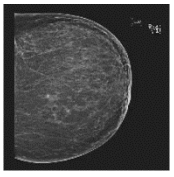
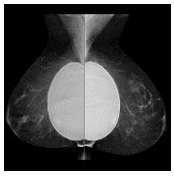
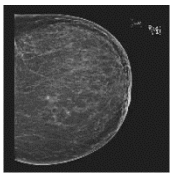
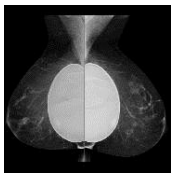
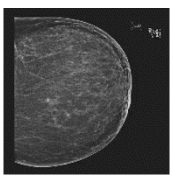
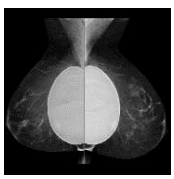
décomposition d'image	structure				
	texture				
Image tatouée **1**					
watermark extrait **1**		Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018	Patient ID: F2018 Name of the patient: M. S Doctor ID: S2018 Name of the doctor: Dr. A Date: 01.08.2018
image taouée **2**					
Watermark extrait **2**					
image tatouée **3**					
watermark extrait **3**					

TABLE 3-3 Résultats dans le cas sans attaques de la méthode proposée pour deux modalités d'images médicales : PET et Mammographie

méthode	Image de test	PSNR	NC
[62]	*IRM*	48.9900	0.9230
	US	50.2100	0.9551
	X-ray	55.0600	0.9692
	CT	47.1800	0.9827
	Moyenne	50.3600	0.9575
[57]	*X-ray*	46.3698	NA
	Moyenne	46.3698	NA
[90]	*IRM*	48 .7200	NA
	Moyenne	48 .7200	NA
[58]	CT	46.5122	NA
	Moyenne	46.5122	NA
[67]	*IRM*	48.5362	0.9932
	US	45.0161	1.0000
	CT	43.2518	1.0000
	Moyenne	45.9372	0.9977
proposée	*IRM 1*	**56.5962**	**1.0000**
	IRM 2	**60.1481**	**1.0000**
	US 1	**60.1514**	**1.0000**
	US 2	**64.8967**	**1.0000**
	X-ray 1	**64.6067**	**1.0000**
	X-ray 2	**62.2407**	**1.0000**
	CT 1	**62.1001**	**1.0000**
	CT 2	**56.6492**	**1.0000**
	PET 1	**64.2074**	**1.0000**
	PET 2	**63.6526**	**1.0000**
	Mammo 1	**61.4457**	**1.0000**
	Mammo 2	**64.6282**	**1.0000**
	Moyenne	**61,7769**	**1.0000**

TABLE 3-4 Comparaison du PSNR (dB) et de la valeur NC de la méthode proposée avec les méthodes existantes

La carte de dissimilarité locale est réalisée entre les images médicales d'entrées et les images tatouées pour mieux visualiser la présence du *watermark* (Figure 3.8). Cependant, ces petites dégradations des images tatouées ne sont pas susceptibles de modifier les informations du diagnostic. Cela indique que le système de tatouage proposé est capable de produire des images médicales tatouées de bonne qualité et d'atteindre le niveau d'imperceptibilité requis.

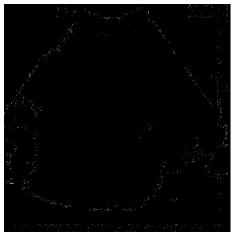
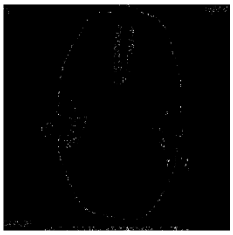
IRM	***Ultrasons***	***X-ray***
		
CT	***PET***	***Mammographie***
		

Figure 3.8 La LDM des images de tests

3.4.4 Analyse de robustesse

Lors de la manipulation d'images médicales tatouées, ces dernières peuvent être modifiées par diverses attaques involontaires et volontaires de traitement d'image. Par conséquent, il est crucial d'évaluer la robustesse de l'approche proposée dans un environnement d'attaque. Dans ce but, un ensemble de 6 images médicales filtrées par le *watermark* (3) sont soumises aux attaques suivantes : Compression JPEG, bruit gaussien, bruit Salt & Pepper, filtrage médian, accentuation, égalisation d'histogramme et rotation.

Dans le tableau 3-5, nous présentons un exemple du processus d'extraction des 3 *watermarks* de test à partir d'une image médicale IRM filtrée. Où QF, V, D et K font référence au facteur de qualité de la compression JPEG, à la variance du bruit blanc gaussien additif, à la densité du bruit poivre et sel et au degré de rotation, respectivement.

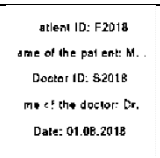
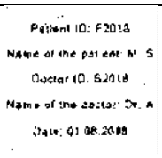
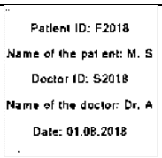
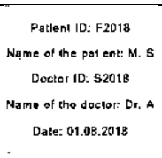
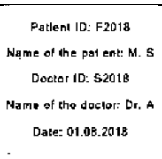
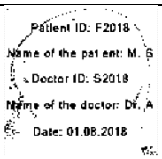
		Watermark 1	**Watermark 2**	**Watermark 3**
Compression JPEG	QF=90	 NC = 0.9318	 NC = 0.9810	 NC =0.9984
Bruit Gaussien	V = 0.01	 NC = 0.9040	 NC =0.8530	 NC = 0.9271
Bruit poivre et sel	D= 0.02	 NC = 0.9223	 NC = 0.8746	 NC = 0.9701
Filtre médian	[3x3]	 NC = 0.9986	 NC = 0.9995	 NC = 0.9992
Sharpening	[3x3]	 NC = 0.9952	 NC = 0.9994	 NC = 0.9977
Egalisation d'histogramme	[3x3]	 NC = 0.9952	 NC = 0.9994	 NC = 0.9977
Rotation	K = 10°	 NC =0.7837	 NC =0.7980	 NC = 0.9318

TABLE 3-5 Watermarks extraits et leurs valeurs NC après diverses attaques

3.4.4.1 *Robustesse à la compression JPEG*

L'attaque de la compression JPEG est caractérisée par la réduction de la bande passante et des exigences de stockage pour la transmission. Le tableau 3-6 montre les valeurs NC obtenues pour les *watermarks* extraits par rapport aux systèmes [62] [74] [76] [68]. Cette comparaison a été effectuée en fonction de différentes valeurs de QF (90 et 50). Notre méthode a atteint, dans la plupart des cas, les valeurs NC les plus élevées.

Méthode	**Images de tests**	**Qf = 90**	**Qf = 50**
[62]	*IRM*	0.9806	0.5945
	US	0.9314	0.6067
	X-ray	0.9713	0.7125
	CT	0.9806	0.6404
[57]	*X-ray*	0.5487	NA
[58]	CT	0.4596	NA
[68]	*IRM*	NA	0.8734
	US	NA	0.8916
	X-ray	NA	0.8337
	CT	NA	0.8793
	PET	NA	0.8879
	Mammographie	NA	0.7525
proposée	*IRM*	**0.9984**	**0.8837**
	US	**0.9992**	**0.8222**
	X-ray	**0.9999**	**0.9356**
	CT	**0.9974**	**0.8479**
	PET	**0.9999**	**0.9433**
	Mammographie	**0.9999**	**0.8380**

TABLE 3-6 Variation de la corrélation normalisée (NC) contre l'attaque de compression JPEG

3.4.4.2 *Robustesse à l'ajout de bruit*

Dans ce test, nous avons utilisé un bruit poivre et sel avec une densité de bruit de 0,1 et un bruit blanc additif gaussien avec une variance égale à 0,002. Les valeurs NC obtenues sont présentées dans le tableau 3-7. Ces résultats indiquent que la technique proposée résiste à différents types de bruit.

méthode	**Images de test**	**D = 0.1**	**V = 0.002**
[62]	*IRM*	0.5817	0.8135
	US	0.7072	0.8049
	X-ray	0.0132	0.9322
	CT	0.7532	0.8620
[57]	*X-ray*	0.9503	NA
[58]	CT	0.9502	0.9763
proposée	*IRM*	**0.9701**	**0.9228**
	US	**0.9879**	**0.9379**
	X-ray	**0.9978**	**0.9378**
	CT	**0.9709**	**0.9292**
	PET	**0.9700**	**0.9330**
	Mammographie	**0.9590**	**0.9190**

TABLE 3-7 Variation de la corrélation normalisée (NC) contre l'attaque d'ajout de bruit

3.4.4.3 *Robustesse aux attaques de filtrage*

Le filtre médian [3x3] est appliqué aux images médicales filtrées, puis les images filtrées sont extraites à l'aide du système proposé. Nous avons testé la robustesse de notre schéma contre le filtre médian avec différentes tailles de fenêtre [2x2], [3x3] et [9x9]. Le tableau 3-8 résume les résultats obtenus. On observe que notre méthode est robuste contre cette attaque, en particulier dans le cas de la taille de filtre [3x3].

méthode	Images de test	[2x2]	[3x3]	[9x9]
[62]	*IRM*	0.9700	NA	NA
	US	0.8943	NA	NA
	X-ray	0.9538	NA	NA
	CT	0.9607	NA	NA
[57]	*X-ray*	NA	0.5439	NA
[58]	CT	NA	0.9502	NA
[68]	*IRM*	NA	NA	0.8766
	US	NA	NA	0.8946
	X-ray	NA	NA	0.8689
	CT	NA	NA	0.8826
	PET	NA	NA	0.8873
	Mammographie	NA	NA	0.8051
Proposée	*IRM*	**0.9678**	**0.9855**	**0.8536**
	US	**0.9123**	**0.9817**	**0.8956**
	X-ray	**0.9895**	**0.9908**	**0.9499**
	CT	**0.9632**	**0.9966**	**0.8848**
	PET	**0.9894**	**0.9959**	**0.9846**
	Mammographie	**0.8756**	**0.9603**	**0.8389**

TABLE 3-8 Variation de la corrélation normalisée (NC) contre l'attaque de filtrage

3.4.4.4 *Robustesse à l'accentuation et l'égalisation d'histogramme*

Les images médicales filtrées sont soumises à une attaque d'accentuation de la netteté avec un masque (3x3) et à une attaque d'égalisation d'histogramme (HE). Le tableau 3-9 rapporte la valeur NC obtenue sous ces attaques. Ces résultats démontrent que notre schéma résiste aux attaques d'accentuation et d'égalisation d'histogramme.

méthode	Images de tests	Sharpening	HE
[62]	*IRM*	0.9408	0.9689
	US	0.9661	0.9720
	X-ray	0.9661	0.9629
	CT	0.9674	0.9708
[57]	*X-ray*	0.5053	0.5044
[58]	CT	0.5190	0.5229
[68]	*IRM*	0.8917	0.8939
	US	0.8984	0.8939
	X-ray	0.8825	0.8790
	CT	0.8965	0.8939
	PET	0.8946	0.6076
	Mammographie	0.8514	0.8296
Proposée	*IRM*	**0.9977**	**0.9989**
	US	**0.9983**	**0.9986**
	X-ray	**0.9989**	**0.9992**
	CT	**0.9967**	**0.9978**
	PET	**0.9990**	**0.9986**
	Mammographie	**0.9984**	**0.9985**

TABLE 3-9 Variation de la corrélation normalisée (NC) contre l'attaque d'accentuation et égalisation d'histogramme

3.4.4.5 *Robustesse à la rotation*

Les images médicales filtrées sont soumises à une rotation de deux degrés différents : 10° et 30°. Nous remarquons du le tableau 3-10 l'efficacité du processus d'incorporation qui a pour résultat de meilleures valeurs NC comparées aux schémas [57] [58] [68]. Notre système est conçu pour être invariant aux attaques par rotation.

méthode	**Images de tests**	**K = 10°**	**K = 30°**
[57]	*X-ray*	0.5439	NA
[58]	CT	0.9579	NA
[68]	*IRM*	NA	0.8869
	US	NA	0.8934
	X-ray	NA	0.8653
	CT	NA	0.8881
	PET	NA	0.8901
	Mammographie	NA	0.8045
Proposée	*IRM*	**0.9318**	**0.8364**
	US	**0.9426**	**0.8182**
	X-ray	**0.9619**	**0.8654**
	CT	**0.9594**	**0.8883**
	PET	**0.9610**	**0.8986**
	Mammographie	**0.9502**	**0.8171**

TABLE 3-10 Variation de la corrélation normalisée (NC) contre la rotation

3.4.5 Analyse de capacité

Pour évaluer la performance globale de la méthode proposée, la capacité est une autre propriété importante du tatouage d'images médicales. Elle fait référence à la quantité d'informations intégrées dans l'image hôte, exprimée en bits par pixel (BPP). Nous comparons notre schéma avec [62], [57] [58] et [91] selon 5 capacités différentes. Le tableau 3-11 montre que les valeurs PSNR obtenues avec notre méthode sont meilleures que les valeurs PSNR obtenues par les autres systèmes.

Taille	méthode	PSNR
64 x 64	[57]	46.3698
	[58]	46.5122
	Proposée	**63.4072**
80 x 80	[91]	58.6617
	Proposée	**62.8344**
104 x 104	[91]	57.4961
	Proposée	**62.1152**
128 x 128	[62]	50.3600
	Proposée	**61.5377**
140 x 140	[91]	56.1818
	Proposée	**61.2123**

TABLE 3-11 Performance de la technique de tatouage proposée en variant la taille du watermark

3.4.6 Analyse des faux positifs

Afin d'évaluer les performances de détection du système proposé, il convient d'analyser les cas de faux positifs. Un faux positif est le résultat de l'extraction d'un *watermark* d'une image non tatouée. Des expériences de l'algorithme d'extraction du *watermark* ont été réalisées sur 100 images médicales non tatouées extraites de la base de données d'images médicales MedPix (MedPixTM) et un *watermark*. Le tableau 3-12 illustre un exemple des résultats subjectifs et objectifs pour 4 images non tatouées. On peut constater à partir de ces exemples que le faux positif survient lorsque le *watermark* extrait révèle une trace visuelle du *watermark* original. Ainsi, nous considérons qu'un faux positif se produit si la valeur NC du *watermark* extrait est supérieure à 0,6 [62]. Nous avons obtenu zéro cas de faux positifs avec notre algorithme d'extraction, ce qui équivaut à une valeur de niveau de précision égale à 1 selon l'équation (58). Notre méthode satisfait les exigences de sécurité du *watermark* [92].

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive} \tag{60}$$

3.4.7 Analyse du temps d'exécution

Le temps d'exécution moyen de la méthode de tatouage proposée est évalué pour chaque modalité d'image médicale. D'après le tableau 3-13, on peut observer que notre système est efficace en termes de temps d'exécution.

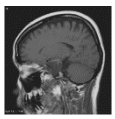
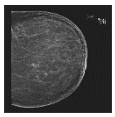
Image non tatouée	**Watermark extrait**	**NC**	**Image non tatouée**	**Watermark extrait**	**NC**
		0.0968			0.0327
		0.0502			0.0370

TABLE 3-12 Résultats des Faux Positifs de notre méthode de tatouage

Méthode	**Temps d'exécution (s)**	
[62]	***moyenne***	29.95
[58], [91], [68]	**-**	NA
proposée	*IRM*	**10.82**
	Ultrasound	**10.96**
	X-ray	**10.94**
	CT	**10.69**
	PET	**10.76**
	Mammographie	**10.71**
	moyenne	**10.81**

TABLE 3-13 Résultats du temps d'exécution de notre méthode de tatouage

3.5 Conclusion

Dans ce chapitre, une nouvelle technique de tatouage d'images médicales de différentes modalités basée sur la décomposition polynomiale a été présentée. La caractéristique principale de cette décomposition est la sélection automatique de la zone d'insertion du *watermark* qui nous permet de répandre l'information du *watermark* sur toute l'image médicale de sorte qu'il soit difficile de détecter son existence. Sur la base des résultats expérimentaux et des comparaisons entre ce travail et les travaux précédents, nous affirmons que le schéma proposé préserve la fidélité de l'image médicale originale et de sa version tatouée. De plus, notre schéma résiste à différents attaques ce qui démontre sa robustesse. Compte tenu des attributs de notre schéma, un bon compromis entre robustesse, imperceptibilité et capacité est atteint en respectant la spécificité des images médicales.

