REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE
ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf - M'sila
Faculté de Technologie
Département d'Electronique

THESE

Présentée en vue de l'obtention du diplôme de
Doctorat en Sciences en Electronique

Présentée par :
MOKHNACHE Salah

THEME

Contribution au développement de méthodes de tatouage dans le domaine des transformées

Soutenue publiquement le :

Devant le jury :

Président :	**Mr SAIGAA Djamel**	**Professeur**	**Univ. M'sila**
Rapporteur :	**Mr CHIKOUCHE Djamel**	**Professeur**	**Univ. M'sila**
Examinateurs :	**Mr BOUGUEZEL Saad**	**Professeur**	**Univ. Sétif 1**
	Mr KADDECHE Mohamed	**Professeur**	**Univ. Annaba**
	Mr LADJAL Mohamed	**Maître de Conférences**	**Univ. M'sila**
	Mr AZIZI Hacene	**Maître de Conférences**	**Univ. Sétif 1**

REMERCIEMENTS

Tout d'abord, j'ai le devoir et le plaisir d'adresser mes remerciements les plus sincères à Monsieur le Professeur ***Djamel CHIKOUCHE****, mon directeur de thèse, pour son aide et conseils constants, pour la confiance et surtout la patience qu'il m'a témoignée durant toutes ces années, et pour son soutien moral et ses encouragements.*

Je souhaite également exprimer profondément mes remerciements les plus sincères à Monsieur ***Djamel SAIGAA****, Professeur à l'Université de M'sila, par l'intérêt qu'il accordé à mon travail et qui m'a fait l'honneur d'être le président de ce jury.*

Je remercie également, Monsieur ***BOUGUEZEL Saad****, Professeur à l'Université de Setif 1, de m'avoir honoré de sa présence, en acceptant d'examiner ce travail. Qu'il reçoit ici l'expression de ma gratitude et mon profond respect.*

Je remercie vivement, Monsieur ***KADDECHE Mohamed****, Professeur à l'Université d'Annaba, d'avoir accepté de juger ce travail et d'en être examinateur. Qu'il reçoit ici l'expression de ma gratitude.*

Je suis très reconnaissant à Monsieur ***LADJAL Mohamed****, Maître de Conférences à l'Université de M'sila, d'avoir accepté de faire partie du jury et d'avoir accepté de juger ce travail et d'en être examinateur.*

Je remercie vivement, Monsieur ***AZIZI Hacene****, Maître de Conférences à l'Université de Setif1, d'avoir accepté de faire partie du jury et d'avoir accepté de juger ce manuscrit et d'en être examinateur.*

Je tiens à remercier, et en particulier mon cher ami ***T. Bekkouche****, pour l'aide qu'il m'a apporté en vue de finir ce modeste travail et beaucoup plus pour l'amitié qu'il m'a témoignée, ainsi que pour son soutien et encouragement, qui m'ont permis de bien concrétiser ce travail.*

Table des figures et liste des Tableaux

Liste des Figures

Liste des Tableaux

Liste des acronymes et abréviations

Liste des acronymes et abréviations

pixel	*Picture Element*
RGB	*RED Green Blue*
BMP	*Bitmap*
TIFF	*Tagged Image Format*
GIF	*Graphic Information Format*
JPEG	*Joint Photograph Experts Group*
PNG	*Portable Network Graphics*
LSB	*Least Significant Bits*
DFT	*Discrete Fourier Transform*
DCT	*Discrete Cosine Transform*
DWT	*Discrete Wavelet Transform*
SVD	*Singular Value Decomposition*
ROP	*Reciproque Orthogonal Parameters*
DHT	*Discrete Hadamard Transform*
PSNR	*Peack Signal to Noise Ratio*
MSE(EQM)	*Mean Square Error*
NCC	*Normalized Cross Correlation*
SSIM	*Structural Similarity Index*
BER	*Bit Error Rate*
LL	*Low-Low*
HL	*High-Low*
LH	*Low-High*
HH	*High-High*
HVS	*Human Visual System*

Table des matières

Sommaire

Introduction générale

INTRODUCTION GENERALE

La prolifération et le récent succès d'Internet, ainsi que la présence d'appareils d'enregistrement et de stockage numériques relativement disponibles et peu coûteux, ont créé un environnement dans lequel il devient très facile d'obtenir, de reproduire et de distribuer du contenu numérique sans perte de qualité. Cela est devenu une grande préoccupation pour les industries de l'édition de contenu multimédia (son, vidéo et image), car il n'existait pas de technologies ou de techniques pour protéger les droits de propriété intellectuelle des médias numériques et empêcher la copie non autorisée. Les technologies de cryptage peuvent être utilisées pour empêcher l'accès non autorisé au contenu numérique. Cependant, le cryptage à ses limites dans la protection des droits de propriété intellectuelle car une fois que le contenu numérique est déchiffré, rien n'empêche un utilisateur non autorisé de le reproduire illégalement. Une autre technologie s'avère évidemment nécessaire pour aider à la fois à établir et prouver les droits de propriété, suivre l'utilisation du contenu, assurer un accès autorisé, faciliter l'authentification du contenu et empêcher la réplication illégale et surtout avec l'ampleur et le grand potentiel d'information dans le domaine de l'imagerie numérique dans de nombreux aspects de la vie courante et professionnelle, la télévision, l'internet, l'audiovisuel, l'imagerie médicale ou encore satellitaire ainsi que la télésurveillance.

Ce besoin a attiré l'attention de la communauté de la recherche et l'industrie menant à la création d'un nouveau formulaire de dissimulation d'information, appelé Tatouage Numérique ou Digital Watermarking, c'est la méthode la plus commode pour traiter le problème de la vie privée et du droit d'auteur et pour assurer l'authenticité des produits multimédias [1] [2].

L'idée de base du watermarking numérique est de créer une métadonnée contenant des informations sur le contenu numérique à protéger, puis de masquer les métadonnées dans ce contenu. Les informations stockées en tant que métadonnées peuvent avoir des formats différents, tels qu'une chaîne de caractères ou un modèle d'image binaire, ou même une image numérique.

Le tatouage numérique des images est réalisé par la dissimulation des informations secrètes dans l'image hôte (document à protéger),il n'est efficace que s'il résiste aux différents traitements que peut subir une image et qu'il survit à plusieurs attaques intentionnelles ou non intentionnelles. Cette information secrète intégrée dans l'image est appelée watermark.

De nos jours plusieurs techniques ont été proposées dans la littérature, certaines d'entre elles sont vues dans [1] [2] [3] [4] .Un algorithme de tatouage efficace devrait satisfaire un ensemble d'exigences, comme la robustesse, l'imperceptibilité, la capacité et la compatibilité du watermark avec l'image originale. Toutes ces exigences doivent être satisfaites sans affecter la qualité de l'image originale [5] [6]. Le tatouage numérique a été utilisé par diverses

méthodes et techniques, ces méthodes sont dues à la diversité du choix de domaine d'insertion utilisé, il peut s'agir d'un domaine spatial ou d'un domaine transformé en fonction de l'application à laquelle le tatouage est dédié. Dans le domaine spatial, les bits de watermark sont directement ajoutés aux pixels de l'image hôte, la méthode du bit le moins significatif (LSB) est un exemple de méthode de domaine spatial dans laquelle la marque est incorporée dans les bits les moins significatifs de l'image de couverture [7]. Dans un domaine transformé, le tatouage utilise comme espace d'insertion un espace résultant d'une transformation et il convient de noter qu'il s'agit d'une transformation dans le domaine fréquentiel où l'incrustation du watermark se fait en modifiant les coefficients de l'image en utilisant des transformées discrètes d'image, comme la transformée en cosinus discrète (DCT) [8] [9], la transformée en ondelettes discrète (DWT) [10] [11], la transformée de Fourier discrète rapide (DFT/FFT) [12],la décomposition en valeur singulière (SVD) [13] et la transformée de Hadamard discrète [14] [15]. Les transformations discrètes ont été utilisées dans le traitement numérique de signal et de l'image, elles ont des applications importantes dans le domaine de tatouage numérique des images.

La présente thèse est structurée en quatre chapitres répartis comme suit :

- Le premier chapitre est consacré essentiellement à l'état de l'art du tatouage numérique des images (images watermarking),où on a définis quelques systèmes de sécurité comme la cryptographie, la stéganographie et bien sûr le tatouage numérique des images, et on a aussi consacré une partie de ce chapitre au schéma général du tatouage des images, la présentation des principaux défis dans un système de tatouage, les méthodes de tatouage telles que le tatouage additif, le tatouage substitutif, les domaines de tatouage des images, les différents types de tatouages, les attaques menaçants le tatouage, les applications du tatouage numérique des images, et à la présentation de quelques métriques d'évaluations pour un bon jugement des approches proposées.
- Le second chapitre décrit quelques transformées discrètes usuelles et la transformée paramétrique orthogonale réciproque (ROP) ainsi que le schéma des algorithmes hybrides de tatouage numérique des images avec l'exploitation du système visuel humain (HVS) pour l'extraction des principales caractéristiques dans une image ce qui permet d'atteindre au maximum les exigences de robustesse et d'imperceptibilité. L'utilisation des caractéristiques d'un système visuel humain HVS aide énormément pour sélectionner les composants les plus appropriés pour insérer la marque. Il existe plusieurs indices utilisés par le système HVS pour la modélisation et la définition de la valeur de facteur de visibilité. Les facteurs utilisés dans notre schéma sont, l'entropie,

l'edge entropie pour une approche et le gradient de l'image pour une deuxième approche comme issue de mesure, car il présente la dérivée spatiale de l'image, ce qui donne une carte topologique de l'image à tatouer, où nous aurons la possibilité de voir et localiser les régions où les perturbations sont intenses et pouvoir également évaluer la douceur moyenne de l'image.

- Le troisième chapitre, présente l'approche d'un schéma de tatouage à base d'un algorithme hybride composé de deux transformées qui sont la DCT et la DWT en exploitant les caractéristiques du système visuel humain, où il exploite la douceur de l'image par le calcul du gradient de l'image pour le choix judicieux des endroits d'incrustation. Une deuxième approche dans ce même chapitre où on a exploité l'entropie et l'edge entropie comme caractéristiques du système visuel HVS en combinant deux transformées discrètes qui sont la SVD et la DCT. L'efficacité des algorithmes hybrides d'un système de tatouage suite à l'évaluation de l'approche par les métriques conçues pour les tests de fiabilité confirment de très bons résultats soit par évaluation objective ou subjective.
- Ce travail traite aussi par une autre approche, dans le quatrième chapitre, le tatouage des images par l'exploitation des transformées discrètes paramétriques orthogonales réciproques (ROP) ,où on a présenté un état de l'art des transformées non paramétriques comme la transformée de Walsh Hadamard et la transformée paramétrique orthogonale (ROP) et sa méthode de développement et de construction. Vu que la ROP se propose comme une nouvelle transformée, son utilisation dans notre approche comme une nouvelle technique de tatouage numérique d'images par blocs et l'exploitation de ces paramètres indépendants comme des clés secrètes pour renforcer la sécurité et consolider la robustesse de notre schéma de tatouage, a donné des résultats expérimentaux très satisfaisants, spécialement l'analyse des attaques malicieuses, qui montre clairement l'efficacité de la paramétrisation de la méthode proposée. En plus, cette méthode présente un avantage de complexité réduite par rapport à celles des méthodes de tatouage d'images existantes, vu qu'elle se base sur le calcul des matrices de Hadamard qui présentent une simplicité dans le calcul car les éléments de la matrice de transformation sont +1 et -1. Par conséquent, le calcul ne nécessite que des opérations d'addition et de soustraction sans effectuer des opérations de multiplication, ce qui réduit le temps de traitement.

Ce manuscrit sera clôturé par une conclusion générale résumant les approches proposées et donnant quelques perspectives pour ce travail.

Chapitre I

Etat de l'art du tatouage numérique des images

INTRODUCTION

Le succès d'internet avec les progrès substantiels des chercheurs où ils se sont penchés à numériser les données et à normaliser les échanges d'information. Ces progrès, bien qu'ils ont facilités la copie, le partage, l'enregistrement et le stockage des données numériques de natures diverses. Ils ont donnés naissance à des problèmes qui sont relatifs à la sécurité et l'authenticité , et pour protéger les droits de propriété intellectuelle des médias numériques appelés aussi "nouveaux médias", qui sont les médias électroniques, interactifs et audiovisuels basés sur des codes numériques, et empêcher la copie non autorisée, le tatouage numérique appelé aussi watermarking vient alors s'annoncer comme une technique visant à contribuer à la sécurité et l'authenticité de ces données électroniques.

Ce chapitre est conçu à la présentation de l'état de l'art du tatouage numérique des images.

A ce propos, nous avons défini quelques systèmes de sécurité comme la cryptographie, la stéganographie et bien sûr le tatouage numérique des images.

Les autres paragraphes s'intéressent au schéma général du tatouage des images, la présentation des principaux défis dans un système de tatouage, les méthodes de tatouage telles que le tatouage additif, le tatouage substitutif, les domaines de tatouage des images, les différents types de tatouages, les attaques menaçant le tatouage, les applications du tatouage numérique des images, la présentation de quelques outils d'évaluations et on termine par une conclusion.

I.1.LES SYSTEMES DE SECURITE

I.1.1. Cryptographie

Au cours des dernières années, il y a eu une amélioration et une émergence considérables des technologies de communication, de codage et de récupération du multimédia numérique. Un tel environnement a permis la réalisation de nombreuses applications multimédia fascinantes liées à presque tous les aspects de la vie. Les entreprises et autres organisations peuvent désormais effectuer des audioconférences et des vidéoconférences en temps réel. Les systèmes de base de données d'imagerie médicale, même ceux des régions éloignées, peuvent instantanément recevoir et examiner des images médicales pertinentes en utilisant la puissance du codage d'image et des techniques de récupération d'images. Cependant, de nombreux réseaux de distribution multimédia sont des canaux publics ouverts et, en tant que tels, ils sont jugés peu sûrs. Une oreille indiscrète peut facilement intercepter et capturer le contenu multimédia sensible et précieux voyageant dans une chaîne publique. Heureusement,

que l'art magique de la cryptographie peut aider à prévenir cela. En général, la sécurité multimédia est obtenue par une méthode ou un ensemble de méthodes utilisées pour protéger le contenu multimédia contre un accès non autorisé ou contre une distribution non autorisée. Ces méthodes sont fortement basées sur la cryptographie et fournissent soit la sécurité de la communication, soit la sécurité contre le piratage. La sécurité de communication des données multimédia peut être accomplie au moyen d'une cryptographie conventionnelle. Les données multimédia peuvent être entièrement cryptées à l'aide d'un système de cryptage adéquat. La cryptographie peut être donc définie comme étant une technique qui vise la protection des données confidentielles. Elle regroupe l'ensemble des algorithmes de chiffrement qui appliquent une transformation dépendante d'un paramètre secret appelé "clé" afin de rendre le message non compréhensible [16,17]. La personne voulant décoder le message crypté doit forcément connaitre la clé ainsi que la méthode de cryptage. Les crypto systèmes classiques comme le cryptage par substitution sont puissants mais limités en termes de données multimédia volumineuses et hautement redondantes. Le cryptage sélectif et le cryptage basé sur le chaos sont souvent utilisés pour fournir une sécurité multimédia plus rapide et de meilleure qualité.

I.1.2.Stéganographie

La dissimulation des données est souvent utilisée comme synonyme de stéganographie. La cryptographie peut être utilisée en combinaison avec la stéganographie, qui ajoute une couche supplémentaire de sécurité.

La stéganographie est donc l'art de la dissimulation de l'information : son objet est de faire passer inaperçu un message dans un autre message de façon que seule la personne connaissant l'astuce soit apte à extraire le message caché [18].

La stéganographie et le tatouage décrivent des techniques qui sont utilisées pour transmettre imperceptiblement l'information en l'incorporant dans les données de couverture. Cependant, la stéganographie se rapporte généralement à une communication cachée point à point entre deux parties. Ainsi, les méthodes stéganographiques ne sont généralement pas robustes contre la modification des données, elles protègent les informations incorporées contre les modifications qui peuvent survenir pendant la transmission et le stockage, comme la conversion de format, la compression ou la conversion numérique-analogique. On cite l'exemple de stéganographie connu sous le nom "principe de l'encre invisible". Cette technique était beaucoup utilisée dans le but d'envoyer des messages secrets. A cette époque,

l'encre était réalisée à base de jus d'oignons et de chlorure d'ammoniac. L'écriture était alors rendue claire en approchant le papier d'une flamme de bougie.

Certaines méthodes stéganographiques associent la cryptographie traditionnelle à la stéganographie **:** l'expéditeur crypte le message secret avant le processus d'intégration. Clairement, une telle combinaison augmente la sécurité du processus de communication global, car il est plus difficile pour un attaquant de détecter le texte chiffré incorporé (qui lui-même a une apparence plutôt aléatoire) dans une couverture. Cependant, les systèmes stéganographiques forts n'ont pas besoin de chiffrement préalable. [19]

Bien qu'un système de stéganographie se compose normalement de trois parties : la détection, l'extraction et la désactivation des informations intégrées, un système est déjà peu sûr si un attaquant est capable de prouver l'existence d'un message secret. En développant un modèle de sécurité formel pour la stéganographie, nous devons supposer qu'un attaquant a un pouvoir de calcul illimité et qu'il est capable d'effectuer une variété d'attaques. S'il ne peut pas confirmer son hypothèse qu'un message secret est inclus dans une couverture, alors le système est théoriquement sécurisé.

I.1.3. Tatouage

Le tatouage numérique est une technique d'intégration d'informations authentiques dans un contenu numérique. Il fait recours à des algorithmes pour intégrer des signatures et des marques afin de protéger les droits d'auteur du contenu numérique. Il est devenu très important dans divers domaines d'application pour la protection et l'authenticité, comme la vidéo, l'audio, le texte et l'image. De nombreux auteurs ont présenté un certain nombre de techniques de tatouage qui se différencient par leurs techniques d'insertion et les algorithmes proposés.

Par définition, le tatouage numérique est une technique qui consiste à insérer une marque, généralement sous forme d'un message ou d'un logo, dans un document numérique dit "document hôte", la marque insérée par un tel schéma de tatouage doit être ineffaçable.

C'est-à-dire qu'une fois insérée, il est impossible de l'enlever sans avoir recours à la clé ou à la méthode d'insertion. D'autre part, elle doit être robuste face à toute attaque susceptible d'altérer le contenu du document hôte [20].

Il y a une classe importante d'applications qu'utilise le tatouage pour assurer un certain niveau de protection des droits de propriété intellectuelle. Les applications de cette classe utilisent des watermaks comme support pour l'information sur la propriété du contenu et les droits de propriété intellectuelle.

Ces applications peuvent être utilisées pour la protection des droits d'auteur, la protection contre la copie illicite et les empreintes digitales. Pour la vérification du contenu, ces classes intègrent des marques dans un contenu numérique multimédia pour garantir que le contenu original n'a pas été modifié et pour aider à déterminer le type et l'emplacement de la modification dans le cas où le contenu original a été modifié. L'internet offre des opportunités et des avantages extraordinaires à ses utilisateurs grâce à son énorme réseau qui est appelé réseau informatique formé d'un ensemble d'équipements reliés entre eux pour échanger des informations.

Mais dans de nombreux cas, les propriétaires sont préoccupés par la sécurité du contenu numérique en raison de la possibilité de produire des imitations de leur contenu d'origine facilement partout dans le monde. Selon les informations sur le marché noir global du Havocscope, les internautes ont reproduit illégalement plus de 400 millions de fichiers numériques rien qu'au Royaume-Uni entre novembre 2012 et janvier 2013 [21, 22]. Ainsi, des techniques de pointe sont nécessaires pour arrêter la falsification, le partage illégal et la réplication des informations et plutôt des techniques normalement utilisées pour réserver les droits de propriété, par exemple, la cryptographie, la stéganographie, et la signature numérique [23].

Le chiffrement ou la cryptographie à clé publique transforme les fichiers d'origine en cryptogramme ou texte chiffré, et sans la clé de décryptage, les documents numériques cryptés ne peuvent pas être visualisés [23]. Mais l'expéditeur n'a aucun moyen de surveiller la façon dont le destinataire traite les informations après le déchiffrement. Cependant, la technique de tatouage numérique n'affecte pas l'originalité de l'image de couverture. Les marques et les signatures numériques ne peuvent pas être récupérées sans logiciel approprié. En outre, des marques numériques sophistiquées sont conçues dans le but de persister dans la visualisation, l'impression ou la distribution ultérieure. Cox et al. [24] ont dévoilé dans une étude que les techniques de tatouage numérique et de cryptage sont comme deux bateaux différents à naviguer pour surmonter la confusion sur les mots à la mode. Depuis 1990, un grand groupe de chercheurs ont montré leur vive attention dans le domaine du tatouage numérique pour son grand potentiel dans le monde de l'internet [25].

Le concept général du tatouage le rapproche en fait beaucoup plus de la stéganographie que de la cryptographie. Cependant, il faut bien mentionner les différences essentielles entre les deux. En particulier, il est indispensable en stéganographie que l'existence même du message soit dissimulée ; au contraire, en tatouage, la connaissance publique de l'existence d'une marque dans un document hôte peut être un moyen de dissuasion contre la copie illicite.

D'autre part, en stéganographie, le message de couverture n'est pas aussi important, qu'en tatouage, il est nécessaire que ce message ne soit pas dénaturé et endommagé, lors de l'insertion de la marque et lors d'une attaque qui vise à détruire cette marque. Le lien entre le message caché ou la marque dissimulée et les documents supports est donc beaucoup plus fort de point de vue imperceptibilité et robustesse [26].

I.2. CYCLE DE VIE DU PROCESSUS DE TATOUAGE NUMERIQUE

Le cycle de vie d'une opération de tatouage, est divisé en trois étapes distinctes : L'insertion (l'incorporation de la marque ou de la signature), la manipulation de l'image (les attaques), et l'extraction (la détection de la marque ou de la signature) [27].

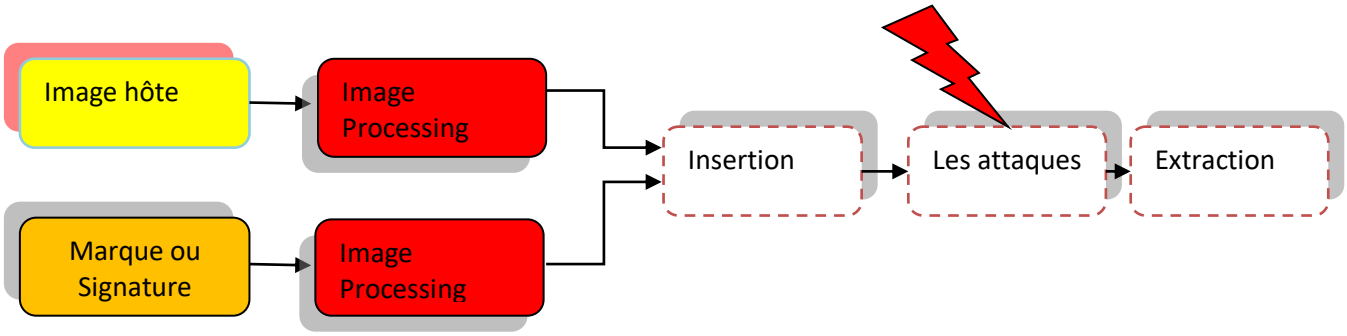


Figure I.1 : Schéma général du tatouage numérique des images

Le schéma général d'un système de tatouage numérique des images peut être décrit principalement par deux phases fondamentales : l'insertion et l'extraction de la marque. Cependant, une troisième étape peut être considérée : la transmission.

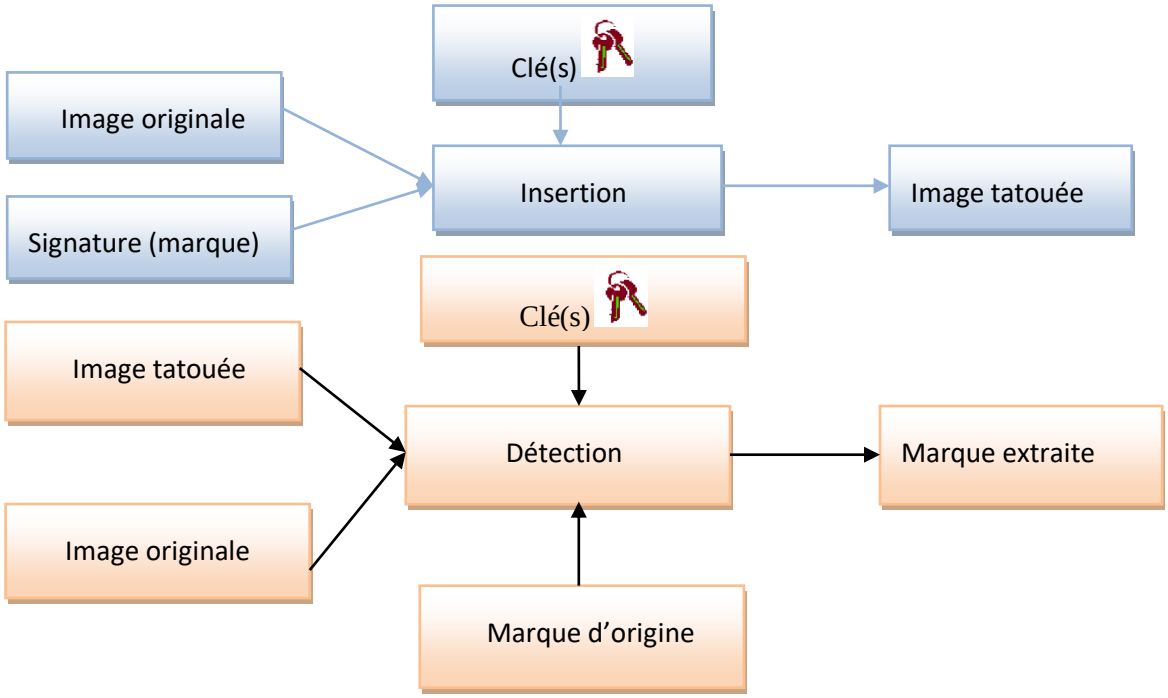


Figure I.2 : Schéma général d'un Watermarking (insertion/extraction)

I.2.1. Insertion de la marque

La phase d'insertion nécessite comme entrée une image hôte, pour qu'elle soit combinée avec la marque à insérer, cette marque peut être choisie par l'utilisateur selon le domaine d'application du tatouage. L'utilisateur peut choisir des informations textuelles, comme ses coordonnées, il peut également choisir une image, comme un logo d'entreprise, des images de construction ou des photos personnelles comme marques, où ces images peuvent être des images en niveau de gris, des images en noir et blanc ou des images en couleur. Ces marques peuvent être intégrées dans des images originales ou de couverture à l'aide de techniques d'insertion. Souvent le schéma utilise en plus une clé d'insertion, où on aura à la sortie une image tatouée. Les images tatouées sont perceptuellement semblables et proches des images hôtes (originales) avec moins de distorsions pour assurer la bonne imperceptibilité de l'opération de tatouage. Ces images tatouées peuvent être communiquées à travers les canaux de communication ou stockées dans des bases de données pour servir à une indexation ou pour une transaction quelconque.

Les schémas d'insertion de tatouage d'images sont classés selon la manière dont la marque est intégrée dans l'image hôte. Soit un schéma de tatouage additif ou de tatouage substitutif.

Le tatouage dit additif réside principalement dans l'ajout d'un "bruit" à l'image et celui dit substitutif consiste essentiellement à substituer la marque à des composantes de l'image.

Selon l'application à laquelle est dédiée le tatouage, l'insertion peut s'effectuer directement sur l'image, c'est ce qu'on appelle le domaine spatial, soit dans le domaine transformé ou domaine fréquentiel suite à l'utilisation de quelques transformées [4] ($DCT, DFT, DWT..$)

I.2.2. Extraction de la marque

Le propriétaire de l'image tatouée doit prouver l'authenticité chaque fois que l'image est dupliquée sans son consentement. L'auteur doit extraire la marque de l'image tatouée qui a subie des attaques de traitement d'image grâce à une fonction de traitement d'extraction bien définie. Donc à la sortie, on aura soit une marque extraite soit une décision indiquant si l'extraction a été faite convenablement ou non.

Selon la méthode d'extraction de la marque, on peut citer les modes les plus connus et les plus utilisée comme :

Le mode non-aveugle, le mode semi-aveugle et le mode aveugle [28]. Ces modes spécifient l'information à priori dont dispose le module d'extraction pour la vérification du tatouage. L'utilisation de tel ou tel mode dépendra de l'application visée et des protocoles utilisés :

- ✓ **Mode non-aveugle :** le récepteur dispose de l'image hôte ainsi que la marque originale. Ce contexte est bien évidement incompatible avec des applications visant à vérifier l'intégrité de l'image, ou à assurer la vérification en temps réel du copyright (problème de temps d'accès à la base de données contenant les informations originales) [28,32].
- ✓ **Mode semi-aveugle :** Le récepteur doit disposer uniquement de la marque originale en plus de la clé d'insertion, il est souvent utilisé via un score de corrélation.
- ✓ **Mode aveugle :** Pour le mode aveugle, les schémas d'extraction utilisent seulement la clé d'insertion lors de la phase de détection [32].

I.3. DOMAINE DE TATOUAGE DES IMAGES

Les techniques de marquage appliquées aux images sont liées aux différents espaces de représentations appelés domaines, et chaque domaine d'insertion dispose de divers schémas de marquage, qui sont dues principalement à la diversité du choix de domaine d'insertion utilisé. Ce dernier peut être soit un domaine spatial soit un domaine transformé [32].

I.3.1. Tatouage dans le domaine spatial

L'insertion consiste à travailler directement sur l'image en modifiant l'intensité des pixels qui vont emporter la marque car les bits de la marque sont directement ajoutés aux pixels de l'image de couverture. Souvent, nous utilisons dans ce domaine des images monochromes mais nous pouvons également marquer sur des images en couleur, où une ou plusieurs composantes d'un espace colorimétrique quelconque seront modifiées.

Ce sont des méthodes simples et peu coûteuses en temps de calcul puisqu'elles ne nécessitent pas une étape préalable de transformation. Elles sont consacrées aux marquages en temps réel demandés dans des environnements de faible puissance.

Les méthodes de domaine spatial peuvent être facilement modélisées et analysées mathématiquement. Cependant, la marque incorporée peut être facilement détruite ou éliminée par des attaques de traitement du signal .La technique du domaine spatial s'appuie sur l'exploitation du système visuel humain, car les données cachées doivent être entièrement imperceptible par le système visuel humain (SVH). L'opération d'insertion ne doit pas affecter le porteur de la marque d'une façon perceptible. L'invisibilité est une propriété fortement liée au marquage invisible. Certaines techniques dans le domaine spatial peuvent être robustes aux

attaques de type transformations géométriques Parmi les transformations géométriques, la plus usuelle est la modification des dimensions de l'image, on cite aussi les transformations affines tels que la translation et le zoom. Quant à l'extraction, une simple corrélation permet de retrouver la marque insérée.

Parmi les nombreux schémas spatiaux d'insertion, soit le schéma de tatouage additif ou le schéma de tatouage substitutif, on cite comme schéma aditif le modèle basé sur l'ajout d'une séquence aléatoire 2D, nous distinguons aussi la technique d'étalement de spectre de Hartung et Girod [29] et la technique du patchwork de Bender et Morimoto [30].

La méthode (LSB) ou la manipulation des bits les moins significatifs est un exemple de méthode de domaine spatial dans laquelle la marque est incorporée dans les bits les moins significatifs de l'image de couverture sachant que la numérisation d'une image analogique introduit un bruit de quantification, qui modifie principalement les bits les moins significatifs de chaque pixel. Il est alors possible de remplacer ce bruit ou de lui ajouter un signal. Comme le montre les travaux de Wolfgang et Delp [31] où ils ajoutent un motif 2D crée à partir de séquences binaires pseudo aléatoires. Les bits les moins significatifs sont très sensibles au bruit, de sorte que la marque peut être facilement éliminée par des manipulations d'image telles que la rotation et le recadrage. Ainsi, la méthode LSB offre une forte imperceptibilité mais moins de robustesse. Il y a aussi le schéma basé sur la corrélation qui est un autre exemple de techniques de domaine spatial , pour cette méthode, la marque est convertie en une séquence pseudo-aléatoire qui est ensuite pondérée et ajoutée aux bits d'image de couverture. L'image tatouée est comparée à l'image de couverture pour détecter la marque insérée. La capacité de dissimulation des données des techniques de domaine spatial est plus élevée que celle des méthodes de domaine fréquentiel.

I.3.2.Tatouage dans le domaine transformé

Les domaines de transformation ont été largement étudiés dans le contexte du codage et de la compression d'images, et de nombreux résultats de recherche peuvent être appliqués au tatouage numérique [32]. La théorie du codage d'image maintient que dans la plupart des images, les couleurs des pixels voisins sont fortement corrélées. Le mappage dans un domaine de transformation spécifique, tel que la DCT ou laDWT, sert à deux fins, il décorrèle les valeurs de l'échantillon original, et il concentre l'énergie du signal original en quelques coefficients seulement. Par exemple, lorsqu'une image typique est mappée dans le domaine de la fréquence spatiale, l'énergie est concentrée dans les termes à faible fréquence, qui sont très

grands, comparés aux termes à fréquence élevée. Cela signifie qu'une image typique est dominée par les composantes basses fréquences. Ces basses fréquences représentent les formes et contours globaux des éléments de l'image, ainsi que leurs caractéristiques de luminance et de contraste.

Ce qui justifie que la robustesse et l'imperceptibilité des images tatouées peuvent être améliorées en effectuant un tatouage dans le domaine fréquentiel et ce qui facilite le choix de l'endroit d'incrustation dans les régions basses et moyennes fréquences. Les techniques de domaine fréquentiel peuvent fournir une meilleure robustesse contre les attaques de compression et de filtrage, car les coefficients de la marque se répartissent dans toute l'image de couverture.

Le domaine fréquentiel et par le biais des transformées, est utilisé pour analyser les propriétés d'un signal ou précisément d'une image. Cela permet d'étudier le spectre pour déterminer les gammes de fréquences présentes dans le signal d'entrée. Les signaux sont convertis du domaine temporel ou spatial vers le domaine fréquentiel par un outil mathématique appelé transformée, comme la transformée de Fourier (FT), transformée de Fourier discrète (DFT), transformée de Fourier rapide (FFT), transformée de Hadamard discrète (DHT), transformée de Walsh Hadamard (WHT), Transformée en cosinus discrète (DCT), et la Transformée en ondelettes discrète (DWT). Ces transformées convertissent l'information du signal en module (magnitude) et en phase. Dans certaines applications, la façon dont la phase varie avec la fréquence peut être un facteur important [32].

L'utilisation des transformées rend le message plus robuste à la compression, puisqu'elle utilise le même espace qui sert au codage de l'image (DCT utilisée par$JPEG$, et la DFT par$MPEG$). Contrairement au domaine spatial, la marque insérée dans le domaine fréquentiel est très sensible aux transformations géométriques car les transformées modifient considérablement les valeurs des coefficients transformés.

La multirésolution par la transformée en ondelettes DWT utilisée par les normes de compression$JPEG2000$, pour les images est aussi un espace qui permet la décomposition de l'image en sous-bandes de fréquence, ceci permet un isolement affiné des composantes basse-fréquences, qui est un espace d'insertion moins sensible tout en gardant un contenu spatial de l'image conservé et qui peut être utile pour l'insertion de l'information. La DWT est considérée comme une décomposition en canaux perceptifs qui facilite l'utilisation d'un modèle psycho visuel lié directement à la perception humaine et qui donne une bonne évaluation qualitative des images tatouées [11,33].

Il est à noter aussi qu'actuellement plusieurs méthodes de tatouage utilisent la projection des caractéristiques originales dans un autre espace tout en éliminant la redondance de l'information, ces transformations peuvent être soit la SVD (singular values decomposition) soit KLT (Transformée de Karhunen-Loeve).

I.3.2.1 Domaine DCT

Le domaine DCT [32] a été largement utilisé pour l'incorporation d'un watermark [34] pour un certain nombre de raisons. En utilisant laDCT, une image est divisée en bandes de fréquences, et le watermark peut être incorporé de manière pratique dans les bandes de fréquences basses à moyennes visuellement importantes. Les sensibilités du système visuel humain aux changements de ces bandes ont été largement étudiées dans le contexte de la compression$JPEG$, et les résultats de ces études peuvent être utilisés pour minimiser l'impact visuel de la distorsion d'inclusion du watermark. De plus, les exigences de robustesse à la compression JPEG peuvent être facilement abordées car il est possible d'anticiper quels coefficients DCT seront rejetés par le système de compression JPEG. Enfin, puisque le codage $JPEG\ /\ MPEG$ est basé sur la décompositionDCT, incorporer un watermark dans le domaine DCT permet d'intégrer le watermarking avec le codage image et vidéo. Cette intégration permet le développement d'applications de tatouage en temps réel.

I.3.2.2 .Domaine DWT

Avec la standardisation de $JPEG2000$, et la décision d'utiliser la compression d'image basée sur les ondelettes au lieu de la compression DCT, les techniques de tatouage fonctionnant dans le domaine de la transformation en ondelettes sont devenues plus attrayantes pour la communauté de recherche de tatouage numérique des images. Les avantages de l'incorporation des watermarks dans le domaine de la transformée en ondelettes sont d'une robustesse inhérente. De plus, la transformée en ondelettes a des propriétés qui peuvent être exploitées par des solutions de tatouage numérique [33]. Par exemple, la transformation en ondelettes fournit une représentation multirésolution des images. Cela peut être exploité pour construire des schémas de détection plus efficaces, lorsque la détection ou l'extraction commence d'abord par les sous-bandes de basse résolution, et si la détection échoue dans ces sous-bandes, on explore les sous-bandes de résolution plus élevée et les coefficients

supplémentaires qu'elle fournit. Zhu et al [35] introduisent une approche du tatouage numérique basée sur le bidimensionnel (2D) d'une transformée en ondelette discrète.

I.3.2.3 Domaine DFT

La transformée de Fourier discrète d'une image est généralement complexe [32], ce qui conduit à une représentation en module et en phase de l'image. Pour une transformée DFT l'incrustation de la marque se fait soit en module soit en phase [36].

L'ajout de la marque à la phase de la DFT [37] améliore la robustesse du tatouage car toute modification des composantes de l'image qui est visuellement importante dans une tentative de suppression de la marque dégradera significativement la qualité de l'image. Une autre raison pour modifier ou moduler les coefficients de phase pour ajouter une marque est basée sur les résultats de la recherche sur la théorie des communications, qui établissent que la modulation de la phase est plus immunisée contre le bruit que la modulation d'amplitude. Enfin, le tatouage par phase est relativement robuste aux changements de contraste de l'image.

Une autre alternative consiste à ajouter la marque aux coefficients de l'amplitude DFT uniquement [36]. L'ajout de la marque aux coefficients d'amplitude DFT est avantageux car les coefficients d'amplitude DFT transmettent très peu d'informations sur une image, et l'incorporation d'une marque dans ces coefficients ne devrait pas introduire une distorsion perceptible. Cependant, étant donné que la distorsion causée par les modifications des coefficients de l'amplitude DFT est beaucoup moins perceptible que la distorsion causée par les modifications de phase [36].

Le domaine amplitude DFT est invariant par translation, et cette propriété peut être très utile pour le tatouage. Le domaine d'amplitude DFT est un invariant en translation car une translation cyclique d'une image dans le domaine spatial n'affecte pas les coefficients d'amplitude DFT. Par conséquent, la marque incorporée dans les coefficients d'amplitude DFT ne sera pas affectée par les translations d'image ou le décalage dans le domaine spatial.

I.4. CLASSIFICATION DES SCHEMAS DE TATOUAGE

Les techniques de tatouage numérique peuvent être classées en fonction de leur robustesse, perceptibilité et capacité. Un tatouage est appelé fragile s'il ne parvient pas à être détecté après la moindre modification. Les tatouages fragiles sont couramment utilisés pour la preuve de l'intégrité. Un tatouage est également appelé semi-fragile s'il résiste à des transformations bénignes mais échoue à la détection après des transformations malignes. Les tatouages semi-

fragiles sont couramment utilisés pour détecter les malignités. Un tatouage est appelé robuste s'il résiste à une classe de transformations désignée. Les tatouages robustes sont couramment utilisés dans les applications de droits d'auteur et les applications de protection contre la copie. Un tatouage est appelé imperceptible si le signal de couverture d'origine et le signal marqué ou l'image tatouée sont des contenus non marqués perceptivement, donc le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée.

On définit l'imperceptibilité en tant que similitude visuelle entre l'image originale et l'image tatouée [38]. De ce fait assurer l'invisibilité de la marque doit respecter la qualité visuelle de l'image tatouée et limiter les dégradations sur l'objet d'origine. C'est la cause que plusieurs algorithmes de tatouage existants ont tendance à insérer la marque dans les zones d'intérêts les moins sensibles à l'œil humain [39].

L'une des taches majeures lors d'une opération de tatouage est d'assurer un bon compromis de la capacité d'insertion ou le taux d'intégration ; on l'appelle aussi ratio, qui est le rapport entre le nombre de données à dissimuler et la taille de l'image hôte. En effet, l'insertion de la marque dépend du nombre de pixels aptes à être changés, de même, la quantité d'infirmation à insérer dépend de l'application ciblée ainsi que des contraintes pratiques imposées.

Dans les toutes premières approches, seul un bit d'information était inséré. Le message retrouvé après détection était donc binaire : donnée marquée ou non. Toutefois, de nos jours une maximisation de la taille de l'information à insérer est demandée selon le domaine et la technique de tatouage appliquée. En pratique plus le taux d'intégration soit faible, plus la robustesse et l'invisibilité peuvent être de plus en plus acceptables.

I.4.1.Compromis entre invisibilité, robustesse et la capacité d'insertion

L'invisibilité, la robustesse et le taux d'intégration sont des propriétés liées les unes aux autres. L'évolution de l'une de ces trois paramètres influe directement sur le sort des attributs qui restent.

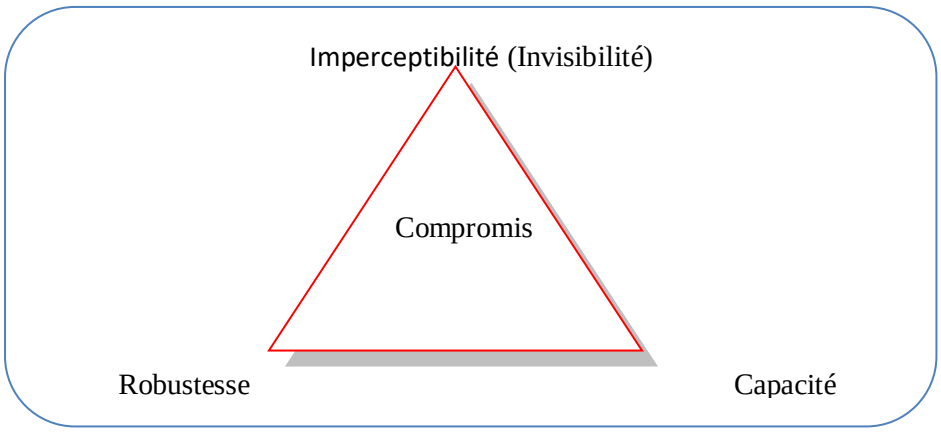


Figure I.3 : Le triangle de contraintes

Bas [40] a confirmé que la croissance de taille de la marque à insérer, peut entraîner, soit une dégradation de l'aspect psycho visuel de l'image soit une réduction au niveau de la sécurité des données à extraire. Il est devenu très important alors de réfléchir à ces trois contraintes lors de la phase d'insertion. La figure I-3 est une présentation du triangle de contraintes montrant la relation entre la capacité, la visibilité et la robustesse.

I.5. ATTAQUES MENACANT LE TATOUAGE

Lorsque les images tatouées sont partagées ou communiquées à travers les canaux de communication, elles sont déformées à cause de divers algorithmes de traitement d'image comme, le rééchelonnement, la compression, le filtrage linéaire et non linéaire, le bruit additif [41]. Dans ces cas, les images tatouées devraient garder la marque même après les attaques. Certaines de ces attaques sont des attaques de suppression, des attaques géométriques, des attaques cryptographiques et des attaques de protocole [41, 42]. La marque peut être retirée de l'image tatouée suite à l'application des techniques de traitement d'image telles que le débruitage, la compression avec perte, la quantification, la démodulation, il y a aussi des attaques de traitement d'image, telles que le recadrage, la rotation, le décalage, et la mise à l'échelle, qui détruiront la marque existante à partir des images tatouées.

Afin de tester la robustesse des algorithmes de tatouage, certaines applications ont été développées, comme les attaques puissantes StirMark qui ont été conçues par un groupe de recherche à l'Université de Cambridge [43].

Il consiste à appliquer un logiciel comportant une série d'attaques standards, telles que la rotation, le fenêtrage, le rehaussement, le changement d'échelle, le découpage, la transformation linéaire, le filtrage, l'ajout de bruit et d'autres transformations géométriques et distorsions géométriques. Le banc de tests StirMark est tellement efficace que trop peu d'algorithmes de tatouage des images numériques fixes lui résistent.

La recherche dans le domaine de tatouage a produit un large éventail de techniques qui peut être subdivisé en divers niveaux de complexité méthodologique.

Chacune de ces méthodes tente de réduire la vulnérabilité dans divers scénarios d'attaque. Les attaques sur les tatouages numériques peuvent être principalement classées en deux groupes: attaques bienveillantes et attaques malveillantes [44].

I.5.1. Attaques bienveillantes

Les attaques bienveillantes appelées aussi attaques non-intentionnelles, elles ne tentent pas à écraser la marque insérée ou à l'effacer, elles figurent dans le domaine des traitements naturels de l'image telles que la conversion analogique numérique, la compression, le filtrage linéaire (passe-bas, passe-haut, passe-bande) ou non linéaire (médian), les attaques géométriques, le scannage, le rehaussement, le moyennage, etc.…

I.5.1.1. Transformations géométriques

Les transformations géométriques ont pour but de modifier la position des informations contenues dans l'image comme par exemple l'inversion horizontale d'une image (symétrie horizontale).

Les opérations géométriques de base sont la translation, la rotation, le recadrement, la mise à l'échelle (étirement vertical ou horizontal de l'image)

Pour chacune de ces opérations, on peut considérer que l'opération est une transformation des éléments de l'image.

I.5.1.2. Compression

La qualité visuelle et perceptuelle des images numériques prend de l'ampleur avec le développement de nouvelles méthodes d'affichage et de nouvelles techniques d'acquisition des formats des images numériques (haute définition HD, UHD ,$4k$). Cependant, la taille de ces images augmente par rapport à leurs qualités, leurs stockages et leurs transmissions ce qui impose donc des enjeux majeurs dans le monde numérique. La compression s'impose comme une étape inévitable pour gérer et optimiser l'utilisation de ces grands volumes d'informations. L'objectif de la compression d'image est de réduire la quantité d'information et les tailles des fichiers images nécessaire à une bonne représentation visuelle de l'image originale. Le format $JPEG$ et $JPEG$ 2000 représentent les standards les plus utilisés pour la compression des images. Les attaques par compression dans le domaine de tatouage des images numériques, affectent et altèrent sensiblement les images tatouées et généralement la détection de la marque après compression devient très sensible car, les algorithmes de compression ne gardent de l'image tatouée que les composantes essentielles.

I.5.1.3. Ajout de bruit

L'ajout de bruit dans le monde de l'imagerie et surtout lors d'une transmission quelconque d'un contenu d'images tatouées est inévitable, il se présente comme une altération de l'image

originale donc non désirable, puisqu'il provoque une dégradation de la qualité visuelle de l'image. A la réception, la récupération de la signature d'une image tatouée bruitée ne sera pas facilement détectable, des exemples de bruit artificiel peuvent être cités :
Le bruit additif comme le bruit gaussien qui consiste à un ajout de bruit successif de valeurs générées aléatoirement à chaque élément de l'image (pixel), le bruit multiplicatif comme le bruit speckle et le bruit impulsionnel appelé Salt & Pepper (sel et poivre) qui transforme aléatoirement plusieurs pixels de l'image en pixels noir ou blanc ou aux valeurs 255 ou 0 (valeurs extrêmes de l'intervalle des niveaux de gris). Ce type de bruit impulsionnel peut apparaître au cours d'une transmission.

I.5.1.4. Filtrage

Enlever un bruit d'une image bruitée veut dire simplement la filtrer, pour rendre l'image plus nette et améliorer sa qualité visuelle. Le filtrage est le processus qui permet de remplacer un pixel par une valeur qui est fonction des données à proximité du pixel.
Des méthodes de filtrage pour le débruitage, issues du traitement du signal, ont été adaptées au traitement des images numériques comme les filtres non linéaires, pour l'atténuation du bruit impulsionnel et le rehaussement des discontinuités tels que les filtres médians ou les filtres morphologiques. Il y a aussi le filtrage linéaire qui a pour but l'élimination de l'effet des perturbations qui peuvent affecter une image en essayant de ne pas toucher aux informations essentielles de l'image (contours, dynamique, textures etc.). Les techniques de filtrage linéaire de base permettent de supprimer les effets d'un bruit additif, on peut citer les filtres linéaires moyenneur et le filtre gaussien, etc.
Malgré leurs importances, les filtres restent des attaques nuisibles au système de tatouage puisqu'ils peuvent altérer ou bien même détruire une signature insérée.

I.5.2. Attaques malveillantes

Afin de pouvoir comparer les systèmes de tatouage, c'est-à-dire leurs robustesse et leurs imperceptibilité, il est nécessaire de tester leur résistance par rapport à des manipulations photométriques et géométriques classiques, compressions mais également à des attaques malveillantes ou intentionnelles effectuées sur un même ensemble d'images de tests représentatives.
Les attaques intentionnelles sont des attaques de désynchronisation et des attaques qui tentent même à altérer et détruire la marque insérée dans le document hôte, parmi de tels logiciels d'évaluation, on peut mentionner le logiciel StirMark [43].

On trouve dans la littérature qui traite les attaques dans le monde du tatouage numérique l'attaque appelée directement l'attaque StirMark qui est une attaque de type géométrique, elle consiste à simuler l'effet d'une impression suivie d'une acquisition par scanner. L'image subit de légères déformations géométriques locales ainsi qu'un bruit additif de faible amplitude [26]. L'image garde une très haute qualité visuelle, seulement, les distorsions géométriques suffisent souvent à faire échouer la détection du tatouage, donc une mauvaise extraction, notamment lorsque celle-ci s'effectue par corrélation.

On cite aussi l'attaque Jittering ou " Jitter -attack ", qui est classée aussi parmi les attaques malveillantes, c'est une attaque qui permet d'inverser, de remplacer certaines lignes ou colonnes de l'image tatouée par d'autres, d'une façon aléatoire. La perception visuelle n'est pas trop altérée après l'opération de remplacement et l'effet sur le détecteur peut être destructeur, ce genre d'attaque est très efficace face à des schémas d'insertion de type étalement de spectre [26].

Il existe aussi l'attaque Mosaïque " Mosaïc-attack " [43] qui consiste à diviser l'image en différentes parties, ce qui divisera la marque en plusieurs morceaux et c'est à cause de cette division, que la détection de la marque ne pourra pas être effectuée sur toute l'image mais seulement sur des parties séparées de l'image, ce qui déroutera le détecteur et ce qui fera échouer la détection.

I.6. APPLICATIONS DU TATOUAGE NUMERIQUE DES IMAGES

Il est souvent nécessaire d'associer des informations supplémentaires à un contenu numérique, tels que, des images, des vidéos ou des enregistrements sonores. Par exemple, un avis de droit d'auteur peut être associé à une image pour identifier le propriétaire légal, un numéro de série peut être associé à une vidéo pour identifier un utilisateur légitime, ou un identifiant peut être associé à une propriété intellectuelle pour localiser une base de données quelconque pour obtenir plus d'informations. Le tatouage numérique s'installe comme la méthode appropriée pour associer cette information supplémentaire, comme des métadonnées, celles-ci sont insérées imperceptiblement comme une marque ou une signature dans un contenu numérique, qui fera le rôle d'une couverture (document hôte) [32].

Il existe une classe importante d'applications qui utilisent des watermarks pour assurer un certain niveau de protection des droits de propriété intellectuelle. Les applications de cette classe utilisent des watermarks comme support d'informations sur la propriété du contenu et les droits de propriété intellectuelle.

Ces applications peuvent être utilisées pour la protection des droits d'auteur, protection contre la copie et la traçabilité des copies "Fingerprinting"

La deuxième classe d'application utilise des watermarks pour la vérification du contenu. Les applications de cette classe intègrent des watermarks dans un contenu numérique multimédia pour garantir que le contenu original n'a pas été modifié et pour aider à déterminer le type et l'emplacement de la modification dans le cas où le contenu original a été modifié.

La troisième classe d'application de tatouage numérique utilise des watermarks pour fournir des informations supplémentaires sur le contenu, comme la surveillance de diffusion d'un contenu numérique, comme un film ou une partie vidéo publicitaire (Broadcast monitoring).

I.6.1. Protection du copyright

La protection du droit d'auteur est l'une des premières applications ciblées par le tatouage numérique. Les métadonnées contiennent des informations sur le propriétaire des droits, et elles sont insérées imperceptiblement comme un watermark dans la couverture à protéger. Si les utilisateurs de contenu numérique (musique, images, et vidéo) ont un accès facile aux détecteurs de la marque, ils devraient être capables de reconnaître et d'interpréter la marque intégrée et identifier le propriétaire des droits du contenu tatoué [32].

Un exemple d'une application commerciale créée à cette fin est la solution ImageBridge de Digimarc Corporation. La technologie Digimarc offre des solutions d'identification et de gestion des médias, de lutte contre la contrefaçon de commerce numérique. Le détecteur de la marque ImageBridge est disponible sous forme de plug-ins pour de nombreuses solutions de traitement d'image populaires, telles qu'Adobe Photoshop ou COREL Photopaint. Lorsqu'un utilisateur ouvre une image à l'aide d'une application compatible Digimarc, le détecteur de la marque de Digimarc reconnaîtra la signature où il contactera ensuite une base de données distante en utilisant la signature comme clé pour trouver un détenteur de copyright et ses coordonnées. Un utilisateur honnête peut utiliser cette information pour contacter le propriétaire du droit d'auteur afin de demander l'autorisation d'utiliser l'image [32].

I.6.2. L'authentification du contenu

Les logiciels d'édition multimédia facilitent de plus en plus la modification du contenu numérique. Comme il est facile d'interférer avec un autre contenu numérique, il est nécessaire de vérifier l'intégrité et l'authenticité du contenu.

Une solution à ce problème peut être empruntée à la cryptographie, où la signature numérique a été étudiée en tant que méthode d'authentification des messages. La signature numérique

représente essentiellement une sorte de résumé du contenu, et si une partie du contenu est modifiée, le résumé de cette signature, va être évidement affecté, rendant possible la détection d'une falsification. Un exemple de la technologie de signature numérique utilisée pour l'authentification de l'image est l'appareil photo numérique fiable [32,45].

L'appareil photo numérique fiable est une application de la technologie existante vers la solution d'un problème social toujours plus troublant, la crédibilité érodée de l'image photographique. Bien qu'il soit toujours possible de mentir avec une photographie (en utilisant des techniques ancestrales telles que la fausse perspective et des légendes trompeuses), le dispositif proposé empêchera l'explosion d'ordinateurs personnels très performants d'augmenter le nombre de photographies truquées. Une solution à ce problème provient du standard de signature numérique (DSS) proposé, qui incorpore des techniques cryptographiques modernes pour authentifier les messages électroniques [45].

I.6.3. La Traçabilité des copies "Fingerprinting"

Le suivi des copies illégales des documents numériques est nommé le Fingerprinting, appelé aussi traçabilité des copies, l'association d'informations uniques avec chaque copie distribuée de contenu numérique est appelée empreinte digitale, et le tatouage numérique est une technologie appropriée pour l'implémenter car la marque incorporée qui contient cette information unique est invisible et inséparable du contenu.

Ce type d'application de traçage est utile pour la surveillance et le suivi des copies illégales. Puisque le tatouage numérique peut être utilisé pour suivre plusieurs transactions qui ont eu lieu dans l'historique de la copie d'un contenu numérique, le terme suivi de transaction a également été utilisé.

I.6.4. Sécurité des données médicales

Pour assurer la déontologie et la protection des secrets médicaux, ainsi que la confidentialité des informations personnelles des images médicales liées à chaque malade et pour l'amélioration de la qualité des services médicaux distants .Le tatouage numérique se place comme le meilleur protocole pour gérer de telles transactions, car le tatouage des images médicales assure la confidentialité des informations par l'exploitation de plusieurs schémas de tatouage aptes et capables de bien protéger les données médicales privées insérées dans l'image médicales et qui doivent être invisibles et ne peuvent être extraites à la réception que par les personnes autorisées à les explorer pour empêcher toute altération qui affecte le bon diagnostique du patient.

I.7. LES OUTILS D'EVALUATION DES PERFORMANCES

Dans un tel environnement de travail comme le tatouage des images numériques, où on cherche que le schéma doit être robuste et imperceptible et répondre aux exigences et contraintes sollicités par les systèmes de tatouage efficaces, les mesures quantitatives de distorsion s'avèrent beaucoup plus efficaces et permettent une comparaison équitable entre les différentes méthodes par rapport aux mesures des résultats de l'évaluation subjective. Plusieurs critères et paramètres entrent en jeu lors de l'évaluation objective des performances d'un algorithme de tatouage.

Les métriques de distorsion qui sont couramment utilisées dans le traitement d'image, comme celui du domaine de tatouage, de codage, de la compression des images et de la vidéo sont le rapport signal sur bruit (SNR) et le rapport signal / bruit crête à crête ($PSNR$ Peack Signal to Noise Ratio). Il est bien connu que ces métriques de distorsion des différences ne sont pas très bien corrélées avec le système visuel humain, et ne peuvent être considérés comme une mesure objective de la qualité visuelle d'une image.

D'autres métriques sont conçues pour mesurer la similarité entre les images, plutôt qu'une différence comme le $SSIM$ (Index de similarité structurelle).

La similarité [46] peut être calculée par le rapport entre la similitude et la dissimilitude de deux images soumises à une comparaison. La similitude mesure et donne le nombre de correspondances tandis que la dissimilitude mesure le nombre de différences. Deux images sont similaires si leur similitude est assez grande et leur dissimilitude tend vers zéro.

Parmi les critères principaux que nous allons utiliser pour conclure sur la robustesse et l'imperceptibilité des schémas et des approches de tatouage utilisées dans ce travail, on cite :

- L'Erreur Quadratique Moyenne (EQM) ou Mean Square Error (MSE)

- Le Rapport Signal sur Bruit (SNR) ou Signal to Noise Ratio

- La Corrélation Normalisée (NCC) ou Normalized Cross Correlation

- **L'**Index de Similarité Structurelle ($SSIM$) ou Structural Similarity Index

- Le Taux d'Erreur Mesuré (BER) ou Bit Error Rate

I.7.1.L'Erreur Quadratique Moyenne (EQM)

Le tatouage des images, est caractérisé généralement par un rajout de bruit à l'image hôte, ce qui montre l'importance de la mesure du degré de perturbation après toute phase d'insertion.

Pour ce faire, il est souvent entendu d'utiliser une métrique d'erreur quadratique moyenne (MSE). Le MSE mesure la moyenne de différence terme à terme entre l'image originale et celle de sortie (l'image tatouée). Plus le MSE est grand, plus le niveau de dégradation est élevé

$$(\mathrm{MSE}) = \frac{1}{\mathrm{M\ x\ N}} \sum_i \sum_j (\mathrm{I(i,j)} - \mathrm{I_w(i,j)})^2. \qquad \text{(I.1)}$$

Où I (i, j) est la valeur de la luminance du pixel (i, j) de référence et I_w(i, j) celle de l'image à tester, les deux images étant de taille$[M\ x\ N]$.

I.7.2.Le Rapport Signal sur Bruit (SNR) *et* ($PSNR$)

La mesure de la distorsion la plus populaire en traitement d'image est le Rapport Signal sur le Bruit SNR (Signal to Noise Ratio) et le $PSNR$ (Peack Signal to Noise Ratio). Elles sont définies respectivement par les formules suivantes :

$$(\mathrm{SNR})_{\mathrm{dB}} = 10\log_{10}\left\{\frac{\sum_{i,j} \mathrm{I^2(i,j)}}{\sum_{i,j}[\mathrm{I(i,j)} - \mathrm{I_w(i,j)}]^2}\right\} \qquad \text{(I.2)}$$

$$(\mathrm{PSNR})_{\mathrm{dB}} = 10\log_{10}\left\{\mathrm{MxN}\frac{\max \mathrm{I^2(i,j)}}{\sum_{i,j}[\mathrm{I(i,j)} - \mathrm{I_w(i,j)}]^2}\right\} \qquad \text{(I.3)}$$

On considère généralement en tatouage d'images qu'un tatouage est imperceptible pour un $PSNR$ supérieur à 36 dB.

I.7.3. La Corrélation Normalisée (NCC)

La mesure du degré de fiabilité d'un watermark détecté ou d'une signature extraite se fait par une métrique très fiable, c'est la corrélation normalisée croisée (Normalized Cross-CorrelationNCC). Les métriques de corrélation permettent de calculer la corrélation entre les pixels aux mêmes indices dans la marque originale et la marque extraite.

De telles métriques mesurent la ressemblance des images donc la similitude des images et leurs impact sur la décision lors de la détection de la marque extraite est très décisif. La corrélation normalisée croisée NCC est défini comme suit :

$$\mathrm{NCC} = \frac{\sum_{i-1}^{P}\sum_{j-1}^{Q} W(i,j) \times W_1'(i,j)}{\sqrt{\sum_{i-1}^{P}\sum_{j-1}^{Q} W(i,j)^2}\sqrt{\sum_{i-1}^{P}\sum_{j-1}^{Q} W_1'(i,j)^2}} \quad \text{(I.4)}$$

Où $W\ (i,j)\ et\ W'\ (i,j)$ représentent la marque originale et la marque extraite respectivement, la valeur de NCC est dans l'intervalle $[0\ -1]$.

On considère généralement en tatouage d'images qu'un tatouage est robuste pour corrélation normalisée croisée $NCC\ \geq\ 0.75$.

I.7.4. Index de Similarité Structurelle ($SSIM$)

Un autre critère pour la mesure de la similitude, c'est le $SSIM$ qui est utilisé régulièrement pour mesurer la similarité entre deux images proposées. Il est défini comme suit :

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad \text{(I.5)}$$

Où
μ_x-moyenne de x.
μ_y-moyenne de y.
σ_x^2-variance de x.
σ_y^2-variance de y.
σ_{xy}-covariance de x y.
$C_1 = k_1 L^2$-Constante pour éviter l'instabilité quand $\mu_x^2 + \mu_y^2$ est proche des zéros ;

$$k_1 = 0.01, L = 255.$$

$C_2 = k_2 L^2$- Constante pour éviter l'instabilité quand $\sigma_x^2 + \sigma_y^2$ est proche des zéros;

$$k_2 = 0.03, L = 255.$$

I.7.5. Le Taux d'Erreur Mesuré (BER)

Le taux d'erreur mesuré est utilisé pour mesurer le taux d'erreur dans la marque extraite après détection par rapport à la marque d'origine. On utilise aussi la métrique BER pour évaluer la similarité entre les deux marques, la marque insérée et la marque extraite.

La valeur qui tend vers zéro signifie que le tatouage présente une bonne fiabilité de point de vue robustesse (la marque extraite est presque similaire à la marque détectée). La formule du taux d'erreur (BER) peut être définie comme suit :

$$\mathrm{BER} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j)\otimes w'(i,j)}{(m\times n)} \qquad \text{(I.6)}$$

Dans lequel W est la marque originale et W ' la marque extraite avec (n × m) la taille de la marque.

⊗ Signifie l'opération OU exclusif $\boldsymbol{Xor}$.

CONCLUSION

Dans ce chapitre, nous avons présenté l'intérêt de la protection de la copie, de l'authenticité et la protection des droits d'auteurs suite à l'amélioration considérables des technologies de la communication, de la télécommunication, et de la récupération du multimédia numérique. Un tel environnement a permis la réalisation de nombreuses applications multimédia fascinantes liées à la protection des donnés numériques et surtout les images numériques, comme le tatouage numérique, les systèmes de sécurité comme la cryptographie, la stéganographie et bien sûr la grosse part a été réservée au tatouage numérique, en s'étalant sur les méthodes de tatouage tels que le tatouage additif, le tatouage substitutif, les domaines de tatouage des images comme le domaine spatial et le domaine transformé.

On a évoqué les classes importantes d'applications du watermarking qui exploitent des schémas de tatouage divers pour assurer un certain niveau de protection des droits de propriété intellectuelle. La diversité de ces applications qui utilisent des watermarks comme support d'informations sur la propriété du contenu et les droits de propriété intellectuelle à savoir la protection des droits d'auteur, la protection contre la copie, la traçabilité des copies "Fingerprinting", la vérification du contenu et la surveillance de diffusion d'un contenu numérique (Broadcast monitoring).

L'appel à des métriques d'évaluation qui valorisent les bonnes méthodes et la fiabilité du tatouage et qui peuvent répondre aux exigences et contraintes imposées par les schémas de tatouage s'avère indispensable dans un cahier de charge d'un système de tatouage. Ces métriques ou critères qui sont la manière objective après celle subjective , et qui feront le constat et l'analyse lors de l'évaluation des performances d'un algorithme de tatouage, et de

décider de sa robustesse et son imperceptibilité .On a cité des métriques à base de calcul des différences et d'autres à base de calcul de similitude, comme l'erreur quadratique moyenne (MSE), le rapport signal sur bruit (SNR), le rapport signal sur bruit crête ($PSNR$), la corrélation normalisée (NCC), l'index de similarité structurelle ($SSIM$) et le taux d'erreur mesurée (BER) Qui sont jugées très utiles pour le jugement d'un bon schéma de tatouage.

Chapitre II

Transformées discrètes et la transformée paramétrique orthogonale réciproque ROP

INTRODUCTION

Les schémas de tatouage numérique des images sont multiples. Ces derniers sont dus principalement à la diversité du choix de domaine d'insertion et à quelle tâche le tatouage est dédié, le domaine d'incrustation peut être soit spatial, soit fréquentiel ou transformé. Le tatouage dans le domaine spatial est le schéma où l'insertion consiste à travailler directement sur l'image en modifiant l'intensité des pixels. Pour le domaine transformé les schémas de tatouage sont traités en utilisant un domaine d'insertion issu d'une transformée.