Chapitre 4. Tatouage des images médicales basé sur les Transformées d'Hermite et de Legendre

Sommaire

4.1 Introduction..... 107

4.2 Tatouage sécurisé des images médicales basé sur la TH 107

4.3 Tatouage robuste basé sur la transformée de Legendre..... 128

4.4 Conclusion 135

4.1 Introduction

Dans nos travaux précédents, nous avons exploité la transformée polynomiale de Chebychev [10]. Les résultats expérimentaux démontrent que cette méthode fonctionne de manière cohérente sur une base de 120 images médicales comprenant 6 modalités (IRM, US, X-ray, CT, PET et mammographie). Deux évaluations principales ont été réalisées : 1) l'imperceptibilité qui est mesurée par le PSNR (63,0151 dB), NC (0,9999) et la LDM; 2) la robustesse qui est testée contre 7 attaques (compression JPEG, bruit gaussien, bruit Poivre et Sel, filtrage médian, Sharpening, égalisation d'histogramme et rotation). Aussi, nous avons obtenu zéro cas de faux positifs par l'utilisation de notre méthode. Seulement, la carte de dissimilarité utilisée pour visualiser la différence perceptuelle entre l'image originale et tatouée a montré la présence de quelques petites altérations. Cela nous a mené à améliorer notre méthode de tatouage afin de mieux l'adapter au contexte médical.

En partant de ce principe, nous présentons dans ce chapitre deux nouvelles approches de tatouage d'images médicales plus efficaces. La première approche se base sur la transformée d'Hermite. L'élaboration d'une telle approche est justifiée par plusieurs motivations. Nous citons en l'occurrence les deux objectifs suivants:

- Préparer l'image médicale pour l'insertion du *watermark* afin de fournir une meilleure stratégie de sélection du ROI en utilisant une autre famille de transformées polynomiales qui représente un bon modèle du système visuel humain (HVS), combiné avec une technique de fenêtrage adaptatif pour mieux sélectionner les régions texturées de l'image dans un nombre réduit de blocs.

- renforcer la sécurité du schéma proposé en appliquant la transformée d'Arnold (AT) au *watermark* avant son insertion tout en préservant un niveau optimal entre les facteurs de robustesse et d'imperceptibilité.

4.2 Tatouage sécurisé des images médicales basé sur la transformée d'Hermite

Dans cette section, nous présentons une nouvelle approche de tatouage sécurisée des images médicales basée sur la transformée d'Hermite et une technique de fenêtrage adaptatif. La

sécurité de cette technique se manifeste par l'utilisation de la transformée d'Arnold pour chiffrer le *watermark.*

4.2.1 Prétraitement

Tout d'abord, la transformée d'Hermite est utilisée pour extraire la composante de texture. Ensuite, une technique de fenêtrage adaptatif est utilisée pour distinguer les blocs texturés des blocs non-texturés. Ce choix est motivé par le fait que les effets de masquage « *Masquing effects »* sont évidents dans les régions de l'image à fort contraste selon l'HVS. Cela signifie que l'HVS supporte des distorsions présentent dans les zones les plus texturées que dans les zones lisses. Par conséquent, la sélection des blocs texturés permet une capacité d'insertion élevée sans problème de distorsion perceptive. Ces blocs, qui sont extraits de la composante texture obtenue par la transformée d'Hermite, sont choisis pour l'insertion du *watermark*. Nous présentons dans ce qui suit les principes de base des techniques utilisées.

4.2.1.1 *Transformée d'Hermite*

La transformée d'Hermite (HT *Hermite Transform*) est un cas particulier des transformées polynomiales. Elle a été appliquée à l'origine en tant que modèle mathématique qui permet d'interpréter les champs réceptifs dans les premiers stades du système de vision humaine (HVS) [93], [94]. Cette propriété est d'une plus grande importance dans le traitement des images, étant donné qu'elle permet un codage efficace des informations visuelles pertinentes pour la perception humaine. Sa popularité a augmenté avec son application sur différents domaines de traitement d'image tels que la compression d'image, l'indexation d'image, et la fusion d'image [95], [96]. Plus spécifiquement, cette transformée est très efficace en analyse d'image (détection et extraction de caractéristiques d'image) [97], [98]. Cependant, à notre connaissance, la HT n'a pas attiré beaucoup d'intérêt pour les applications de tatouage d'images médicales. Pour cette raison, notre étude a cherché à améliorer l'efficacité de cette transformée dans un tel domaine.

Les polynômes d'Hermite satisfont l'équation différentielle (22) sous les conditions suivantes :

$$\sigma(x) = 1\,, \qquad \omega(x) = e^{x^{-2}}, \qquad \tau(\mathrm{x}) = -2x \; et \; \lambda_n = 2n \tag{61}$$

Les polynômes orthogonaux d'Hermite $H_n(x)$ d'ordre n sont définit par :

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{x^{-2}} \, , n \geq 0 \, , x \in]-\infty, \infty[\tag{62}$$

Les polynômes d'Hermite sont orthogonaux sur l'intervalle $]-\infty, \infty[$ relativement à la function de poids $\omega(x) = e^{x^{-2}}$ et vérifient la relation d'orthogonalité suivante :

$$\int_{-\infty}^{\infty} H_n(x) H_m(x) e^{x^{-2}} \, dx = 2^n \, k_n \, \delta_{n,m} \, , \; k_n = n! \sqrt{\pi} \tag{63}$$

Avec $\delta_{n,m}$ delta de Kronecker qui est définie par :

$$\delta_{n,m} = \begin{cases} 0 \, ; & n \neq m \\ 1 \, ; & \text{n} = m \end{cases} \tag{64}$$

La version normalisée de ces polynômes est mise à l'échelle et modulée par une gaussienne $x \rightarrow x/\sigma$ et normalisée par $\sqrt{k_n}$

Ils satisfont la relation de récurrence à trois termes suivante :

$$H_{n+1}(x) = 2xH_n(x) - 2nH_{n-1}(x), n \geq 1 \tag{65}$$

Avec $H_0(x) = 1$ et $H_1(x) = 2x$.

Dans le cas 2D, on considère la fonction de poids suivante avec un écart-type σ:

$$\omega(x, y) = \frac{1}{\sigma\sqrt{\pi}} \, exp\left[-\frac{x^2 + y^2}{2 \, \sigma^2}\right] \tag{66}$$

Cette fonction a l'avantage de constituer un bon modèle pour les profils des champs réceptifs de la vision humaine. Plus précisément, elle est utilisée comme modèle pour les réponses cellulaires simples dans le cortex visuel primaire.

Enfin, l'extraction de la composante texture de l'image se fait en se basant sur le principe général des transformations polynomiales présenté dans le chapitre 2 section 2.2 et la transformée d'Hermite qu'on vient de présenter.

4.2.1.2 *Technique de fenêtrage adaptatif*

Afin d'améliorer la robustesse et l'imperceptibilité de notre méthode de tatouage, nous établissons un processus pour extraire les régions texturées avec plus de précision dans la composante texture de l'image médicale originale. Pour cette raison, une sélection des blocs texturés est effectuée en utilisant une technique de fenêtrage adaptatif « *sliding windows technique* ». Pour se faire, l'entropie est utilisée dans cette technique. Elle représente une mesure statistique utilisée pour caractériser la texture d'une image. Elle mesure le caractère aléatoire de la distribution des intensités de niveaux de gris dans une image. C.à.d. elle permet de sélectionner les régions avec des valeurs faibles qui représentent les régions lisses tandis que les valeurs les plus élevées représentent les régions texturées. L'entropie est donnée comme suit :

$$Entropy = -\sum_{i=0}^{N-1} P_i . log_2(P_i) \tag{67}$$

Tel que P_i représente la probabilité d'occurrence du niveau i et N représente le niveau de couleur de l'image.

À la lumière des propriétés de HT présentées dans ce qui précède, en particulier son adéquation avec les champs réceptifs du HVS, les régions présentant une entropie plus élevée sont les plus texturées ce qui rend difficile à la perception de détecter les altérations dans ces régions. Ainsi, ces régions sont les plus appropriées pour l'insertion du *watermark*.

L'algorithme ci-dessous représente le pseudo code de cette technique de fenêtrage adaptatif.

Algorithme 1: pseudo code de la technique de fenêtrage adaptatif « *sliding window* »

Entrée: fenêtre (région)

Sortie: blocs avec entropie maximale

Début

Lire la partie texture de l'image originale de taille N x N

Lire la taille de la fenêtre

Initialiser la fenêtre au pixel (i=0, j=0)

Pour pixel i=0 **à** N - $size_{watermark}$ **par** pas=p **Faire**

Pour pixel j=0 **à** N - $size_{watermark}$ **par** pas=p **Faire**

Calculer l'entropie de la fenêtre courante

Sauvegarder la fenêtre de la région ayant l'entropie maximale

Fin Pour

Fin Pour

Fin

4.2.1.3 *Transformée d'Arnold*

La transformation d'Arnold, également appelée CAT Map d'Arnold (la fonction du chat) en reconnaissance du mathématicien russe Vladimir I. Arnold, est une transformation qui randomise apparemment l'organisation originale des pixels de l'image sans changer la valeur de ses pixels[99]. Cependant, si on réitère la fonction assez du temps, l'image originale réapparaît.

Si (x,y) est un point d'un pixel d'une image carrée N×N, alors la transformation du CAT Map est:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & b \\ \mathrm{a} & \mathrm{ab}+1 \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} \ mod\ N_w \tag{68}$$

Tel que a et b représentent les paramètres du chiffrement.

L'inverse de cette transformation est donnée par :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \mathrm{ab}+1 & -b \\ -\mathrm{a} & 1 \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} \ mod\ N_w \tag{69}$$

Comme cette transformation est de nature périodique, l'image originale réapparaît après un certain nombre d'itérations nommé la période. Ce nombre est utilisé comme clé secrète pour crypter le *watermark*. La période de ce processus dépend de la taille de l'image. Dans le contexte du tatouage, si le *watermark* est détecté par des pirates, ils doivent posséder la clé secrète pour récupérer le *watermark original*.

4.2.2 Approche proposée

L'approche proposée se compose de deux phases principales: l'insertion du *watermark* et l'extraction du *watermark*.

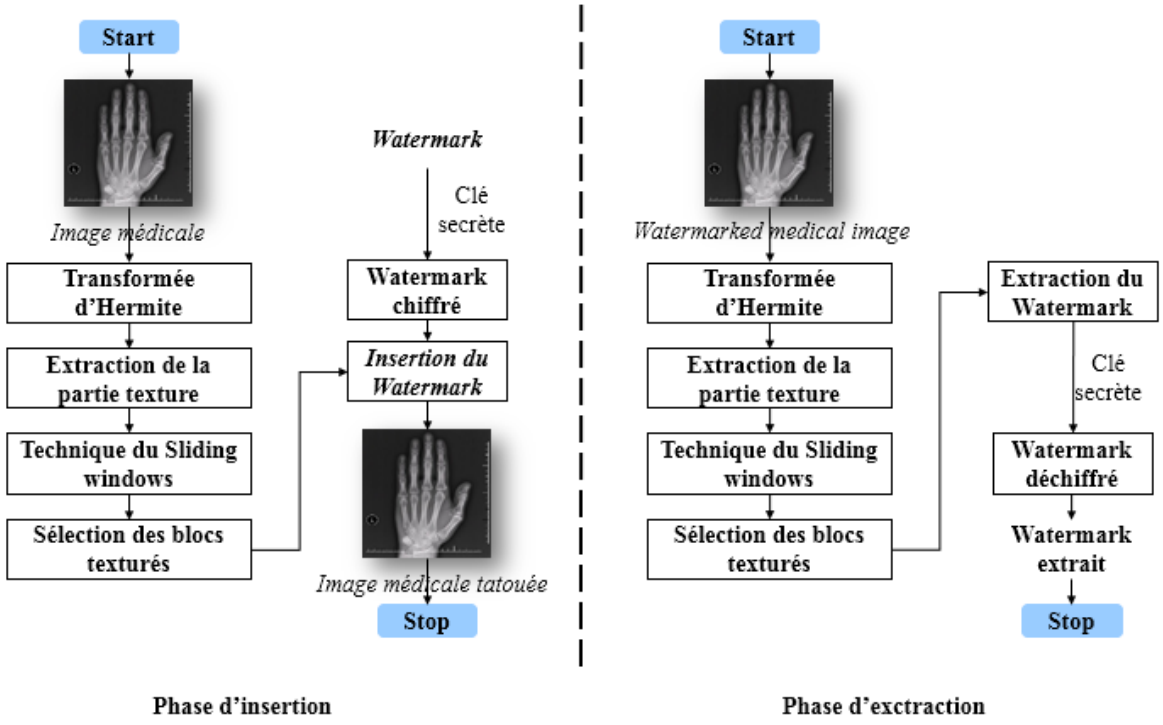


Figure 4.1 Schéma général de l'approche de tatouage proposée

Les détails concernant ces phases sont fournis dans les sous-sections suivantes. La structure générale de l'approche proposée est illustrée dans la figure 4.1.

4.2.2.1 *Algorithme d'insertion*

Tout d'abord, un prétraitement est appliqué au *watermark*. Nous voulons créer un *watermark* adapté aux applications médicales dans un contexte de sécurisation. Par exemple, l'image du *watermark* contenant les informations sur le patient et le nom de l'institution, est utilisée pour confirmer la fiabilité (intégrité et authenticité) des données tatouées. Dans cette optique, et afin d'améliorer la robustesse de l'ensemble du processus de tatouage, le chiffrement du *watermark* basé sur la transformation d'Arnold est utilisé (voir section précédente). L'idée derrière cette transformation est de rendre le *watermark* inaccessible sans une clé de décryptage à un utilisateur non autorisé. Ainsi, rendre l'extraction du *watermark* original extrêmement difficile, voire impossible, sans connaître l'algorithme de chiffrement et ses paramètres.

L'algorithme d'insertion utilisée comporte les étapes suivantes:

Etape 1. Charger l'image originale de dimensions NxN ainsi que le *watermark binaire* W.

Etape 2. Utiliser la transformation d'Arnold pour chiffrer le *watermark* $W(i,j)$ en vue d'obtenir une version chiffrée $W_s(i,j)$ en utilisant n itérations. Ce n va servir de clé K.

Etape 3. Extraire la partie texture de l'image en se basant sur la transformée d'Hermite.

Etape 4. Initialiser une fenêtre de taille 8x8 et calculer son entropie. Cette taille est choisie en prenant en considération qu'il s'agit d'une partie texture de l'image originale.

Etape 5. Appliquer la technique du fenêtrage adaptatif sur la texture T et répéter ce procédé tant que la taille de la fenêtre est inférieure à la taille du *watermark*.

Etape 6. Tester si l'entropie est croissante (entropie courante > entropie maximale) alors mettre à jour l'entropie maximale et ajouter un pas. Sinon, ajouter le pas et sauvegarder le bloc représenté par cette fenêtre.

Etape 7. Sélectionner 3 blocs (non-overlapping windows) B_k d'entropie maximale pour insérer les bits du *watermark* par l'équation suivante :

$$S_k^* = S_k + \alpha * W_s \tag{70}$$

Etape 8. Combiner la texture tatouée et la structure non modifiée pour déduire l'image médicale tatouée.

4.2.2.2 *Algorithme d'extraction*

Le processus d'extraction du *watermark* suit les étapes suivantes :

Etape 1. Charger l'image tatouée de dimensions NxN.

Etape 2. Extraire la partie texture de l'image tatouée en se basant sur la transformée d'Hermite.

Etape 3. Appliquer la technique du fenêtrage adaptatif de taille 8x8 sur la texture T et répéter ce procédé tant que la taille de la fenêtre est inférieure à la taille du *watermark.*

Etape 4. Tester si l'entropie est croissante (entropie courante > entropie maximale) alors mettre à jour l'entropie maximale et ajouter un pas. Sinon, ajouter le pas et sauvegarder le bloc représenté par cette fenêtre.

Etape 5. Sélectionner 3 blocs (non-overlapping windows) B_k d'entropie maximale pour extraire les bits du *watermark* par l'équation suivante :

$$W_s^* = (S_k^* - S_k)/\alpha \tag{71}$$

Etape 6. Appliquer la transformée inverse d'Arnold sur W_s^* pour extraire le *watermark* initial.

4.2.3 Expérimentations et résultats

L'analyse des performances du tatouage proposé est étudiée dans cette section. Les tests sont effectués sur MATLAB, sur 200 images médicales. Pour faciliter la comparaison, toutes les images originales sont redimensionnées à (512 × 512 pixels) et converties en niveaux de gris. Ces images sont extraites de la base de données Radiopaedia.org. 8 modalités d'images médicales sont utilisées pour ces tests. Un exemple de ces modalités est disponible sur la figure 4.2. Ces images sont de type IRM (imagerie par résonance magnétique), Ultrasons, Baryum, Rayons X, Fluoroscopie, Angiographie, CT (Tomographie assistée par ordinateur) et mammographie. D'autre part, deux images binaires de taille 128 x 128 sont utilisées comme des *watermarks* (figure 4.2). L'efficacité du système de proposée médical proposé est évaluée de manière approfondie en le soumettant à plusieurs attaques, notamment la compression JPEG, l'ajout de

bruit, le filtrage, le recadrage, la rotation, l'égalisation d'histogramme et d'autres attaques. La force d'insertion de notre algorithme de tatouage est fixée à 0,1, en vue d'atteindre le compromis optimal entre robustesse et imperceptibilité. En effet, les valeurs élevées de la valeur de la force du tatouage fournissent un PSNR plus faible mais avec une forte robustesse contre les différentes attaques et vice versa. C'est pourquoi nous avons sélectionné la valeur de la force de manière à ce que le PSNR soit supérieur à 50dB et qu'une forte robustesse soit assurée. Les résultats expérimentaux sont divisés en deux parties principales : la première évalue la qualité visuelle tandis que la seconde évalue la robustesse contre diverses attaques. En outre, comparée à d'autres techniques de tatouage (basées sur les moments), la performance temporelle, la capacité et l'analyse des faux positifs du schéma proposé sont données dans cette section.