La popularité des transformées dans le domaine fréquentiel en traitement de signal et spécialement en traitement des images est du non seulement à leur utilité mais aussi à l'existence d'algorithmes efficaces pour leur calcul rapide [47]

Les transformations discrètes ont été longtemps utilisées dans les traitements de signal et le traitement de l'image numérique, elles ont des applications importantes dans le domaine du watermarking.

Dans ce chapitre, on va se concentrer sur les algorithmes rapides et les applications de quelques transformées qui ont données un progrès aux traitements des images dans le domaine du watermarking en mode fréquentiel, telles que la Transformée en Cosinus Discrète (DCT), la Transformée en Ondelette Discrète (DWT),la Décomposition en Valeurs Singulières (SVD), la transformée de Hadamard discrète(DHT) et on finira par la transformée paramétrique orthogonale (ROP) qui est marquée par une paramétrisation de la transformée de Hadamard et cela suite au succès des transformées populaires existantes mentionnées précédemment, ce qui a motivé beaucoup de chercheurs ces dernières années pour généraliser et paramétrer ces transformées [48] afin d'élargir le domaine de leurs applications et de fournir plus de flexibilité dans la représentation, l'interprétation et le traitement de signal.

Les paramètres indépendants d'une transformée sont très utiles dans la caractérisation des signaux et peuvent être également utilisés comme une clé secrète supplémentaire pour des applications telles que le tatouage et le cryptage. Par exemple, les paramètres indépendants d'une transformée Fractionnaire discrète ont été utilisés comme une clé secrète supplémentaire dans [48] pour le tatouage et dans [49] pour le cryptage.

II.1. TRANSFORMEE DISCRETES

Les transformations, et en particulier les transformations intégrales, sont principalement utilisées pour réduire la complexité des problèmes mathématiques. Les équations différentielles et les équations intégrales peuvent, par l'application judicieuse de transformations appropriées, se transformer en équations algébriques, dont les solutions sont plus facilement obtenues. Il est donc important de dériver les propriétés mathématiques de base de ces transformées avant d'envisager les applications. L'analyse de transformation, telle qu'elle est appliquée dans le traitement du signal numérique, a un objectif similaire [50]. La transformée de Fourier, qui décompose un signal en ses composantes fréquentielles, et la transformée de Karhunen-Loéve (KLT) [51] qui décorrèle une séquence de signal, sont des exemples bien connus dans le domaine du traitement du signal numérique.

Ahmed, Natarajan et Rao [52], ont mis en équation la DCT et se sont pointés directement vers l'utilité de cette transformation. C'est une transformation mathématique qui transforme un ensemble de données d'un domaine spatial en un spectre de fréquence.

II.1.1. La DCT

La DCT (Discrete Cosine Transform) [50] est une transformation dominante dans le milieu de la compression vidéo et de traitement d'images numériques. C'est la transformation qui est très utilisée dans les normes de compression $JPEG$ (Joint Photography Expert Group).

C'est une transformation déduite de la transformée de Fourier discrète (DFT) dont le noyau de projection est un cosinus et génère donc des cœfficients réels, elle est donc facile à mettre en œuvre et elle a notamment l'avantage de générer un signal transformé réel.

La DCT a une bonne localisation fréquentielle, un compactage de l'énergie qui surpasse celui obtenu avec la transformée de Fourier discrète(DFT).

Après transformation de l'image de son environnement spatial à celui fréquentiel par le biais de laDCT, l'information sera essentiellement portée par le coefficient DC (Direct Component) ou coefficient continu qui présente les basses fréquences pour les images naturelles [50]. Le reste de l'information sera porté par les coefficients AC (Alternative Component) qui présentent les amplitudes des fréquences spatiales.

La transformée DCT est généralement réalisée non pas sur l'image entière mais sur des blocs de taille [8*8] pixels. Si x et y désignent les dimensions spatiales de l'image, u et v désignent les dimensions dans le domaine des fréquences de l'image, M le nombre d'échantillons en x et y (M généralement égale à 8), I l'image (ou matrice de [8*8] de l'image) originale et F

l'image transformée, la DCT fait correspondre à chaque valeur de $I\,(x,y)$ une valeur de $F\,(u,v)$ donnée par la formule suivante :

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

La DCT inverse est donnée par l'expression suivante :

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

Où

$$c(u) = c(v) = \begin{cases} \sqrt{\frac{1}{N}} & pour\ u,v = 0 \\ \sqrt{\frac{2}{N}} & ailleurs \end{cases} \qquad \text{(II.3)}$$

On peut représenter la répartition des fréquences de la DCT d'une matrice de 8×8 éléments par la figure suivante :

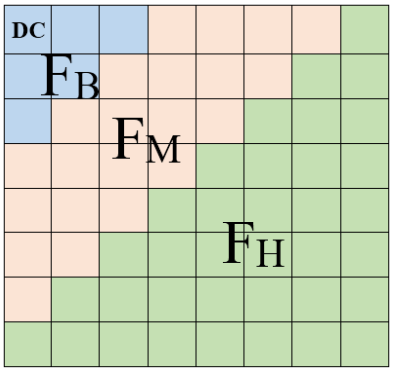


Figure II.1 : Répartition des fréquences dans un bloc DCT 8x8.

Cette transformée se caractérise par un effet de séparation des basses fréquences (FB), de celles des moyennes fréquences (FM) et des hautes fréquences(FH), donnant ainsi la possibilité de bien choisir quelle gamme de fréquences peut-on utilisé pour une bonne insertion d'une marque qui sera compatible avec le système visuel humainHVS.

La figure II.2 représente l'image de Lena et sa transformée discrèteDCT. On remarque que les valeurs les plus élevées se concentrent dans le coin supérieur gauche (basses fréquences) et les valeurs les plus faibles dans le coin inférieur droit (hautes fréquences).

Figure II.2: Image Lena et sa transformée DCT.

II.1.2. La *DWT*

La transformée discrète en ondelettes DWT permet la décomposition de l'image, après analyse multirésolution, en sous-bandes au moyen de sous-échantillonnages successifs de l'image pour permettre une isolation raffinée des composantes basses fréquences afin de former un espace d'insertion moins sensible.

Les transformées d'ondelettes discrètes sont généralement orthogonales et permettent la reconstruction du signal initial par la transformée en ondelettes inverses [53,54]. La DWT décompose une image en quatre sous-bandes, à savoir une sous-bande LL et trois sous-bandes $LH, HH, et\ HL$ correspondant respectivement aux détails verticaux, diagonaux et horizontaux. Cette décomposition est réalisée à l'aide de deux filtres, un filtre passe-haut et un filtre passe-bas appliqués séparément sur les lignes et les colonnes de la même image. La lettre H correspond au filtre passe-haut et la lettre L au filtre passe-bas. Donc, pour les images, appliquer la transformée DWT correspond au traitement de l'image par deux filtres. Les filtres divisent l'image d'entrée en quatre sous-bandes multi-résolutions non superposées.

La sous-bande LL représente les coefficients DWT à échelle grossière, tandis que les sous-bandes $LH, HL\ et\ HH$ représentent l'échelle fine des coefficients DWT. Pour obtenir la prochaine échelle plus grossière des coefficients d'ondelettes, la sous-bande LL est ensuite traitée jusqu'à ce qu'une certaine échelle finale N soit atteinte. Lorsque N est atteint, nous aurons $3N + 1$ sous-bandes constituées des sous-bandes multirésolution LL_N, LH_N, HL_N et HH_N [55]. La figure II.3 montre la décomposition successive par la transformée discrète en ondelettes d'une image pour deux niveaux de résolution avec les sous-bandes correspondantes, et la figure II.4 montre un exemple de la transformée DWT sur une image "Parrot" niveau 1[56].

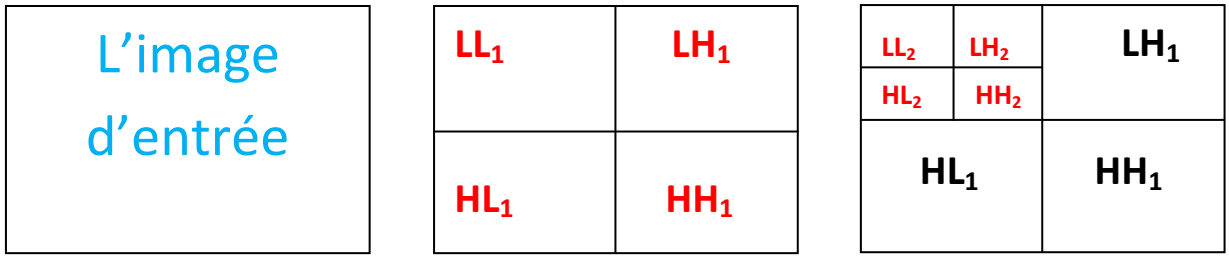
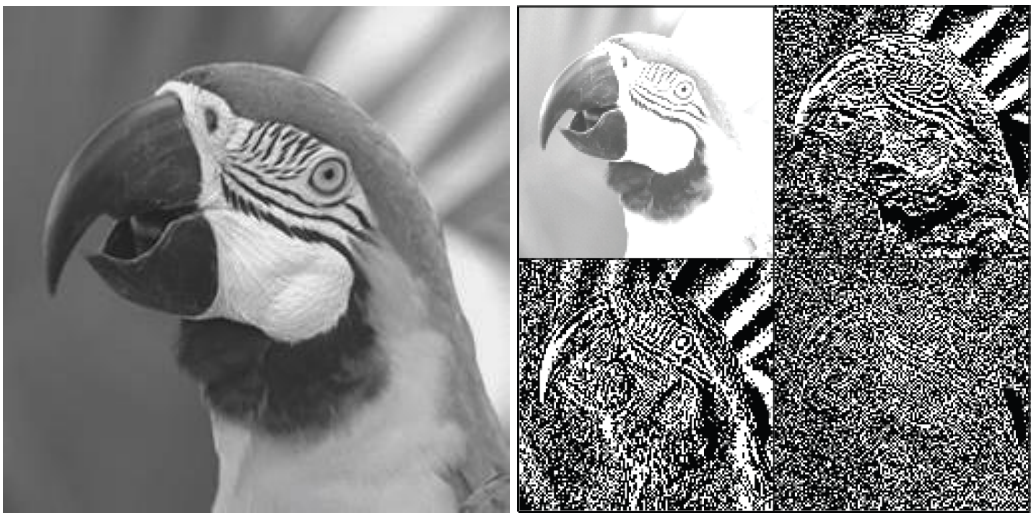


Figure II.3 : Décomposition successive par DWT



(a) Image originale (b) La DWT à un niveau de résolution

Figure II.4 :l'image originale et sa transformée DWT niveau 1.

En raison de ses excellentes propriétés de localisation spatio-fréquentielle, la transformée en ondelettes discrète est très appropriée pour localiser les zones dans l'image hôte où la marque peut être intégrée efficacement. Ces propriétés permettent d'incorporer la marque sans être perçue par l'œil humain. Le compromis adopté par de nombreux algorithmes de tatouage basés sur DWT est d'incorporer la marque dans les sous-bandes de fréquence moyenne LH et HL où des performances acceptables d'imperceptibilité et de robustesse pourraient être obtenues.

La DWT n'est pas efficace pour analyser les signaux non stationnaires. Alors que la transformée de Fourier de courte durée est un outil efficace pour faire cette opération, mais l'inconvénient c'est qu'elle donne une résolution constante à toutes les fréquences, tandis que la DWT et vue ses propriétés fournit une description à la fois spatiale et fréquentielle d'une image à multirésolution. La propriété multirésolution de la transformée en ondelettes peut être utilisée pour exploiter le fait que la réponse visuelle de l'œil humain (la perception) n'est pas la même pour les composantes hautes fréquences et les composantes basses fréquences de l'image (les parties lisses et les parties perturbées).

La DWT est très appropriée pour identifier les zones dans l'image hôte où une marque peut être intégrée efficacement. En particulier, cette propriété permet l'exploitation de l'effet de masquage du système visuel humain tel que si un coefficient DWT est modifié, seule la région correspondant à ce coefficient sera modifiée. En général, la plus grande partie de l'énergie de l'image est concentrée dans les sous-bandes de fréquences inférieures LLx et par conséquent, l'incorporation de la marque dans ces sous-bandes peut altérer significativement l'image tatouée. Toutefois, l'intégration dans les sous-bandes de basse fréquence pourrait augmenter considérablement la robustesse. D'autre part, les sous-bandes haute fréquence HHx incluent les bords et les textures de l'image et l'œil humain n'est pas généralement sensible aux changements dans ces sous-bandes. Cela permet à la marque d'être intégrée sans être perçue par l'œil humain. Le compromis adopté par de nombreux algorithmes de tatouage basés sur la DWT consiste à incorporer la marque dans les sous-bandes à fréquence moyenne LHx etHLx, ce qui permet d'obtenir des performances acceptables d'imperceptibilité et de robustesse.

II.1.3. La SVD

La plupart des schémas proposés pour les techniques de tatouage qui se basent sur les domaines transformés sont les schémas qui fonctionnent avec les transformées$DCT\ et\ DWT$. Cependant, la décomposition en valeur singulière (SVD) est l'une des techniques d'analyse numérique les plus puissantes ; elle est utilisée dans diverses applications de tatouage où elles montrent des schémas robustes et imperceptibles [57,58]

En algèbre linéaire, la décomposition en valeurs singulières (SVD) est une factorisation importante d'une matrice complexe, ce qui a contribué à plusieurs applications dans le traitement du signal, et spécialement dans le traitement des images [59].

La particularité de la SVD est qu'elle peut être effectuée sur des matrices réelles pas nécessairement carrée (comme le cas de la DCT) de taille $m \times n$.

Dans la transformationSVD, une matrice peut être décomposée en trois matrices de même taille que la matrice d'origine. Étant donné une matrice $m \times n$ réelle, cette matrice peut être transformée en trois composantes,U, S et V respectivement.

$$[U\ S\ V] = SVD(A) \tag{II.4}$$

$$A = USV^T = \sum_{i=1}^{r} \sigma_i\, U_i V_i^T \tag{II.5}$$

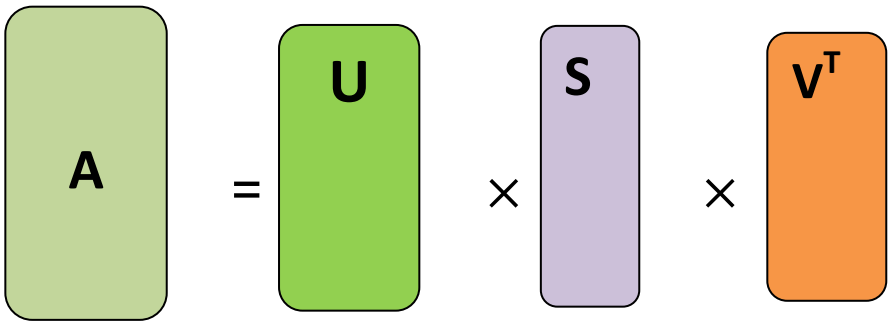


Figure II.5 factorisation de A à USV^T

Où U et V sont des matrices orthogonales, respectivement de dimensions $m \times m$ et $n \times n$. S est la matrice diagonale de taille $m \times n$ formée des valeurs singulières σ_i, non négatives disposées dans un ordre décroissant, sur la diagonale et T est l'opérateur de transposition. $S = diag(\sigma_1, \sigma_2, .., \sigma_r)$, telles que $\sigma 1 \geq \sigma 2 \geq .... \geq \sigma r > 0$ où $r = min(m, n)$ le rang de la matrice , égale au nombre de valeurs singulières (SVs) non nulles que possède la matrice A.

L'utilisation de la SVD dans le traitement d'image numérique a ses avantages, tout d'abord, la taille des matrices de la transformation SVD n'est pas fixe et peut être carrée ou rectangulaire. Deuxièmement, les valeurs singulières dans une image numérique sont moins affectées si le traitement d'image général est effectué. Troisièmement, les valeurs singulières contiennent des propriétés d'image algébriques intrinsèques [59].

Les trois matrices$U$, S et V, qui résultent de la décomposition SVD décrivent les propriétés géométriques de l'image par les matrices U et V et la matrice S décrit la luminance. Ces matrices peuvent être rectangulaires ou carrées. [60]

L'insertion de la marque dans les composantes de la matrice orthogonale U au lieu des composantes de la matrice orthogonale V et la matrice diagonale S a été adoptée dans pas mal de schéma qui visent la robustesse et l'imperceptibilité [61]. Pour les composantes de la matrice orthogonale U de laSVD, la modification des coefficients des vecteurs colonnes entraînera une distorsion moins visible que la modification des coefficients des vecteurs lignes.

La méthode prend son ampleur suite à la stabilité des valeurs singulières***SVs***, lorsque l'on rajoute des informations (marquage) à l'image, leurs valeurs singulières ***SVs*** ne changent pas significativement. A cause de cette propriété plusieurs algorithmes de tatouage utilisent les valeurs singulières ***SVs*** pour insérer des watermaks numériques.

La SVD fait un compactage d'énergie comme la DCT qui se classe parmi les plus utiles en tatouage car elle range le maximum d'énergie de l'image dans un minimum de valeurs singulières, la compression est obtenue donc intuitivement en forçant les valeurs singulières les plus faibles à zéro, ce qui permet une grande robustesse à la compression, en utilisant les valeurs singulières SVs significatives [62].

II.2. LA TRANSFORMEE DE WALSH HADAMARD

II.2.1. La présentation de la série de Walsh

Soit un signal $x(t)$ continu est défini sur un intervalle $t \in [0,1]$. Il a été montré [63] que l'ensemble des fonctions de Walsh $\{wal_{\omega}(i,t)\}$ est fermé. Ainsi, chaque signal $x(t)$ qui est absolument intégrable t ϵ [0, 1) peut être étendu dans une série de la forme :

$$x(t) = \sum_{k=0}^{\infty} d_k \, wal_{\omega}(k,t) \qquad \text{(II.6)}$$

Depuis l'ensemble des fonctions $\{wal_{\omega}(k,t)\}$ forme un système orthonormé dans l'intervalle fermé t ϵ [0, 1], les coefficients $d_k$sont donnés par :

$$d_k = \int_0^1 x(t)\, wal_{\omega}(k,t)dt, \qquad k = 0,1,2,\ldots \qquad \text{(II.7)}$$

Nous rappelons que :

$$wal_{\omega}(k,t) = cal(s_k,t) \qquad k\ pair \qquad \text{(II.8)}$$

$$wal_{\omega}(k,t) = sal(s_k,t) \qquad k\ impair \qquad \text{(II.9)}$$

Les notations **cal** et **sal** mettent l'accent sur la ressemblance des fonctions de Walsh aux fonctions de la série de Fourier **sin** et **cos**.

Autrement dit, ce sont les différentes formes de la transformée de Walsh-Hadamard.

Où s_k est la séquence (sequency) de $Wal_{\omega}(k,t)$, qui est défini comme étant

$$s_k = \begin{cases} 0 & k = 0 \\ k/2 & kpair \\ (k+1)/2 & kimpair \end{cases} \qquad \text{(II.10)}$$

Avec $wal_{\omega}(k,t)$ exprimé en termes de sal et cal, l'expression de l'équation (II.6) devient :

$$x(t) = a_0 wal_\omega(0,t) + \sum_{k=0}^{\infty}[a_k cal(k,t) + b_k sal(k,t)] \quad \text{(II.11)}$$

$$\text{Où} \quad \begin{matrix} a_0 = d_0 \\ a_k = d_{2k} \\ b_k = d_{2k-1} \end{matrix} \quad \text{(II.12)}$$

Afin d'obtenir une expression de la série finie qui se compose de N termes, où N est de la forme $N = 2^n$, on tronque la série ci-dessus pour obtenir :

$$x(t) \simeq a_0 wal_\omega(0,t) + \sum_{k=0}^{N/2-1}[a_k cal(k,t) + b_k sal(k,t)] + b_{N/2} sal(N/2,t) \quad \text{(II.13)}$$

Les conditions de convergence suivantes pour la série dans l'équation. (II.13) ont été données par Walsh [63]et Paley [64] :

(i) Si x (t) est continue t ϵ [0, 1), la série converge uniformément vers la valeur de x(t); ce qui signifie que :

$$\lim_{k\to\infty}\{a_k, b_k\} = 0 \quad \text{(II.14)}$$

(ii) Aux points où x (t) est discontinue en t ϵ [0, 1), il y a convergence vers la valeur moyenne.

D'après les passages précédents, il est évident de dire que la représentation de Walsh est analogue et similaire à la représentation de Fourier, en raison de la forte ressemblance entre les sinusoïdes de Fourier et les fonctions de Walsh, comme il est illustré sur la figure II.6 pour le cas N = 8.

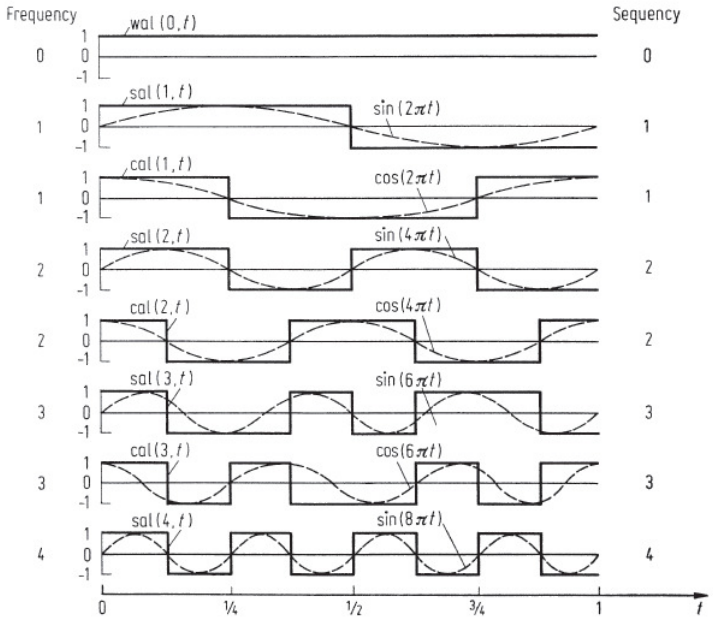


Figure II-6 : Fonctions de Walsh et les sinusoïdes de Fourier.

Les transformations de type Walsh-Hadamard sont utilisées pour la représentation des séquences de données de Walsh. Les fonctions de Walsh peuvent être exprimées en termes de matrices de Hadamard H(n). Ces matrices peuvent être générées en utilisant la relation de récurrence suivante :

$$H(k) = \begin{bmatrix} H(k-1) & H(k-1) \\ H(k-1) & -H(k-1) \end{bmatrix}, \qquad k = 1,2,\dots,n \tag{II.15}$$

Où $H(0) = 1$ et n=$\log_2 N$.

Par exemple, avec k=1 et k=2, l'équation (6) devient :

$$H(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H(2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Il est facile de montrer que les matrices H(k) ont les propriétés suivantes:

(i) H(k) est une matrice symétrique :

$$H(k)' = H(k) \tag{II.16}$$

(ii) $H(k)$ est orthogonal :

$$H(k)' \times H(k) = 2^k \times I(k) \tag{II.17}$$

Où I(k) est la matrice identité

(iii) L'inverse $de\ H(k)$ est proportionnel à elle-même :

$$[H(k)]^{-1} = \frac{1}{2^k} H(k) \qquad \text{(II.18)}$$

Où $[H(k)]^{-1}$ et l'inverse de $H(k)$.

II.2.2.La transformée de Hadamard

La transformée de Hadamard est une classe généralisée d'une transformée de Fourier (BIFORE ou HADAMARD TRANSFORM) [65]. Elle effectue une opération linéaire et involutive avec une matrice orthogonale et symétrique sur $\boldsymbol{2^n}$ nombres réels ($\boldsymbol{n}$ est un nombre entier qui précise le nombre d'échantillons$N = \boldsymbol{2^n}$). On appelle ces matrices les matrices de Hadamard.

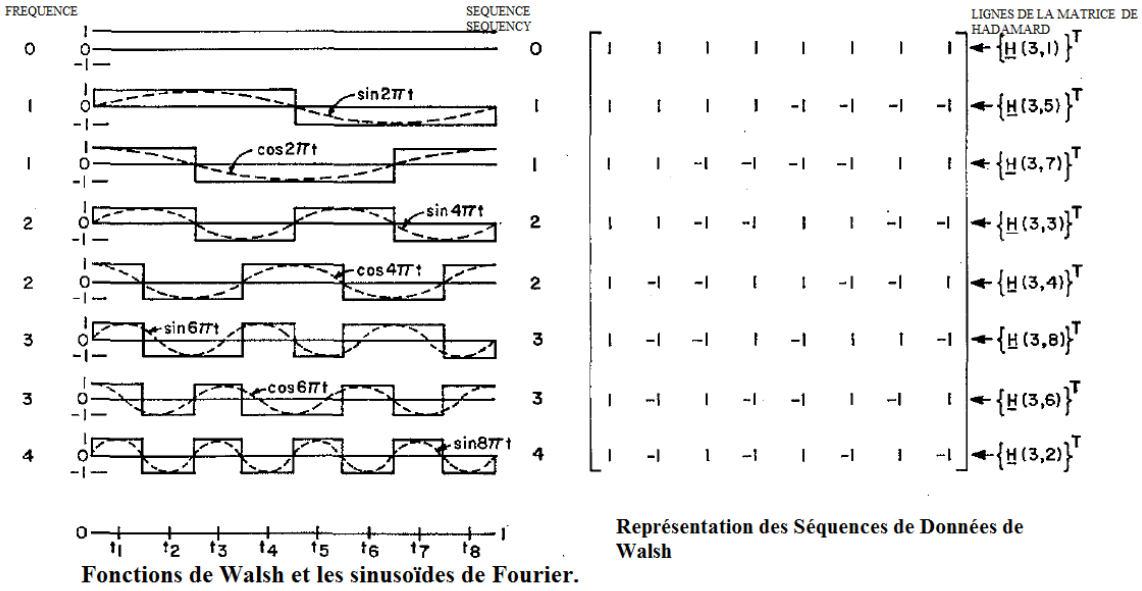


Figure II.7 : Sinusoïdes de Fourier, Fonctions de Walsh et la matrice de Hadamard N=8

II.2.3.La matrice de Hadamard

Une matrice de Hadamard est une matrice carrée dont les coefficients sont 1 ou –1 (voir figure II.7) (représentation des séquences de données de Walsh) et dont les lignes (et les colonnes) sont toutes orthogonales entre elles.

Si $\boldsymbol{H}$ est une matrice de Hadamard d'ordre$N \times N$, le produit de $\boldsymbol{H}$ et de sa transposée $\boldsymbol{H}^*$donne la matrice d'identité $\boldsymbol{I}$

$$\boldsymbol{H}\boldsymbol{H}^* = \boldsymbol{N}\boldsymbol{I} \qquad \text{(II.19)}$$

Où $\boldsymbol{I}$ est la matrice d'identité.

La propriété d'une matrice de Hadamard où les lignes (colonnes) peuvent être échangées avec une autre sans affecter les propriétés d'orthogonalité de la matrice, la symétrie de la matrice de Hadamard permet d'écrire que :

$$\boldsymbol{HH = NI} \qquad \text{(II.20)}$$

L'ordre le plus bas de la matrice de Hadamard est de l'ordre de deux.

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

La construction la plus simple est une matrice de Hadamard d'ordre $N = \boldsymbol{2^n}$ où $\boldsymbol{n}$ est un nombre entier.

$$G = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

L'ensemble des matrices de Hadamard connues est suffisamment nombreux pour satisfaire presque toutes les exigences de taille pour le codage d'images.

$$N = 2 \begin{bmatrix} + & + \\ + & - \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix} \; sequency$$

$$\mathrm{N} = 4 \left|\begin{matrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{matrix}\right| \begin{matrix} 0 \\ 3 \\ 1 \\ 2 \end{matrix} \; \text{Sequency ...}$$

$$\mathrm{N} = 8 \left|\begin{matrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{matrix}\right| \begin{matrix} 0 \\ 7 \\ 3 \\ 4 \\ 1 \\ 6 \\ 2 \\ 5 \end{matrix} \; \text{sequency}$$

Figure II.8 : Séquences de la matrice de Hadamard d'ordre $N = \boldsymbol{2^n}$.

Une interprétation de fréquence peut être accordée à la matrice de Hadamard. Le long de chaque ligne de la matrice, la fréquence est appelée le nombre de changements de signe. Harmuth a inventé le mot "séquence", "sequency" pour désigner le nombre de changements de signe [66]. La figure. II.8 donne l'interprétation de séquence pour plusieurs matrices de Hadamard d'ordre binaire. Il est possible de construire une matrice de Hadamard d'ordre $N = \boldsymbol{2^n}$ qui a des composantes de fréquence à chaque nombre entier de 0 à $N - 1$.

Cette interprétation de la fréquence des lignes d'une matrice de Hadamard amène à considérer les rangées équivalentes à des ondes rectangulaires comprises entre ±1. Ces fonctions sont

appelées fonctions de Walsh et sont en outre liées aux fonctions de Rademacher [63]. Ainsi, dans ce contexte, la matrice de Hadamard effectue simplement la décomposition d'une fonction d'un ensemble de formes d'ondes rectangulaires, plutôt que les formes d'onde en sinus et de cosinus associées à la transformée de Fourier.

II.3.L'APPLICATION DE LA TRANSFORMEE DE HADAMARD AUX IMAGES

La transformation matricielle de Hadamard étant orthogonale, elle s'accompagne d'une méthode d'inversion pour pouvoir revenir dans le domaine spatial. Soit $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})$ qui représente les échantillons de l'intensité d'une image originale, et $\boldsymbol{F}(\boldsymbol{u},\boldsymbol{v})$ la transformation de Hadamard à deux dimensions de $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})$, la matrice transformée$[\boldsymbol{F}(\boldsymbol{u},\boldsymbol{v})]$ est donnée par le produit :

$$[F(u,v)] = [H(u,v)][f(x,y)][H(u,v)] \quad \text{(II.21)}$$

Où

$[H(u,v)]$ est une matrice de Hadamard d'ordre N.

$[F(u,v)]$ représente le coefficient de la ligne u et la colonne v de la matrice transformée.

$[f(x,y)]$ représente l'élément de la ligne x et de la colonne y de la matrice dans le domaine spatial.

La multiplication de part et d'autre de la transformée $[F(u,v)]$ par la matrice de Hadamard donne :

$$[H(u,v)][F(u,v)][H(u,v)] = [H(u,v)][H(u,v)][f(x,y)][H(u,v)][H(u,v)] \quad \text{(II.22)}$$

Pour une matrice de Hadamard symétrique, on peut écrire que :

$$[f(x,y)] = \frac{1}{N^2}[H(u,v)][F(u,v)][H(u,v)] \quad \text{(II.23)}$$

II.4 LA TRANSFORMEE PARAMETRIQUE RECIPROQUE ORTHOGONALE *ROP*

Divers essais ont été faits pour la généralisation et la paramétrisation des matrices de Hadamard [67]. Cependant, les transformées basées sur les matrices généralisées de Hadamard présentées dans [67 ,68] ont des complexités de calcul et de structure très élevées. La transformée réciproque-orthogonale (ROP) proposée dans [69] en combinant convenablement un nouveau vecteur paramétrique avec la matrice de Hadamard possède une structure simple et une complexité de calcul réduite.

II.4.1. Définition

La transformée ROP d'une séquence complexe (k) de taille $N = 2^r$ est définie par :

$$X(n) = \sum_{k=0}^{N-1} x(k) a_{k,s(n)} (-1)^{kon} \qquad n = 0,1,\ldots\ldots,N-1 \tag{II.24}$$

Et la transformée inverse est donnée par :

$$x(n) = \frac{1}{N} \sum_{n=0}^{N-1} X(n) \frac{1}{a_{k,s(n)}} (-1)^{kon} \quad , \qquad k = 0,1,\ldots\ldots,N-1 \tag{II.25}$$

Où $\boldsymbol{kon = k_0 n_0 + k_1 n_1 + \cdots + k_{r-1} n_{r-1}}$, $\mathrm{S}(\boldsymbol{n}) = \boldsymbol{(-1)^{(N-1)\,on}}$

$a_{k,1}$ et $a_{k,-1}$ sont des paramètres complexes non nuls qui doivent satisfaire la condition suivante d'existence de la transformée inverse :

$$\boldsymbol{a_{k,1} a_{N-1-k,-1} = a_{k,-1} a_{N-1-k,1}} \tag{II.26}$$

Les équations **(II.24)** et **(II.25)** peuvent être exprimées sous forme matricielle comme suit

$$X = P_N . x \tag{II.27}$$

$$x = P_N^{-1} . X \tag{II.28}$$

Où $\mathrm{P_N}$ est la matrice paramétrique de la transformée ROP par contre P_N^{-1} est la matrice inverse de $\mathrm{P_N}$.

II.4.2. Rappels mathématiques des transformations paramétriques

Dans cette partie, nous rappelons les bases mathématiques de transformation orthogonale réciproque basée sur la transformation de Hadamard proposé en [69].

Soit N une séquence de longueur N qui est un entier de puissance 2, $N = 2^{\mathrm{r}}$ ou r est un entier positif.