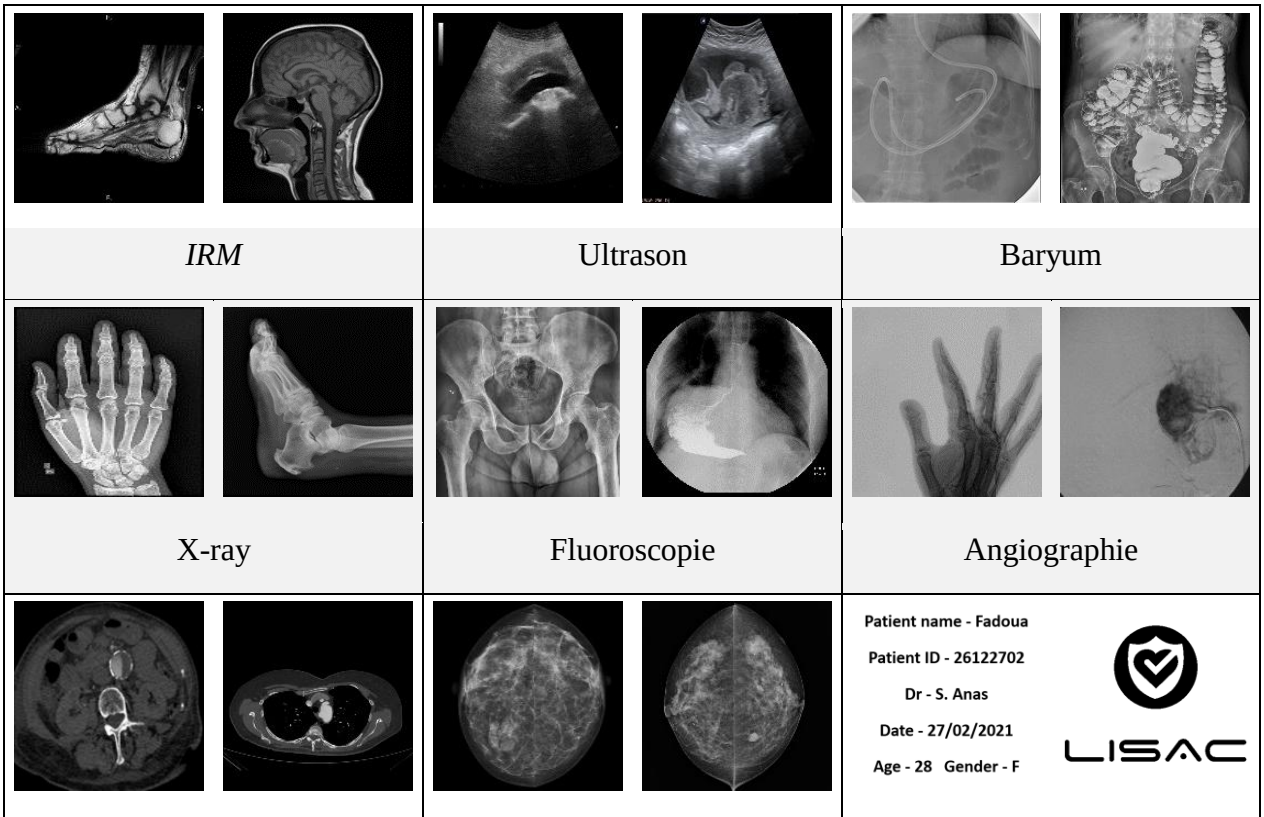


Figure 4.2 Exemple d'images médicales et des watermarks utilisés pour faire les tests

Les tests effectués de l'approche proposée est évaluée en fonction des mesures suivantes : Le rapport signal-bruit de pointe (PSNR), l'indice de similarité structurelle (SSIM), la corrélation normalisée (NC) et le taux d'erreur binaire (BER) (pour de plus amples détails, cf. le chapitre 1). En effet, plus le PSNR, la NC, la SSIM et le BER sont élevés, plus les méthodes de tatouage sont performantes.

4.2.3.1 *Analyse d'invisibilité*

Dans cette sous-section, l'évaluation de l'imperceptibilité de notre approche de tatouage est mesurée par le PSNR.

Le tableau 4-1 illustre le résultat visuel des composants résultants en utilisant notre schéma. Pour une meilleure compréhension, la première colonne est attribuée aux résultats des régions d'insertions du *watermark* sélectionnées par la HT combinée avec la technique de fenêtrage adaptatif. Chaque modalité est testée selon deux images. La deuxième colonne illustre les images médicales tatouées obtenues et la dernière colonne représente le résultat des *watermarks* extraits. On peut observer que notre technique d'insertion ne présente aucune modification observable de la qualité visuelle des images tatouée. De plus, les watermarks extraits sont similaires à leurs versions originales.

Dans le tableau 4-2, le PSNR est calculé pour les images médicales tatouées (les mêmes images illustrées dans le tableau 4-1). De plus, les valeurs de NC, SSIM et BER sont calculées pour les *watermarks* extraits en se référant au même tableau. Nous remarquons que les valeurs du PSNR sont supérieures à 61 dB. Prenons l'exemple des images d'angiographie, notre système a obtenu la valeur PSNR la plus élevée, 72,3073 dB. La valeur moyenne de la SSIM obtenu est d'environ 0,9975 tandis que les valeurs NC et BER calculées sont égales à leurs valeurs idéales dans les cas sans attaque. Cela indique que notre approche a un bon niveau d'imperceptibilité avec une extraction complète du *watermark*.

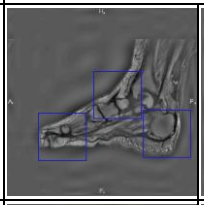
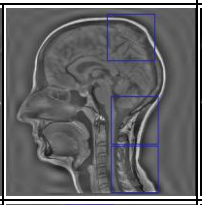
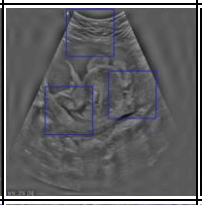
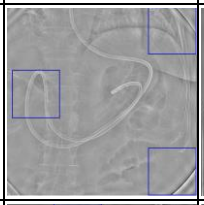
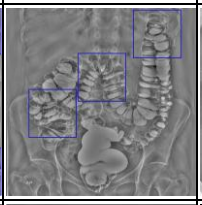
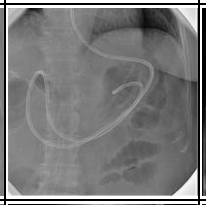
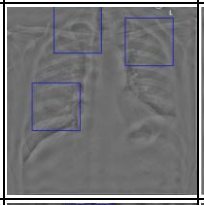
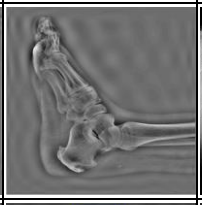
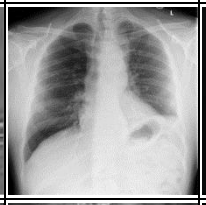
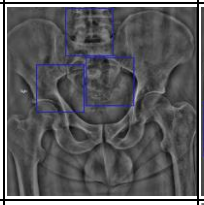
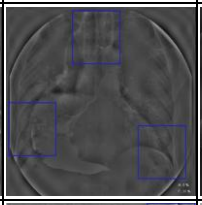
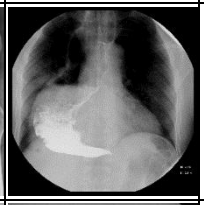
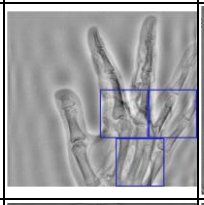
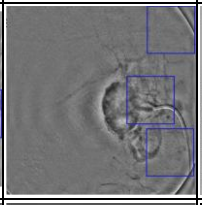
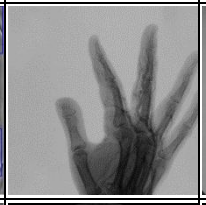
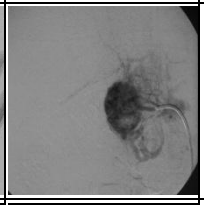
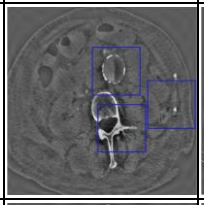
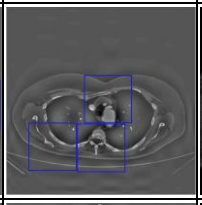
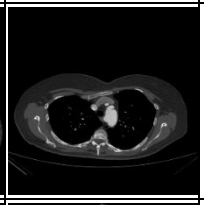
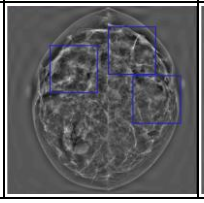
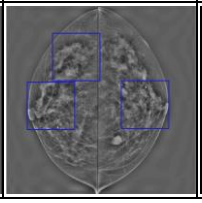
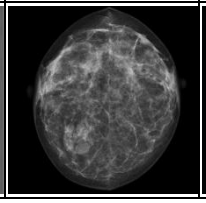
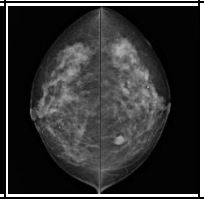
Input	Texture component		Watermarked images		Extracted watermarks	
IRM					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
ultrason					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
Baryum					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
X-ray					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
Fluoroscopie					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
Angiographie					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
CT					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC
Mammographie					Patient name - Fadoua Patient ID - 26122702 Dr - S. Anas Date - 27/02/2021 Age - 28 Gender - F	LISAC

TABLE 4-1 Résultats visuels de l'exemple d'implémentation de notre algorithme sur différents modalités

Image	PSNR	NC	SSIM	BER	Image	PSNR	NC	SSIM	BER
IRM 1	62.4249	1.0000	0.9998	0	***F 1***	63.5709	1.0000	0.9994	0
IRM 2	61.7621	1.0000	0.9997	0	***F 2***	65.0105	1.0000	0.9986	0
US 1	66.5443	1.0000	0.9973	0	***A 1***	70.1809	1.0000	0.9965	0
US 2	65.8164	1.0000	0.9989	0	***A 2***	72.3073	1.0000	0.9951	0
B 1	68.6493	1.0000	0.9964	0	***CT 1***	63.9717	1.0000	0.9996	0
B 2	62.2207	1.0000	0.9997	0	***CT 2***	64.7127	1.0000	0.9989	0
Xray 1	70.3821	1.0000	0.9959	0	***M 1***	67.5425	1.0000	0.9976	0
Xray 2	69.9783	1.0000	0.9963	0	***M 2***	68.1228	1.0000	0.9974	0

TABLE 4-2 PSNR des images tatouées

Les résultats obtenus sont comparés à ceux de [10], [22], [21] et [26] dans le tableau 4-3 en termes de PSNR et de valeurs NC. D'après ce tableau, notre schéma surpasse les méthodes similaires.

méthode	image	PSNR	NC	méthode	image	PSNR	NC
[100]	*X-ray*	60.8100	1	[86]	*X-ray*	63,4237	1
	CT	60.8900	1		*CT*	59,3747	1
	IRM	60.9200	1		*IRM*	58.3722	1
	US	60.9600	1		*US*	62.5241	1
[66]	*X-ray*	53.7501	1		*Mam*	63,0369	1
	CT	53.8454	1	**proposée**	***IRM***	**62.0935**	**1**
	IRM	52.8659	1		***US***	**66.1804**	**1**
	US	54.5383	1		***B***	**65,4350**	**1**
	Mam	53.8014	1		***X-ray***	**70.1802**	**1**
[69]	*X-ray*	56.9684	0.9998		***F***	**64,2907**	**1**
	CT	58.3692	0.9997		***A***	**71,2441**	**1**
	IRM	59.7386	0.9996		***CT***	**64.3422**	**1**
					M	**67.8327**	**1**

TABLE 4-3 Comparaison des résultats en terme de PSNR et NC

Les résultats expérimentaux sont également fournis en faisant varier la taille du *watermark*. Le tableau 4-4 présente les résultats du l'approche de tatouage proposée en termes de PSNR, NC et SSIM.

Taille du Watermark	méthode	PSNR	NC	SSIM
64 x 64	[69]	49.8995	0.9976	0.9942
	Ours	65.9478	0.9999	0.9953
128 x 128	[69]	54.4426	0.9990	0.9978
	Ours	66.4498	1.0000	0.9979
256 x 256	[69]	59.3824	0.9995	0.9997
	Ours	67.0511	1.0000	0.9998

TABLE 4-4 Comparaison des résultats en faisant varier la taille du Watermark.

Des tests ont été mises en œuvre sur 160 images médicales dans le cas sans attaque. Le tableau 4-5 montre ces expériences en termes de NC et PSNR respectivement. Nous remarquons que ces valeurs sont proches de la valeur idéale. Cela implique que les *watermarks* originaux et extraits sont similaires et sont totalement récupérés en cas d'absence d'attaques. La performance globale de notre approche varie avec des résultats satisfaisants pour chaque modalité d'image médicale.

4.2.3.2 *Analyse de robustesse*

Dans cette sous-section, la robustesse de l'approche proposée de tatouage d'images médicales est testée selon 15 diverses attaques y compris la compression JPEG, l'ajout de bruit, le filtrage, les attaques géométriques, d'accentuation, égalisation d'histogramme, etc. Ces attaques sont appliquées sur des images médicales IRM. La qualité des *watermarks* extraits est évaluée en fonction de la SSIM, la NC et le BER comme indiqué dans les tableaux 4-11, 4-12 et 4-13. Les attaques de manipulation d'images réalisées sur les images de test sont les suivantes :

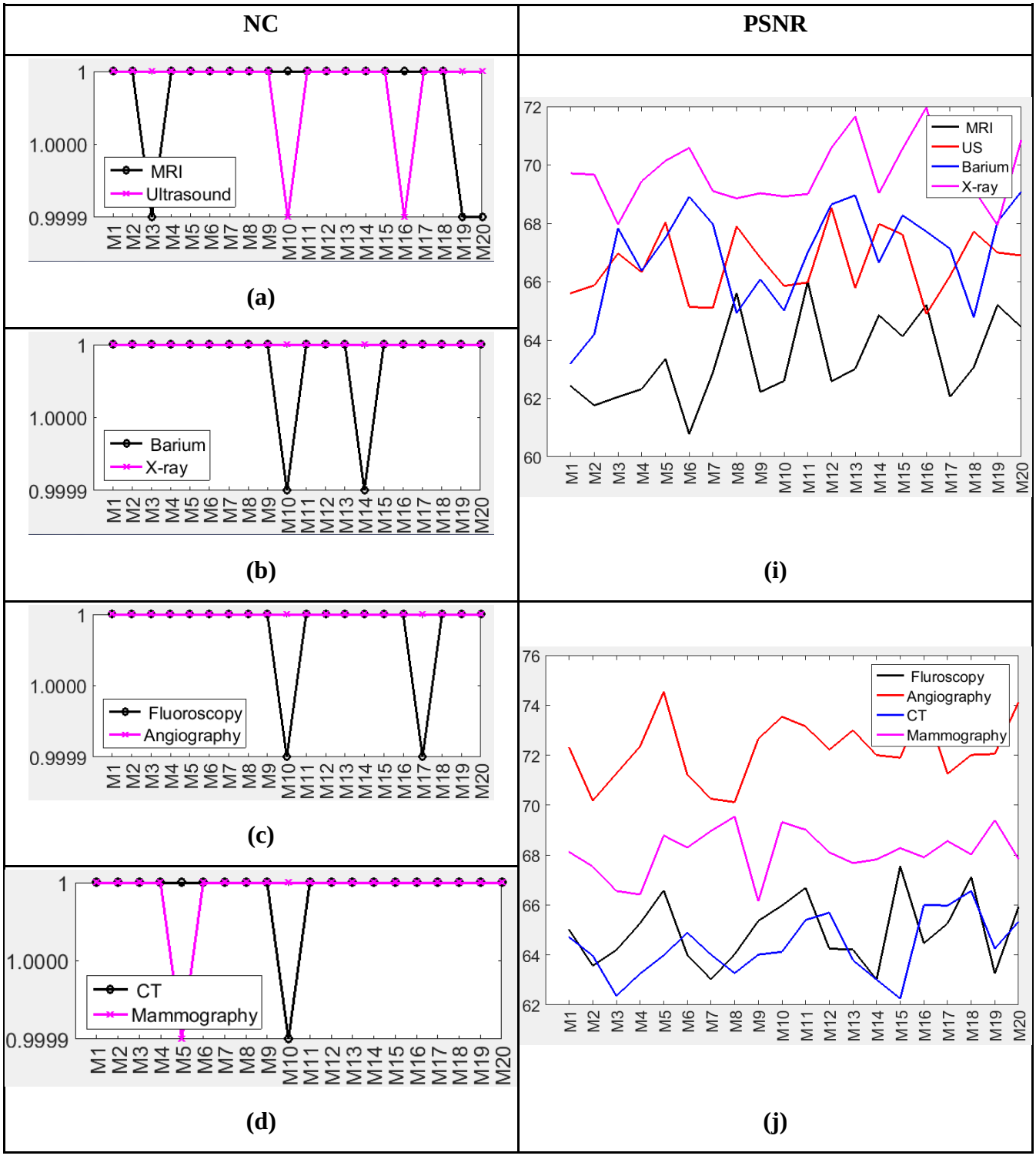


TABLE 4-5 Résultats de notre méthode e termes de PSNR et NC de 160 images médicales

a. Compression JPEG

En général, l'attaque de la compression JPEG se produit fréquemment dans les applications multimédia. Pratiquement toutes les images médicales qui sont actuellement distribuées sur Internet sont compressées. Le tableau 4-6 présente les *watermarks* extraits et leurs valeurs NC selon différents facteurs de qualité QF. On remarque que notre approche présente une bonne robustesse même si le facteur de qualité de la compression JPEG diminue.

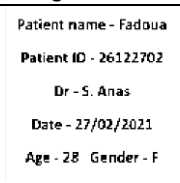
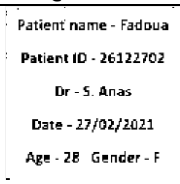
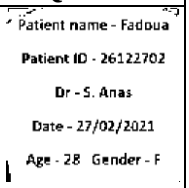
	QF = 90	**QF = 70**	**QF = 50**
Watermark 1			
NC	0.9999	0.9939	0.9595
Watermark 2			
NC	0.9999	0.9992	0.9775

TABLE 4-6 Robustesse de la méthode proposée à la compression JPEG

b. Ajout de bruit

Le succès d'une technique de tatouage dépend également de sa capacité à résister à l'ajout de bruit. Le tableau 4-7 illustre les *watermark* extraits et leurs valeurs NC avec l'ajout de quatre types de bruits, y compris les bruits Poivre et Sel avec une variance V=0,01, Gaussien avec une variance V=0,01, Poisson et Speckle. Dans la plupart des cas, l'augmentation de la quantité de bruit augmente la distorsion des images tatouée. Enfin, les résultats de robustesse sont également satisfaisants pour les attaques par ajout de bruit.

c. Filtrage

Nous avons étudié la robustesse contre les attaques de filtrage, notamment le filtrage médian, gaussien et de Wiener. D'après les résultats du tableau 4-8, *Watermark* 2 résiste mieux

que *Watermark* 1 lorsqu'il est exposé à une attaque par filtrage avec une fenêtre de taille 3 x 3. Dans la plupart des cas, notre méthode permet une extraction réussie du *watermark*.

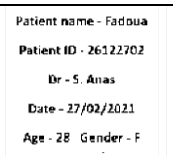
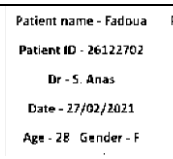
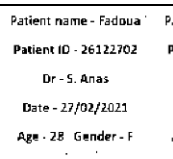
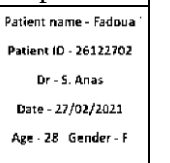
	Poivre et Sel	Gaussian	Poisson	Speckle
Watermark 1				
NC	0.9959	0.9995	0.9980	0.9997
Watermark 2				
NC	0.9989	0.9984	0.9986	0.9998

TABLE 4-7 Robustesse de la méthode proposée à l'ajout de bruit

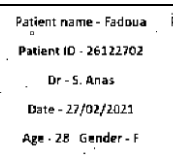
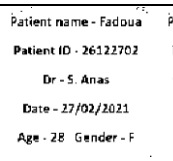
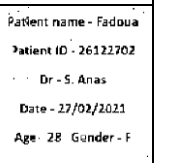
	Median	Gaussian	Wiener
Watermark 1			
NC	0.9974	0.9985	0.9962
Watermark 2			
NC	0.9998	0.9994	0.9995

TABLE 4-8 Robustesse de la méthode proposée au filtrage

d. Attaques géométriques

Les images tatouées sont soumises à un recadrage, qui consiste à supprimer certains pixels de l'image tatouées. Elles sont également soumises à une rotation d'un certain degré d'angle et à une attaque de changement d'échelle avec un certain facteur (voir Tableau 4-9).

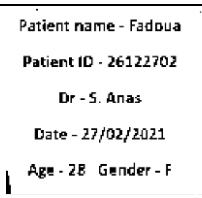
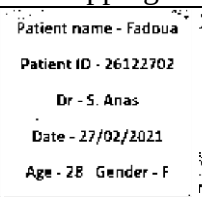
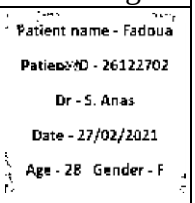
	Rotation	Cropping	scaling
Watermark1			
NC	0.9831	0.9903	0.9805
Watermark 2			
NC	0.9907	0.9958	0.9957

TABLE 4-9 Robustesse de la méthode proposée aux attaques géométriques

e. Autres attaques

D'autres attaques sont aussi utilisées pour cette évaluation de robustesse : Sharpening, Egalisation d'histogramme, Sobel et Blurring (4-10).

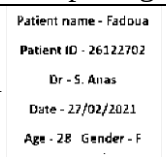
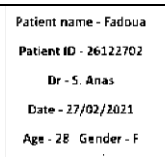
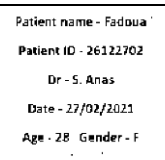
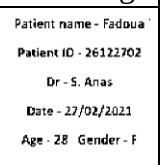
	Sharpening	HE	Sobel	Blurring
Watermark 1				
NC	0.9959	0.9995	0.9980	0.9997
Watermark 2				
NC	0.9989	0.9984	0.9986	0.9998

TABLE 4-10 Robustesse de la méthode proposée aux autres attaques

f. Comparaison de résultats

Nous présentons dans cette partie les résultats de comparaison numérique des valeurs de NC des marques extraites (Tableau 4-11, 4-12, 4-13).

Type d'attaque	**Paramètres**	[66]	[69]	**Notre méthode**
Compression JPEG	*QF = 90%*	NA	0.9886	**0.9891**
	QF = 75%	0.9780	NA	**0.9882**
Filtre Médian	*3*3*	0.9740	0.9756	**0.9802**
Filtre Gaussien	*3*3*	NA	NA	**0.9798**
Bruit Gaussien	*V = 0.0002*	0.9640	NA	**0.9745**
		NA	0,9946	**0.9952**
Bruit de Poisson		0.9590	NA	**0.9943**
Cropping	*20 %*	0.9990	NA	**0.9992**
		NA	0.8373	**0.9992**
Rotation	*5 °*	0.9350	NA	**0.9774**
Bruit Poivre et Sel	*D = 0.001*	NA	0,9735	**0.9689**
		0.9350	NA	**0.9465**
Bruit Speckle		0.9610	0.9870	**0.9868**
Sharpening		0.9590	0.9967	**0.9981**
Sobel		NA	NA	**0.9979**
Blurring		0.9560	NA	**0.9612**
HE		0.8470	0.7422	**0.8105**
Scaling		0.9550	0.9992	**0.9990**
Filtre Wiener	*3 × 3*	0.9530	0,9783	**0.9811**

TABLE 4-11 Comparaison numérique des valeurs de SSIM des watermarks extraits

Type d'attaques	**Paramètres**	[100]	[69]	[101]	**Notre méthode**
Compression JPEG	*QF = 90%*	0.9768	0.9997	1	**0.9999**
	QF = 70%	0.7876	NA	0.9940	**0.9965**
	QF = 50%	NA	NA	0.9020	**0.9205**
Filtre Médian	*3*3*	0.8413	0.9984	0.9941	**0.9986**
	*5*5*	NA	NA	0.9940	**0.9981**
Filtre Gaussien	*3*3*	NA	NA	0.9820	**0.9985**
	*5*5*	NA	NA	0.9636	**0.9973**
Bruit Gaussien	*V = 0.01*	0.7912	NA	1	**0.9989**
	V=0.0002	NA	0,9998	NA	**0.9539**
Bruit de Poisson		NA	NA	NA	**0.9983**
Cropping	*20 %*	0.8682	0.9964	NA	**0.9930**
Rotation	*5 °*	NA	NA	0.9823	**0.9869**
	10°	NA	NA	0.9941	**0.9821**
Bruit Poivre et Sel	*D = 0.01*	NA	NA	0.9940	**0.9974**
	D = 0.005	0.8468	NA	NA	**0.9984**
	D = 0.001	NA	0,9987	NA	**0.9990**
Speckle		0.9017	0.9997	NA	**0.9998**
Sharpening		NA	0.9998	NA	**0.9999**
Sobel		NA	NA	NA	**0.9997**
Blurring		NA	NA	NA	**0.9992**
HE		NA	0.9984	NA	**0.9983**
scaling	*75%*	NA	NA	0.9880	**0.9881**
	90%	0.9843	NA	NA	**0.9856**
	150%	0.9621	NA	0.9940	**0.9926**
	200%	1	NA	0.9940	**0.9985**
Filtre de Wiener	*3 × 3*	NA	0,9986	NA	**0.9987**

TABLE 4-12Comparaison numérique des valeurs de NC des watermarks extraits

Type d'attaque	**Paramètres**	[102]	[101]	**Notre méthode**
Compression JPEG	*QF = 90%*	0.0001	0	**0.0002**
	QF = 75%	0.0002	NA	**0.0011**
	QF = 70 %	NA	0.0010	**0.0012**
	QF = 50%	0.0006	0.0176	**0.0165**
Filtre Médian	*3*3*	0.1732	0.0010	**0.0011**
	*5*5*	NA	0.0010	**0.0009**
Filtre Gaussien	*3*3*	0.0530	0.0029	**0.0026**
	*5*5*	NA	0.0059	**0.0060**
Bruit Gaussien	*v=0.01*	0.0609	0	**0.0005**
Bruit de Poisson		0.0000	0	**0.0004**
Cropping	*20 %*	NA	NA	**0.0052**
Rotation	*5 °*		0.0029	**0.0027**
	10°	0.0012	0.0010	**0.0012**
Bruit Poivre et Sel	*D = 0.01*	NA	0.0010	**0.0008**
	D = 0.2	0.1131	NA	**0.0015**
Speckle		0.1835		**0.0097**
Sharpening		NA	NA	**0.1254**
Sobel		NA	NA	**0.2369**
Blurring		NA	NA	**0.1794**
HE		NA	NA	**0.1579**
Scaling	*0.75*	NA	0.0020	**0.0019**
	150 % 1.5	NA	0.0010	**0.0016**
	200 % 2	NA	0.0010	**0.0017**
Filtre Wiener	*3 × 3*	NA	NA	**0.0024**

TABLE 4-13 Comparaison numérique des valeurs de SSIM des watermarks extraits

4.2.3.3 *Analyse des faux positifs*

Afin de valoriser le niveau de la fiabilité apportée par notre technique de tatouage, nous présentons les résultats des tests de faux positifs. La détection de faux positifs (FPD *False positive detection*) est le résultat de l'extraction du *watermark* d'une image médicale non tatouée et qui n'a pas été tatouée à l'origine. Dans un tel cas, le FPD se produit qui nous mène à dire que le tatouage manque de fiabilité. Dans cette sous-section, le processus d'extraction proposé est

testé sur la même base de données que celle présentée dans ce qui précède. Quelques échantillons d'images non tatouées et les deux *watermark* W1 et W2 sont utilisés pour ces expériences. Le tableau 4-14 montre le résultat visuel des *watermarks* extraits avec leurs valeurs NC. Les valeurs obtenues sont plus grandes que 0.01. En général, nous acceptons que le FPD se produise si les NC sont supérieurs à 0,6 [62]. En gardant cela à l'esprit, le résultat obtenu pour le FPD de la technique proposée est zéro. Cependant, notre schéma surmonte le problème des faux positifs et est suffisamment sécurisé.

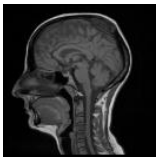
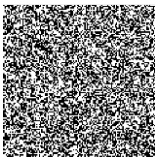
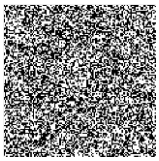
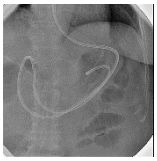
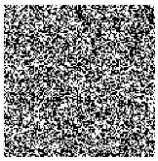
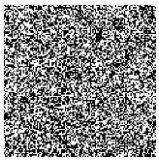
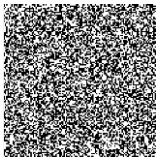
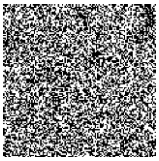
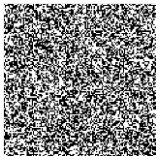
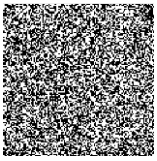
Image non tatouée	watermark 1 extrait	NC	watermark 2 extrait	NC
		0.0035		0.0017
		0.0179		0.0175
		0.0069		0.0010
		0.0096		0.0084

TABLE 4-14 Résultats des Faux Positifs

4.2.3.4 *Analyse du temps d'exécution*

Le temps d'exécution des processus d'insertion et d'extraction pour la méthode proposée du tatouage d'images médicales est évalué. D'après le tableau 4-15, nous observons que notre système est efficace en termes de temps d'exécution.

Méthode	Insertion (s)	Extraction (s)	Global (s)
[62]	-	-	29.95
[69]	4.28	4.6	8,54
[66]	10.80	5.80	16.6
[86]	-	-	10.81
Proposée	**4.17**	**4.09**	**8.26**

TABLE 4-15 performances en temps d'exécution de la méthode proposée

4.3 Tatouage robuste basé sur la transformée de Legendre

Nous proposons dans cette section, un tatouage basé sur la transformée de Legendre pour des images IRM et US [88]. L'objectif principal de ce modèle mathématique est d'approximer l'image médicale en utilisant un nombre limité de polynômes, afin d'obtenir une image de dimension spatiale plus faible [104] . Les moments de Legendre sont utilisés dans cette approche comme un moyen de réduire la complexité du calcul des moments de l'image en limitant la quantité d'information redondante par les approximations.

4.3.1 Prétraitement

En raison du caractère sensible des images médicales, en particulier les images IRM et US, l'étape du prétraitement de l'image est primordiale si on veut conserver l'information médicale intacte. En effet, la **IRM** permet la visualisation discrète des tissus mous ou des parties non osseuses du corps et donc permet de générer des images avec plus de détails et sont les plus utilisées pour faire des tests en traitement d'images. Tandis que les **Ultrasons** sont par nature de moindre qualité visuelle en raison des variations temporelles et acoustiques mais contrairement à d'autres technologies, l'US se fait en temps réel et elle est considérée la plus accessible et l'un des examens les plus fréquemment utilisés en médecine.

Nous présentons dans ce qui suit les principes fondamentaux de la transformée de Legendre en se basant sur le formalise mathématique présenté dans le chapitre 2 section 2.2.

Les polynômes de Legendre sont définis à partir de la formule de Rodriguez

$$P_n(x) = \frac{(-1)^n}{2^n n!} \frac{d^n}{2dx^n} [(1-x^2)^n], x \in]-1,1[\quad (72)$$

Les polynômes orthogonaux de Legendre satisfont la relation de récurrence à trois termes suivante :

$$(n+1)P_{n+1}(x) = (2n+1)xP_n(x) - nP_{n-1}(x) \quad (73)$$

Avec $P_0(x) = 1$ et $P_1(x) = x$.

Les polynômes de Legendre satisfont la relation d'orthogonalité relativement à la fonction de poids $\omega(x) = 1$ sur l'intervalle $]-1,1[$:

$$\int_{-1}^{1} P_n(x)P_m(x)dx = \frac{2}{2n+1}\delta_{n,m} \quad (74)$$

La décomposition de l'image médicale en composantes structure/texture est établie en se basant sur ce modèle mathématique et le modèle de décomposition d'image présenté dans le Chapitre2 (section 2.2).