Soit l'entier n tel que $0 \leq \mathrm{n} \leq \mathrm{N}\text{-}1$.

n peut être décomposée en :

$$n = n_{r-1} 2^{r-1} + n_{r-2} 2^{r-2} + \cdots + n_1 2 + n_0 \tag{II.29}$$

Où le bit binaire $\mathrm{n_i}$ vaut 0 ou 1.

Appelons $(-1)^{\sum_{i=1}^{r-1} n_i} = -1$ minus entier

Les lignes d'une telle matrice NxN sont codées en binaire et à partir de là, nous déterminons minus entier.

Soit A une matrice carrée d'ordre N, et soit A^{RT} la matrice réciproque transposée.

La matrice A est dite orthogonale réciproque si $A.A^{RT}= N.I$, où I est la matrice identité, la matrice A est dite normalisée si les entrées de la première ligne et ceux de la première colonne valent toutes 1.

La transformation paramétrique (ROP) peut être construite à partir des étapes suivantes :

Etape 1: Formons le vecteur ligne paramétrique :

$$\mathbf{V}= \left[\mathbf{1} \quad \boldsymbol{a_1} \quad \boldsymbol{a_2} \quad \dots \quad \boldsymbol{a_{\frac{N}{2}-1}} \quad \boldsymbol{a_{\frac{N}{2}-1}} \quad \dots \quad \boldsymbol{a_2} \quad \boldsymbol{a_1} \quad \mathbf{1}\right] \tag{II.30}$$

Les $a_{i:}$ sont des paramètres arbitraires choisis du plan complexe.

Etape 2 : Construisons la matrice ROP d'ordre N désignée par T_N, en multipliant élément par élément les lignes indexées par les lignes correspondantes de la matrice de Hadamard H si minus entier$= -1$, et en gardant les mêmes lignes de la matrice de Hadamard dans le cas contraire.

Prenant comme exemple le cas $N = 8$

$$\mathbf{V} = [1 \quad a_1 \quad a_2 \quad a_3 \quad a_3 \quad a_2 \quad a_1 \quad 1]$$

$$\mathbf{T}_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -a_1 & a_2 & -a_3 & a_3 & -a_2 & a_1 & -1 \\ 1 & a_1 & -a_2 & -a_3 & a_3 & a_2 & -a_1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & a_1 & a_2 & a_3 & -a_3 & -a_2 & -a_1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -a_1 & -a_2 & a_3 & -a_3 & a_2 & a_1 & -1 \end{bmatrix}$$

La matrice inverse:

$$\frac{1}{8}\mathbf{T}_8^{\mathrm{RT}} = \frac{1}{8}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\frac{1}{a_1} & \frac{1}{a_1} & -1 & \frac{1}{a_1} & -1 & 1 & -\frac{1}{a_1} \\ 1 & \frac{1}{a_2} & -\frac{1}{a_2} & -1 & \frac{1}{a_2} & 1 & -1 & -\frac{1}{a_2} \\ 1 & -\frac{1}{a_3} & -\frac{1}{a_3} & 1 & \frac{1}{a_3} & -1 & -1 & \frac{1}{a_3} \\ 1 & \frac{1}{a_3} & \frac{1}{a_3} & 1 & -\frac{1}{a_3} & -1 & -1 & -\frac{1}{a_3} \\ 1 & -\frac{1}{a_2} & \frac{1}{a_2} & -1 & -\frac{1}{a_2} & 1 & -1 & \frac{1}{a_2} \\ 1 & \frac{1}{a_1} & -\frac{1}{a_1} & -1 & -\frac{1}{a_1} & -1 & 1 & \frac{1}{a_1} \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Si M est un bloc de $8x8$ d'une image P, alors la transformation orthogonale paramétrique est :

$$\mathrm{ROP(M)= T8 .M .}\frac{1}{8}\mathrm{T}_8^{\mathrm{RT}}$$

La transformation orthogonale paramétrique inverse est :

$$\mathrm{ROP^{-1}(M)=}\frac{1}{8}\mathrm{T}_8^{\mathrm{RT}}\mathrm{.ROP(M).T_8}$$

Où $\mathrm{T}_8^{\mathrm{RT}}$ est la matrice réciproque transposée.

Nous pouvons aussi généraliser pour un bloc de NxN.

Quant aux nombre des paramètres nous rappelons que

Pour un bloc de NxN, nous avons $\frac{N}{2}-1$ paramètres indépendants.

Si N=8, il ya 03 paramètres indépendants

Pour N=16, il ya 07 paramètres indépendants

Pour N=32, il ya 15 paramètres indépendants

Et pour N=64, il ya 31 paramètres indépendants

Ces paramètres sont utilisés comme clés supplémentaires dans l'opération du tatouage.

II.4.3. Propriétés de la transformée ROP

La matrice $\boldsymbol{P_N}$ de la transformée ROP est une matrice réciproque-orthogonale qui satisfait la relation suivante :

$$P_N \times P_N^{-1} = P_N \times (1/N) P_N^{RT} = N I_N \qquad \text{(II.31)}$$

Où P_N^{RT} est la matrice réciproque transposée de $\boldsymbol{P_N}$ avec ses éléments sont donnés par :

$$P_N^{RT}(i,j) = 1/P_N(j,i) \qquad i,j = 1,2,\ldots\ldots,N \qquad \text{(II.32)}$$

La matrice ROP a $3N/2$ paramètres indépendants qui peuvent être arbitrairement choisis du plan complexe. Il est simple de remarquer que quand $a_{k,1}$= 1, k = 0,1, ⋯, − 1 et$a_{0,-1}$ = 1, la matrice $\boldsymbol{P_N}$ devient une matrice normalisée dont tous les éléments de sa première ligne et sa première colonne sont des +1. Dans ce cas, le vecteur S_{-1} devient symétrique et le nombre de paramètres indépendants de la matrice ROP réduit à $\boldsymbol{N/2 - 1}$.

Par conséquent, la construction de la matrice ROP normalisée d'ordre N consiste simplement d'une multiplication élément par élément [70] de chaque ligne indexée négativement de la matrice $\boldsymbol{H_N}$ par le vecteur$\boldsymbol{S_{-1}}$.

Pour offrir de meilleures solutions au problème de la sécurité des images, plusieurs techniques du tatouage d'images ont été développées dans le domaine fréquentiel, l'exploitation de la transformée ROP qui a une complexité réduite et un nombre élevé de paramètres indépendants, s'avère une technique du tatouage d'images efficace, de point de vue robustesse et sécurité par l'exploitation des paramètres indépendants comme des clés secrètes dans une opération de tatouage.

II.5.LES ALGORITHMES HYBRIDES DE TATOUAGE NUMERIQUE DES IMAGES

Suite au développement des techniques prédatrices et pour contrecarrer la falsification des copies le tatouage que se soit dans le domaine spatial ou dans le domaine transformé s'avère impuissant devant toute sorte d'attaques intentionnelles ce qui ouvre la porte à une nouvelle conception de schémas de tatouage utilisant des algorithmes hybrides qui utilisent parfois plus de deux transformées pour assurer de plus en plus la robustesse et donner des qualités d'images très imperceptible. Parmi ces algorithmes, on cite ceux de [71] et [72]. Su et Kuo [71] ont présenté un schéma afin d'avoir plus de robustesse contre la rotation et la mise à

l'échelle. Afin d'accroitre le taux d'imperceptibilité et d'intégration de watermark, Shih et Wu [72] proposent un système de tatouage numérique qui combine le domaine spatial et fréquentiel pour l'insertion et l'extraction de la marque. On cite aussi un schéma de tatouage composé de trois transformées [73]. L'article présente un nouveau schéma pour mettre en œuvre un tatouage d'image aveugle basé sur un domaine composite incluant la transformée en ondelette discrète (DWT), la décomposition en valeurs singulières (SVD) et la transformée en cosinus discrète (DCT). Plusieurs bits peuvent être intégrés dans un seul bloc d'image en ajustant les paramètres via une technique de modulation d'indice de quantification progressive. L'extraction de la marque sans se référer à l'image originale. Les résultats Expérimentaux montrent que les marques incorporées présentent une robustesse exceptionnelle vis-à-vis des attaques de compression en utilisant les normes de codage $JPEG$, $JPEG2000$.

II.6. LES CARACTERISTIQUES DU SYSTEME VISUEL HUMAIN HVS

Pour l'extraction des principales caractéristiques dans une image on fait recours à l'exploitation du système visuel humain HVS dans les schémas de tatouage, ce qui permet d'atteindre au maximum les exigences de robustesse et d'imperceptibilité. L'utilisation des caractéristiques d'un système HVS aide énormément pour sélectionner les composants les plus appropriés pour insérer la marque. Il existe plusieurs indices utilisés par le système HVS pour la modélisation et la définition de la valeur de facteur de visibilité. Les facteurs utilisés dans notre schéma sont :

II.6.1.Entropie et L'edge entropie

L'entropie et l'edge entropie ont été utilisés pour sélectionner les régions d'insertion importantes, car elles contiennent des informations importantes sur l'image. L'entropie (information moyenne) est donc la quantité moyenne d'information qui est utilisée pour mesurer la corrélation spatiale des pixels voisins. La formule mathématique utilisée pour calculer l'entropie est celle définie par Shannon pour un ensemble N d'éléments [60].

$$E_{entropie} = -\sum_{i=1}^{n} p_i \log_2 (p_i) \qquad \text{(II.33)}$$

Où p_i Représente la probabilité d'occurrence d'un événement i avec $0 \leq p \leq 1$

$$\sum_{i=1}^{n} p_i = 1$$

La valeur dépend uniquement de la distribution de probabilité de l'intensité du pixel et ne considère pas la cooccurrence des valeurs de pixel. Le facteur E (entropie) mesure la redondance dans l'image, elle atteint de fortes valeurs pour une texture aléatoire. L'edge entropie d'un bloc d'image est également envisagée pour la sélection des régions d'intégration. Elle est aussi considérée comme identifiant des régions appropriées dans l'image pour insérer la marque. L'edge entropie d'un bloc d'image est définie comme suit [60].

$$E_{\text{edge entropie}} = \sum_{i=1}^{n} p_i \exp^{u_i} = \sum_{i=1}^{n} p_i \exp^{1-p_i} \quad \text{(II.34)}$$

Où u_i = 1 - p_i indique l'incertitude de la valeur du pixel.

Les blocs des valeurs d'entropie et edge entropie les plus faibles sont sélectionnés comme les meilleures régions pour insérer la marque.

II.6.2. Gradient de l'image

Malgré le grand avantage ramené par les transformées discrètes. La transformée discrète, comme les ondelettes (DWT) , qui permet la décomposition de l'image après analyse multi-résolution en sous-bandes au moyen de sous-échantillonnages successifs de l'image pour permettre une isolation raffinée des composantes basse fréquence afin de former un espace d'insertion moins sensible et la transformée en cosinus discrète (DCT) qui est caractérisée par un effet de séparation des hautes fréquences, des basses fréquences et des fréquences moyennes, donnant ainsi la possibilité d'utiliser une gamme de fréquences incluant des coefficients à fort degré d'énergie, pour la sélection des lieux adaptés à l'insertion de la marque et pour assurer un compromis entre l'invisibilité et la robustesse. On doit faire recours à d'autre paramètres qu' utilisent la sensibilité du système visuel humain (HVS) comme la douceur de l'image qui est évaluée en fonction du degré de variation des valeurs spatiales de l'image. Pour cela on fait appel à un outil mathématique qui est le gradient de l'image comme issue de mesure car il présente la dérivée spatiale qui donne une carte topologique de l'image. Où nous aurons la possibilité de voir et localiser les régions où les perturbations sont intenses et pouvoir également évaluer la douceur moyenne de l'image.

Nous savons qu'une image peut être définie comme une fonction bidimensionnelle$f\ (x, y)$, où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées (x, y) est appelée l'intensité ou le niveau de gris de l'image.

Pour une fonction $f(x,y)$, le gradient de $\boldsymbol{f}$ aux coordonnées (x,y) est défini comme le vecteur de colonne bidimensionnel:

$$\nabla f = \begin{bmatrix} G_x \\ G_Y \end{bmatrix} = \begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \end{bmatrix} \quad \text{(II.35)}$$

Le module de ce vecteur est donné par:

$$\nabla f = mag(\nabla f) = \left[G_x^2 + G_y^2\right]^{1/2} = \left[\left(\frac{\partial f}{\partial x}\right)^2 + \left(\frac{\partial f}{\partial y}\right)^2\right]^{\frac{1}{2}} \quad \text{(II.36)}$$

Les composantes du vecteur de gradient lui-même sont des opérateurs linéaires, mais le module de ce vecteur ne l'est pas évidemment est c'est du aux opérations de quadrature et de la racine carrée. Il est de pratique courante d'approcher l'amplitude du gradient en utilisant des valeurs absolues au lieu des carrés et de la racine carrée [74]:

$$\nabla f = |G_x| + |G_y| \quad \text{(II.37)}$$

La direction du vecteur gradient est également une quantité importante. Soit $\alpha\,(x,y)$ l'angle de direction du vecteur ∇f à (x,y). Puis, à partir de l'analyse vectorielle

$$\alpha(x,y) = tan^{-1}\left(\frac{G_y}{G_x}\right) \quad \text{(II.38)}$$

Le calcul du gradient d'une image est basé sur l'obtention des dérivées partielles $\frac{\partial f}{\partial x}$ et $\frac{\partial f}{\partial y}$ à chaque emplacement de pixel. La valeur élevée du gradient permet de localiser les zones des hautes fréquences qui montrent clairement les régions perturbées de l'image, contrairement aux basses fréquences où elles se situent par les valeurs où le gradient prend des valeurs relativement faibles qui montrent les régions lisses de l'image. Comme nous venons de le décrire, le gradient sert d'outil de mesure efficace pour déterminer le degré de douceur de l'image.

CONCLUSION

Les transformées discrètes comme $la\,DCT, la\,DWT, la\,SVD$ et la paramétrisation des matrices de Hadamard qui découle sur la transformée réciproque-orthogonale et paramétrique (ROP) . Confirment efficacement leurs utilisation dans le domaine de traitement des images et spécialement pour le tatouage numérique des images qui consolident et améliorent la robustesse et l'imperceptibilité des images tatouées dans le domaine fréquentiel. Vu que les transformées discrètes travaillent dans un domaine transformé fréquentiel et accordent la

possibilité, pour l'incorporation de la marque en effectuant une modification des coefficients d'image en utilisant des transformations d'image et offrent la possibilité d'étaler et de faire propager les coefficients de la marque ou la signature dans toute l'image de couverture ce qui donne un grand avantage par rapport au domaine spatial qui n'utilise pas de transformées. En plus de ces transformées nous avons montré l'intérêt et l'avantage suite à l'exploitation du système visuel humain VHS par le biais de plusieurs indices pour la modélisation et la définition de la valeur de facteur de visibilité, comme le calcul de l'entropie, le calcul de l'edge entropie et le calcul du gradient de l'image.

Cependant faire recours à l'espace spatial ou bien transformé lors de la conception d'un schéma pour donner un bon système de tatouage n'est pas toujours la meilleure solution.

Une nouvelle stratégie qui a envahi le monde de tatouage numérique des images, c'est la combinaison des transformées ou les schémas de tatouage à base des algorithmes hybrides, afin d'assurer un taux acceptable d'imperceptibilité et d'intégration de watermark et d'avoir plus de robustesse contre les attaques ce qui mène à une combinaison de transformées comme la $DCT - SVD$ et la$DWT - DCT$, d'où l'appellation des algorithmes hybrides.

Chapitre III

Approches des Schémas Hybrides Proposées et Résultats

INTRODUCTION

Dans ce chapitre nous proposons deux approches à base d'algorithmes hybrides de tatouage des images numériques, la première approche applique un schéma de tatouage par combinaison de deux transformées, la transformée en cosinus discrète (DCT) et la décomposition en valeurs singulières(SVD), avec l'exploitation du système visuel humain (HVS) par l'utilisation de deux indices qui sont l'entropie et l'edge entropie. L'entropie selon Claude Shannon [75] est une fonction mathématique, qui correspond à la quantité d'information contenue ou délivrée par une source d'information. Cette source peut être un signal électrique ou encore un fichier informatique quelconque, comme une image numérique, une vidéo ou un enregistrement sonore.

La deuxième approche c'est la combinaison de la DCT avec la DWT avec l'exploitation de la douceur de l'image qui est évaluée en fonction du degré de variation des valeurs spatiales de l'image. Dans cette approche, nous utilisons l'indice gradient de l'image comme un outil de mesure, car il présente une dérivée spatiale qui donne une carte topologique de l'image.

Cette étape est importante comme celle qui exploite l'entropie pour localiser les régions où les perturbations sont intenses et permet également d'évaluer la douceur moyenne de l'image. Ces approches viennent pour répondre aux exigences d'un bon schéma de tatouage qui doit satisfaire un ensemble de critères, y compris la robustesse, l'imperceptibilité et la compatibilité du watermark avec l'image originale.

III.1. SCHEMA D'UN TATOUAGE NUMERIQUE A BASE DE LA DCT ET LA SVD UTILISANT L'ENTROPIE

Les simulations sont faites avec des images tests en niveau de gris de taille égales (512×512) mais de formats différents $(BMP, PNG, TIFF, et\ JPEG)$ très connues dans le monde de traitement des images nommées respectivement Lena, Livingroom , Mandrill ou Baboon et Peppers. La marque à insérer est de taille inferieure par rapport à la taille des images hôtes et qui présente un logo binaire de taille $(32 \times 32).bmp$.

"Lena" "Livingroom" "Mandrill" "Peppers"

Figure III.1 : les images originales

Figure III.2 : la marque à insérer

III.2. ALGORITHME PROPOSE

III.2.1. Principe d'insertion

1- Lecture de l'image hôte et la marque à insérer.

2- Diviser l'image hôte en blocs de (8×8).

3- Calcul de l'entropie et l'edge entropie de chaque bloc.

4- Classer la somme de l'entropie et l'edge entropie par ordre croisant et déduire le seuil d'insertion du watermark dans les endroits à faible taux d'information.

5- Appliquer la DCT au niveau des blocs sélectionnés de l'image hôte.

6- Appliquer la SVD aux blocs sélectionnés suite à la transforméeDCT, pour décomposer chaque bloc en trois matrices$U$,S,et V.

7- Insérer la marque dans les coefficients sélectionnés de la première colonne de la matrice U.

8- Appliquer la SVD inverse à chaque bloc de la DCT.

9- Appliquer la DCT inverse $iDCT$ pour obtenir l'image tatouée.

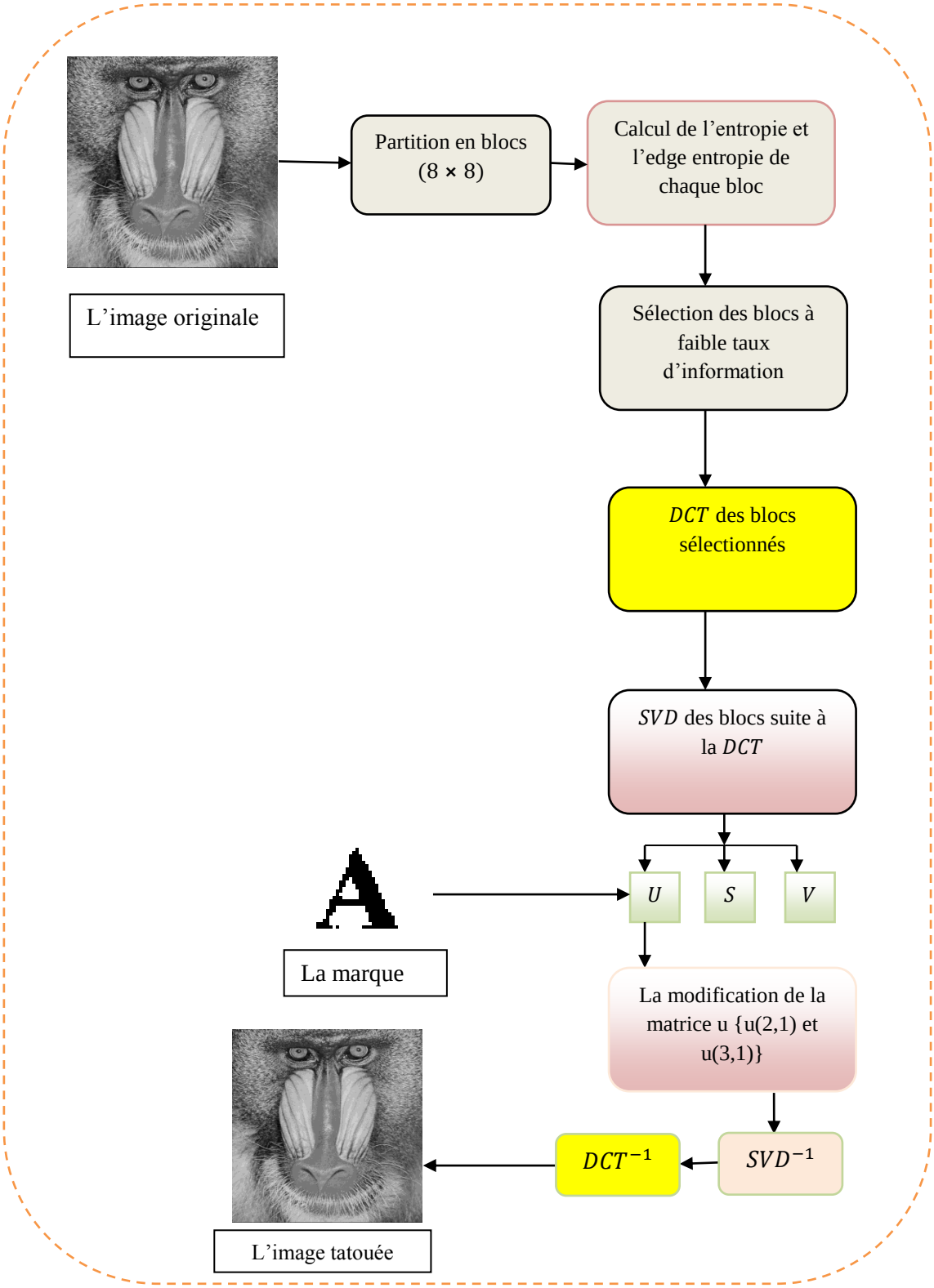


Figure III-3 : Algorithme d'insertion de la marque.

III.2.2. Principe d'extraction

1- Diviser l'image tatouée en blocs de(8×8).

2- Sélectionner le nombre des blocs utilisés dans le processus d'insertion

3- Appliquer la DCT à chaque bloc sélectionné de l'image tatouée.

4- Appliquer la SVD à chaque bloc suite à la transformée DCT.

5- Détecter le deuxième et le troisième coefficient de la première colonne de U

6- Appliquer la SVD inverse et la DCT inverse $iDCT$ pour extraire la marque.

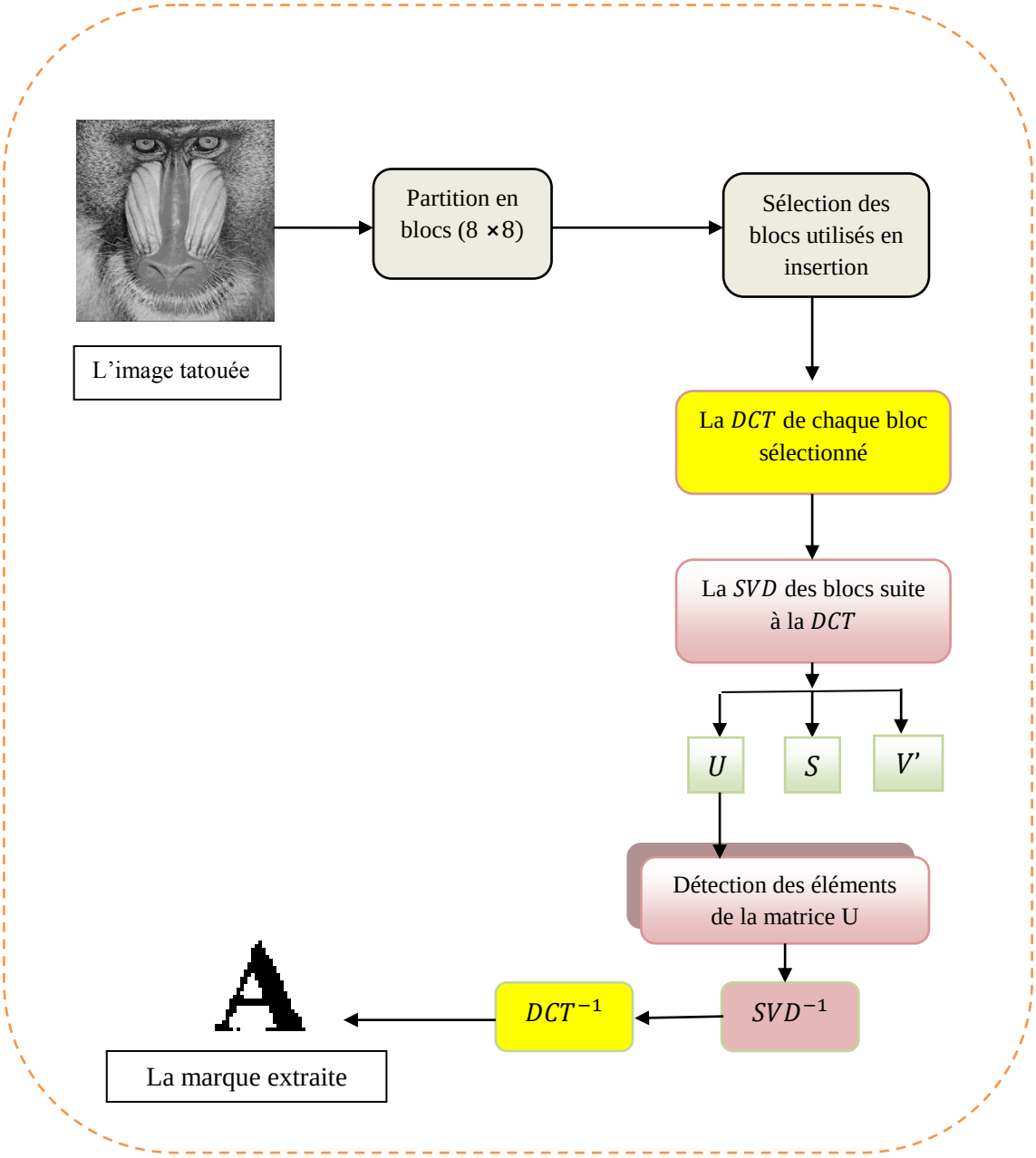


Figure III.4 : Algorithme d'extraction de la marque

III.3. Simulations et résultats

Avec différentes valeurs de seuil d'insertion du watermark dans les endroits à faible taux d'information ($Threshold\ \boldsymbol{T} = 0.002, 0.012, 0.02\ et\ 0.04$), on a procédé à l'incrustation de la marque selon la procédure d'insertion citée ci-dessus dans les différentes images test (Lena, Living-room, Mandrill et Pepper).

- ✓ Les seuils pour tous les tests sont choisis comme suit :

$(a)\ T = 0{,}002$ $(b)\ T = 0{,}012$ $(c)\ T = 0{,}02$ $(d)\ T = 0{,}04.$

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

Figure III.5 : Image Lena tatouée avec différents seuils.

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

Figure III.6 : marque extraite de l'image Lena avec différents seuils.

Tableau III.1 : Evaluation de PSNR, NCC après insertion et NCC, SSIM et BER après extraction de la marque de l'image Lena.

Lena	L'insertion		L'extraction		
	PSNR (dB)	NCC	NCC	SSIM	BER
T=0.002	52.0387	0.9999	0.8927	0.9993	0.0470
T=0.012	48.7536	0.9998	1	1	0
T=0.02	45.9577	0.9996	1	1	0
T=0.04	40.9118	0.9989	1	1	0

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

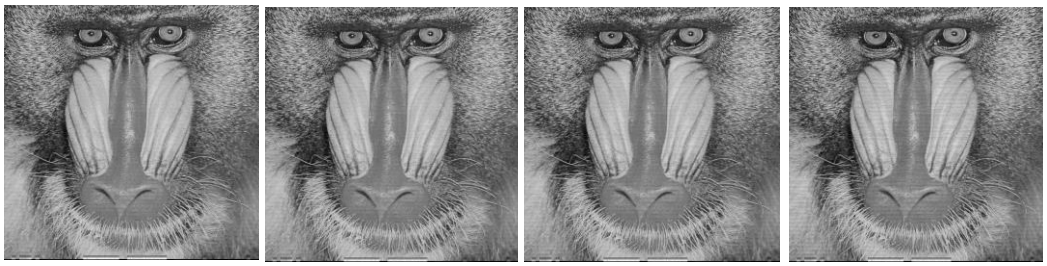
Figure III.7: Image Living-room tatouée avec différents seuils.

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

Figure III.8: marque extraite de l'image Living-room avec différents seuils.

Tableau III.2 : Evaluation de PSNR, NCC après insertion et NCC, SSIM et BER après extraction de la marque de l'image Living-room.

Living-room	L'insertion		L'extraction		
	PSNR dB	NCC	NCC	SSIM	BER
T=0.002	45.5953	0.9995	0.8480	0.9984	0.0692
T=0.012	44.9958	0.9995	0.9913	1	0.0037
T=0.02	44.0072	0.9993	0.9971	1	0.0012
T=0.04	40.9950	0.9987	0.9971	1	0.0012



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

Figure III.9 : Image Mandrill tatouée avec différents seuils.

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

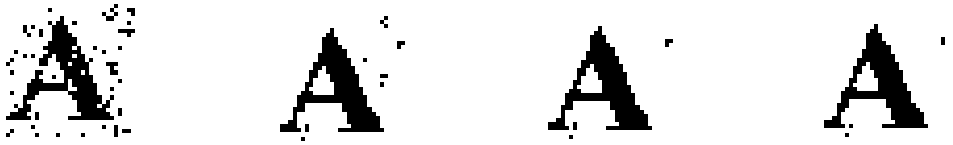
Figure III.10 : marque extraite de l'image Mandrill avec différents seuils.

Tableau III.3 : Evaluation de PSNR, NCC après insertion et NCC, SSIM et BER après extraction de la marque de l'image Mandrill.

Mandrill	L'insertion		L'extraction		
	PSNR dB	NCC	NCC	SSIM	BER
T=0.002	34.3819	0.9934	0.9415	0.9998	0.0260
T=0.012	34.2226	0.9931	1	1	0
T=0.02	34.0271	0.9928	1	1	0
T=0.04	33.3379	0.9916	1	1	0

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

Figure III.11 : Image Peppers tatouée avec différents seuils.



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

Figure III.12 : marque extraite de l'image Peppers avec différents seuils.

Tableau III.4 : Evaluation de PSNR, NCC après insertion et NCC, SSIM et BER après extraction de la marque de l'image Peppers.

Peppers	L'insertion		L'extraction		
	PSNR dB	NCC	NCC	SSIM	BER
T=0.002	47.2191	0.9998	0.7874	0.9980	0.1014
T=0.012	46.2246	0.9997	0.9629	0.9998	0.0161
T=0.02	44.8138	0.9996	0.9825	0.9999	0.0074
T=0.04	41.1344	0.9991	0.9913	1	0.0037

Interprétation des résultats :

L'absence des attaques sur notre système de tatouage donne une bonne imperceptibilité en termes de qualité de l'image tatouée et une bonne robustesse en termes des données extraites. Nous remarquons aussi d'après les résultats exhibés dans les tableaux présentés ci-dessus que la valeur choisie pour les seuils T influe directement sur la valeur du $PSNR$ (entre l'image originale

et l'image tatouée) pour la phase d'insertion et influe aussi sur le NCC (entre la marque originale et la marque extraite) pour la phase d'extraction, et par conséquent la valeur la plus adaptée pour notre système de tatouage adaptatif non visible lors de l'insertion est $T = 0.002$ où on a pu atteindre une valeur de PSNR très acceptable (PSNR=52dB). Pour l'extraction de la marque la valeur de seuil la plus adaptée est $T = 0.04$ (NCC=1) pour l'ensemble des images test choisies.

La deuxième remarque qui persiste, c'est l'impact sur le choix des formats des images utilisés, où on trouve pour quelques cas des valeurs de PSNR qui descendent jusqu'à 33dB, ce qui met en évidence le choix des images test multi formats.

III.4. TESTS VIS-A-VIS DES ATTAQUES

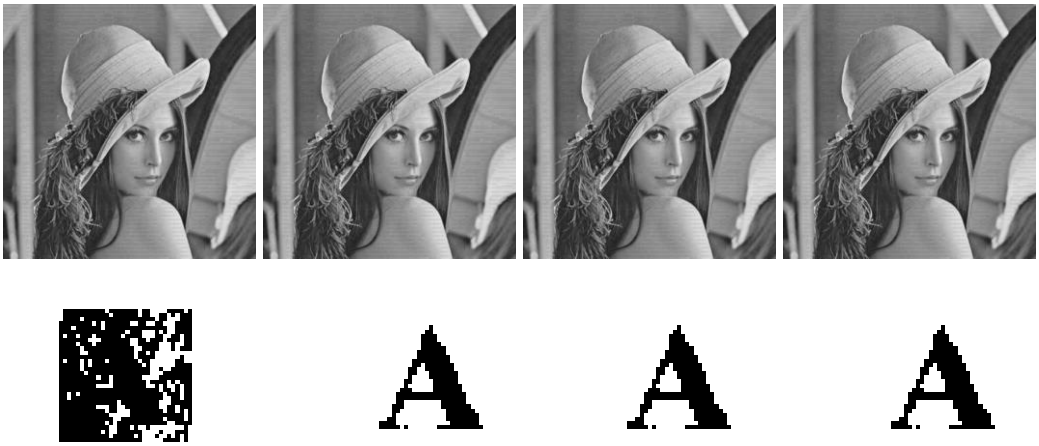
La robustesse de l'approche proposée va être testée par la simulation de plusieurs attaques qui vont être appliquées sur l'image tatouée afin de juger la fiabilité du système de tatouage proposé vis-à-vis des attaques intentionnelles ou non intentionnelles.