4.3.2 Approche proposée

La technique proposée est une technique de tatouage robuste dont l'objectif est la protection de l'image médicale en assurant son authenticité. En effet, le *watermark* inséré représente un logo de l'hôpital pour s'assurer de l'origine de l'image.

4.3.2.1 *Algorithme d'insertion*

Dans cet algorithme, nous appliquons une décomposition polynomiale basée sur la transformée de Legendre afin d'extraire la partie texture de l'image. Cet algorithme se compose des étapes suivantes:

Etape 1. Lire l'image originale et convertir le logo choisi comme *watermark* en binaire.

Etape 2. Décomposer l'image en structure / texture en utilisant la transformée de Legendre.

Etape 3. segmenter la composante texture en blocs de tailles 8x8.

Etape 4. Insérer les bits du *watermark* w_i dans k blocs de la composante texture $T_i(t_1, \dots, t_k)$ selon une force de tatouage S par l'équation:

$$T_i^* = T_i(1 + w_i * S) \tag{75}$$

Etape 5. Combiner la texture tatouée avec la structure non modifiée en vue d'obtenir une l'image médicale tatouée.

4.3.2.2 *Algorithme d'extraction*

Dans cet algorithme, nous devons extraire la marque de l'image médicale tatouée. Cet algorithme se compose des étapes suivantes:

Etape 1. Décomposer l'image tatouée en structure / texture en utilisant la transformée de Legendre.

Etape 2. segmenter la composante texture tatouée en blocs de tailles 8x8.

Etape 3. extraire les bits du *watermark* w_i par l'équation:

$$w_i^* = \frac{T_i^*}{T_i} - 1 \tag{76}$$

Etape 4. Reconstruire le *watermark*

- Si $w_i^* < 0$ Alors $watermark_i = 0\ bit$
- Sinon $watermark_i = 1$ bit

4.3.3 Expérimentations et résultats

La technique de tatouage proposée a été testée sur 80 images médicales variées de taille 960 x 960. Les modalités IRM et US sont choisis comme images originales. Un logo binaire de taille 120 x 120 représente le *watermark.* Des exemples de ces images sont représentés sur la figure 4.5. Ces images proviennent de la base de données d'images médicales MedPix (MedPixTM). Les composantes de la décomposition polynomiale des images de tests, les images médicales tatouées et le *watermark* extrait sont illustrés dans la figure 4.5. La valeur de la force de tatouage est choisie expérimentalement et est fixée sur S=0.1. Les résultats montrent clairement que l'algorithme proposé n'affecte pas l'information du diagnostic assisté par ordinateur des images médicales. Les tests de performances sont mis en œuvre en utilisant MATLAB 2015.

Pour évaluer les performances du système proposé en termes d'invisibilité et de robustesse du *watermark*, nous utilisons les trois mesures suivantes: PSNR, NC et SSIM. (Voir chapitre 1 pour plus de détails).



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

Figure 4.3 Les images de tests: (a) et (b) la modalité IRM, (c) et (d) la modalité US, (e) le watermark

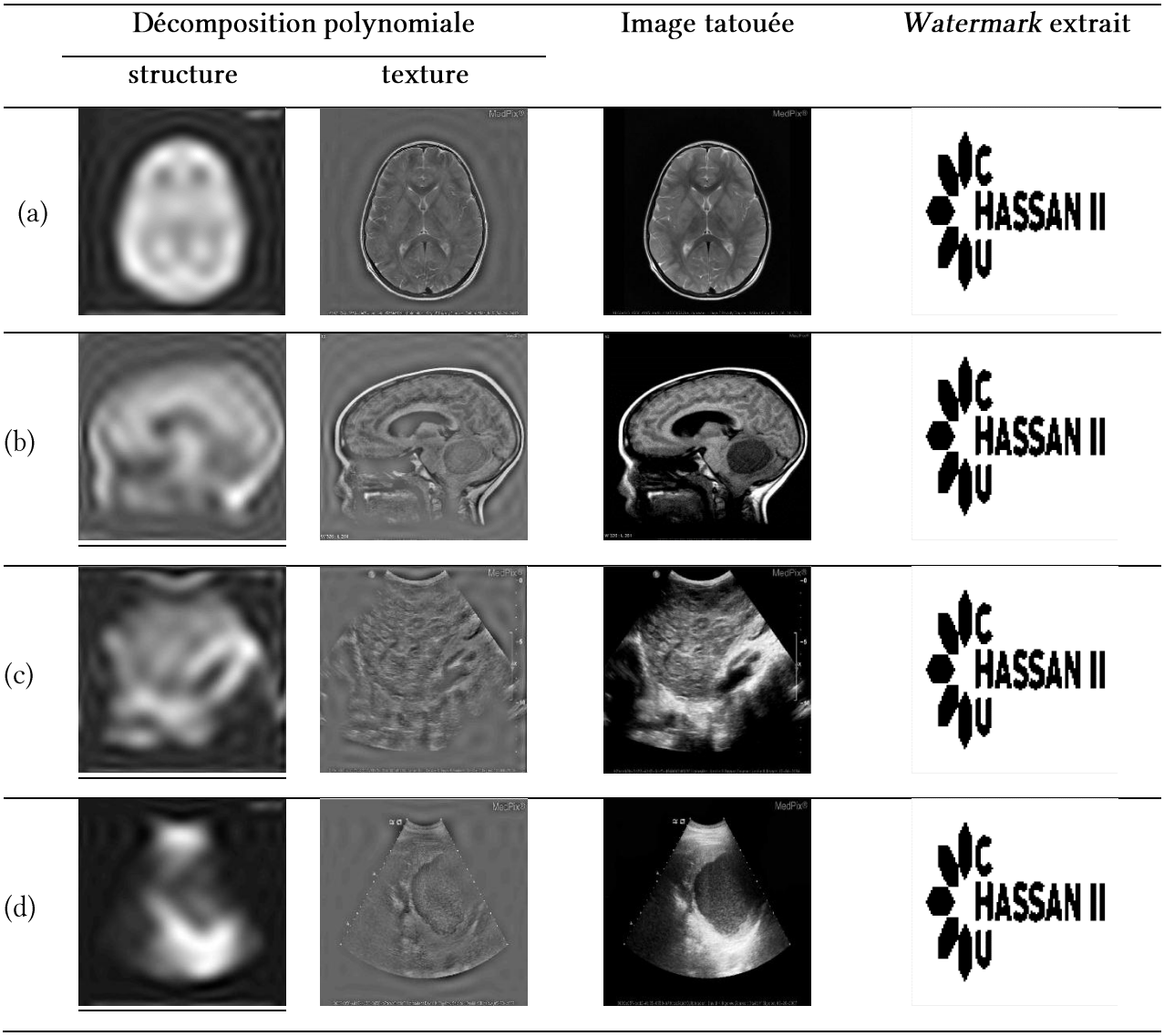


Figure 4.4 Illustration des résultantes des étapes de notre méthode de touage

4.3.3.1 *Analyse d'invisibilité*

Les images médicales tatouées ne doivent en aucun cas révéler de distorsions perceptives susceptibles d'entraîner un mauvais diagnostic. Il est donc nécessaire de vérifier la qualité de la transparence perceptive de l'algorithme proposé. Le PSNR et la SSIM sont calculés entre les images originales et leurs versions tatouées. Les valeurs obtenues sont comparées à d'autres méthodes apparentées [67], [105]–[108] et sont présentées dans le tableau 1.

méthode	PSNR		SSIM	
	IRM	US	IRM	US
proposée	(a) 58. 00 (b) 56.51	(c) 59.67 (d) 63.65	(a) 0.9997 (b) 0.9998	(c) 0.9999 (d) 0.9999
[67]	48.536	45.0161	-	-
[105]	36.64	37.20	0.9610	0.9390
[106]	56.23	-	-	-
[107]	56.183	-	0.9977	-
[108]	46.11	-	0.9547	-

TABLE 4-16 Comparaison des résultats en terme de PSNR et SSIM

Comme le montre le tableau ci-dessus, les moyennes des valeurs PSNR obtenues (57,25 db pour la IRM et 61,66 db pour l'échographie) sont acceptables et les valeurs SSIM sont très proches de la valeur idéale. L'algorithme proposé est capable de garantir l'intégrité du contenu de l'image et il est plus efficace en termes d'invisibilité car nos résultats ont atteint des valeurs PSNR plus élevées que les méthodes rapportées [67], [105]–[108] . En outre, comme on peut le remarquer sur la figure 4.6, les images médicales originales et tatouées sont similaires et le processus d'insertion du *watermark* ne présente aucune différence observable.

4.3.3.2 *Analyse de robustesse*

Les images tatouées peuvent être altérées par diverses attaques volontaires et involontaires. Par conséquent, il est important de prouver la robustesse de la technique utilisée dans un environnement d'attaques. Le tableau 2 montre l'analyse comparative en termes de NC entre notre algorithme proposé et ceux de [67], [105], [106] avec et sans la présence d'attaques. Les images tatouées sont soumises aux attaques suivantes : Compression JPEG, Ajout de bruit, Égalisation de l'histogramme, Rotation. Comme on peut le remarquer dans le tableau 3, les valeurs NC obtenues de l'algorithme utilisé sont presque proches de 1, supérieures à 0,9695 et sont supérieures aux autres méthodes. En effet, on sait qu'il n'existe pas d'algorithme de tatouage sans erreur contre les attaques en imagerie médicale. La méthode proposée est robuste à différents attaques. Le premier cas de robustesse est testé contre la compression JPEG, il est clair que nous avons obtenu une robustesse plus élevée par rapport à [106] ce qui nous amène à dire

que notre algorithme peut résister à ce type d'attaques. Ensuite, la robustesse est testée sous l'attaque d'ajout de bruit. Notre méthode a obtenu des valeurs NC élevées et peut résister à des valeurs de densité plus élevées. La robustesse est également évaluée sous l'égalisation d'histogramme et les attaques de rotation et comparée à [67] [106], [109] [15]. Cependant, même après avoir soumis les images tatouées à ces attaques, le schéma proposé est capable de préserver l'authenticité de l'image médicale avec un minimum d'altération possible.

Attaque	**Intensité**	**méthode**	**NC**	
			IRM	**US**
Sans présence d'attaques	-	**proposée**	**(a) 1.0000 (b) 1.0000**	**(c) 1.0000 (d) 1.0000**
		[67]	0.9932	1.0000
		[105]	0.9999	0.9999
		[106]	1.0000	-
Compression JPEG	Q=80	**proposée**	**(a) 0.9890 (b) 0.9912**	**(c) 0.9919 (d) 0.9930**
		[106]	-	0.8300
Ajout de bruit	D = 0.001	**proposée**	**(a) 0.9981 (b) 0.9986**	**(c) 0.9999 (d) 0.9999**
		[105]	0.9960	0.9999
		[106]	0.9934	0.9895
	D = 0.01	**Ours**	**(a) 0.9695 (b) 0.9699**	**(c) 0.9750 (d) 0.9769**
		[67]	0.8416	-
		[105]	0.9662	0.9558
Égalisation de l'histogramme	-	**Ours**	**(a) 0.9840 (b) 0.9849**	**(c) 0.9867 (d) 0.9874**
		[67]	0.9835	-
		[106]	0.8500	-
Rotation	A = 10°	**Ours**	**(a) 0.9112 (b) 0.9154**	**(c) 0.9255 (d) 0.9317**
		[109]	0.7122	**-**

TABLE 4-17 Comparaison des valeurs NC des watermarks extrait avec et sans attaques

4.3.3.3 *Analyse du temps d'exécution*

Le temps d'exécution des processus d'insertion et d'extraction pour la méthode proposée du tatouage d'images médicales est évalué. D'après le tableau 4-18, nous observons que notre système est efficace en termes de temps d'exécution comparés aux méthodes précédentes

Méthode	**Insertion (s)**	**Extraction (s)**	**Global (s)**
[62]	-	-	29.95
[69]	4.28	4.6	8,54
[66]	10.80	5.80	16.6
Proposée (Chebychev) [86]	5,71	5.10	10.81
Proposée (Hermite)	4.17	4.09	8.26
Proposée (Legendre)	**3.80**	**3.12**	**6.92**

TABLE 4-18 Comparaison en temps d'exécution

4.4 Conclusion

Nous avons présenté dans cette section deux nouvelles techniques de tatouage des images médicales basées sur les transformées d'Hermite et de Legendre. Les résultats d'expérimentations de la première méthode ont montré l'efficacité de la méthode en termes de la robustesse du *watermark* face à 15 types d'attaques selon trois mesures différents (NC, SSIM, et BER). L'étude expérimentale nous a permis de souligner les avantages de la technique proposée en satisfaisant quatre facteurs du compromis suivant : invisibilité, robustesse, capacité et sécurité du *watermark.* Nous avons ensuite proposé une nouvelle technique de tatouage des images médicales basée sur la transformée de Legendre afin d'optimiser les performances en terme du temps d'exécution. A partir des résultats obtenus, nous avons en effet, montré l'amélioration au niveau du temps d'exécution en préservant un compromis optimal entre invisibilité et robustesse de la marque.

Chapitre 5. Tatouage des séquences vidéos médicales basé sur la Transformée de Krawtchouk

Sommaire

5.1 Introduction 137

5.2 Méthode proposée 137

5.3 Expérimentations et résultats 142

5.4 Conclusion 146

5.1 Introduction

Dans ce chapitre, nous présentons une cinquième contribution qui concerne le tatouage des séquences vidéos médicales basé sur les polynômes orthogonaux de Krawtchouk[110]. L'identité du patient est incorporée, en tant que watermark, dans les vidéos médicales. Un algorithme est adopté pour sélectionner les images (frames) optimales dans chaque plan (shot) vidéo. La décomposition polynomiale choisie permet d'identifier les régions d'insertion du *watermark* permettant d'obtenir le compromis optimale entre robustesse / invisibilité du watermark.

5.2 Méthode proposée

Cette contribution porte sur le développement d'un système efficace de tatouage des vidéos médicales. On propose une technique permettant d'abord de segmenter la vidéo médicale en images clés (key frames), puis à décomposer ces images en composantes significatives afin de sélectionner des régions où les petites altérations sont imperceptibles et indétectables par l'œil humain. Le schéma proposé est décrit dans la figure 5.1 ci-dessous.

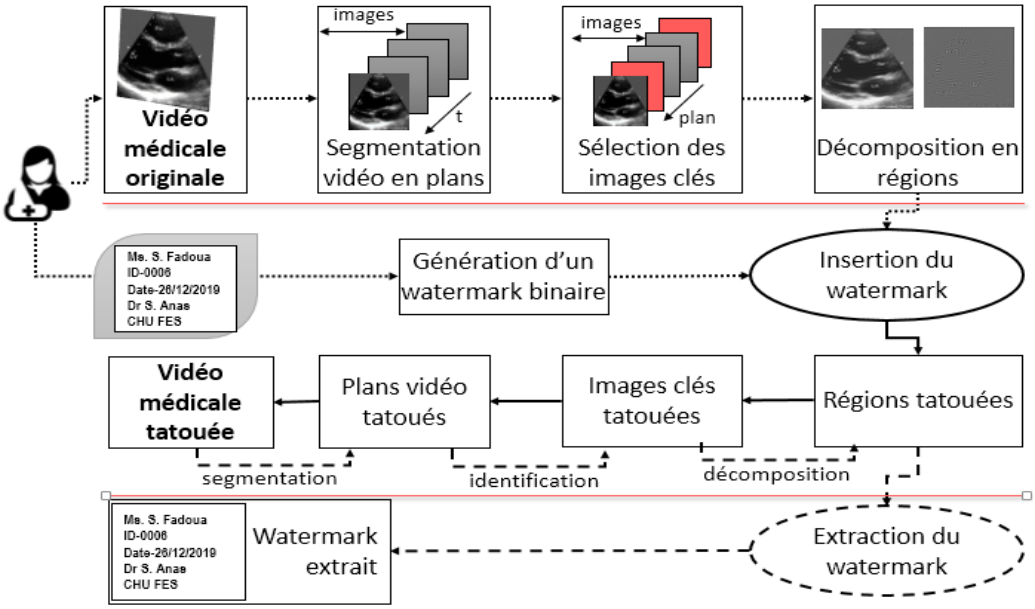


Figure 5.1 Schéma de la méthode proposée du tatouage des vidéos médicales

5.2.1 Prétraitement

La préparation de la vidéo médicale avant l'application du processus de tatouage est détaillée dans cette section. L'objectif de cette méthode étant de diviser la séquence vidéo originale en images clés et chacune d'entre elles est décomposée par une transformation polynomiale afin d'extraire les meilleures zones d'intégration du watermark.

Pour ce faire, la séquence vidéo originale est divisée en plans « **shots** » de sorte que chaque plan soit représenté comme une séquence continue de l'image à un moment donné. Les plans de la vidéo sont détectés en utilisant la méthode de la différence d'histogramme entre des images consécutives[40], [111]. La différence entre deux images en ce qui concerne la composante de luminance est calculée à l'aide de l'équation ci-dessous :

$$HD_k = \sum_{i=1}^{N} | H_k(i) - H_{k-1}(i)| \tag{77}$$

Tel que H_k représente l'histogramme de luminance de l'image à la position k avec N bins.