Nous présentons un éventail de différentes attaques appliquées sur des images de test où on a choisi trois images : "Lena, Mandrill et Peppers" avec l'évaluation des résultats par le biais de trois métriques d'évaluation des performances pour mettre en évidence la similitude et la similarité entre la marque originale et la marque extraite après attaques et qui sont :

- ✓ NCC : Correlation Normalisée
- ✓ SSIM : Index de similarité structurelle
- ✓ BER : Taux d'erreur mesurée

- On note que toutes les attaques sont faites avec un seuil T=0.04.

III.4.1. Attaque par Compression JPEG.

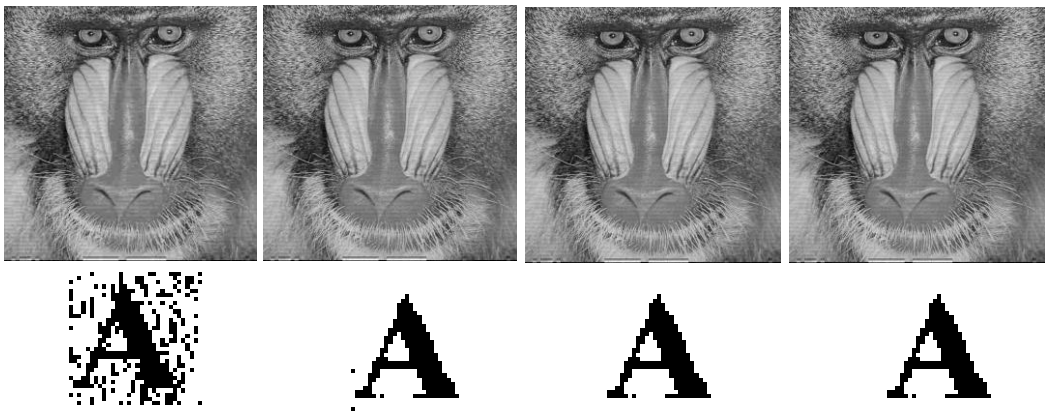


10% 30% 50 % 90%

Figure III-13 : Résultats de la robustesse de l'image Lena après des attaques par compression JPEG.

Tableau III.5 : Evaluation de NCC, SSIM et BER après attaque par compression JPEG de l'image Lena.

L'image Lena			
Taux %	NCC	SSIM	BER
10	0.2806	0.9686	0.7108
30	1	1	0
50	1	1	0
90	1	1	0

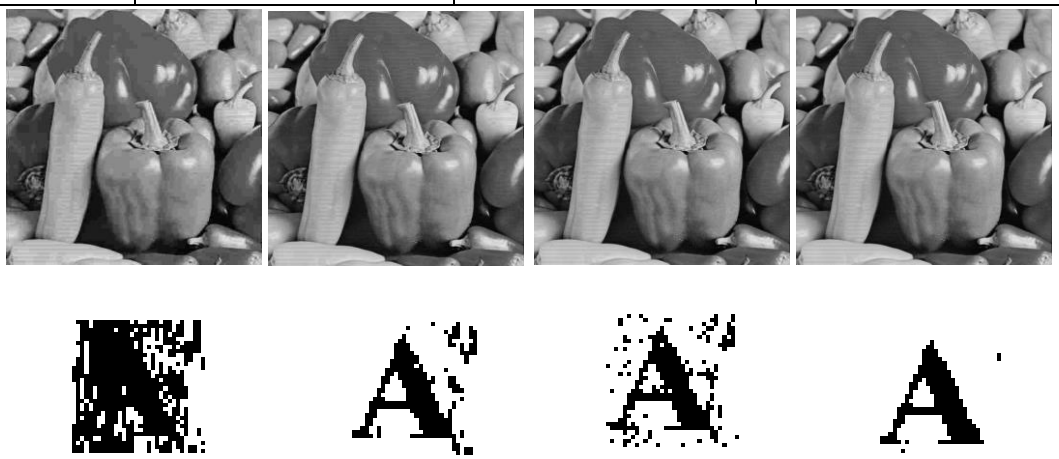


10 % 30% 50 % 90%

Figure III.14 : Résultats de la robustesse de l'image Mandrill après des attaques par compression JPEG.

Tableau III-6 : Evaluation de NCC, SSIM et BER après des attaques par compression JPEG de l'image Mandrill.

L'image Mandrill			
Taux %	NCC	SSIM	BER
10%	0.6275	0.9938	0.2398
30%	0.9941	1	0.0025
50%	1	1	0
90%	1	1	0



10% 30% 50% 90%

Figure III.15 : Résultats de la robustesse de l'image Peppers après des attaques par compression JPEG.

Tableau III.7 : Evaluation de NCC, SSIM et BER après des attaques par compression JPEG de l'image Peppers.

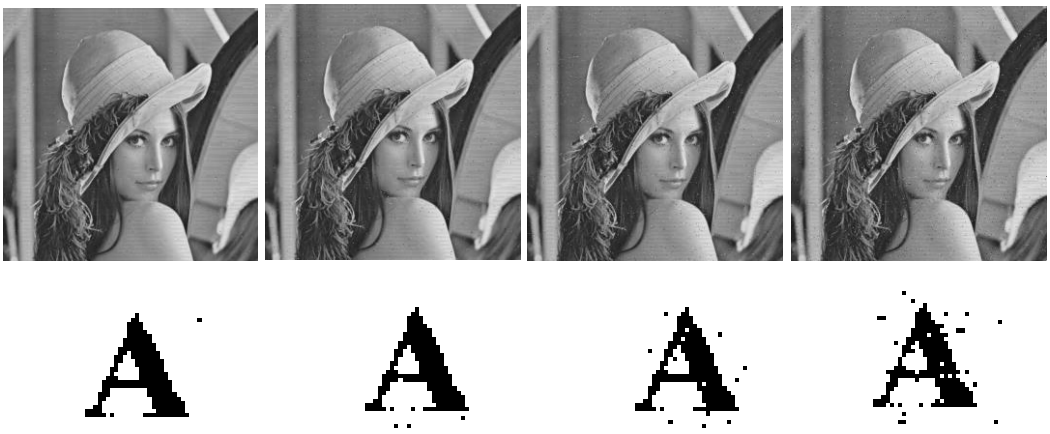
L'image Peppers			
Taux %	NCC	SSIM	BER
10	0.3515	0.9656	0.5983
30	0.8329	0.9981	0.0841
50	0.9031	0.9993	0.0445
90	0.9913	1	0.0037

Un signe positif, suite aux diagnostiques des valeurs des métriques choisies pour l'évaluation de la marque extraite, qui sont le NCC, le SSIM et le BER vis-à-vis des attaques JPEG, où on peut distinguer que la récupération de la marque est presque parfaite à partir d'un taux de compression supérieur à 30%, ce constat est confirmé aussi par une analyse subjective des marques extraites vu qu'elles présentent une belle qualité visuelle.

III.4.2. Attaque par ajout de bruit

III.4.2.1. Ajout de bruit Salt & Pepper

Voici les résultats des images tatouées et des marques extraites suite à des attaques par ajout de bruit Salt & Peppers suite aux changements des densités du bruit appliqué

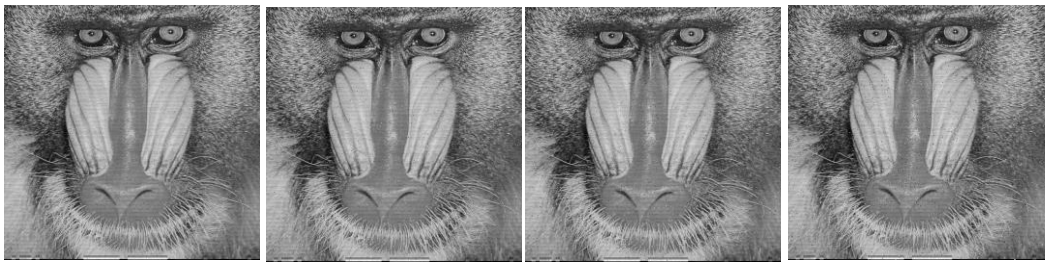


Densité=0.001 Densité =0.003 Densité =0.005 Densité =0.009

Figure III.16 : Résultats de la robustesse de l'image Lena après l'attaque par un bruit "Salt & Pepper".

Tableau III.8 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Salt & Pepper" de l'image Lena

L'image Lena			
Densité	NCC	SSIM	BER
0.001	0.9971	1	0.0025
0.003	0.9851	0.9999	0.0062
0.005	0.9624	0.9998	0.0161
0.009	0.9119	0.9991	0.0297

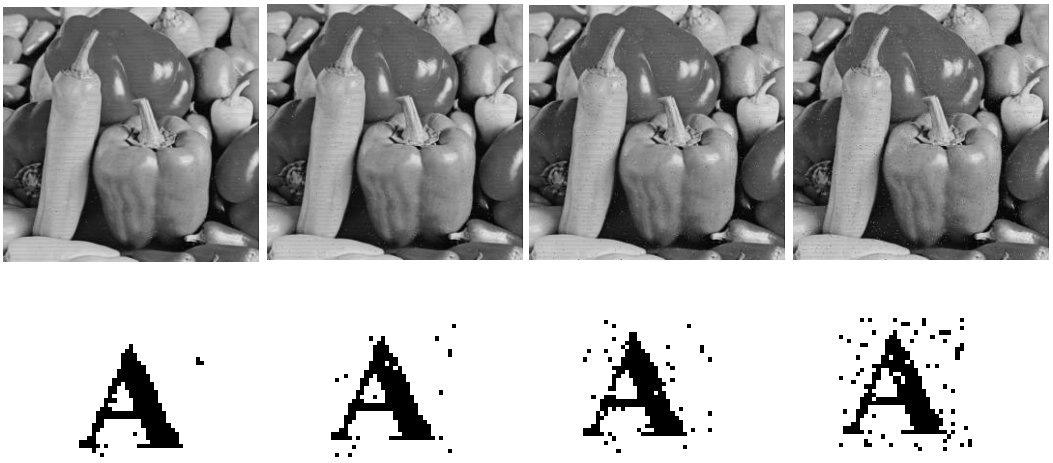


Densité=0.001 Densité =0.003 Densité =0.005 Densité =0.009

Figure III.17: Résultats de la robustesse de l'image Mandrill après l'attaque par un bruit "Salt & Pepper".

Tableau III.9 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Salt & Pepper" de l'image Mandrill.

L'image Mandrill			
Densité	NCC	SSIM	BER
0.001	0.9883	0.9999	0
0.003	0.9794	0.9998	0.0074
0.005	0.9678	0.9997	0.0148
0.009	0.9234	0.9995	0.0371



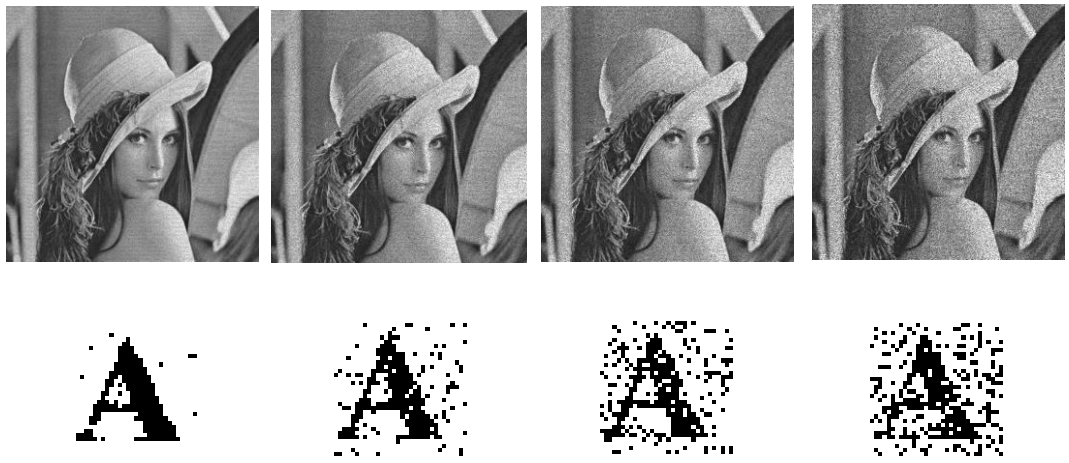
Densité=0.001 Densité =0.003 Densité =0.005 Densité =0.009

Figure III.18 : Résultats de la robustesse de l'image Peppers après l'attaque par un bruit "Salt & Pepper".

Tableau III.10 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Salt & Pepper" de l'image Peppers.

L'image Peppers			
Densité	NCC	SSIM	BER
0.001	0.9798	0.9999	0.0087
0.003	0.9544	0.9998	0.0198
0.005	0.8960	0.9991	0.0470
0.009	0.8352	0.0779	0.9985

III.4.2.2 Ajout de bruit Speckle

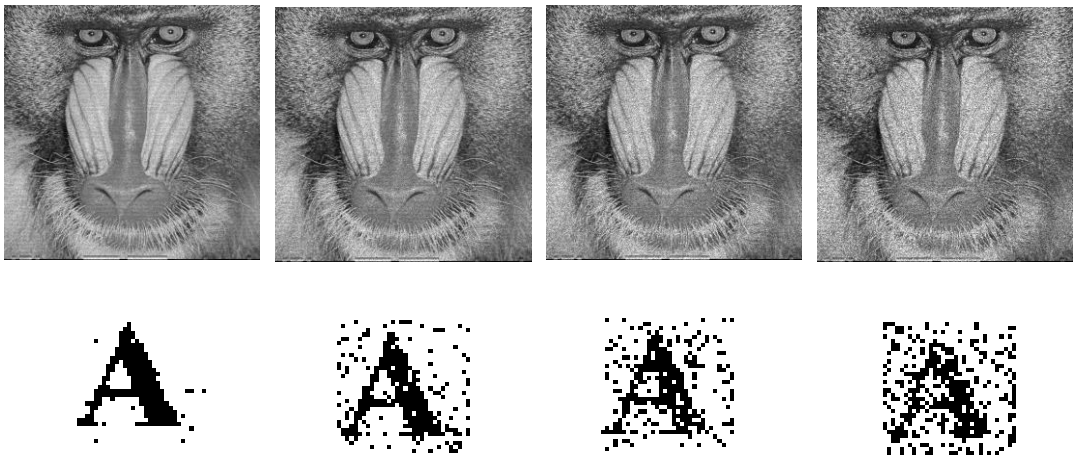


Var = 0.01 Var = 0.03 Var = 0.05 Var = 0.09

Figure III.19 : Résultats de la robustesse de l'image Lena après l'attaque par un bruit " Speckle ".

Tableau III.11 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Speckle". Pour l'image Lena.

L'image Lena			
Variance	NCC	SSIM	BER
0.01	0.9765	0.9998	0.0198
0.03	0.7116	0.9970	0.1397
0.05	0.5828	0.9941	0.2373
0.09	0.4086	0.9898	0.2954

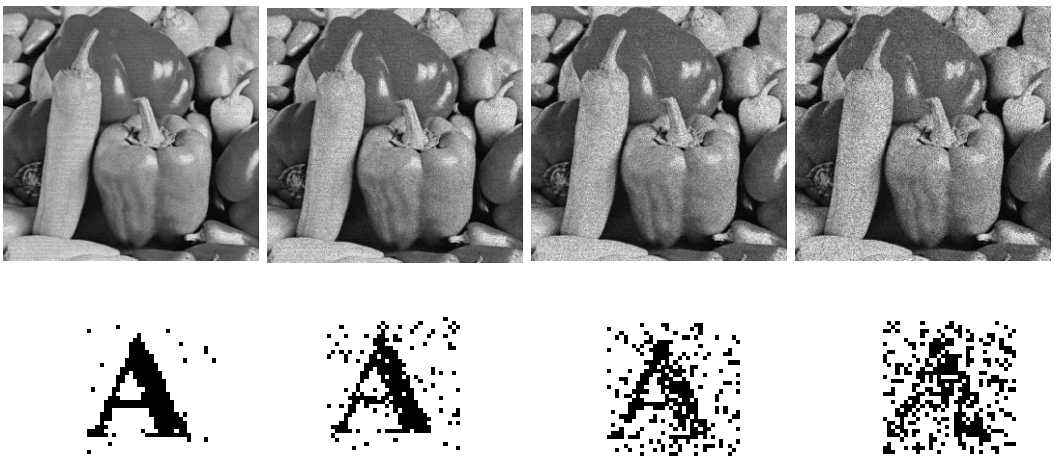


Var = 0.01 Var = 0.03 Var = 0.05 Var = 0.09

Figure III.20 : Résultats de la robustesse de l'image Mandrill après l'attaque par un bruit "Speckle".

Tableau III.12 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Speckle" Pour l'image Mandrill.

L'image Mandrill			
Variance	NCC	SSIM	BER
0.01	0.9629	0.9997	0.0198
0.03	0.7148	0.9978	0.1187
0.05	0.6256	0.9948	0.1965
0.09	0.4618	0.9927	0.3152



Var = 0.01 Var = 0.03 Var = 0.05 Var = 0.09

Figure III.21: Résultats de la robustesse de l'image Peppers après l'attaque par un bruit "Speckle".

Tableau III.13 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Speckle" pour l'image Peppers.

L'image Peppers			
Variance	NCC	SSIM	BER
0.01	0.9437	0.9997	0.0247
0.03	0.7528	0.9979	0.1150
0.05	0.5592	0.9945	0.2213
0.09	0.3996	0.9902	0.3337

III.4.2.3 Ajout de bruit Gaussien

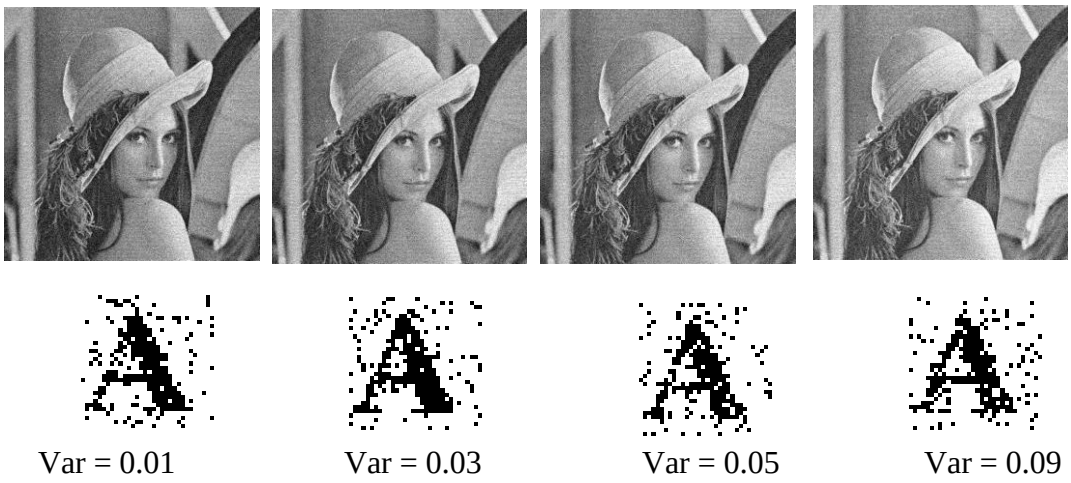


Figure III.22 : Résultats de la robustesse de l'image Lena après l'attaque par un bruit "Gaussien".

Tableau III-14 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Gaussien" Pour l'image Lena.

L'image Lena			
Variance	NCC	SSIM	BER
0.01	0.7612	0.9976	0.1286
0.03	0.726	0.9973	0.1335
0.05	0.7190	0.9969	0.1075
0.09	0.7013	0.9967	0.1273

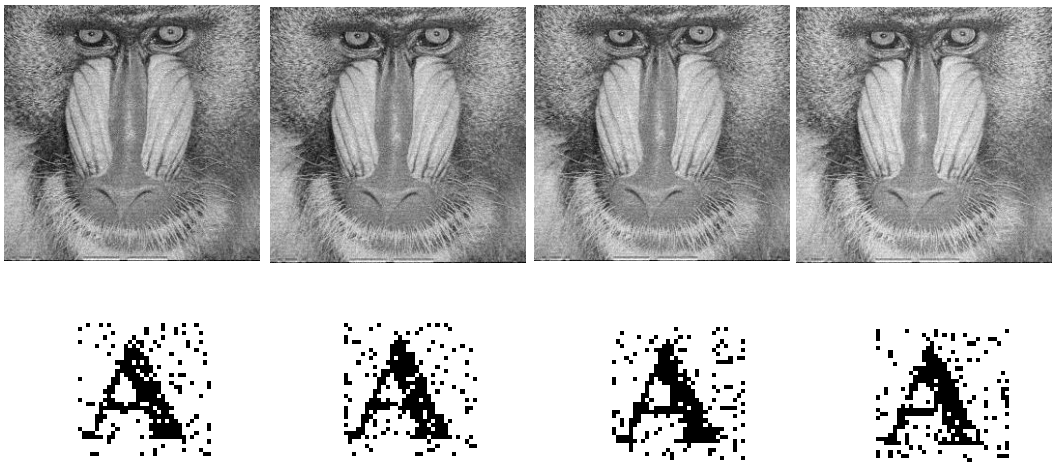


Figure III-23 : Résultats de la robustesse de l'image Mandrill après l'attaque par un bruit "Gaussien".

Tableau III.15 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Gaussien" pour l'image Mandrill.

L'image Mandrill			
Variance	NCC	SSIM	BER
0.01	0.7140	0.9971	0.1162
0.03	0.7087	0.9971	0.1483
0.05	0.7059	0.9970	0.1162
0.09	0.6924	0.9969	0.1323

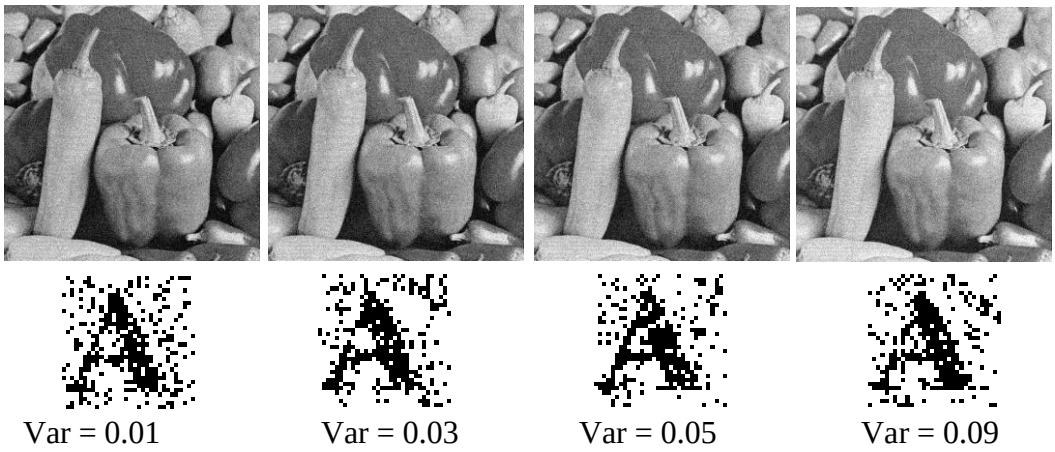


Figure III.24: Résultats de la robustesse de l'image Peppers après l'attaque par un bruit "Gaussien".

Tableau III.16 : Evaluation de NCC, SSIM et BER après l'attaque par un bruit "Gaussien" Pour l'image Peppers.

L'image Pepper			
Variance	NCC	SSIM	BER
0.01	0.6140	0.9939	0.2398
0.03	0.6225	0.9956	0.2163
0.05	0.6189	0.9952	0.2027
0.09	0.6266	0.9957	0.1953

Le test des attaques par l'ajout de bruit pour les trois ajouts simulés, le bruit Salt & Peppers, le bruit Spekle et le bruit Gaussien s'avère très encourageant suite à la qualité visuelle de la marque extraite (la marque est détectable).

III.4.3. Attaques par filtrage

Le test de la robustesse des schémas de tatouage vis-à-vis des opérations de filtrage est indispensable dans le monde de traitement des images et spécialement dans le domaine de tatouage numérique des images. Trois types de filtres, le filtre médian, le filtre passe-bas et le filtre gaussien, seront testés avec un masque de taille [3 3], pour la mise en évidence de la robustesse de cette approche.

III.4.3.1 Attaques par filtrage Médian

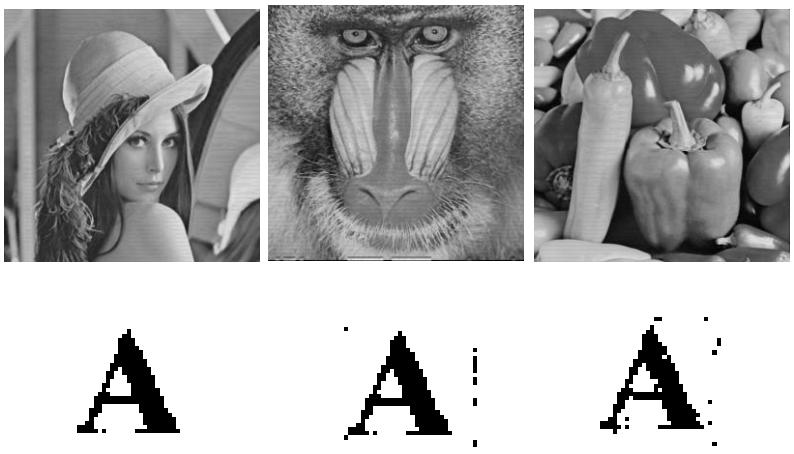


Figure III.25: Résultats de la robustesse des images "Lena, Mandrill et Pepper" après l'attaque par un filtre "Médian".

Tableau III.17 : Evaluation de NCC, SSIM et BER après l'attaque par un filtre "Médian" pour l'image Lena, l'image Mandrill et l'image Peppers.

L'image	taille	NCC	SSIM	BER
Lena	[3 3]	1	1	0
Mandrill	[3 3]	0.9578	1	0.0185
Peppers	[3 3]	0.9535	0.9997	0.0198

III.4.3.2.Attaques par filtrage passe-bas

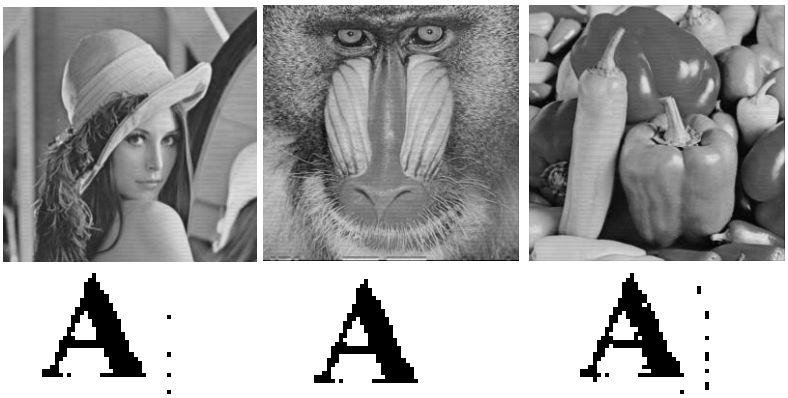


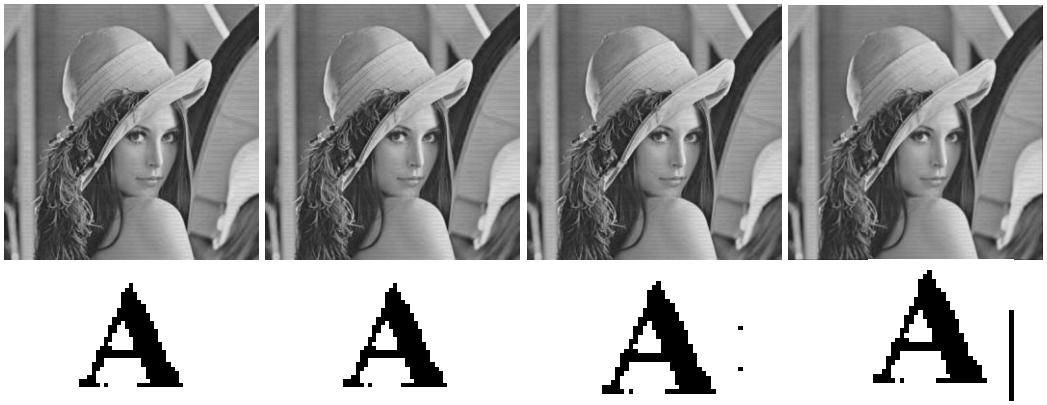
Figure III-26: Résultats de la robustesse des images "Lena, Mandrill, et Peppers " après l'attaque par un filtre "Passe-bas".

Tableau III.18 : Evaluation de NCC, SSIM et BER après l'attaque par un filtre "Passe bas" pour l'image Lena, l'image Mandrill et l'image Peppers.

L'image	taille	NCC	SSIM	BER
Lena	[3 3]	0.9884	1	0.0049
Mandrill	[3 3]	1	1	0
Peppers	[3 3]	0.9510	0.9998	0.0210

III.4.3.3.Attaques par filtrage gaussien

Avec des sigmas différents (0.1, 0.3, 0.5 et 0.9 et le même masque [3 3] on trouve :

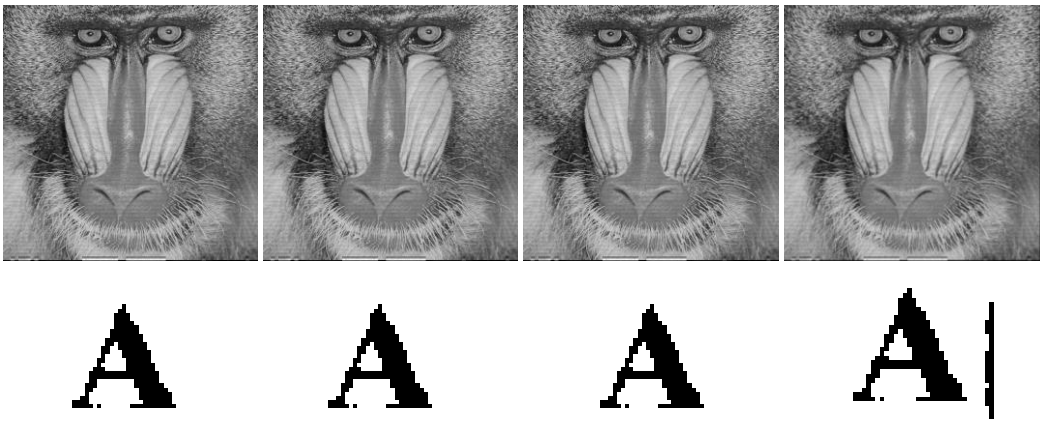


Sigma =0.1 Sigma =0.3 Sigma =0.5 Sigma =0.9

Figure III.27 : Résultats de la robustesse de l'image Lena après l'attaque par un filtre "Gaussien".

Tableau III-19 : Evaluation de NCC, SSIM et BER après l'attaque par un filtre "Gaussien" pour l'image Lena.

L'image Lena			
Sigma	NCC	SSIM	BER
0.1	1	1	0
0.3	1	1	0
0.5	0.9913	1	0.0037
0.9	0.9446	1	0.0247



Sigma =0.1 Sigma =0.3 Sigma =0.5 Sigma =0.9

Figure III.28: Résultats de la robustesse de l'image Mandrill après l'attaque par un filtre "Gaussien".

Tableau III.20 : Evaluation de NCC, SSIM et BER après l'attaque par un filtre "Gaussien" pour l'image Mandrill.

L'image Mandrill			
Sigma	NCC	SSIM	BER
0.1	1	1	0
0.3	1	1	0
0.5	1	1	0
0.9	0.8952	1	0.0494

Sigma =0.1 Sigma =0.3 Sigma =0.5 Sigma =0.9

Figure III.29 : Résultats de la robustesse de l'image Peppers après l'attaque par un filtre "Gaussien".

Tableau III.21 : Evaluation de NCC, SSIM et BER après l'attaque par un filtre "Gaussien" pour l'image Peppers.

L'image Peppers			
Sigma	NCC	SSIM	BER
0.1	0.9913	1	0.0037
0.3	0.9913	1	0.0037
0.5	0.9538	0.9998	0.0198
0.9	0.8936	0.9996	0.0482

Les filtres restent des attaques nuisibles au système de tatouage, car ils peuvent altérer ou bien même détruire une signature insérée, puisque le filtrage est un processus qui remplace un pixel par une valeur qui est fonction des données à proximité de ce pixel.

Dans cette approche et suite aux résultats présentés dans les tableaux ci-dessus, l'extraction de la marque après des attaques par filtrage est acceptable où on voit que la marque est très lisible et les valeurs des métriques s'annoncent dans les normes, ce qui met en évidence une autre fois la robustesse de notre approche contre ce type d'attaque.