Si la valeur de H_k est supérieur à un seuil T, alors dans ce cas la k^{ème} image est une image d'arrêt « **cut frame** ». Ensuite un ensemble de plans vidéos est formé, et chaque plan ayant significativement le même histogramme (inférieur à une seuil T), est divisé en groupes d'images similaires continus (images candidates). Une image de chaque groupe est choisie comme image représentative du groupe nommée « **image clé** » et en anglais « **key frame** ».

Le seuil optimal T dépend de l'application prévue du tatouage. En effet, si on augmente le nombre d'images clés pour rendre le tatouage plus robuste, cela prendra plus de temps, et inversement, le tatouage devient moins robuste si le nombre d'images clés est réduit. La position de chaque image clé est enregistrée dans l'information clé K, qui sera utilisée ultérieurement dans le processus d'extraction du watermark. Ensuite, chaque image clé est décomposée en utilisant une décomposition polynomiale afin d'obtenir les meilleures régions d'insertion du *watermark* sur l'image d'origine, à savoir les régions lisses et les régions texturées. La première partie représente l'approximation de l'image et contient les aspects de basses fréquences. Tandis que la

seconde représente la composante de texture. La procédure sera répétée pour toutes les images clés sélectionnées. Cette décomposition se présente suivant les étapes ci-dessous,

On considère l'image de la vidéo « Frame » comme une fonction à deux variables $F(x, y)$ de taille $(N_1 + 1) * (N_2 + 1)$ définie dans Ω :

$$\begin{cases} F : \Omega \subset \mathbb{R}^2 \rightarrow \mathbb{R} \\ (x, y) \mapsto F(x, y) \end{cases} \tag{78}$$

Soit l'espace linéaire des polynômes bidimensionnels de coefficients $a_{i,j}$

$$P_{N_1,N_2}(x, y) = \sum_{i,j}^{(i+j)\leq N_1,N_2} a_{i,j} x_1^i \, x_2^j \tag{79}$$

Afin de déterminer la famille de polynôme utilisée pour cette décomposition, on présente un rappel concernant les polynômes orthogonaux de Krawtchouk. Ces polynômes notés $K_n(x; p; N)$ d'une seule variable satisfont l'équation de différences partielles du second ordre suivante (d'après équation (28)) :

$$(1 - p)x \, \Delta\nabla \, K_n(x; p; N) + (\mathrm{Np} - \mathrm{x})\Delta K_n(x; p; N) + nK_n(x; p; N) = 0 \tag{80}$$

Avec $x, n = 0,1,2,..,N$ et $0 < p < 1$

Le nième polynôme de Krawtchouk est défini en utilisant la fonction hypergéométrique suivante :

$$K_n(x; p; N) = \, {}_2F_1(-n, -x, -N; \frac{1}{p}) \tag{81}$$

Les deux premiers ordres $n = 0$ et $n = 1$ sont donnés par :

$$\widetilde{K}_0(x; p; N) = \sqrt{\frac{N! \, p^x (1 - p)^{N-x}}{x! \, (N - x)!}} \tag{82}$$

$$\widetilde{K}_1(x;p;N) = (-p(N-x) + x(1-p))\sqrt{\frac{(N-1)!\,p^{x-1}(1-p)^{N-x-1}}{x!\,(N-x)!}}$$

Les autres valeurs de polynômes de Krawtchouk $2 \leq n \leq N$ sont déduites de la relation de récurrence de Gram-Schmidt définie dans la section 2.2.1.

Ainsi, on déduit les polynômes orthogonaux discrets bivariables de Krawtchouk $K_{n,m}(x,y;p;N_1,N_2)$ qui sont orthogonaux par rapport à la fonction de poids suivante :

$$\omega(x,y;p;N_1,N_2) = \omega(X;p;N) = \binom{N}{X} p^X (1-p)^{N-X} \tag{83}$$

Enfin, on obtient l'approximation $\tilde{F}$ de l'image vidéo en utilisant les polynômes orthogonaux de Krawtchouk de coefficients $\tilde{f}_{i,j}$:

$$\begin{cases} \tilde{F} = P_{M_1,M_2}(x,y) = \sum_{n=0}^{M_1-1} \sum_{m=0}^{M_2-i} \tilde{f}_{n,m}\, K_{n,m}(x,y) \\ \tilde{f}_{n,m} = \dfrac{\langle F | K_{n,m} \rangle_\omega}{\langle K_{n,m} | K_{n,m} \rangle_\omega} \end{cases} \tag{84}$$

Et c'est à partir de cette équation qu'on obtient la partie texture F^T de l'image vidéo F:

$$F^T = F - \tilde{F} \tag{85}$$

5.2.2 Algorithme de la phase d'insertion

L'algorithme d'insertion du *watermark* se dénonce comme suit :

Algorithme : insertion du watermark

Entrées : vidéo médicale originale, *Watermark w*

Sorties : vidéo médicale tatouée

Etape 5. Diviser la vidéo originale en plans (shots).

Etape 6. Sélectionner les images clés de chaque plan de la vidéo et enregistrer leurs positions dans une information clé K.

Etape 7. Décomposer les images sélectionnées en régions texturées en utilisant le procédé de décomposition à base du polynôme de Krawtchouk présenté précédemment.

Etape 8. Diviser la composante texture en blocs de tailles 8x8.

Etape 9. Insérer les bits du *watermark* w_i dans k blocs $FB_i(FB_1, \dots, FB_k)$ avec une force de tatouage S par l'équation:

$$FB_i^* = FB_i(1 + w_i * S) \quad (86)$$

Etape 10. Combiner les blocs tatouées afin d'obtenir une composante texture tatouée sui servira pour obtenir la vidéo médicale tatouée

5.2.3 Algorithme de la phase d'extraction

De la même manière que la phase d'insertion, l'algorithme d'extraction du *watermark* suit les mêmes étapes mais utilise une logique inverse et se présente comme suit :

Algorithme : extraction du watermark

Entrées : vidéo médicale tatouée, vidéo originale

Sorties : *watermark* extrait

Etape 11. Diviser la vidéo tatouée en plans (*shots*).

Etape 12. Sélectionner les images clés de chaque plan de la vidéo par leurs positions en utilisant la clé K.

Etape 13. Décomposer les images sélectionnées en régions texturées en utilisant le procédé de décomposition à base du polynôme de Krawtchouk présenté précédemment.

Etape 14. Diviser la composante texture tatouée en blocs de tailles 8x8.

Etape 15. extraire les bits du *watermark* w_i depuis les blocs $FB_i(FB_1, \dots, FB_k)$ avec une force de tatouage S par l'équation:

$$w_i^* = \frac{FB_i^*}{FB_i} - 1 \quad (87)$$

Etape 16. Reconstruire le *watermark*

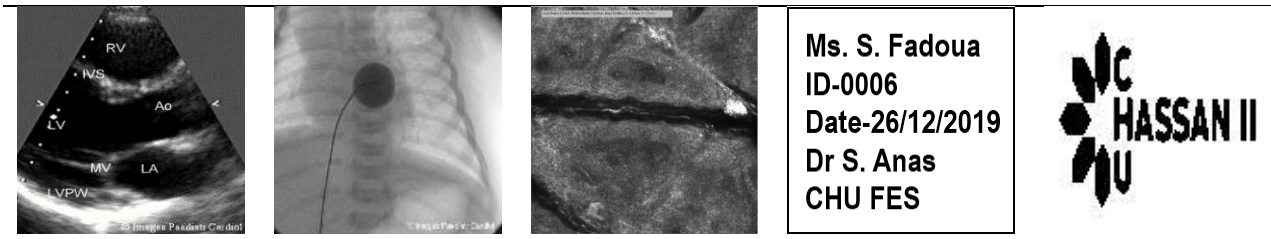
Si $w_i^* < 0$ Alors $watermark_i = 0\ bit$

Sinon $watermark_i = 1$ bit

5.3 Expérimentations et résultats

Les exigences les plus importantes d'un système de tatouage médical efficace sont la transparence et la robustesse, qui doivent être démontrées par des expériences. La performance de notre système de tatouage d'une vidéo médicale proposé est testée sur trois séquences de vidéos médicales, extraites de la base de données d'images MedPixTM, ainsi que deux watermarks. Les vidéos de tests contiennent 100 images chacune de modalités différentes : Ultrasons, X-ray, et microscopie.

En effet, il convient de noter que si on augmente le nombre d'image clés dans les plans sélectionnés cela entraînera une invisibilité réduite, et de même, si on diminue le nombre d'images clés cela entraînera une robustesse diminuée. C'est pour cela que le nombre d'images clés utilisés dans cette technique est de deux images dans chaque plan de la vidéo. La taille des images des vidéos médicales est de 512 x 512, tandis que la taille du *watermark* binaire est de 120 x 120. Le facteur de force du tatouage proposé choisi pour ces tests est sélectionné expérimentalement et fixé sur S=0.1. La figure 5.2 ci-dessous illustre 3 échantillons d'images des vidéos médicales originales ainsi que 2 watermarks.



a. b. c. d. e.

Figure 5.2 Supports de tests: a. ultrasons, b. x-ray, c. microscopie, d. watermark 1, e. watermark 2

5.3.1 Sans attaques

Le processus de tatouage doit être réalisé d'une manière la plus invisible possible pour les yeux humains afin d'éviter la probabilité du risque d'un mauvais diagnostic. En effet, si un tatouage est réalisé avec une dégradation minimale de la qualité visuelle de la vidéo médicale, il est considéré le plus demandé dans le domaine médical. Par conséquent, la qualité visuelle de la vidéo médicale tatouée en utilisant notre méthode est démontrée par des expériences en termes de PSNR et NC. Le tableau ci-dessous illustre un exemple de la représentation visuelle des composantes principales de notre processus de tatouage. Il représente les images clés originales des plans de la vidéo, les régions texturées de l'image, les images tatouées ainsi que les watermarks extraits.

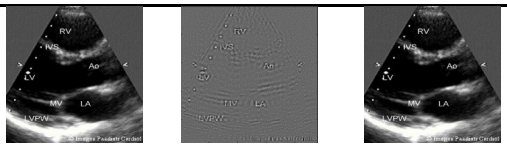
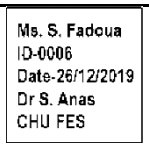
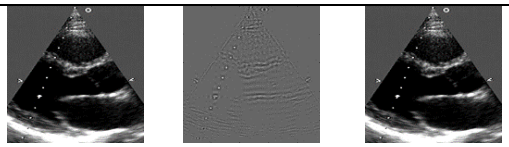
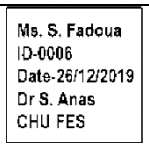
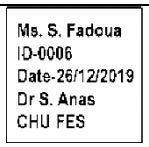
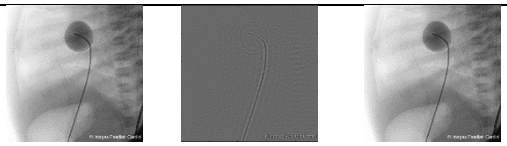
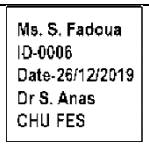
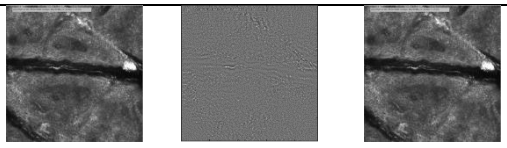
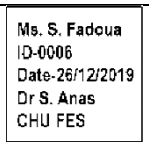
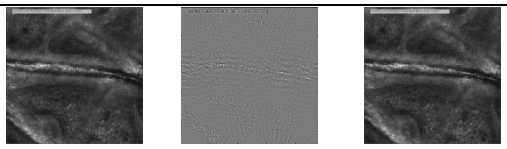
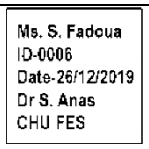
Vidéo originale		**Images clés** **Textures** **Images tatouées**	**Watermarks extraits**	
1.	**Plan 1**	 PSNR = 60.1278	 NC = 1.0000	 NC = 1.0000
	Plan 2	 PSNR = 60.4540	 NC = 1.0000	 NC = 1.0000
2.	**Plan 1**	 PSNR = 68.5800	 NC = 1.0000	 NC = 1.0000
	Plan 2	 PSNR = 67.4404	 NC = 1.0000	 NC = 1.0000
3.	**Plan 1**	 PSNR = 61.0253	 NC = 1.0000	 NC = 1.0000
	Plan 2	 PSNR= 63.0091	 NC = 1.0000	 NC = 1.0000

TABLE 5-1 La représentation visuelle des principales composantes de notre méthode de tatouage

Les résultats des simulations sont testés sur différentes tailles du watermark. Les résultats obtenus sont comparés aux travaux précédents dans le tableau ci-dessous. D'après les deux tableaux, la valeur la plus élevée du PSNR est 61,4394 dB pour le *watermark* de taille 120x120 et la moyenne des valeurs de NC est 1,0000. Les valeurs trouvées en utilisant notre méthode sont acceptables pour le diagnostic. Par conséquent, notre méthode de tatouage s'effectue sans afficher de différences observables entre les vidéos originales et celles tatouée. Il s'agit, en effet, d'une solution potentielle au problème classique lié à la capacité limitée de la taille du watermark. En outre, notre schéma de tatouage de vidéos médicales est plus performant que les méthodes précédentes même en variant la taille du watermark.

méthode	**Taille du watermark**	**PSNR (moyenne)**	**NC (moyenne)**
proposée	32 x 32	68.5600	0.9999
	45 x 45	66.9560	0.9999
	64 x 64	64.0244	0.9999
	120 x 120	61.4394	1.0000
[112]	NA	32.478	NA
[41]	16 x 16	60.4600	0.9962
	32 x 32	53.4300	NA
	64 x 64	46.0666	NA
[44]	32 x 32	65.6869	NA
[103]	120 x 120	59.4575	0.9998
[86]	64 x 64	63.4072	1.0000
	128 x 128	61.5377	1.0000

TABLE 5-2 Comparaison sommaire en termes des moyennes du PSNR et NC pour différentes tailles du watermark

5.3.2 Avec attaques

La robustesse face aux attaques intentionnelles et non intentionnelles est une propriété cruciale du tatouage numérique. C'est-à-dire que le *watermark* doit être extrait de la vidéo tatouée même si elle est soumise à différentes attaques. Afin d'évaluer les performances de robustesse de notre méthode, les vidéos médicales tatouée ont subi 3 attaques : La compression JPEG avec

différents facteurs (QF=90, 80,50), un filtrage médian de taille [3x3] et l'égalisation d'histogramme. Le tableau ci-dessous présente un exemple des watermarks extraits avec leurs valeurs NC correspondantes. Ainsi, qu'une comparaison est établie avec d'autres méthodes et présenté dans le tableau X.

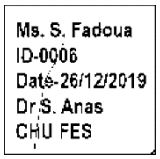
Compression JPEG QF = 80	**Filtre Médian [3x3]**	**HE**
		
NC = 0.9871	NC = 0.9997	NC = 0.9989
		
NC = 0.9859	NC = 0.9987	NC = 0.9969

TABLE 5-3 Watermarks extraits après les attaques en termes de NC

attaque	**méthode**	**paramètre**	**NC (moyenne)**
Compression JPEG	proposée	QF = 90	0.9985
		QF = 80	0.9865
		Qf = 50	0.8752
	[103]	Qf = 80	0.9913
	[86]	Qf = 90	0.9704
Filtre Médian	proposée	[3 x 3]	0.9992
	[39]	[3 x 3]	0.9965
	[86]	[3 x 3]	0.9851
Egalisation d'histogramme	proposée		0.9979
	[86]		0.9986

TABLE 5-4 Comparaison de la robustesse de notre méthode avec d'autres techniques en termes de NC

D’après les résultats présentés précédemment, les valeurs NC obtenues en utilisant notre méthode sont proches de la valeur idéale (NC=1), elles sont supérieures à 0,8752 et sont supérieures à celles obtenues par les autres méthodes. De plus, étant donné qu'il n'existe pas de schéma de tatouage sans erreur contre les attaques en imagerie médicale, ces résultats positifs nous amènent à dire que notre méthode conserve une forte robustesse contre différentes attaques.

5.4 Conclusion

Dans ce chapitre, on a proposé un nouveau procédé de tatouage des vidéos médicales pour les applications de télémédecine. D'après les résultats expérimentaux, notre algorithme présente de nombreux avantages. En particulier, les valeurs obtenues en termes de PSNR et NC sont élevées, ce qui justifie que les altérations de la vidéo médicale tatouée sont perceptiblement transparentes pour les yeux humains et sont parfaitement robustes contre diverses attaques (compression JPEG, filtrage médian et égalisation d'histogramme).