III.4.4. Attaque par Sharppening

L'attaque par Sharppening ou attaque par accentuation de la netteté a mis aussi en évidence la robustesse de ce schéma de tatouage numérique. Comme nous pouvons constater que la marque a été parfaitement récupérée pour les trois images test, l'image Lena, l'image Mandrill et l'image Peppers.

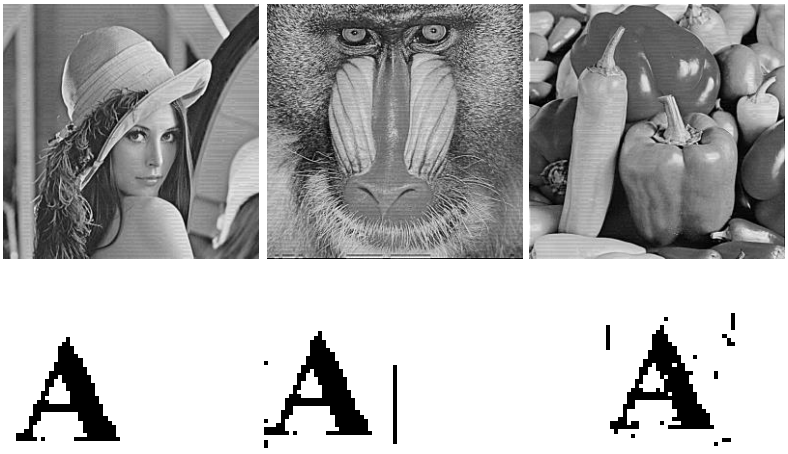


Figure III.30 : Résultats de la robustesse des images "Lena, Mandrill et Peppers» après l'attaque par "Sharppening"

Tableau III-22 : Evaluation de NCC, SSIM et BER après l'attaque par Sharppening pour l'image Lena, l'image Mandrill et l'image Peppers.

L'image	NCC	SSIM	BER
Lena	1	1	0
Mandrill	0.9317	1	0.0317
Peppers	0.9066	0.9995	0.0420

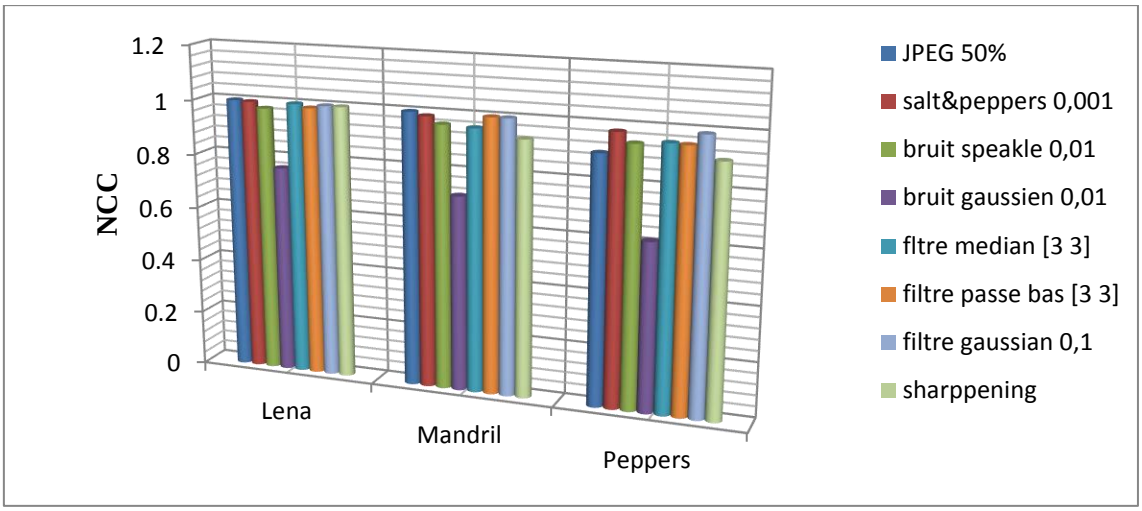
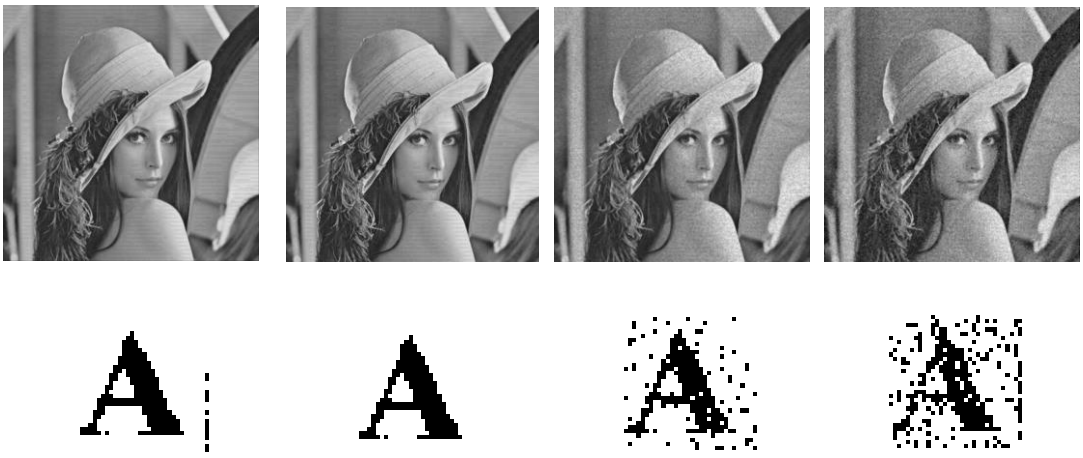


Figure III.31 : Variation de la valeur de NCC après des attaques appliquées pour les images «Lena, Mandrill et Peppers".

La moyenne de la variation de la NCC est supérieure à 0.9 et il y a des valeurs qui frôlent l'unité (NCC=1) qui est une valeur parfaite pour un jugement par le biais de la corrélation normalisée, donc c'est une mise en évidence de la robustesse de la méthode proposée.

III.5. COMBINAISON DES ATTAQUES

La simulation de plusieurs attaques simultanées sur la même image tatouée va sans doute mettre en évidence la robustesse de l'approche proposée.



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

Figure III.32 : (a) Compression JPEG 70% + filtre passe bas, (b) Compression JPEG 70% + filtre médian, (c) Compression JPEG 70% + bruit Speckle, (d) Compression JPEG 70% + bruit gaussien.

Tableau III. 23 : Evaluation de NCC, SSIM et BER des quatre combinaisons d'attaque.

	NCC	SSIM	BER
(a)	0.9798	1	0.0087
(b)	1	1	0
(c)	0.8013	0.9986	0.0939
(d)	0.6118	0.9960	0.2052

La décision visuelle subjective est très acceptable, on peut déduire que même pour une combinaison d'attaques que les valeurs obtenues par les métriques d'évaluation de la performance sont très satisfaisantes ce qui met en exergue la robustesse de la méthode.

III.6. MISE EN EVIDENCE DE L'EXPLOITATION DES BLOCS A FAIBLE ENTROPIE

Le schéma de notre système de tatouage se base sur l'exploitation du système visuel humain donc l'utilisation de deux indices, l'entropie et l'edge entropie. Le choix des blocs à faibles valeurs de l'entropie et l'edge entropie dans une image tatouée mène à la sélection des meilleures régions pour une bonne insertion de la marque pour assurer l'imperceptibilité et la robustesse. Pour les tests on a pris uniquement l'image Lena aves des seuils d'incrustation différents, ce qui a donné les résultats suivants :

(T=0.002) (T=0.012) (T=0.02) (T=0.04)

Figure III.33 : Image tatouée après insertion dans les régions à faibles valeurs de l'entropie et l'edge entropie avec différentes valeurs de seuil T.

Tableau III.24 : Evaluation de PSNR et NCC entre l'image originale (Lena) et l'image tatouée après ,insertion dans les régions à faibles valeurs de l'entropie et l'edge entropie avec différentes valeurs seuils.

Seuils	PSNR	NCC
T=0.002	52.0387	0.9999
T=0.012	48.7536	0.9998
T=0.02	45.9577	0.9996
T=0.04	40.9118	0.9989

Dans le deuxième cas on va inverser les endroits d'incrustation, donc insérer la marque dans les blocs à fortes valeurs de l'entropie et de l'edge entropie et voir l'impact de cette insertion.

(T=0.002) (T=0.012) (T=0.02) (T=0.04)

Figure III.34 : Image tatouée après insertion dans les régions à taux élevé de l'entropie et l'edge entropie avec différentes valeurs de seuil.

Tableau III. 25 : Evaluation de PSNR et de NCC entre l'image originale (Lena) et l'image tatouée après insertion dans les régions à taux élevé de l'entropie et l'edge entropie avec différentes valeurs seuils.

Seuils	PSNR	NCC
T=0.002	29.6821	0.9847
T=0.012	29.6644	0.9846
T=0.02	29.6344	0.9845
T=0.04	29.4984	0.9840

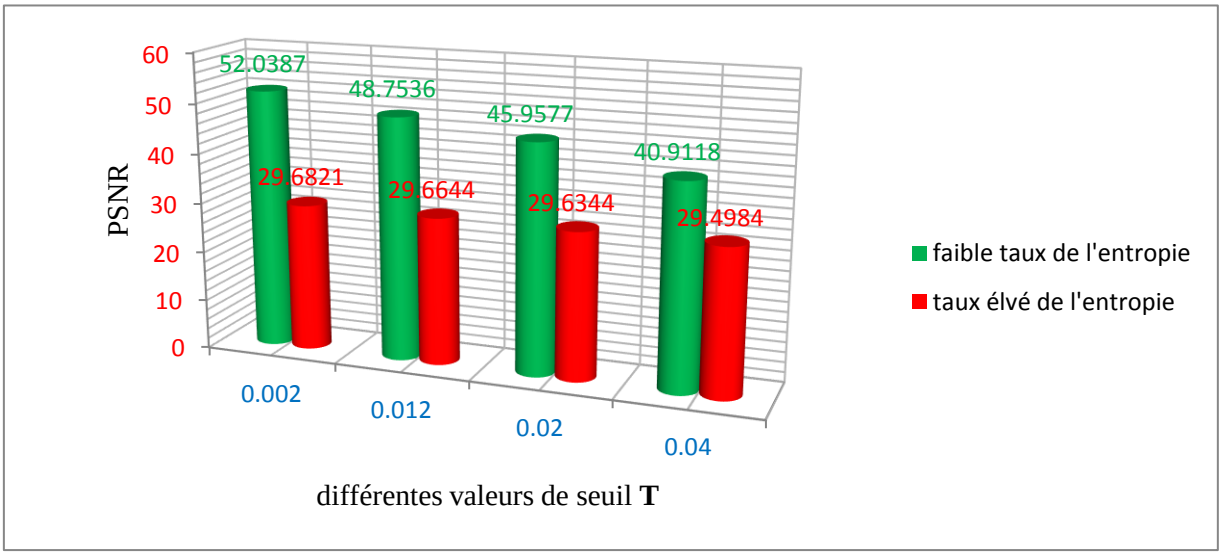


Figure III.35 : Variation de PSNR avec le choix des endroits à faible entropie et les endroits à taux élevé d'entropie.

L'impact est flagrant, les résultats affichés ci-dessus confirment bien que le recours au système visuel humain HVS et grâce aux indices de l'entropie et l'edge entropie pour le choix des endroits d'incrustation à faible entropie pour l'insertion de la marque se montrent comme une bonne opportunité dans le monde de tatouage numérique des images et offre une bonne imperceptibilité contrairement au second choix des endroits à forte valeurs d'entropie

CONCLUSION

L'approche proposée des algorithmes hybrides par la combinaison de deux transformées $DCT - SVD$, la transformée en cosinus discrète et la décomposition en valeurs singulières avec le choix de l'outil d'incrustation basé sur le système visuel humain HVS pour la localisation des zones où on a le faible taux d'information par le calcul des deux indices, l'entropie et de l'edge entropie et à travers les résultats présentés, que ce soit la partie sans attaques où on a bien mis en évidence la bonne imperceptibilité avec plusieurs images tests qui présentaient plusieurs formats, soit la partie test de robustesse vis-à-vis des attaques susceptibles d'altérer la marque avant détection, confirme bien la fiabilité des algorithmes de tatouage hybrides de point de vue imperceptibilité et robustesse. Ce qui met en perspective l'utilisation des algorithmes hybrides pour des schémas de tatouage robustes et imperceptibles.

III.7. SCHEMA D'UN TATOUAGE NUMERIQUE A BASE DE LA DWT ET LA DCT UTILISANT LE GRADIENT DE L'IMAGE

Dans cette seconde partie, nous proposons aussi un autre schéma de tatouage par combinaison de deux transformées. La transformée discrète en ondelettes (DWT) qui permet la décomposition de l'image après analyse multirésolution en sous-bandes au moyen de sous-échantillonnages successifs de l'image pour permettre une isolation raffinée des composantes basses fréquences afin de former un espace d'insertion moins sensible, et la transformée en cosinus discrète (DCT) qui est caractérisée par un effet de séparation des hautes fréquences, des basses fréquences et des moyennes fréquences, donnant ainsi la possibilité d'utiliser une gamme de fréquences incluant des coefficients à fort taux d'énergie. Pour la sélection des lieux adaptés à l'insertion de notre marque et pour assurer un compromis entre l'invisibilité et la robustesse on utilise la douceur de l'image qui est évaluée en fonction du degré de variation des valeurs spatiales de l'image. Dans cette approche, nous utilisons le gradient de l'image comme outil de mesure car il présente une dérivée spatiale qui donne une carte topologique de l'image. Cette étape est importante pour localiser les régions où les perturbations sont intenses et permet également d'évaluer la douceur moyenne de l'image.

III.7.1 Algorithme Proposé

Dans cette section, nous présentons l'algorithme utilisé dans notre approche pour l'insertion et l'extraction de la marque. Cet algorithme traite le tatouage non-aveugle, ce qui nécessite la présence de l'image originale pour l'extraction de la marque.

Comme on a vu ci-dessus, le paramètre gradient de l'image nous sert comme indice efficace de mesure pour déterminer le degré de douceur de l'image, car les valeurs élevées du gradient permettent de bien localiser les zones hautes fréquences qui désignent les régions perturbées de l'image, tandis que les faibles fréquences sont localisées par les faibles valeurs du gradient et qui désignent les régions douces de l'image.

Notre but est de fixer une échelle de mesure qui nous permet de classifier les images selon leurs douceurs et bien sûr, pour mieux adapter les paramètres de notre algorithme aux caractéristiques perceptuels et visuels de l'image, des paramètres liés à la texture (Sharpness) et la finesse des détails d'une image, pour cela on calcule la moyenne du gradient de chaque bloc pour déterminer le degré de douceur local, ensuite on calcule la moyenne totale du gradient de l'image pour déterminer le degré de douceur de l'image. Le rapport entre les deux moyennes calculées, facilite la décision du choix de l'endroit d'incrustation.

III.7.1.1 Procédure d'insertion

1-Lecture de l'image originale.

2-Application de la transformée DWT de Haar niveaux 1 et 2.

3-Calcul de la DCT des blocs de LH_2 et HL_2.

4-Calcul du gradient moyen local de chaque bloc 8x8 de la partie LH_2 et HL_2.

5-Calcul du gradient moyen total des parties LH_2 et HL_2.

6-Seuillage et sélection des blocs lisses, moyennement lisses et des blocs perturbés pour LH_2et HL_2.

7-Division de la marque en deux parties, pour insertion dans LH_2 et dans HL_2.

8- Incrustation dans LH_2 et HL_2.

9- Reconstitution de LH_2 et HL_2 à base de la $iDCT$.

10-Reconstitution aussi de la partie approximation (LL_1) par le biais de la DWT inverse ($iDWT$) niveau 2.

11-Reconstitution de l'image marquée à base de l'iDWT niveau 2.

12-Sauvegarde des clés des endroits d'incrustation de LH_2, HL_2 et l'image tatouée.

III.7.1.2 Procédure d'extraction

1-Lecture des clés des endroits d'incrustation de LH_2 et HL_2

2-Lecture de l'image tatouée et de l'image originale.

3-Application de la DWT niveaux 1 et niveau 2 sur l'image originale et l'image tatouée.

4-Calcul de la DCT des parties LH_2et HL_2 de l'image originale et de l'image tatouée.

5-Extraction des deux parties de la marque incrustées à partir de LH_2 et HL_2 de l'image originale et de l'image tatouée.

6-Retour au domaine spatial pour retrouver la marque incrustée par le biais de $l'iDCT$.

III.7.2 SIMULATION ET TESTS

Pour évaluer les performances du schéma de tatouage proposé, un certain nombre de tests sont réalisés sur deux images de taille égales (512 × 512) et de format bmp, à savoir l'image Clown et l'image Mandrill avec une marque présentée par un logo binaire de la lettre $\boldsymbol{A}$ de taille (32×32) et du même format.

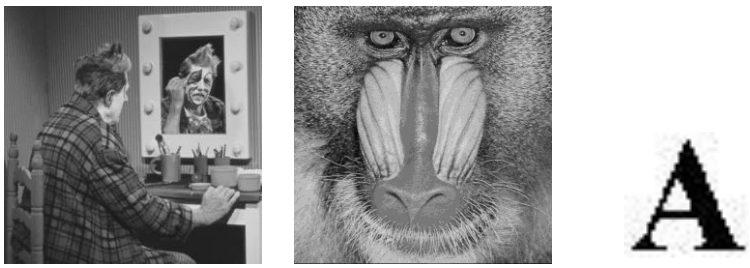
Notre schéma de tatouage est basé sur la combinaison de deux transformées, la DWT et la DCT utilisant le gradient de l'image comme indice pour mesurer et déterminer le degré de douceur de l'image.

Comme toute procédure de tatouage numérique, on doit passer par un banc de tests pour mettre en évidence la fiabilité de notre schéma de tatouage que ce soit en terme d'imperceptibilité qui est la phase d'insertion ou en terme de robustesse qui est liée à la phase d'extraction.

L'approche a été vérifiée par rapport à diverses expériences en termes d'imperceptibilité par visualisation subjective entre les images originales et les images tatouées, et par les valeurs de l'outil de mesure de performance conçu pour cela qui est le$PSNR$. En termes de robustesse, l'approche a été aussi mise en évidence suite aux attaques simulées sur les images tatouées, avant l'extraction de la marque.

III.7.2.1. Tests d'imperceptibilité

Avec un choix judicieux des endroits de l'emplacement des zones d'insertion du watermark on a procédé à l'incrustation de la marque selon la procédure d'insertion citée ci-dessus dans les différentes images test (image Clown et image Mandrill).



(a) (b) (c)

Figure III.36 : (a) Image *clown* (b) image *Mandrill* et (c) logo.

Figure III.37 : Images tatouées

A partir des figures tatouées, on remarque qu'il est difficile de différencier les images originales des images tatouées. L'imperceptibilité de l'image tatouée est excellente avec un rapport signal sur bruit de 43dB pour l'image clown et de 42 dB pour l'image mandrill. Sachant que la valeur minimale acceptable de $PSNR$ pour une imperceptibilité optimisée est de 36dB, nous pouvons donc confirmer que la contrainte d'invisibilité est vérifiée car l'insertion de la marque est effectuée dans les coefficients de fréquence moyenne de la DCT des sous bandes ($LH\ et\ HL$). Pour évaluer la performance de notre méthode et estimer la similarité entre la marque incrusté et celle extraite, nous utilisons la corrélation croisée normalisée (NCC) et l'erreur de débit binaire (BER). Dans la littérature, une valeur de Corrélation Normalisée (NCC) qui est égale ou supérieure à 0,75 indique une marque extraite acceptable et pour le BER la valeur proche de zéro signifie qu'il n'y a pas d'erreur dans la marque extraite. Les résultats obtenus en mesurant $NCC\ et\ BER$ entre la marque insérée et la marque extraite sont très satisfaisants (Tableau III.26).

Tableau III.26 : Evaluation de PSNR, NCC et BER après insertion de l'image Clown et Mandrill.

L'image test	PSNR dB	NCC	BER
Clown	43	1	0,0008
Mandrill	42	1	0,0006

Figure III.38 : Marques extraites sans attaques

III.7.3 Tests vis-à-vis des attaques

Pour le test de la robustesse, les attaques sélectionnées telles que les attaques JPEG, le filtrage (filtre Médian), l'ajout de bruit et les transformations géométriques (Cropping) sont les plus courantes, elles sont utilisées avec divers paramètres pour tester correctement la robustesse de notre approche.

III.7.3.1 Les attaques par ajout de bruit

L'attaque par ajout de bruit dans le monde de l'imagerie et surtout lors d'une transmission quelconque d'un contenu d'images tatouées est inévitable, il se présente comme une dégradation de l'image hôte donc non désirable dans une opération de tatouage, puisqu'il provoque une altération de la qualité visuelle de l'image. A la réception ou à la détection, la récupération de la signature d'une image tatouée bruitée ne sera pas facilement détectable, et pour mettre en évidence notre approche, on a exposé les images tatouées à deux sortes d'attaque par bruitage, le bruit Gaussien et le bruit impulsionnel (Salt & Pepper).

III.7.3.1.1. Les attaque par bruit Gaussien

Le bruit Gaussien est un bruit additif qui consiste à un ajout de bruit successif de valeurs générées aléatoirement à chaque élément de l'image (pixel). Les résultats montrent que pour un bruit gaussien d'une variance de 0,003, la récupération de la marque est moyenne, et pour une variance de 0,001 la récupération est bonne avec très peu d'erreurs de détection.

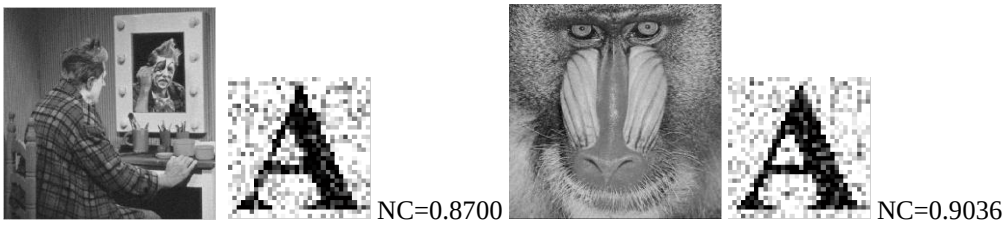


Figure III.39 : Evaluation de la NCC suite à l'attaque par bruit gaussien (variance =0.001)

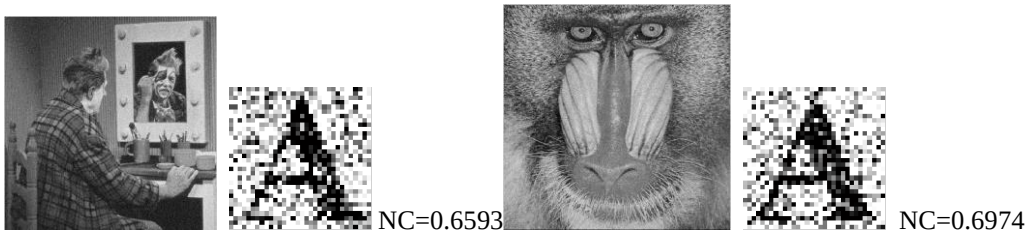


Figure III.40 : Evaluation de la NCC suite à l'attaque par bruit gaussien (variance =0.003).

III.7.3.1.2. Les attaque par bruit Salt & Pepper

Le bruit impulsionnel appelé Sal t& Pepper (sel et poivre) transforme aléatoirement plusieurs pixels de l'image en pixels noir ou blanc ou aux valeurs 255 ou 0 (valeurs extrêmes de l'intervalle des niveaux de gris).

On remarque pour l'ajout de bruit Salt & Pepper, la récupération de la marque est très acceptable pour les faibles densités (0,01 0,02) mais moins acceptable pour une densité supérieur à 0,05.

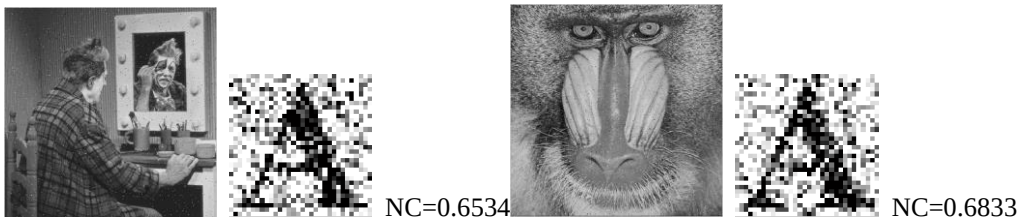


Figure III.41 : Evaluation de la NCC suite à l'attaque par bruit Salt & Pepper (densité=0.01)

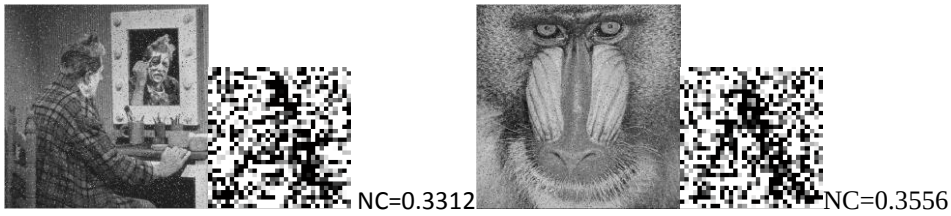


Figure III.42 : Evaluation de la NCC suite à l'attaque par bruit Salt & Pepper (densité=0.05)

III.7.4. Les attaque par JPEG

La compression s'impose comme une étape inévitable pour gérer et optimiser l'utilisation des grands volumes d'informations. L'objectif de la compression d'image est de réduire la quantité d'information et les tailles des fichiers images nécessaires à une bonne représentation visuelle de l'image originale.

Le format $JPEG$ représente l'un des standards les plus utilisés pour la compression des images. Les attaques par compression dans le domaine de tatouage des images numériques, affectent et altèrent sensiblement les images tatouées et généralement la détection de la marque après compression devient très sensible, car les algorithmes de compression ne gardent de l'image tatouée que les composantes essentielles de l'image suite à la réduction de la quantité d'information. On dit souvent qu'un bon schéma de tatouage résiste bien à l'opération de

compression, ce qui est présenté par des valeurs très acceptables par notre approche de la $NCC = 0.9734$ (une valeur qui frôle l'unité$NCC = 1$).

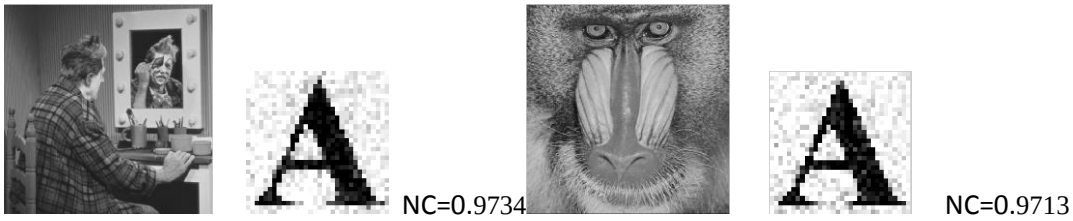


Figure III.43 : Evaluation de la NCC suite à l'attaque JPEG

III.7.5. Les attaque par filtre Median

Malgré leurs importances, les filtres restent des attaques nuisibles au système de tatouage puisqu'ils peuvent altérer ou bien même détruire une signature insérée.

Des méthodes de filtrage, issues du traitement du signal, ont été adaptées au traitement des images numériques comme les filtres non linéaires, pour l'atténuation du bruit impulsionnel et le rehaussement des discontinuités tels que les filtres médians.

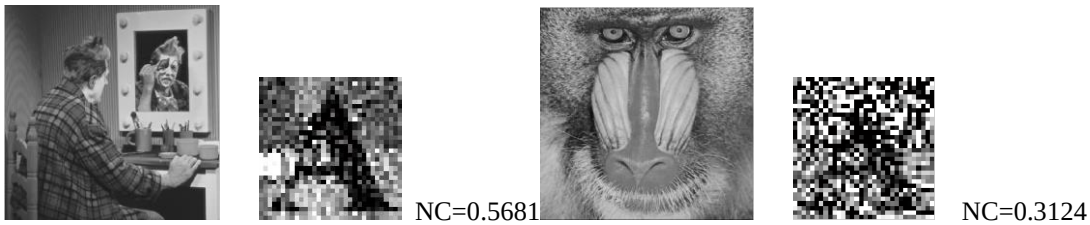
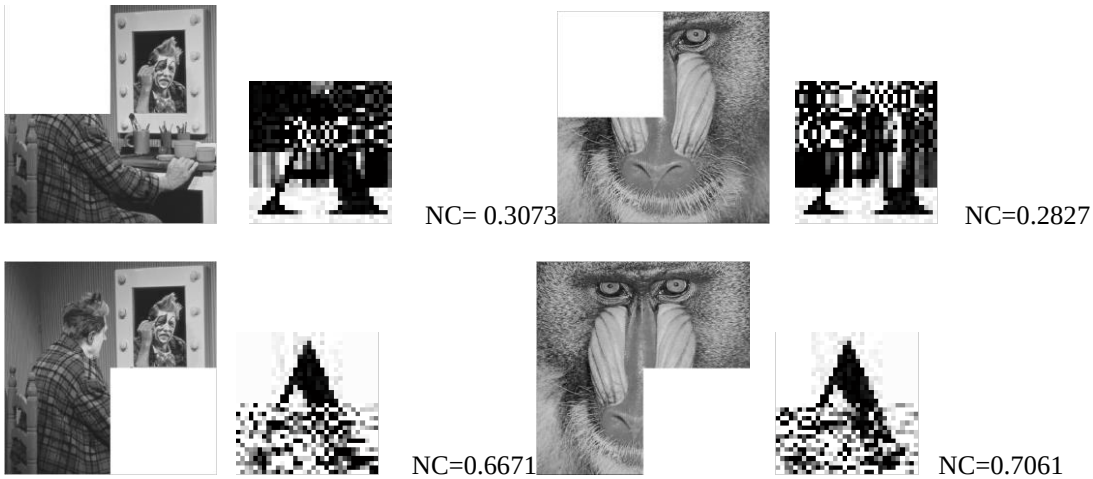


Figure III.44 : Evaluation de la NCC suite à l'attaque par filtrage Médian.

III.7.6. Les attaques géométriques (Cropping)

La marque a été parfaitement récupérée à la suite d'un cropping de 1/4 de l'image tatouée à différents endroits comme il est montré dans les figures ci-dessous :



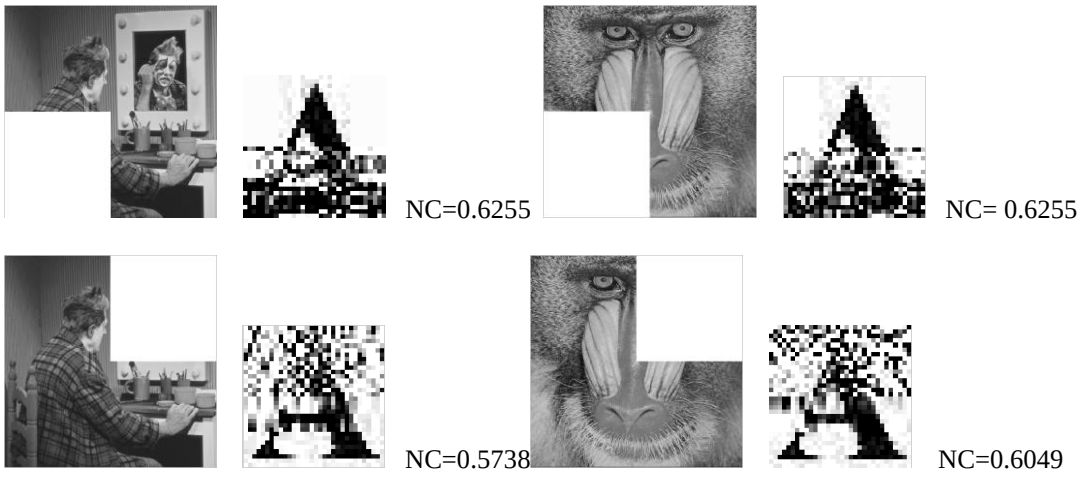
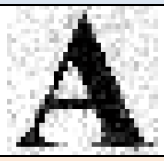
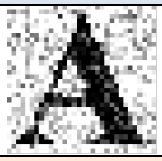
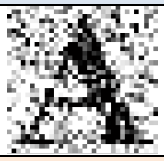


Figure III.45 : Evaluation de la NCC suite à l'attaque par Cropping

III.8. COMPARAISON DE L'APPROCHE Avec D'AUTRES TRAVAUX

Par rapport à quelques travaux précédents, l'approche proposée donne des résultats satisfaisants que de nombreux algorithmes, que ce soit pour l'imperceptibilité lors de l'insertion ou pour la robustesse vis-à-vis des attaques lors de l'extraction, le tableau III.27 montre une comparaison de notre approche avec celle de Patel[76], (D. Patel et al, 2011) .

Tableau III.27 : Comparaison de la NCC de notre approche avec les résultats publiés dans la référence (D. Patel et al, 2011) "Robust Image Watermarking Based on Average and Significant Difference" vis-à-vis des différentes attaques.

Notre Méthode	JPEG 60%	Bruit Gaussien	Bruit Salt & Pepper
N C	0.97	0.87	0.65
			
Méthode D. Patel	JPEG 60%	Bruit Gaussien	Bruit Salt & Pepper
N C	0.96	0.54	0.77
			

En plus, de la première comparaison nous avons aussi comparé le schéma de la méthode proposée avec la référence [77] (E.Li et al 2006). Les résultats sont présentés dans le tableau III.28. Où nous pouvons voir que la méthode proposée a réalisé une bonne imperceptibilité et une plus grande robustesse vis-à-vis de plusieurs attaques.

Tableau III.28 : Comparaison de la NCC de notre approche avec les résultats publiés dans la référence (E. Li et al, 2006) vis-à-vis plusieurs attaques.

Différentes Attaques	**Correlation Normalisé NCC**	
	(E.Li et al 2006) PSNR=40.6dB	Notre Méthode PSNR=43dB
Cropping 1/4	0.61	0.66
Filtre Médian	0.35	0.56
JPEG	0.78	0.97
Bruit Gaussien	/	0.87

CONCLUSION

Les résultats de l'approche proposée par la combinaison de deux transformées, la transformée discrète en ondelettes (DWT) et la transformée discrète en cosinus (DCT), en utilisant le gradient d'image comme outil de mesure donnant une carte topologique de l'image, a été très efficace pour localiser les régions où les perturbations sont intenses ce qui a permis une bonne incrustation (imperceptibilité) et une robustesse à notre watermarking. Les résultats ont été exposés de manière à permettre un jugement direct, subjectif ou objectif, et à évaluer la qualité de l'image tatouée et de la marque extraite par les métriques d'évaluation, le $PSNR$ pour l'incrustation et la corrélation normalisée NCC pour la marque extraite. On peut conclure que ce soit pour l'imperceptibilité ou pour la robustesse que les systèmes de tatouage numérique qui utilisent des algorithmes hybrides approuvent plus de fiabilité.

Chapitre VI

Tatouage des Images Couleurs par la Transformée Paramétrique Orthogonale Reciproque ROP

INTRODUCTION

La manipulation de l'image numérique prend de l'ampleur de plus en plus sur les réseaux de communication suite à l'intérêt considérable qu'elle éprouve et suite au taux d'information qu'elle peut contenir ou qu'elle peut délivrer. La protection numérique des images devient importante pour de nombreuses raisons telles que la confidentialité, l'authenticité et l'intégrité. Actuellement, la façon la plus répandue pour résoudre le problème de la confidentialité et du copyright des images est le tatouage numérique des images appelé aussi watermarking, qui se fait par l'association des informations supplémentaires à un contenu numérique tel que des images ou des vidéos.

Par exemple, un avis de droit d'auteur peut être associé à une image pour identifier le propriétaire légal, un numéro de série peut être associé à une vidéo pour identifier un utilisateur légitime, ou un identifiant peut être associé à une propriété intellectuelle. Le tatouage numérique s'installe comme la méthode appropriée pour associer cette information supplémentaire, comme des indices ou des signatures, qui sont insérés imperceptiblement dans un contenu numérique, qui fera le rôle d'une couverture (document hôte, image de couverture….).

Le tatouage numérique n'est efficace que s'il résiste aux divers traitements de l'image, comme la compression, le filtrage, le redimensionnement, la copie, le scannage, l'ajout de bruit, le changement de contraste etc.

Dans ce chapitre, on propose une méthode de tatouage des images couleurs par l'exploitation de la composante luminance Y (intensité lumineuse) de l'image couleur issue de l'espace couleur Luminance/Chrominance bleue/Chrominance rouge ($YCbCr$).

L'insertion de la marque se fait dans le plan qui compose la partie luminance Y sans appel aux deux autres plans de la chrominance bleue et la chrominance rouge ce qui donne un schéma d'insertion peu encombrant avec un temps de calcul très réduit, bien sûr l'image finale est obtenue par synthèse additive des trois composantes (luminance, chrominance bleu et chrominance rouge $YCbCr$) .

La méthode développée se base sur les transformées discrètes paramétriques orthogonales. Cette approche propose une technique de tatouage basée sur la paramétrisation de la transformée de Hadamard dite ROP.

Les paramètres indépendants d'une transformée sont très utiles dans la caractérisation des signaux et peuvent être également utilisés comme une clé secrète supplémentaire pour des applications telles que le tatouage et le cryptage.

Le tatouage par blocs tout en exploitant les paramètres indépendants de la transformées ROP offre une simplicité remarquable de calcul et un nombre de paramètres assez important pour servir

dans la phase de détection qui sera presque la phase de décryptage et d'extraction qu'on peut appelé crypto-watermarking.

Dans le chapitre précédent, nous avons présenté quelques transformées telles que la transformée de Walsh-Hadamard, la transformée de Hadamard et la transformée paramétrique réciproque-orthogonale ROP. Dans ce chapitre on va exposer quelques résultats suite à l'application de la méthode du tatouage des images fixes par la transformation paramétrique orthogonale réciproque ROP, nous traitons également les performances de notre approche comme l'imperceptibilité et la robustesse du tatouage vis à vis des attaques intentionnelles et non intentionnelles .

IV.1. APPROCHE DE TATOUAGE PROPOSEE PAR LA TRANSFORMEE ROP

Nous allons utiliser dans ces tests une image couleur originale Lena de taille $(512x512)$ et de format bitmap (bmp), que nous allons tatouer avec une marque1 (Logo de l'université Ferhat Abbas Sétif1) et une autre marque2 (Logo de l'université Mohamed Boudiaf M'sila) qui sont de la même taille et du même format que l'image hôte Lena $(512x512).bmp$.

Figure IV.1 : image hôte (Lena) et les deux marques (univ Setif1 et univ M'sila)

IV.2. ALGORITHME PROPOSE

IV.2.1. Phase d'insertion

1. Charger l'image couleur originale I et la marque à insérer W.

2. Convertir l'image RGB en YUV et prendre la matrice de luminance Y concernée par le marquage.

3. Calculer la transformée ROP de la luminance Y utilisant la méthode par blocs choisie $(8x8)$, $(16x16)$ ou $(32x32)$.

4. Calculer la transformée ROP de la marque W utilisant la méthode par blocs choisie $(8x8), (16x16)$ ou $(32x32)$.

5. Fixer la force du tatouage **α**.

6. Appliquer la procédure du tatouage additif.

7. Calculer la transformée inverse $iROP$ par blocs de $(8x8)$, $(16x16)$ ou $(32x32)$.

8. Reconstruire les couleurs de base RGB (image couleur tatouée)

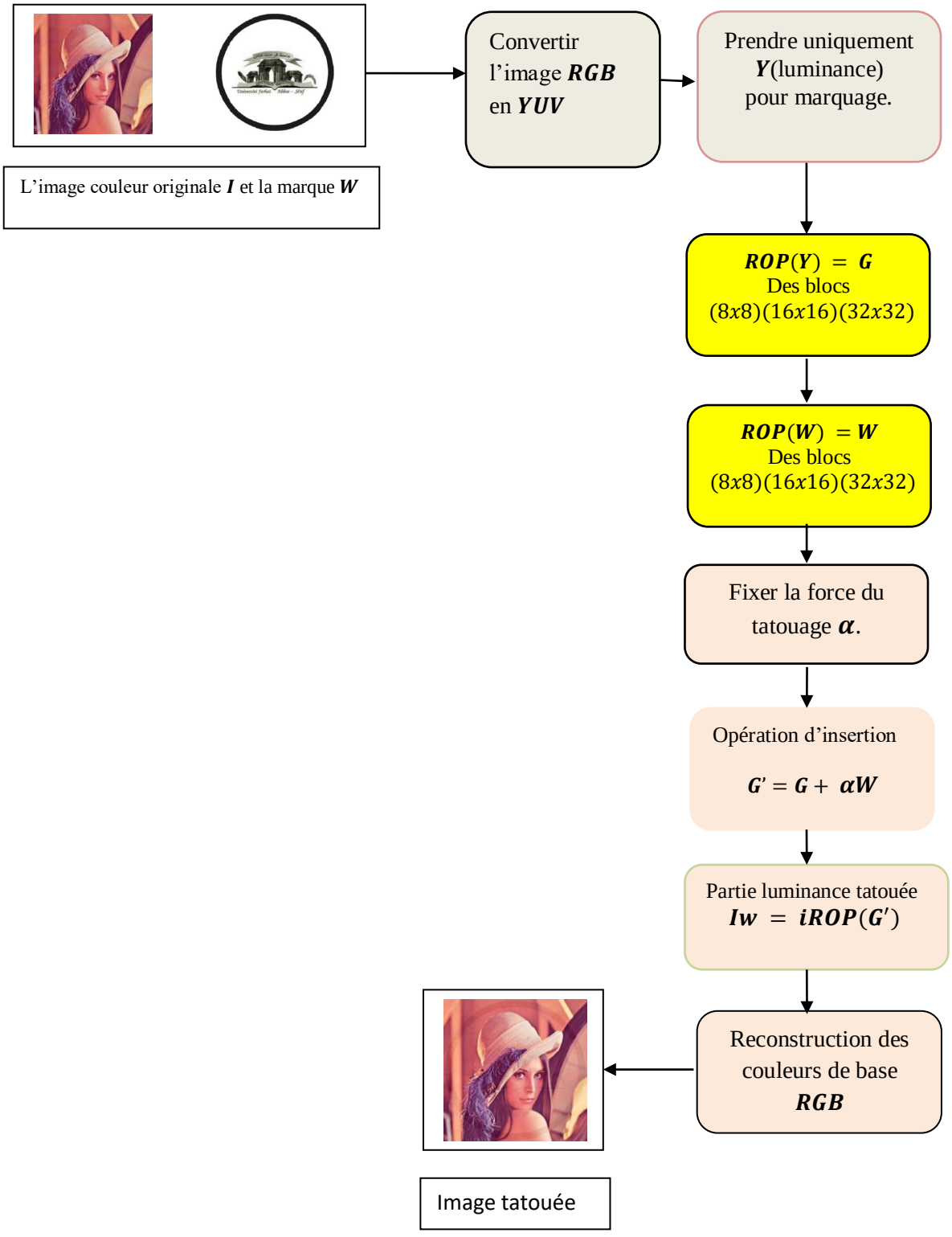


Figure IV-2 : Algorithme d'insertion de la marque.

IV.2.2. Phase d'extraction

1. Charger l'image couleur originale I et l'image tatouée.

2. Convertir l'image originale et l'image tatouée RGB en YUV et prendre leurs matrices de luminance Y et Y' concernées par l'extraction.

3. Calculer les transformées ROP de la luminance Y , la luminance Y' et la transformée $ROP(W)$.

4. Fixer la force de tatouage $\boldsymbol{\alpha}$ (la même valeur que celle de l'insertion).

5. Extraire la marque dans le domaine des transformées, et calculer sa transformée inverse .

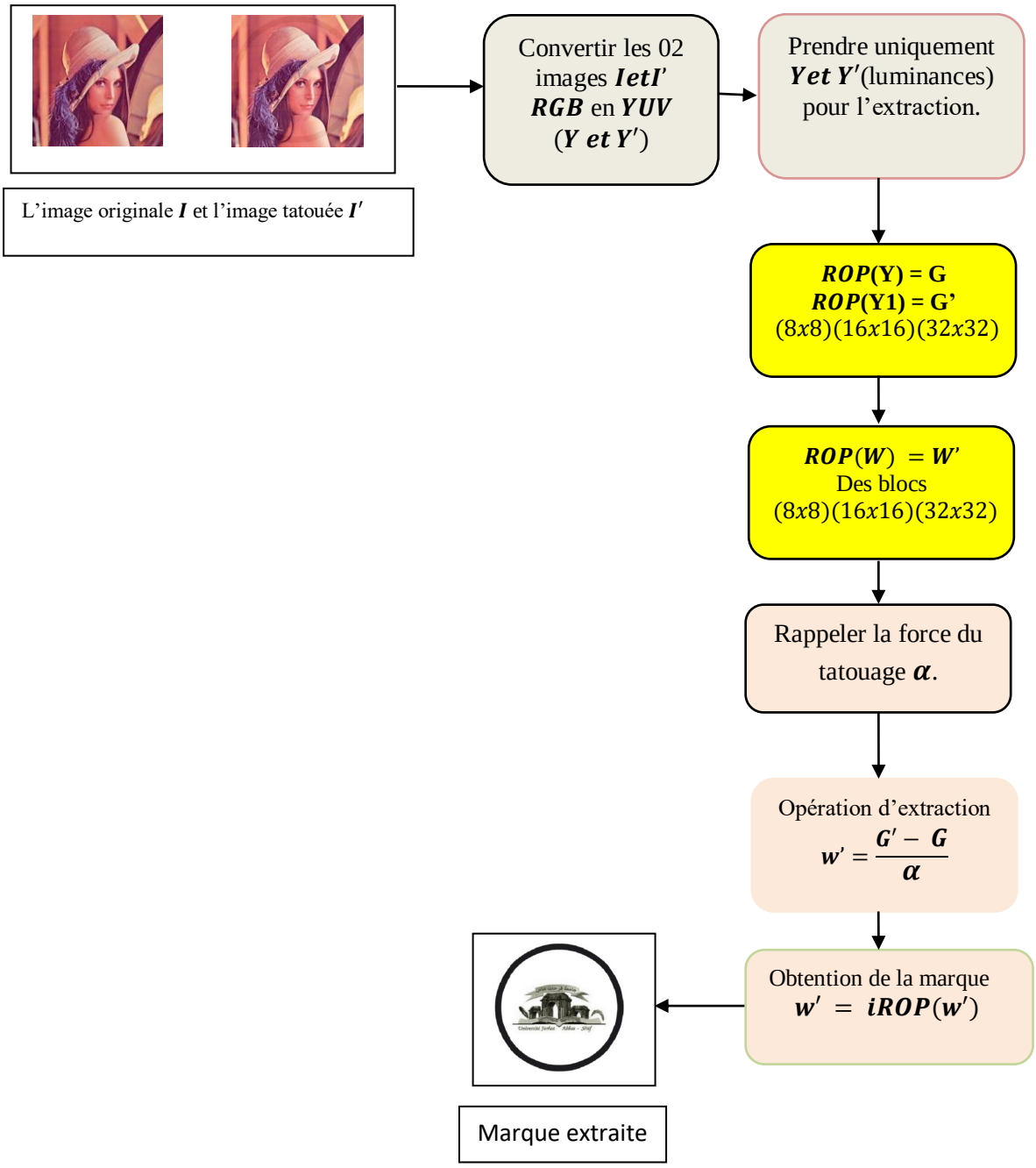


Figure IV-3 : Algorithme d'extraction de la marque.

IV.3. TEST DE L'IMPERCEPTIBILITE

IV.3.1. Insertion de la marque 1 pour des blocs de $(8x8)$

Image originale	**Image tatouée**		
			
PSNR dB	**PSNR=46.2183** **α =0.005**	**PSNR=25.7243** **α =0.05**	**PSNR= 7.7691** **α =0. 5**

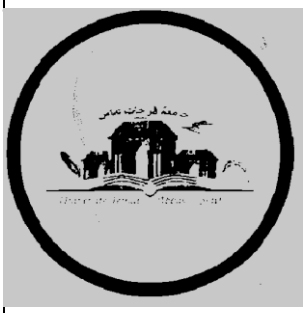
Marque originale	**Marque extraite**		
			
NCC	**NCC=0.9409** **α =0.005**	**NCC=0.9975** **α =0.05**	**NCC= 0.7948** **α =0. 5**

Figure IV. 4 : images tatouées et marques extraites avec α =0.005, α =0.05 et α =0.5 pour (8x8)

IV.3.2. Insertion de la marque 2 pour des blocs de $(8x8)$

Image originale	Image tatouée		
			
PSNR dB	**PSNR=45.5836** **α =0.005**	**PSNR=25.3764** **α =0.05**	**PSNR= 7.2376** **α =0.5**

Marque originale	Marque extraite		
			
NCC	**NCC=0.3697** **α =0.005**	**NCC= 0.9915** **α =0.05**	**NCC= 0.5431** **α =0. 5**

Figure IV. 5 : images tatouées et marques extraites avec α =**0.005, α =0.05** et **α =0. 5,** pour (8x8).

IV.3.3. Insertion de la marque 2 pour des blocs de $(32x32)$.

On a choisis une autre image "F16.bmp" couleur avec la deuxième marque (Logo univ M'sila) pour des blocs $(32x32)$ .Voici les résultats trouvés

Image originale	**Image tatouée**		
			
PSNR dB	**PSNR=45.8071** **α =0.005**	**PSNR=25.3751** **α =0.05**	**PSNR= 9.6319** **α =0.5**

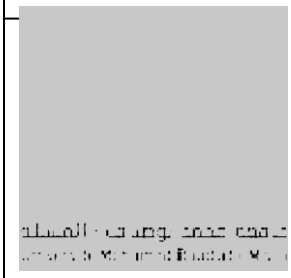
Marque originale	**Marque extraite**		
			
NCC	**NCC=0.3752** **α =0.005**	**NCC= 0.9968** **α =0.05**	**NCC= 0.1241** **α =0.5**

Figure IV. 6 : images tatouées et marques extraites avec α =**0.005, α =0.05** et **α =0. 5 pour (32x32)**

Interprétation des résultats

D'autres tests sur la même image "Lena.bmp" couleur avec la marque1, pour garder le même environnement des tests de l'approche avec la transformée $\boldsymbol{ROP16}$ et $\boldsymbol{ROP32}$, ont menés aux résultats récapitulés dans le tableau ci-dessous (Tableau IV.1)

Tableau IV.1 : Evaluation de PSNR et de NCC de la ROP8, la ROP16 et la ROP32 avec **α =0.005, α =0.05 et α =0. 5** pour l'image Lena avec la marque1.

	Alpha	**α =0.005**	**α =0.05**	**α =0. 5**
ROP* 8** ***Image Lena	PSNR dB	46.2185	25.7246	7.7720
	NCC	0.9410	0.9975	0.7948
Rop* 16** ***Image Lena	PSNR dB	46.2184	25.7251	7.7729
	NCC	0.9410	0.9975	0.7949
ROP* 32** ***Image Lena	PSNR dB	46.2186	25.7250	7.7734
	NCC	0.9410	0.9975	0.7949

Tableau IV.2 : Evaluation de PSNR et de NCC de la ROP8, et laROP32 avec **α =0.005, α =0.05 et α =0. 5** pour l'image Lena et l'image F16 avec la marque 2.

	Alpha	**α =0.005**	**α =0.05**	**α =0. 5**
ROP* 8** ***Image Lena	PSNR dB	45.5836	25.3764	7.2376
	NCC	0.3697	0.9915	0.5431
ROP* 32** ***Image F16	PSNR dB	45.8071	25.3751	9.6319
	NCC	0.3752	0.9968	0.2141

Nous remarquons d'après les résultats mentionnés dans les deux tableaux, que le choix de la valeur de la force de tatouage α influe directement sur la valeur du $PSNR$ (entre l'image originale et l'image tatouée) et sur le NCC (entre la marque originale et la marque extraite). Et par conséquent, on détient que la valeur la plus adaptée pour un tatouage adaptatif non visible est pour une valeur de $\alpha = 0.005$ où on a une bonne imperceptibilité de l'image tatouée avec une valeur du métrique $PSNR = 46.2186\ dB$. Pour l'extraction de la marque et d'une manière subjective de point de vue similarité entre la marque insérée et la marque extraite, on remarque que la valeur la plus adaptée pour la force de tatouage est α=0.05 pour une valeur de la corrélation $NC = 0.9975$, pour l'ensemble de la méthode par blocs choisie $(8x8, 16x16, 32x32)$

IV.4. TESTS VIS-A-VIS DES ATTAQUES

La troisième approche, qui se base sur la paramétrisation, va cibler beaucoup plus les attaques intentionnelles, que les attaques non-intentionnelles pour mettre en exergue l'efficacité des paramètres indépendants de la transformée réciproque orthogonale ROP qui sont au nombre de $((N/2) - 1))$, et qui vont être utilisés comme des clés secrètes lors de la détection de la marque, ce qui donnera plus de sécurité pour une extraction assurée uniquement pour le récepteur qui détient la totalité des clés avec lesquels on a sécurisé l'envoi.

Ensuite, on passe aux attaques non intentionnelles comme la compression JPEG, la rotation, l'ajout de bruit et le filtrage, qui résident toujours dans les bancs de tests subis par les schémas de tatouage.

IV.4.1.Attaques intentionnelles

On présente dans un tableau la marque originale et la marque extraite avec le nombre des clés que détient le récupérateur de la marque pour l'extraction, sachant que ce nombre change avec le changement du nombre des blocs $((N/2)-1)$. La présentation de la marque extraite, c'est pour un jugement subjectif qui s'avère indispensable pour la mise en évidence de la similarité ou la non similarité des deux marques.

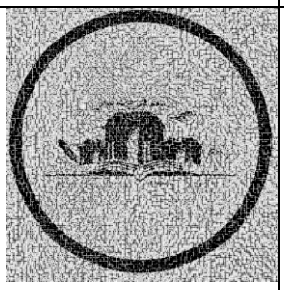
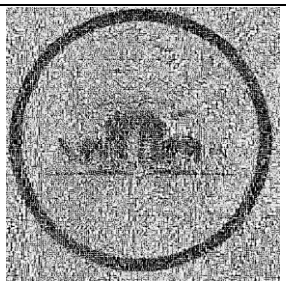
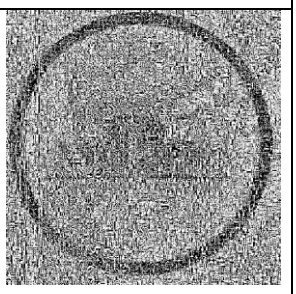
Marque originale	**Marque extraite (force de tatouage α =0.005) Clés erronées /parmi 3 clés (ROP8)**		
	1/3 clés	**2/3 clés**	**3/3 clés**
			
NCC	**0.5146**	**0.2948**	**0.1776**

Figure IV. 7 : marques extraites avec α **=0.005, pour ROP (8x8).**

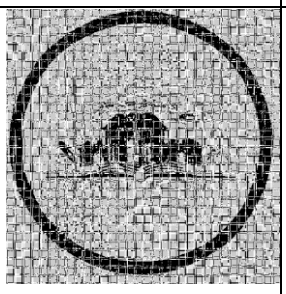
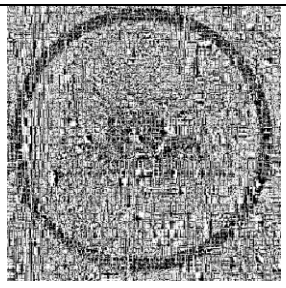
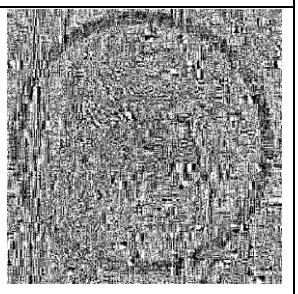
Marque originale	**Marque extraite (force de tatouage α =0.005) Clés erronées /parmi 7 clés (ROP16)**		
	2/7 clés	**5/7 clés**	**7/7 clés**
			
NCC	**0.4827**	**0.1840**	**0.0993**

Figure IV. 8 : marques extraites avec α **=0.005 pour ROP (16x16)**

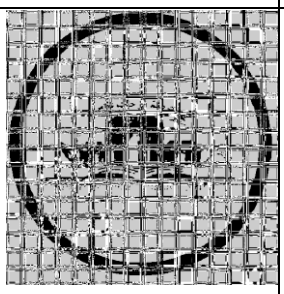
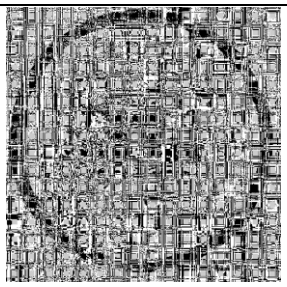
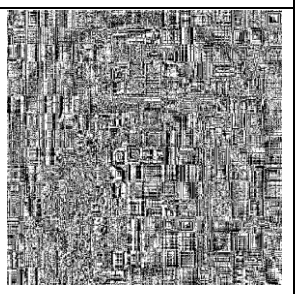
Marque originale	Marque extraite(force de tatouage α =0.005) Clés erronées /parmi 15 clés (ROP32)		
	5/15 clés	10/15 clés	15/15 clés
			
NCC	0.3890	0.1664	0.0739

Figure IV. 9 : marques extraites avec α **=0.005, pour ROP (32x32).**

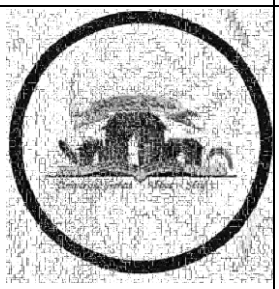
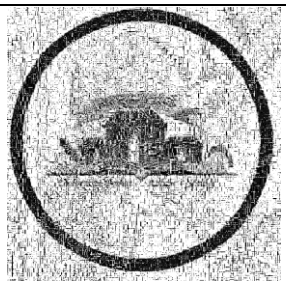
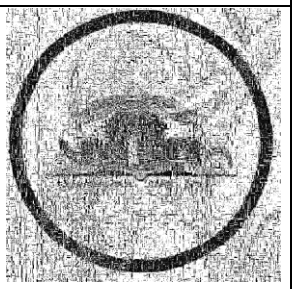
Marque originale	Marque extraite (force de tatouage α =0.05) Clés erronées /parmi 3 clés (ROP8)		
	1/3 clés	2/3 clés	3/3 clés
			
NCC	0.7377	0.5823	0.4870

Figure IV. 10 : marques extraites avec **α =0.05 pour ROP (8x8).**

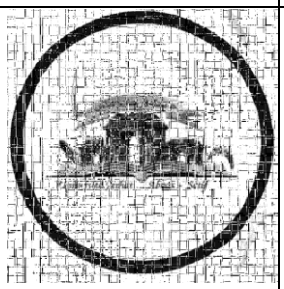
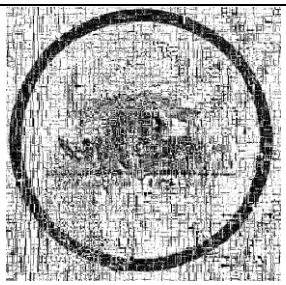
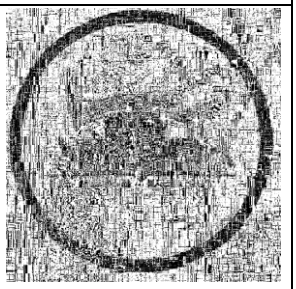
Marque originale	Marque extraite (force de tatouage α =0.05) Clés erronées /parmi 7 clés (ROP 16)		
	2/7 clés	5/7 clés	7/7 clés
			
NCC	0.6803	0.4437	0.357

Figure IV. 11 : marques extraites avec **α =0.05 pour ROP(16x16)**

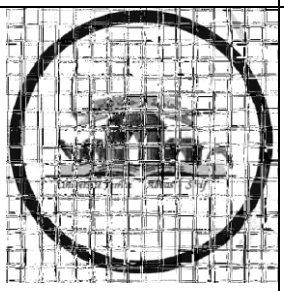
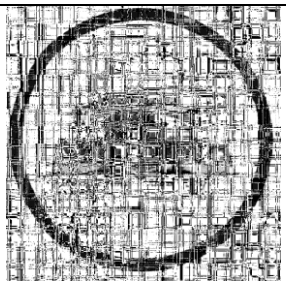
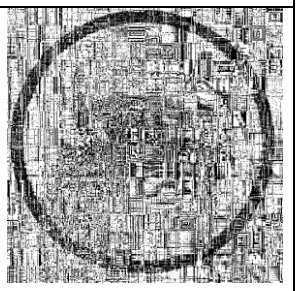
Marque originale	Marque extraite (force de tatouage α =0.05) Clés erronées /parmi 15 clés (ROP32)		
	5/15 clés	10/15 clés	15/15 clés
			
NCC	0.5907	0.3862	0.2741

Figure IV. 12 : marques extraites avec **α =0.05 pour ROP(32x32).**

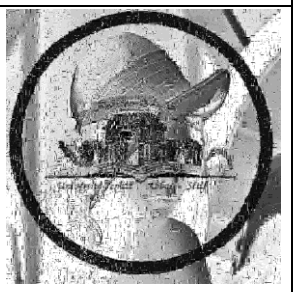
Marque originale	Marque extraite (force de tatouage α =0. 5) Clés erronées /parmi 3 clés (ROP8)		
	1/3 clés	2/3 clés	3/3 clés
			
NCC	0.7216	0.6682	0.6330

Figure IV. 13 : marques extraites avec **α =0. 5 pour ROP(8x8).**

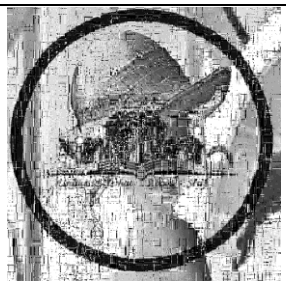
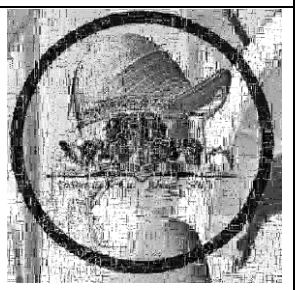
Marque originale	Marque extraite (force de tatouage α =0. 5) Clés erronées /parmi 7 clés (ROP 16)		
	2/7 clés	5/7 clés	7/7 clés
			
NCC	0.6901	0.5897	0.546

Figure IV. 14 : marques extraites avec **α =0. 5 pour (16X16).**

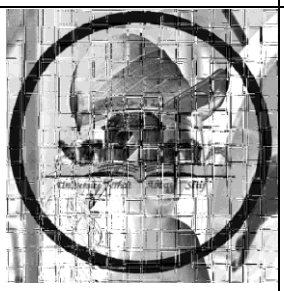
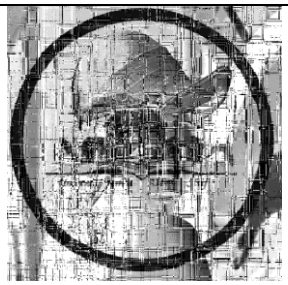
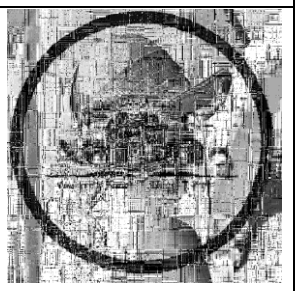
Marque originale	Marque extraite (force de tatouage α =0. 5) Clés erronées /parmi 15 clés(ROP32)		
	5/15 clés	10/15 clés	15/15 clés
			
NCC	0.6408	0.538	0.4883

Figure IV. 15 : marques extraites avec **α =0. 5 pour ROP (32x32).**

Interprétation des résultats

Les simulations sont faites de façon qu'on se mette dans le cas où l'attaquant ne détient que quelques clés de la totalité disponible pour détecter la marque insérée dans l'image hôte, donc c'est une détection qui n'est pas synchronisée avec la partie émettrice , vu que l'attaque intentionnelle ne détient pas la totalité des clés , c'est l'avantage de travailler en plusieurs blocs avec plusieurs clés erronées où on prétend que l'attaquant détient soit le 1/3 des clés, le 2/3 des clés ou la totalité des clés. Pour différentes valeurs de la force de tatouage $\boldsymbol{\alpha}$ et en fonction aussi du nombre des blocs utilisés $(8x8, 16x16, 32x32)$. On remarque que l'attaquant commence à s'affronter aux difficultés de détection pour extraire la marque, une fois qu'on augmente le nombre des blocs utilisés N, ce qui augmentera le nombre des paramètres (nombre de paramètres $((N/2 - 1))$ et par évidence le nombre des clés. A travers les résultats récapitulés dans les tableaux ci-dessus nous constatons que la marque extraite est complètement embrouillée bien que l'attaquant détient le 2/3 des clés et les valeurs du métrique de la corrélation normalisé NCC sont complètement dégradées, cela confirme et consolide l'intérêt de la paramétrisation des transformations pour le développement des méthodes de tatouage numérique des images et notamment pour la sécurité lors de la détection et l'extraction des marques insérées et des signatures qui accompagnent n'importe quel document pour le copy right et l'authenticité

IV.4.2. Attaque par compression $JPEG$

Voici les résultats des marques extraites suite à des attaques de compression $JPEG$ pour des blocs (8x8) avec une force de tatouage α =0.05et avec des taux de compression qui varient de 50% à90%

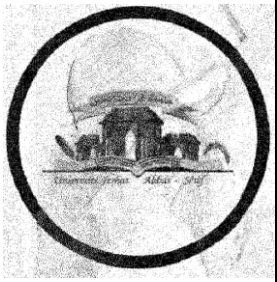
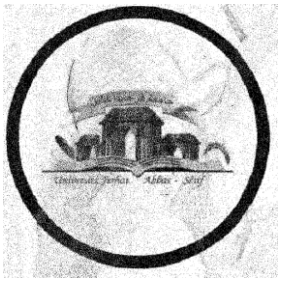
Marque originale	Marque extraite		
	50%	60%	90%
			
NCC	0.8370	0.8560	0.9827

Figure IV. 16 : marques extraites avec α =0. 05 pour ROP (8x8) vis-à-vis des attaques JPEG.

Voici les résultats des marques extraites suite à des attaques de compression JPEG pour des blocs (32x32) avec une force de tatouage α =0.05, pour la deuxième marque (Logo Univ M'sila) avec des taux de compression qui varient entre 50% et 90%.