Conclusion générale

Dans cette section, nous allons succinctement rappeler l'ensemble des résultats obtenus dans la présente thèse et ensuite, proposer des perspectives de recherche déduites de ces travaux.

La sécurité des images médicales est un critère indispensable pour leur partage avec des professionnels de santé ou d'autres. Le tatouage numérique est une technique fiable qui permet d'assurer cette sécurité. Elle consiste à insérer une marque invisible et robuste à différents attaques. Cependant, l'introduction d'altérations visibles dans l'image médicale est de toute évidence intolérable et peut conduire à une erreur du diagnostic. Vu le caractère sensible de l'image médicale et afin de surmonter cette limitation, nous proposons une technique de tatouage basé sur les transformations polynomiales. Les avantages fournis par ces transformations nous ont permis d'extraire la composante texture de l'image avec des combinaisons linéaires de polynômes orthogonaux. L'extraction de la texture est déduite généralement après avoir extrait la partie géométrique (structure) de l'image dont le problème est connu dans la littérature par "la décomposition d'image". L'originalité de notre approche consiste à extraire la texture d'une image donnée que par projection sur une base de polynômes orthogonaux bivariables.

Nous avons réalisé cinq méthodes de décomposition d'images en utilisant les familles de polynômes suivant : Laguerre, Chebychev, Hermite, Legendre, et Krawtchouk. Ces méthodes sont effectuées en projetant l'image médicale originale sur une base bivariable en considérant la composante structure comme le résultat de la reconstitution partielle et la composante texture comme la différence entre l'image originale et sa partie structure.

Dans un premier temps, nous avons présenté dans le **chapitre 1,** les notions et concepts de base du tatouage numérique dans la première section. Dans la deuxième section, nous nous sommes intéressés aux techniques de tatouage des images médicales. Dans cette section, nous avons décrit l'importance de la sécurité de l'image médicale, les exigences à respecter pendant la conception d'un algorithme de tatouage dans un tel domaine.

Nous avons proposé dans le **chapitre 2** la première méthode de tatouage basée sur la transformée de Laguerre combinée avec la DCT pour des images classiques. Ce choix permet

d'extraire les moyennes fréquences de la composante texture extraite par la décomposition polynomiale, afin d'insérer la marque du tatouage. Cette combinaison nous a permis d'apporter plus de robustesse à l'algorithme de tatouage. Cette méthode a été comparée avec d'autres méthodes existantes. Les résultats expérimentaux on été satisfaisants et ont démontré une bonne invisibilité et une forte robustesse à différents attaques.

Etant donné que la méthode de tatouage à base de la décomposition polynomiale est adapté pour la protection des images à caractère sensible telles que les images médicales ; nous avons donc réalisé, dans le **chapitre 3**, une méthode de tatouage à base de la transformée de Chebychev. Les expérimentations réalisées ont montré un bon compromis invisibilité/robustesse de la marque. Nous avons obtenu avec cette méthode zéro cas de faux positifs. Seulement, la carte de dissimilarité utilisée pour visualiser la différence perceptuelle entre l'image originale et tatouée a montré la présence de quelques petites altérations. Cela nous a mené à améliorer notre méthode de tatouage afin de mieux l'adapter au contexte médical.

Partant de ce principe et dans le contexte de fournir une protection sécurisée de l'image médicale, nous avons donc introduit la technique du fenêtrage adaptatif pour mieux sélectionner les régions texturées de l'image dans un nombre réduit de blocs. Ainsi, nous avons utilisés la transformation d'Arnold pour renforcer le facteur de sécurité de notre méthode. Cette nouvelle technique a été élaborée dans le **chapitre 4** qui est combinée avec la transformée d'Hermite pour l'étape du prétraitement de l'image médicale. L'utilisation de cette transformée, qui dispose d'une propriété proche du Système Visuel Humain, a démontrée une plus grande imperceptibilité en terme de PSNR. Les résultats d'expérimentations que nous avons menés ont montré l'efficacité de la méthode en termes de la robustesse du *watermark* face à 15 types d'attaques selon trois mesures différents (NC, SSIM, et BER). Ces résultats ont été comparés avec d'autres techniques de tatouage proches de notre contexte. L'étude expérimentale nous a permis de souligner les avantages de la technique proposée en termes des facteurs du compromis suivant : invisibilité, robustesse, capacité et sécurité du *watermark.* Nous avons ensuite proposé une nouvelle technique de tatouage des images médicales basée sur la transformée de Legendre afin d'optimiser les performances en terme du temps d'exécution. A partir des résultats obtenus, nous avons en effet, montré l'amélioration au niveau du temps d'exécution en préservant un compromis optimal entre invisibilité et robustesse de la marque.

Enfin, nous avons présenté dans le **chapitre 5** une méthode de tatouage de séquences des vidéos médicales basé sur une décomposition polynomiale de type Krawtchouk. Cette méthode a été combinée avec une technique qui permet de sélectionner les images optimales (*key frames*) dans chaque plan de la vidéo (video shot). Cette méthode a été comparée avec d'autres méthodes de base**.**

En guise de perspectives et de suites de ce travail de recherche, plusieurs axes de recherche sont identifiés. En effet, les méthodes de tatouages présentées dans ce mémoire de thèse peuvent être améliorées. Dans ce sens, nous envisageons améliorer dans un premier temps l'outil d'extraction des caractéristiques de l'image afin d'améliorer le compromis du tatouage.

Par ailleurs, la protection numérique ne devrait pas se limiter à l'imagerie médicale. Il serait très intéressent de faire la généralisation du tatouage comme moyen de sécurité à l'ensemble des documents numériques.

Enfin, la marque du tatouage à insérer est choisie d'une manière aléatoire comme signe de référence. Toutefois, il serait beaucoup plus intéressant de concevoir une signature à partir du contenu du document numérique concerné, comme le code QR par exemple, et l'insérer par la suite dans la zone la plus appropriée. Cependant, toute modification ultérieure de l'image serait en déphasage par rapport à la marque.

Publications de l'auteur

Articles dans des revues

F. Sabbane and H. Tairi, "Medical image watermarking technique based on polynomial decomposition," Multimedia Tools and Applications, vol. 78, no. 23, pp. 34129–34155, Dec. 2019, doi: 10.1007/s11042-019-08134-7.

F. Sabbane and H. Tairi, "Imperceptible watermarking scheme for security of medical images in telemedicine applications," en révision pour publication à Biomedical Signal Processing and Control, Elsevier.

Articles dans des actes de conférences internationales

F. Sabbane, N. Aherrahrou, and H. Tairi, "A new robust watermarking scheme based on polynomial decomposition," in 2017 Intelligent Systems and Computer Vision (ISCV), IEEE, Fez, Morocco, Apr. 2017, pp. 1–6. doi: 10.1109/ISACV.2017.8054947.

F. Sabbane, N. Aherrahrou, and H. Tairi, "A new region based watermarking scheme for medical images," in Proceedings of the New Challenges in Data Sciences: Acts of the Second Conference of the Moroccan Classification Society - SMC '19, ACM, Kenitra, Morocco, 2019, pp. 1–6. doi: 10.1145/3314074.3314094.

F. Sabbane and H. Tairi, "Medical Video Watermarking Scheme for Telemedicine Applications," in 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), IEEE, Meknes, Morocco, Apr. 2020, pp. 1–6. doi: 10.1109/IRASET48871.2020.9091982.

Articles dans des actes de conférences nationales

F. Sabbane and H. Tairi, "Les transformations polynomiales: application au tatouage des images médicales ", 6ème édition des journées doctorales du laboratoire LIIAN (JDLIIAN) 28-29 Décembre 2017, Fès, Maroc.

Bibliographie

[1] A. M. Al-Haj, Advanced techniques in multimedia watermarking: image, video and audio applications: image, video and audio applications. IGI Global, 2010.

[2] R. E. Moubtahij, B. Augereau, H. Tairi, and C. Fernandez-Maloigne, “A spatial image polynomial decomposition with application to video classification,” p. 29.

[3] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and applications of digital watermarking and content protection. Boston: Artech House, 2003.

[4] H. Berghel and L. O’Gorman, “Protecting ownership rights through digital watermarking,” Computer, vol. 29, no. 7, pp. 101–103, Jul. 1996, doi: 10.1109/2.511977.

[5] I. J. Cox, Ed., Digital watermarking and steganography, 2nd ed. Amsterdam ; Boston: Morgan Kaufmann Publishers, 2008.

[6] K. Tanaka, Y. Nakamura, and K. Matsui, “Embedding secret information into a dithered multi-level image,” in IEEE Conference on Military Communications, Monterey, CA, USA, 1990, pp. 216–220. doi: 10.1109/MILCOM.1990.117416.

[7] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, “Watermarking Techniques used in Medical Images: a Survey,” Journal of Digital Imaging, vol. 27, no. 6, pp. 714–729, Dec. 2014, doi: 10.1007/s10278-014-9700-5.

[8] A. Singh, B. Kumar, G. Singh, and A. Mohan, Medical Image Watermarking: techniques and Applications. New York, NY: Springer Science+Business Media, 2017. doi: 10.1007/978-3-319-57699-2.

[9] C. Chou and K. Liu, “Performance Analysis of Color Image Watermarking Schemes Using Perceptually Redundant Signal Spaces,” in 2006 International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA, Dec. 2006, pp. 651–654. doi: 10.1109/IIH-MSP.2006.265086.

[10] V. Darmstaedter, J.-F. Delaigle, J. J. Quisquater, and B. Macq, "Low cost spatial watermarking," Computers & Graphics, vol. 22, no. 4, pp. 417–424, Aug. 1998, doi: 10.1016/S0097-8493(98)00031-4.

[11] S. Kumar and B. K. Singh, "Entropy based spatial domain image watermarking and its performance analysis," Multimed Tools Appl, vol. 80, no. 6, pp. 9315–9331, Mar. 2021, doi: 10.1007/s11042-020-09943-x.

[12] H. Zhang, C. Wang, and X. Zhou, "A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain," Future Internet, vol. 9, no. 3, 2017, doi: 10.3390/fi9030045.

[13] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," Soft Comput, vol. 22, no. 1, pp. 91–106, Jan. 2018, doi: 10.1007/s00500-017-2489-7.

[14] J.-S. Pan, H.-C. Huang, and L. C. Jain, Intelligent Watermarking Techniques: (With CD-ROM). WORLD SCIENTIFIC, 2004. doi: 10.1142/5471.

[15] W. Bender, D. Gruhi, and N. Morimoto, "Techniques for data hiding," p. 10.

[16] L. Zhang and D. Wei, "Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization," Multimedia Tools and Applications, vol. 78, no. 19, pp. 28003–28023, Oct. 2019, doi: 10.1007/s11042-019-07902-9.

[17] K. Fares, A. Khaldi, K. Redouane, and E. Salah, "DCT & DWT based watermarking scheme for medical information security," Biomedical Signal Processing and Control, vol. 66, p. 102403, 2021, doi: https://doi.org/10.1016/j.bspc.2020.102403.

[18] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," Forensic Science International, vol. 320, p. 110691, 2021, doi: https://doi.org/10.1016/j.forsciint.2021.110691.

[19] K. Prabha and I. S. Sam, "Robust color image watermarking by elliptical phase modification based on Walsh Hadamard Transform and Triangular Vertex Transform," Sādhanā, vol. 46, no. 1, p. 38, Dec. 2021, doi: 10.1007/s12046-020-01553-5.

[20] R. Thanki, K. Borisagar, and S. Borra, "Speech watermarking technique using the finite ridgelet transform, discrete wavelet transform, and singular value decomposition," in Advance compression and watermarking technique for speech signals, Springer, 2018, pp. 27–45.

[21] J. Zhang and others, "A Robust Digital Watermarking Algorithm Based on Finite-Set Discrete Radon Transform Tight Frame," Journal of Computer and Communications, vol. 8, no. 12, p. 123, 2020.

[22] J. S. Gaikwad and U. Verma, "Digital Image Watermarking by Fusion of Wavelet and Curvelet Transform," in Advances in Signal and Data Processing, Springer, 2021, pp. 545–559.

[23] L.-H. Gong, C. Tian, W.-P. Zou, and N.-R. Zhou, "Robust and imperceptible watermarking scheme based on Canny edge detection and SVD in the contourlet domain," Multimedia Tools and Applications, vol. 80, no. 1, pp. 439–461, 2021.

[24] P. K. Dhar, A. H. Chowdhury, and T. Koshiba, "Blind Audio Watermarking Based on Parametric Slant-Hadamard Transform and Hessenberg Decomposition," Symmetry, vol. 12, no. 3, p. 333, 2020.

[25] S. Burgett, E. Koch, and J. Zhao, "A novel method for copyright labeling digitized image data," Fraunhofer Inst. Comput. Graphics, Darmstadt, Germany, Tech. Rep, 1994.

[26] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. on Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997, doi: 10.1109/83.650120.

[27] A. Piva, M. Barni, and F. Bartolini, "Copyright protection of digital images by means of frequency domain watermarking," in Mathematics of Data/Image Coding, Compression, and Encryption, 1998, vol. 3456, pp. 25–35. doi: 10.1117/12.330369.

[28] V. Solachidis and I. Pitas, “Self-similar ring shaped watermark embedding in 2-D DFT domain,” in 2000 10th European Signal Processing Conference, 2000, pp. 1–4.

[29] Atta-ur-Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, and M. Mahmud, “Reversible and Fragile Watermarking for Medical Images,” Computational and Mathematical Methods in Medicine, vol. 2018, pp. 1–7, Jul. 2018, doi: 10.1155/2018/3461382.

[30] A. Shehab et al., “Secure and Robust Fragile Watermarking Scheme for Medical Images,” IEEE Access, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[31] F. Huma, M. Jahan, I. B. Rashid, and M. A. Yousuf, “Wavelet and LSB-Based Encrypted Watermarking Approach to Hide Patient’s Information in Medical Image,” in Proceedings of International Joint Conference on Advances in Computational Intelligence, 2021, pp. 89–104.

[32] M. Nazari and M. Mehrabian, “A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images,” Multimedia Tools and Applications, vol. 80, no. 7, pp. 10615–10655, 2021.

[33] M. Turuk and A. Dhande, “A Novel Texture-Quantization-Based Reversible Multiple Watermarking Scheme Applied to Health Information System,” Journal of Digital Imaging, vol. 31, no. 2, pp. 167–177, Apr. 2018, doi: 10.1007/s10278-017-0024-0.

[34] T.-S. Nguyen, “Fragile watermarking for image authentication based on DWT-SVD-DCT techniques,” Multimedia Tools and Applications, pp. 1–13, 2021.

[35] Z. Gong, N. Qin, and G. Zhang, “Visible watermarking in document images using two-stage fuzzy inference system,” The Visual Computer, Jan. 2021, doi: 10.1007/s00371-020-02045-7.

[36] C. Yan, G. Zhang, A. Wang, L. Liu, and C.-C. Chang, “Visible 3D-model Watermarking Algorithm for 3D-Printing Based on Bitmap Fonts,” p. 8.

[37] W. Qi, Y. Liu, S. Guo, X. Wang, and Z. Guo, “An Adaptive Visible Watermark Embedding Method based on Region Selection,” Security and Communication Networks, vol. 2021, pp. 1–11, Mar. 2021, doi: 10.1155/2021/6693343.

[38] J. Qu, W. Song, X. Liu, L. Zhao, and X. Zhao, “A Novel Improved Reversible Visible Image Watermarking Algorithm Based on Grad-CAM and JND,” Security and Communication Networks, vol. 2021, pp. 1–17, Jan. 2021, doi: 10.1155/2021/6652897.

[39] Z. Bahrami and F. Akhlaghian Tab, “A new robust video watermarking algorithm based on SURF features and block classification,” Multimedia Tools and Applications, vol. 77, no. 1, pp. 327–345, Jan. 2018, doi: 10.1007/s11042-016-4226-0.

[40] Y. Bendraou, F. Essannouni, D. Aboutajdine, and A. Salam, “Video shot boundary detection method using histogram differences and local image descriptor,” in 2014 Second World Conference on Complex Systems (WCCS), Agadir, Morocco, Nov. 2014, pp. 665–670. doi: 10.1109/ICoCS.2014.7060883.

[41] N. I.Yassin, N. M. Salem, and M. I. El Adawy, “Medical Video Watermarking Scheme for Electronic Patient Records,” International Journal of Computer Applications, vol. 76, no. 1, pp. 12–17, Aug. 2013, doi: 10.5120/13210-0591.

[42] Y. Li and H.-X. Wang, “Robust H.264/AVC video watermarking without intra distortion drift,” Multimedia Tools and Applications, vol. 78, no. 7, pp. 8535–8557, Apr. 2019, doi: 10.1007/s11042-018-6942-0.

[43] N. Patil and V. R. Udupi, “Development of Reversible Video Watermarking Algorithm based on Hybrid DWT-SVD,” vol. 8, no. 4, p. 5, 2019.

[44] H. Zarrabi, A. Emami, N. Karimi, and S. Samavi, “Adaptive Reversible Watermarking for Medical Videos Based on Linear Prediction,” p. 6, Jan. 2018.

[45] M. T. Ahvanooey, Q. Li, X. Zhu, M. Alazab, and J. Zhang, "ANiTW: A novel intelligent text watermarking technique for forensic identification of spurious information on social media," Computers & Security, vol. 90, p. 101702, 2020.

[46] A. A. Alkhafaji et al., "Payload Capacity Scheme for Quran Text Watermarking Based on Vowels with Kashida," CMC Computer, Materials and Continua, vol. 67, no. 3, pp. 3865–3885, 2021.

[47] U. Khadam, M. M. Iqbal, S. Saeed, S. H. Dar, A. Ahmad, and M. Ahmad, "Advanced security and privacy technique for digital text in smart grid communications," Computers & Electrical Engineering, vol. 93, p. 107205, 2021.

[48] X. Liang and S. Xiang, "Robust reversible audio watermarking based on high-order difference statistics," Signal Processing, vol. 173, p. 107584, 2020.

[49] E. Salah, K. Amine, K. Redouane, and K. Fares, "A Fourier transform based audio watermarking algorithm," Applied Acoustics, vol. 172, p. 107652, 2021.

[50] P. Singh and R. S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks," vol. 2, no. 9, p. 12, 2013.

[51] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking-Attacks and Countermeasures, vol. 1. Boston, MA: Springer US, 2001. doi: 10.1007/978-1-4615-4375-6.

[52] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Trans. on Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004, doi: 10.1109/TIP.2003.819861.

[53] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," in Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. ITAB-ITIS 2000. Joint Meeting Third IEEE EMBS International Conference on Information Technology Applications in Biomedicine

(ITAB'00). Third Works, Arlington, VA, USA, 2000, pp. 250–255. doi: 10.1109/ITAB.2000.892396.

[54] H. L. Khor, S.-C. Liew, and J. Mohd. Zain, "Region of Interest-Based Tamper Detection and Lossless Recovery Watermarking Scheme (ROI-DR) on Ultrasound Medical Images," Journal of Digital Imaging, vol. 30, no. 3, pp. 328–349, Jun. 2017, doi: 10.1007/s10278-016-9930-9.

[55] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "A Heuristic Automatic and Robust ROI Detection Method for Medical Image Warermarking," Journal of Digital Imaging, vol. 28, no. 4, pp. 417–427, Aug. 2015, doi: 10.1007/s10278-015-9770-z.

[56] P. Murali and V. Sankaradass, "An efficient ROI based copyright protection scheme for digital images with SVD and orthogonal polynomials transformation," Optik, vol. 170, pp. 242–264, Oct. 2018, doi: 10.1016/j.ijleo.2018.04.050.

[57] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," Journal of Biomedical Informatics, vol. 66, pp. 214–230, Feb. 2017, doi: 10.1016/j.jbi.2017.01.006.

[58] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "A New Reversible and high capacity data hiding technique for E-healthcare applications," Multimedia Tools and Applications, vol. 76, no. 3, pp. 3943–3975, Feb. 2017, doi: 10.1007/s11042-016-4196-2.

[59] W. Pan, D. Bouslimi, M. Karasad, M. Cozic, and G. Coatrieux, "Imperceptible reversible watermarking of radiographic images based on quantum noise masking," Computer Methods and Programs in Biomedicine, vol. 160, pp. 119–128, Jul. 2018, doi: 10.1016/j.cmpb.2018.03.011.

[60] A. Roček, K. Slavíček, O. Dostál, and M. Javorník, "A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters," Biomedical Signal Processing and Control, vol. 29, pp. 44–52, Aug. 2016, doi: 10.1016/j.bspc.2016.05.005.

[61] P. Selvam, S. Balachandran, S. Pitchai Iyer, and R. Jayabal, “Hybrid transform based reversible watermarking technique for medical images in telemedicine applications,” Optik, vol. 145, pp. 655–671, Sep. 2017, doi: 10.1016/j.ijleo.2017.07.060.

[62] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, “An efficient medical image watermarking scheme based on FDCuT–DCT,” Engineering Science and Technology, an International Journal, vol. 20, no. 4, pp. 1366–1379, Aug. 2017, doi: 10.1016/j.jestch.2017.06.001.

[63] S. Ramly, S. A. Aljunid, and H. Shaker Hussain, “SVM-SS Watermarking Model for Medical Images,” in Digital Enterprise and Information Systems, vol. 194, E. Ariwa and E. El-Qawasmeh, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 372–386. doi: 10.1007/978-3-642-22603-8_34.

[64] A. Rai and H. V. Singh, “SVM based robust watermarking for enhanced medical image security,” Multimedia Tools and Applications, vol. 76, no. 18, pp. 18605–18618, Sep. 2017, doi: 10.1007/s11042-016-4215-3.

[65] D. S. Chauhan, A. K. Singh, A. Adarsh, B. Kumar, and J. P. Saini, “Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images,” Multimedia Tools and Applications, vol. 78, no. 10, pp. 12647–12661, 2019, doi: 10.1007/s11042-017-5348-8.

[66] R. Bamal and S. S. Kasana, “Dual hybrid medical watermarking using walsh-slantlet transform,” Multimed Tools Appl, vol. 78, no. 13, pp. 17899–17927, Jul. 2019, doi: 10.1007/s11042-018-6820-9.

[67] Y. Gangadhar, V. S. Giridhar Akula, and P. C. Reddy, “An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation,” Biomedical Signal Processing and Control, vol. 43, pp. 31–40, May 2018, doi: 10.1016/j.bspc.2018.02.007.

[68] S. Vellaisamy and V. Ramesh, “Inversion attack resilient zero-watermarking scheme for medical image authentication,” IET Image Processing, vol. 8, no. 12, pp. 718–727, Dec. 2014, doi: 10.1049/iet-ipr.2013.0558.

[69] P. Khare and V. K. Srivastava, “A Secured and Robust Medical Image Watermarking Approach for Protecting Integrity of Medical Images,” Trans Emerging Tel Tech, vol. 32, no. 2, Feb. 2021, doi: 10.1002/ett.3918.

[70] S. Fadoua, A. Noura, and T. Hamid, “A new robust watermarking scheme based on polynomial decomposition,” in 2017 Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, Apr. 2017, pp. 1–6. doi: 10.1109/ISACV.2017.8054947.

[71] G. Szego, “ORTHOGONAL POLYNOMIALS,” p. 440.

[72] B. Xiao, L. Li, Y. Li, W. Li, and G. Wang, “Image Analysis by Fractional-order Orthogonal Moments,” Inf. Sci., vol. 382, no. C, pp. 135–149, Mar. 2017, doi: 10.1016/j.ins.2016.12.011.

[73] S. H. Abdulhussain, A. R. Ramli, B. M. Mahmmod, M. I. Saripan, S. A. R. Al-Haddad, and W. A. Jassim, “Shot boundary detection based on orthogonal polynomial,” Multimedia Tools and Applications, vol. 78, no. 14, pp. 20361–20382, Jul. 2019, doi: 10.1007/s11042-019-7364-3.

[74] K. Rahbar, “Image segmentation through modeling the illumination probability distribution function using the Krawtchouk polynomial,” Signal Processing, vol. 164, pp. 1–9, Nov. 2019, doi: 10.1016/j.sigpro.2019.05.033.

[75] D. Rivero-Castillo, H. Pijeira, and P. Assunçao, “Edge detection based on Krawtchouk polynomials,” Journal of Computational and Applied Mathematics, vol. 284, pp. 244–250, Aug. 2015, doi: 10.1016/j.cam.2014.11.017.

[76] S. K. Suslov, “The theory of difference analogues of special functions of hypergeometric type,” Russian Mathematical Surveys, vol. 44, no. 2, pp. 227–278, 1989.

[77] M. Eden, M. Unser, and R. Leonardi, “Polynomial representation of pictures,” Signal Processing, vol. 10, no. 4, pp. 385–393, Jun. 1986, doi: 10.1016/0165-1684(86)90046-0.

[78] A. F. Nikiforov, V. B. Uvarov, and S. K. Suslov, “Classical orthogonal polynomials of a discrete variable,” in Classical orthogonal polynomials of a discrete variable, Springer, 1991, pp. 18–54.

[79] R. Koekoek and R. F. Swarttouw, “The Askey-scheme of hypergeometric orthogonal polynomials and its q-analogue,” arXiv preprint math/9602214, 1996.

[80] A. K. Khanna, N. R. Roy, and B. Verma, “Digital image watermarking and its optimization using genetic algorithm,” in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 1140–1144. doi: 10.1109/CCAA.2016.7813888.

[81] T. T. Takore, P. R. Kumar, and G. L. Devi, “A modified blind image watermarking scheme based on DWT, DCT and SVD domain using GA to optimize robustness,” in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 2725–2729. doi: 10.1109/ICEEOT.2016.7755190.

[82] R. Choudhary and G. Parmar, “A robust image watermarking technique using 2-level discrete wavelet transform (DWT),” in 2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS), 2016, pp. 120–124. doi: 10.1109/CCIntelS.2016.7878213.

[83] N. Muhammad and N. Bibi, “Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain,” IET Image Processing, vol. 9, no. 9, pp. 795–803, 2015.

[84] M. Ali and C. W. Ahn, “An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain,” Signal processing, vol. 94, pp. 545–556, 2014.

[85] L. Chen and J. Zhao, “Adaptive contourlet-based image watermarking robust to geometric transformations and image compression,” in 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings, 2016, pp. 1–6.

[86] F. Sabbane and H. Tairi, “Medical image watermarking technique based on polynomial decomposition,” Multimedia Tools and Applications, vol. 78, no. 23, pp. 34129–34155, Dec. 2019, doi: 10.1007/s11042-019-08134-7.

[87] A. Maalouf and M. Larabi, “Low-complexity enhanced lapped transform for image coding in JPEG XR / HD photo,” in 2009 16th IEEE International Conference on Image Processing (ICIP), Nov. 2009, pp. 5–8. doi: 10.1109/ICIP.2009.5413933.

[88] M. Favorskaya, A. Pyataeva, and A. Popov, “Texture analysis in watermarking paradigms,” Procedia Computer Science, vol. 112, pp. 1460–1469, Jan. 2017, doi: 10.1016/j.procs.2017.08.019.

[89] M. Ghadi, L. Laouamer, L. Nana, and A. Pascu, “A Robust Watermarking System Based on Formal Concept Analysis and Texture Analysis,” p. 6.

[90] F. Y. Shih and X. Zhong, “High-capacity multiple regions of interest watermarking for medical images,” Information Sciences, vol. 367–368, pp. 648–659, Nov. 2016, doi: 10.1016/j.ins.2016.07.015.

[91] S. L. Gomez-Coronel, E. Moya-Albor, B. Escalante-Ramírez, and J. Brieva, “Watermarked cardiac CT image segmentation using deformable models and the Hermite transform,” Cartagena de Indias, Colombia, Jan. 2015, p. 928717. doi: 10.1117/12.2073432.

[92] I. J. Cox, M. L. Miller, and J. A. Bloom, “Watermarking Applications and Their Properties,” in Proceedings of the The International Conference on Information Technology: Coding and Computing (ITCC’00), Washington, DC, USA, 2000, pp. 6-. [Online]. Available: http://dl.acm.org/citation.cfm?id=851038.856655

[93] J.-B. Martens, “The Hermite transform-applications,” IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 38, no. 9, pp. 1607–1618, Sep. 1990, doi: 10.1109/29.60076.

[94] G. M. C. R. L. C. S. Department and R. A. Young, The Gaussian Derivative Theory of Spatial Vision: Analysis of Cortical Cell Receptive Field Line-weighting Profiles. General Motors Research Laboratories, 1985. [Online]. Available: https://books.google.co.ma/books?id=PFuEGwAACAAJ

[95] L. Barba-J, L. Vargas-Quintero, J. A. Calderon, and C. Torres Moreno, “An image fusion method based on the Hermite transform applied to nuclear medicine and x-ray tomographic modalities,” Journal of Physics: Conference Series, vol. 1547, p. 012017, May 2020, doi: 10.1088/1742-6596/1547/1/012017.

[96] J.-B. Martens, “The Hermite Transform: A Survey,” EURASIP Journal on Advances in Signal Processing, vol. 2006, no. 1, Dec. 2006, doi: 10.1155/ASP/2006/26145.

[97] A. M. van Dijk and J.-B. Martens, “Feature-based image compression with steered Hermite transforms,” in Proceedings of 3rd IEEE International Conference on Image Processing, Lausanne, Switzerland, 1996, vol. 1, pp. 205–208. doi: 10.1109/ICIP.1996.559469.

[98] C. J. Rivero-Moreno and S. Bres, “Texture feature extraction and indexing by Hermite filters,” in Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004., Cambridge, UK, 2004, pp. 684-687 Vol.1. doi: 10.1109/ICPR.2004.1334266.

[99] L. Wu, J. Zhang, W. Deng, and D. He, “Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm,” in 2009 First International Conference on Information Science and Engineering, Nanjing, China, 2009, pp. 1164–1167. doi: 10.1109/ICISE.2009.347.

[100] A. Bastani and F. Ahouz, “High Capacity and Secure Watermarking for Medical Images Using Tchebichef Moments,” RADIOENGINEERING, vol. 29, no. 4, pp. 636–643, Dec. 2020, doi: 10.13164/re.2020.0636.

[101] K. M. Hosny, M. M. Darwish, K. Li, and A. Salah, “Parallel Multi-Core CPU and GPU for Fast and Robust Medical Image Watermarking,” IEEE Access, vol. 6, pp. 77212–77225, 2018, doi: 10.1109/ACCESS.2018.2879919.

[102] M. K. Singh, S. Kumar, M. Ali, and D. Saini, “Application of a novel image moment computation in X-ray and MRI image watermarking,” IET Image Processing, vol. 15, no. 3, pp. 666--682, 2021, doi: https://doi.org/10.1049/ipr2.12052.

[103] F. Sabbane, N. Aherrahrou, and H. Tairi, “A new region based watermarking scheme for medical images,” in Proceedings of the New Challenges in Data Sciences: Acts of the Second Conference of the Moroccan Classification Society - SMC ’19, Kenitra, Morocco, 2019, pp. 1–6. doi: 10.1145/3314074.3314094.

[104] M. Sayyouri, A. Hmimid, and H. Qjidaa, “A Fast Computation of Novel Set of Meixner Invariant Moments for Image Analysis,” Circuits, Systems, and Signal Processing, vol. 34, no. 3, pp. 875–900, Mar. 2015, doi: 10.1007/s00034-014-9881-7.

[105] J. C. Dagadu and J. Li, “Context-based watermarking cum chaotic encryption for medical images in telemedicine applications,” Multimedia Tools and Applications, vol. 77, no. 18, pp. 24289–24312, Sep. 2018, doi: 10.1007/s11042-018-5725-y.

[106] Swaraja K, “Medical image region based watermarking for secured telemedicine,” Multimedia Tools and Applications, vol. 77, no. 21, pp. 28249–28280, Nov. 2018, doi: 10.1007/s11042-018-6020-7.

[107] A. Kunhu, H. Al-Ahmad, and F. Taher, “Medical images protection and authentication using hybrid DWT-DCT and SHA256-MD5 hash functions,” in 2017 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Batumi, Dec. 2017, pp. 397–400. doi: 10.1109/ICECS.2017.8292084.

[108] S. M. Mousavi, A. Naghsh, A. A. Manaf, and S. A. R. Abu-Bakar, “A robust medical image watermarking against salt and pepper noise for brain MRI images,” Multimedia Tools and Applications, vol. 76, no. 7, pp. 10313–10342, Apr. 2017, doi: 10.1007/s11042-016-3622-9.

[109] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, “Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains,” Computer Methods and Programs in Biomedicine, vol. 159, pp. 11–21, Jun. 2018, doi: 10.1016/j.cmpb.2018.02.021.

[110] F. Sabbane and H. Tairi, “Medical Video Watermarking Scheme for Telemedicine Applications,” in 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, Apr. 2020, pp. 1–6. doi: 10.1109/IRASET48871.2020.9091982.

[111] S. P. Waghmare and A. S. Bhide, “Shot Boundary Detection using Histogram Differences,” vol. 3, no. 11, p. 5, 2014.

[112] K. Vinothini, S. K. Mydhili, S. Periyanayagi, and G. Sukanya, “Dual Watermarking in Tele-radiology using DWT for Data Authentication and Security,” in 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, Apr. 2019, pp. 0887–0891. doi: 10.1109/ICCSP.2019.8697935.