Marque originale	Marque extraite		
	50%	60%	90%
			
NCC	0.6096	0.6366	0.9456

Figure IV. 17 : marques extraites avec α =0. 05 pour ROP (32x32) vis-à-vis des attaques JPEG

Interprétation des résultats

La compression des images s'impose comme une étape inévitable pour gérer et optimiser l'utilisation des grandes tailles des images dans le monde des traitements des images. L'objectif de la compression d'image est de réduire la quantité d'information et la taille des fichiers images nécessaires à une bonne représentation visuelle de l'image originale.

Le format $JPEG$ représente l'un des standards les plus utilisés pour la compression des images. Les attaques par compression dans le domaine de tatouage des images numériques, affectent et altèrent sensiblement les images tatouées et généralement la détection de la marque après compression devient très sensible car les algorithmes de compression ne gardent de l'image tatouée que les composantes essentielles de l'image suite à la réduction de la quantité d'information.

La compression $JPEG$, est généralement considérée comme une attaque dure contre les systèmes de tatouage d'image, c'est pour cela qu'un bon résultat suite à une attaque par compression déclare la robustesse du système conçu pour le tatouge. Les résultats de notre approche dévoilent une bonne robustesse vis-à-vis des attaques de compression avec une similarité entre les deux marques (incrustée et extraite), la mesure du degré de fiabilité par la corrélation normalisée croisée (Normalized Cross-Correlation NCC) a donné un NCC de l'ordre de l'unité ($NC = 0.9827$)

IV.4.3. Attaque par rotation

Voici les résultats des marques extraites suite à des attaques par la transformation géométrique rotation pour des blocs (8x8) avec une force de tatouage α =0.05,avec un angle $\boldsymbol{\theta}$ variable.

Marque originale	**Marque extraite**		
	$\boldsymbol{\theta = 15°}$	$\boldsymbol{\theta = 45°}$	$\boldsymbol{\theta = 130°}$
			
NCC	**0.9989**	**0.9992**	**0.9993**

Figure IV. 18 : marques extraites avec α =0. 05 pour ROP ($8x8$) vis-à-vis des attaques par rotation.

Voici les résultats des marques extraites suite à des attaques par la transformation géométrique rotation pour des blocs (32x32) avec une force de tatouage α =0.05 , avec un angle $\boldsymbol{\theta}$ variable.

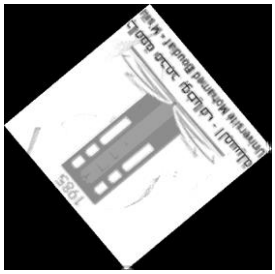
Marque originale	**Marque extraite**		
	$\boldsymbol{\theta = 15°}$	$\boldsymbol{\theta = 45°}$	$\boldsymbol{\theta = 130°}$
			
NCC	**0.9960**	**0.9981**	**0.9988**

Figure IV. 19 : marques extraites avec α =0. 05 pour ROP (32x32) vis-à-vis des attaques par rotation.

Interprétation des resultats

Les transformations géométriques ont pour but la modification de la position des informations contenues dans l'image, on cite quelques opérations géométriques de base comme la translation, la rotation, le recadrement et la mise à l'échelle (étirement vertical ou horizontal de l'image).

Afin d'évaluer la robustesse de notre méthode contre l'attaque géométrique on a choisis l'attaque par la transformation géométrique rotation de l'image tatouée avec divers angles θ(15°, 45°, 130°). Les valeurs de NCC s'averent très acceptable par rapport à la valeur normalisée de la corrélation ($NC = 0.9990$), ce qui qualifie que la méthode proposée de tatouage est robuste vis-à-vis des attaques de rotation et cela pour plusieurs valeurs des forces de tatouage $\boldsymbol{\alpha}$ et aussi pour des blocs de $(16x16)$ et $(32x32)$.

IV.4.4. Attaque par ajout de bruit

Le bruit se présente comme une altération de l'image originale donc non désirable, puisqu'il provoque une dégradation de la qualité visuelle de l'image. A la réception, la récupération de la marque d'une image tatouée bruitée ne sera pas aisément détectable.

Dans cette approche, on a fait recours à deux types de bruit, un bruit multiplicatif et un bruit additif. Le bruit multiplicatif comme le bruit impulsionnel appelé aussi "Salt & Pepper" (sel et poivre) qui transforme aléatoirement plusieurs pixels de l'image en pixels noir ou blanc ou aux

valeurs 255 ou 0, le bruit additif comme le bruit gaussien qui consiste à un ajout de bruit successif de valeurs générées aléatoirement à chaque élément de l'image (pixel).

IV.4.4.1. Attaque par ajout de bruit "Salt & Peppers"

On a voulu illustré l'impact du rajout de bruit sur l'image tatouée pour voir l'altération de l'image suite aux changements des densités du bruit appliqué, ensuite on passe à l'extraction de la marque sous l'effet de l'attaque ajout de bruit.

Image tatouée	**Image tatouée bruitée (**Salt & Peppers)		
	Densité=0.02	**Densité=0.08**	**Densité=0.5**
			
PSNR	**20.5780**	**15.7187**	**8.1182**
NCC	**0.9900**	**0.9643**	**0.7130**

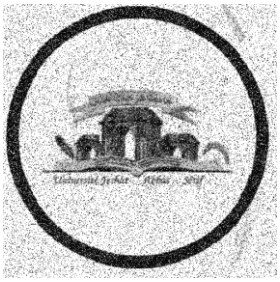
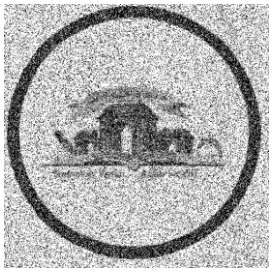
Marque originale	**Marque extraite (Bloc 8x8)Pour α =0.05**		
	Densité=0.02	**Densité=0.08**	**Densité=0.5**
			
NCC	**0.8988**	**0.6786**	**0.4404**

Figure IV. 20 : images tatouées et marques extraites avec α =0. 05 pour ROP (8x8) vis-à-vis des attaques ajout de bruit Salt & Peppers.

IV.4.4.2. Attaque par ajout de bruit Gaussien

Voici les résultats des images tatouées et des marques extraites suite à des attaques par ajout de bruit Gaussien de moyenne nulle et de variance entre (0.003-0.009), pour des blocs (32x32) avec une force de tatouage α =0.05 pour la deuxième marque.

De la même façon on a illustré l'impact du rajout de bruit sur l'image tatouée pour voir l'altération de l'image suite aux changements des variances du bruit appliqué, ensuite on passe à l'extraction de la marque sous l'effet de l'attaque ajout de bruit Gaussien.

Image tatouée	**Image tatouée bruitée (Gaussien)**		
	Var=0.001	**Var=0.003**	**Var=0.009**
			
PSNR	**30.0527**	**25.3509**	**20.6944**

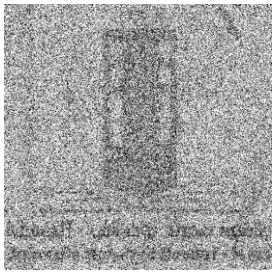
Marque originale	**Marque extraite (Bloc 32x32) Pour α =0.05**		
	Var=0.001	**Var=0.003**	**Var=0.009**
			
NCC	**0.4689**	**0.2636**	**0.1516**

Figure IV. 21 : images tatouées et marques extraites avec α =0. 05 pour ROP (32x32) vis-à-vis des attaques ajout de bruit Gaussien.

Interprétation des resultats

Pour l'attaque sur l'image tatouée par ajout de bruit "Salt & Peppers", on remarque que la récupération de la marque est très bonne pour une densité qui varie entre 0.02 et 0.08 avec des valeurs de la corrélation normalisée proches de la valeur acceptable pour une bonne extraction, qui est de l'ordre de NCC=0.75.

Concernant la deuxième attaque simulée sur l'image tatouée par ajout de bruit Gaussien, on remarque que la récupération de la marque n'est pas très acceptable pour des variances au delà de 0,003 et les valeurs de la corrélation sont inferieurs à 0,75.

IV.4.5. Attaque par filtrage

Des méthodes de filtrage, issues des techniques de traitement du signal, ont été adaptées au traitement des images numériques comme les filtres linéaires et les filtres non linéaires. Les techniques de filtrage linéaire de base permettent de supprimer les effets d'un bruit additif on peut citer les filtres linéaires moyenneur et le filtre gaussien. Les filtres non linéaires sont destinés à l'atténuation du bruit impulsionnel et le rehaussement des discontinuités tels que les filtres médians ou les filtres morphologiques.

IV.4.5.1. Attaque par filtrage Gaussien

Voici les résultats des marques extraites suite à un filtrage Gaussien aves une variété de masque [3 3], [5 5] et [11 11] pour les blocs $(32x32)$ $et\ \alpha = 0{,}05$, pour la marque 1.

Marque originale	**Marque extraite (Bloc 32x32) Pour α =0.05** **Filtrage Gaussien**		
	Masque [3 3]	**Masque [5 5]**	**Masque [11 11]**
			
NCC	**0.9950** **Sigma=0.5**	**0.9941** **Sigma=0.7**	**0.9930** **Sigma=0.9**

Figure IV. 22 : marques extraites avec α =0. 05 pour ROP (32x32) vis-à-vis des attaques par filtrage Gaussien pour la marque 1

Voici les résultats des marques extraites suite à un filtrage Gaussien aves une variété de masque [3 3], [5 5] et [11 11] pour les blocs (32x32) avec une force de tatouage α =0.05, pour la marque2.

Marque originale	**Marque extraite**		
	Masque [3 3]	**Masque [5 5]**	**Masque [11 11]**
			
NCC	**0.9830** **Sigma=0.5**	**0.9816** **Sigma=0.7**	**0.9801** **Sigma=0.9**

Figure IV. 23 : marques extraites avec α =0. 05 pour ROP (32x32) vis-à-vis des attaques par filtrage Gaussien pour la marque 2.

Interprétation des résultats

Pour tester la robustesse de cette approche on a utilisé le filtre gaussien, l'extraction de la marque après attaque a donné de très bons résultats, où on peut conclure suite à la détection par contrôle subjectif de la qualité visuelle de la marque extraite après attaque et par la métrique de corrélation entre la marque extraite et celle insérée qui donne un NCC très acceptable, que notre approche reste robuste contre l'attaque par filtrage.

IV.5. COMPARAISON DE L'APPROCHE Avec D'AUTRES TRAVAUX

La mise en exergue de l'application de la transformation paramétrique orthogonale réciproque ROP dans le domaine de tatouge numérique des images, nous a poussé à faire une comparaison avec un travail existant où ils ont utilisés dans leurs approche la transformée de Hadamard discréte. Ce qui favorise vraiment une comparaison entre les résultats des travaux d'une transformation paramétrique avec une transformation non paramétrique (Transformée de Hadamard).

Donc, pour confirmer l'intérêt de la paramétrisation on a préféré garder le même environnement que celui pris par V. Santhi et al de l'université Vellore-632 014, Tamilnadu, India[78]. On a conservé les mêmes images déjà utilisées avec la transformée de Hadamard où l'image originale

est celle nommée Lena ($512x512.bmp$) et la marque (w) à insérer porte le symbole de l'université VIT (University, Vellore-632 014, Tamilnadu, India) de la même taille et du même format que l'image hôte ($512x512.bmp$).

On a jugé utile l'utilisation des deux outils d'évaluation d'un bon système de tatouage, l'évaluation de la qualité visuelle de la marque extraite après attaque qui engendre une dégradation et une altération qui est une forme subjective ; en plus on a utilisé la mesure objective par la comparaison des valeurs des pixels de la marque originale et celle extraite pour l'évaluation de la similarité entre les deux marques par la métrique de corrélation normalisée NCC

Figure IV.24 : Image Lena (Image originale) et la marque originale

Tableau IV.3 : Simulation des attaques malveillantes d'une ROP 32.

Marque Originale	**Marque Extraite Clés Erronées/Parmis 15 clés**									
	0/15keys	**1/15keys**	**2/15keys**	**3/15keys**	**4/15keys**	**6/15keys**	**9/15keys**	**11/15keys**	**12/15keys**	**15/15keys**
										
NCC	0.9817	0.8739	0.7916	0.5987	0.4387	0.3523	0.2943	0.2789	0.2518	0.2053

On a simulé des attaques malicieuses, sachant que l'attaquant à chaque tentative d'extraction ne détient que quelques clés à la réception pour détecter la marque ciblée.

Les résultats qui s'affichent sur le **Tableau IV.3** confirment bien l'éfficacité de l'utilisation des paramètres comme des clés secrètes lors de la détection de la marque, donc uniquement la bonne synchronisation entre l'émetteur et le récepteur qui détiennent tous les deux les bonnes clés, arrivent à détecter la marque complète similaire à la marque originale insérée.

CONCLUSION

Nous avons présenté une nouvelle approche sur la méthode du tatouage des images fixes par les transformées paramétriques réciproques orthogonales ROP, les tests appliqués confirment bien la robustesse ainsi que la fiabilité du schéma de tatouage numérique proposé. Le marquage a été validée à l'aide des attaques malicieuses, où nous avons montré que la paramétrisation a amélioré nettement la robustesse par la création de clés secrètes qui sont au même nombre que celui des paramètres indépendants de la transformées $((N/2)-1)$), donc même si l'attaquant détient la totalité des paramètres, il ne pourra détériorer la marque insérée. Quant aux attaques non malicieuses (compression $JPEG$, rotation, ajout de bruit et filtrage), les résultats obtenus confirment bien l'imperceptibilité et la robustesse du tatouage par les transformées paramétriques.

Conclusion générale

CONCLUSION GENERALE

Le grand potentiel d'information que peut délivrer une image, éprouve un intérêt majeur dans le domaine des réseaux de télécommunication et surtout lorsqu'il s'agit d'image comportant des solutions ou des confidentialités comme l'imagerie satellitaire, l'imagerie militaire, l'imagerie commerciale, l'imagerie médicale et l'imagerie confidentielle comme les réseaux de communication entre états , ce qui a accentué réellement les problèmes de confidentialité dans la manipulation et le transfert des images surtout avec la multiplication des transferts sur les réseaux et sur les supports de données numériques, ce qui a imposé un nouveau challenge pour la protection des propriétés intellectuelles dans sa norme universelle.

Pour contourner ces problèmes, une nouvelle technique a été développée pour contribuer à protéger et sécuriser ces données numériques, c'est le tatouage numérique.
Le tatouage numérique des images appelé aussi "watermarking" et vu les approches qui s'articulent autour de ce nouveau remède dans le monde de la protection des droits d'auteur et des contenus multimédias, il se propose comme une bonne solution pour remédier aux problèmes de l'authentification et la protection de la copie.

Les schémas et les approches actuels du watermarking sont diverses soit dans le domaine spatial ou le domaine transformé et qui tentent tous à assurer un tatouage robuste et imperceptible, mais ces approches lors de la conception d'un système de tatouage ne répondent pas aux exigences auxquelles est dédié ce tatouage et au moment ou la communauté des chercheurs s'appuie sur les propositions les plus efficaces, plusieurs travaux se lancent sur des algorithmes hybrides qui sont à base d'une combinaison de transformées afin d'avoir plus de robustesse et pour augmenter le taux d'imperceptibilité.

Notre approche découle dans ce sens, où on a choisis une combinaison de deux transformées DCT-DWT et DCT-SVD avec l'exploitation des caractéristiques du système visuel humain HVS. Cet outil HVS est devenu un outil de pointe dans les schémas de tatouage du moment qu'il exploite le système de vision humaine pour bien choisir les endroits d'incrustation pour permettre une bonne imperceptibilité des images tatouées.

La mise en œuvre des schémas proposés et suite aux tests des méthodes, le diagnostic des résultats de simulation pour l'évaluation de la robustesse et de l'imperceptibilité dévoile des résultats très encourageants que ce soit pour la phase d'insertion où on a trouvé de bons

résultats concernant l'imperceptibilité avec une valeur du métrique PSNR très satisfaisante. Pour la robustesse, et suite aux attaques simulées, les valeurs des métriques d'évaluation montrent des chiffres très encourageants avec un NCC et SSIM qui frôlent l'unité et un BER presque nul.

On peut confirmer que dans les deux approches où on a utilisé des algorithmes hybrides par la combinaison de deux transformées et avec l'exploitation du système visuel humain par l'utilisation de deux indices qui sont l'entropie et l'edge entropie, pour la première approche et le gradient des images pour la deuxième approche que les résultats trouvés sont très acceptables.

On a aussi contribué par une approche qui traite le tatouage des images numériques couleurs dans le domaine des transformées en utilisant une transformée paramétrique réciproque orthogonale **ROP** qui est basée sur la paramétrisation de la transformée de Hadamard en combinant convenablement un nouveau vecteur paramétrique avec la matrice de Hadamard qui possède une structure simple et une complexité de calcul réduite.
La mise en test de la méthode et suite à un diagnostic des résultats de simulation pour l'évaluation de la robustesse et les mesures objectives effectuées sur les images tatouées soumises aux différentes attaques ont mis en exergue la fiabilité de la méthode soit en phase d'insertion ou la phase d'extraction de la marque sans attaques pour des valeurs adaptées de la force de tatouage pour l'ensemble de la méthode par blocs choisis (8x8, 16x16, 32x32).

Le banc des tests des attaques malicieuses, nous a montré que la paramétrisation a amélioré nettement la robustesse par la création de clés secrètes qui sont au même nombre que celui des paramètres indépendants de la transformées (N/2-1), où l'attaquant ne pourra altérer la marque insérée même s'il détient la totalité des paramètres. Quant aux attaques non malicieuses (compression JPEG, rotation, ajout de bruit et filtrage), les résultats obtenus confirment bien la fiabilité du tatouage suite à l'utilisation des transformées paramétriques.

Comme perspectives de ce travail, nous souhaitons l'amélioration de ce que a été proposé et d'entreprendre le domaine du tatouage vidéo, qui est une extension du tatouage d'image et d'essayer de trouver et de former un système de protection vidéo qui sera une solution de protection des contenus vidéos et qui sera sûrement un centre d'intérêt prometteur et un sujet d'étude grandissant pour la communauté des systèmes des communications.

Références bibliographiques

Références Bibliographiques

[1] C.S.Lu and H.Y.Liao,"Multipurpose Watermarking for Image Authentification and Protection", IEEE Transactions on image processing Vol. **10**, pp.1579-1592, 2001.

[2] Y.Wang, J.F. Dohorty and R.Evan Dyck, "A Wavelet Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE Transactions on image processing, Vol.**11**, pp.77-88 , 2002.

[3] Y. Govindarajan and S. Dakshinamurthi , "Novel Reversible Watermarking Scheme for Authentication of Military Images", Int. J. Signal and Imaging Systems Engineering,Vol. **2,** 2009.

[4] I.Cox,J.Kilian,F.Leighton and T.Shamoon , "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. Image Processing, Vol. **6**, pp. 1673–1687, 1997.

[5] M. Kutter and S. Winkler, "A Vision Based Masking Model for Spread Spectrum Image Watermarking", IEEE Trans. Image Processing, Vol. **11**, 2002.

[6] H.T. Wu and Y.M. Cheung,"Reversible Watermarking by Modulation and Security Enhancement", IEEE Trans. Instrum. Meas., Vol. **59**, no. 1, pp. 221–228, 2010.

[7] D. Kannan and M.Gobi, "An Extensive Research on Robust Digital Image Watermarking Techniques", *International Journal of Signal and Imaging Systems Engineering*, Vol. **8**, No. 1/2, pp.89–104, 2015.

[8] Barni, F. Bartolini and A. Piva, "A DCT Domain System for Robust Image Watermarking", IEEE Transactions on Signal Processing. 66, pp.357-372, 1998.

[9] W.C.Chu,"DCT Based Image Watermarking Using sub Sampling", IEEE Trans. Multimedia 5,pp. 34-38, 2003.

[10] K. J. Giri, M. A. Peer, and P. Nagabhushan, "A Channel Wise Color Image Watermarking Scheme Based on Discrete Wavelet Transformation", in Proceeding of IEEE International Conference on Computing For Sustainable Global Environment transaction, pp.758-762, 2014.

[11] E. Li, H. Liang, and X. Niu,"Blind Image Watermarking Scheme Based on Wavelet Tree Quantization Robust to Geometric Attacks", *Proc. IEEE. WCICA*, pp. 10256–10260, 2006.

[12] E. Ganic, SD. Dexter, and AM. Eskicioglu,"Embedding Multiple Watermarks in the DFT Domain Using Low and High Frequency Bands", In: Proc. Security .Steganography and Watermarking of Multimedia Contents, pp. 175–84, 2005.

[13] D. Vaishnavi and T.S. Subashini, "Robust and Invisible Image Watermarking in RGB Color Space Using SVD", International Conference on Information and Communication Technologies, 2014.

[14] W. Pratt, J. Kane and Andrews HC, "Hadamard Transform Image Coding", In Proceedings of the IEEE. Vol. **57**, no. 1 , 1969.

[15] Ho. AT, J. Shen and SH. Tan , "Robust Digital Image -In-Image Watermarking Algorithm Using the Fast Hadamard Transform", International symposium on optical science and technology. International society for optics and photonic, 2003.

[16] J. Guo, P. Zheng and J. Huang, "Secure Watermarking Scheme Against Watermark Attacks in the Encrypted Domain", Journal of Visual Communication and Image Representation, Vol. **30** ,pp.125-135 ,2015.

[17] A. Tareef and A. Al-Ani, "A highly Secure Oblivious Sparse Coding-Based Watermarking System for Ownership Verification", Expert Systems with Applications, Vol.**42** ,pp. 2224–2233 ,2015.

[18] C. Whitelam, N. Osia and T.Bourlai, "Securing Multimodal Biometric Data Through Watermarking and Steganography", Technologies for Homeland Security (HST), IEEE International Conference, pp.61-66, 2013.

[19] S. Katzenbeisser and F. Peticolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, INC. 685 Canton Street Norwood, MA 02062,2000.

[20] R.Warkar, P. More and D. Waghole, "Digital Audio Watermarking and Image Watermarking for Information Security", Pervasive Computing (ICPC), International Conference on, pp.1-5. 2015

[21]. URL: http://www.havocscope.com/tag/music-piracy/

[22]. URL: http://www.guardian.co.uk/music/2009/jan/17/music-piracy

[23] T. Kin Tsui and Z. Xiao-Ping , "Color Image Watermarking Using Multidimensional Fourier Transforms", IEEE Transactions on Information Forensics and Security, Vol. **3**, no. 1, pp. 16-28,2008.

[24] I.J.Cox ,G.Doerr and T Furon , "Watermarking is not Cryptography", Proc. Int. Workshop on Digital Watermarking, pp. 1–15,2006.

[25] A. Haouzia and R. Noumeir, "Methods for Image Authentication a Survey", Multimedia Tools Applications, Vol. **39**, pp. 1-46, 2008

[26] P. Nguyen, S.Baudry, "Le Tatouage de Données Audiovisuelles", les cahiers du numérique, Vol **4**, pp 135-165,2003.

[27] G. Boato, N. Conci, V.Conotter, F.G.B. De Natale and C Fontanari, "Multimedia Asymmetric Watermarking and Encryption", Electronics Letters, Vol. **44**, pp. 601-602, 2008.

[28] Chun-Shien Lu "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", IDEA GROUP PUBLISHING, 2005.

[29] F.Hartung and B.Girod ,"Watermarking of Uncompressed and Compressed Video", Signal Processing,Vol. **66**,pp. 283-333, 1998.

[30] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", IBM Systems Journal, Vol.**35**, pp.131-336, 1996.

[31] R.B .Wolfgang and E.J. Delp, "A Watermark for Digital Images",IEEE ICIP, Vol.**3**, pp. 219-222,1996.

[32] B.Furht, E. Muharemagic and D. Socek ,"Multimedia Encryption and Watermarking", Multimedia Systems and Applications Series,Vol.**28** Springer Science+Business Media, Inc, 2005.

[33] Anuradha and R. P. Singh , "DWT based watermarking algorithm using Haar wavelet", Journal of Electronics and Computer Science Engineering, pp.1-6, 2012.

[34] I.J.Cox , J.Kilian ,F.T.Leighton and T.Shamoon,"Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing,* Vol.**6**,no.12 pp.1673-1687,1997.

[35]Wenwu Zhu, Zixiang Xiong and Ya-Qin Zhang. "Multiresolution Watermarking for Images and Video: a Unified Approach", *in Proc. of* 1998 *Intl. Conference on Image Processing,* Vol. **1**, pp.465-468, 1998.

[36] M.Ramkumar, A.N. Akansu and A.A.Alatan, "A Robust Data Hiding Scheme for Images Using DFT", *in Proc. of* 1999 *Intl.Conference on Image Processing,*Vol.**2**, pp. 2 11-215,1999.

[37] J.J.K.O.Ruanaidh,W.J.Dowling and F.M.Boland ,"PhaseWatermarking of Digital Images", *in Proc. of Intl. Conference on Image Processing,* Vol. **3**, pp. 239-242,1996.

[38] J. Cox, L. Miller, A. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography ", 2nd edition, Morgan Kaufmann Publishers, USA, 2008.

[39]Y.S. Kim, O-H. Kwon, R. H. Park, "A Wavelet Based Watermarking Method for Digital Images Using the Human Visual System ", Electronic Letters, Vol.**35,** no.6 , pp.466-467, 1999.

[40] P. Bas, J-M. Chassery "Tatouage Couleur Adaptatif Fondé sur l'Utilisation d'Espaces Perceptifs Uniformes", Laboratoire des Images et des Signaux, Saint Martin d'Hères, France. Traitement du Signal , Vol. **21 ,** pp.517-531, 2004.

[41] M. Kutter and F.A.P. Petitcolas ,"A Fair Benchmark for Image Watermarking Systems", Security and Watermarking of Multimedia Contents, Proceedings of SPIE, Vol. **3657**, pp. 1-14, 1999.

[42] N. Hayashi, M. Kuribayashi and M. Morii, "Collusion Resistant Finger Printing Scheme Based on the CDMA-Technique", International Workshop on Security, pp. 28–43, 2007.

[43] A. P. Petitcolas, J. Anderson, G. Kuhn. "Attacks on Copyright Marking Systems", Information Hiding, Second International Workshop, IH'98, Portland, Oregon, U.S.A, pp. 219-239, 1998.

[44] A. Hanjalic , C. Langelaar, G. van Roosmalen, j. Biemond, and L. Langendijk, "Image and Video Databases: Restauration, Watermarking and Retrieval ", Amsterdam: Elsevier Publisher, The Netherlands, 2000.

[45]G.L.Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image", IEEE Transaction on Consumer Electronics,Vol.**39**,no.4,pp.905-910,1993.

[46] S. Santini and R. Jain , "Similarity Measures", IEEE Trans. on PAMI, Vol.**12**, no. 9, pp. 871 – 883, 1999.

[47] D. F. Elliott and K. R. Rao, "Fast Transforms: Algorithms, Analyses and Applications", Academic Press, NewYork, NY, 1982.

[48] C.C.Tseng, "Eigenvalues and Eigenvectors of Generalized DFT, Generalized DHT, DCT-IV and DST-IV matrices", *IEEE Transactions on Signal Processing*, Vol. **50** ,no. 4, pp. 866–877, 2002.

[49] J. M. Vilardy, J. E. Calderon, C. O. Torres, and L. Mattos, "Digital Images Phase Encryption Using Fractional Fourier Transform", *in Proceedings IEEE Conference. Electronics, Robotics and Automotive Mechanics*, Vol. **1**, pp.15–18, 2006.

[50] G. Strang, "The discrete cosine transform", *SIAM Review*, Vol. **41**, no. 1, pp.135–147, 1999.

[51] V, Britanak, P.C. Yip, K.R. Rao, **"**Discrete Cosine and Sine Transforms**",** 1st Edition, Academic Press, 2006.

[52] N. Ahmed, T. Natarajan and K. R. Rao, "Discret Cosine Transform", IEEE Transactions On Computers, pp. 90-93, 1974.

[53] Y.Hu, W.Q.Liu, Y. Deng ,W. He and J. Dai ,"Readable Watermarking Algorithm Based on Wavelet Tree Quantization", Communications, Circuits and Systems, ICCCAS. International Conference on , Vol.**1**, pp.579 – 583,2004.

[54] J. Zan, M.O. Ahmad, and M.N.S. Swamy, "Object-based Image Watermarking Technique Using Wavelets ", Electrical and Computer Engineering. Canadian Conference on, Vol. **2**, pp.1143 – 1146, 2004.

[55] P.S. Murty and P. Rajesh Kumar, "A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DCT-SVD Technique", IJCSNS International Journal of Computer Science and Network Security, Vol.**10** ,no.10, 2010,

[56] X. Wu, J. Fan, J. Xu and Y. Wang, "Wavelet Domain Multidictionary Learning for Single Image Super-Resolution" ,Journal of Electrical and Computer Engineering, Vol **2015**, Article ID 526508,2015.

[57] H.C. Andrews and C.L. Patterson, "Singular Value Decomposition (SVD) Image Coding", IEEE Trans. Comm. COM, pp.425–432, 1976.

[58] R. Sun and T. Yao , "A SVD And Quantization Based Semi-Fragile Watermarking Technique for Image Authentication", Proc. Internat. Conf. Signal Process, pp. 1952–1955, 2002.

[59] C-C. Chang, P. Tsai and C-C. Lin , "SVD-based Digital Image Watermarking Scheme" ,Pattern Recognition Letters Vol.**26**, pp.1577-1586, 2005.

[60] N. M. Makbol1, B. E. Khoo1, and T. H. Rassem ,"Block-Based Discrete Wavelet Transform Singular Value Decomposition Image Watermarking Scheme Using Human Visual System Characteristics", 2015.

[61] K. L. Chung , W. N. Yang, Y. H. Huang, *S. T.* Wu, and Y. C. Hsu , "On SVD-Based Watermarking Algorithm", Applied Mathematics *and Computation* ,Vol. **188**, no. 1, pp. 54-57, 2007.

[62] B. Razafindradina and P. A. Randriamitantsoa, "Robust and Blind Watermarking in the Singular Values Domain", *Journal Marocain de l'Automatique, de l'Informatique et du Traitement de Signal*, 2010.

[63] J. L.Walsh, "A Closed Set of Orthogonal Functions", *Amer. J. of Mathematics* Vol.**45** pp.5-24,1923.

[64] R. E. A. C. Paley, "A Remarkable Series of Orthogonal Functions", *Froc. London Math. Soc*.pp.241-279,1932.

[65] N. Ahmed, K. Rao , A.Abdussattar , "BIFORE or Hadamard Transform", IEEE Transactions on Audio and Electroacoustics ,1971.

[66] H.F. Harmuth,"A generalized Concept of Frequency and Some Applications", IEEE Trans Information Theory, pp.375-382, 1968.

[67] P. Dita , "Some Results on The Parameterization of Complex Hadamard Matrices", Journal of Physics A. Mathematical and General,Vol.**37**,no 20.pp.5355-5374,2004.

[68] A.T. Butson, "Generalized Hadamard matrices", Proceeding of the American Mathematical Society. Vol **13**.pp894-898,1962.

[69] **S.**Bouguezel, M.O. Ahmad, and M.N.S. Swamy**,** "A New Class of Reciprocal-Orthogonal Parametric Transforms", *IEEE Trans. Circuits and Syst. I,Regular Papers*, Vol.**56**, pp.795-805, 2009.

[70] S. Bouguezel, M.O. Ahmad and M.N.S. Swamy, "Image Encryption Using the Reciprocal-Orthogonal Parametric Transforms", *International Symposium on Circuits and Systems (ISCAS)*, pp. 2542-2545, 2010.

[71] P.C. Su and C.Kuo. "An Image Watermarking Scheme to Resist Generalized Geometrical Transformations", In SPIE Conference on Multimedia Systems and Applications, pp.354-365, 2000.

[72]F.Y.Shih and S.Y.Wu. "Combinational Image Watermarking in The Spatial and Frequency Domains", Pattern Recognition, Vol.**36** pp.969-975, 2003.

[73]H-T. Hu and Ling-Yuan Hsu, "Exploring DWT–SVD–DCT Feature Parameters For Robust Multiple Watermarking Against JPEG and JPEG2000 Compression", Computers and Electrical Engineering.Vol.**41**,pp.52-63,2015.

[74] R.C. Gonzalez and E.R. Woods, "Digital Image Processing" (New Jersey: Prentice Hall), 2002.

[75] C. E. Shannon, "A Mathematical Theory of Communication", Bell System Technical Journal, Vol. **27**, pp. 379-423 , 1948.

[76] D. Patel and S. Patnaik , "Robust Image Watermarking Based on Average and Significant Difference", Proceedings of the World Congress on Engineering and Computer Science , San Francisco, USA, 2011.

[77] E. Li, H. Liang, and X. Niu, "Blind Image watermarking scheme based on wavelet tree quantization robust to geometric attacks", *Proc. IEEE. WCICA*, pp.10256–10260, 2006.

[78] V.Santhi, P.Arulmozhivarman 'Hadamard transform based adaptive visible/invisible watermarking scheme for digital images", Journal of Information Security and Applications, Vol.**18** pp.167-179,2013.

Thèse de Doctorat : **« Contribution au développement de méthodes de tatouage dans le domaine des transformées »**

Présentée par : **Mr MOKHNACHE Salah**
Encadrée par : **Prof. CHIKOUCHE Djamel**

ملخص:

لقد اقترح الوشم الرقمي كوسيلة للحصول على الحماية الرقمية للمعطيات و تلبية و تقديـر الشـروط الثلاثة (الصـلابـة و الإخفـاء و القدرة). تقدم هذه الدراسة خطة قوية لوشم صورة بناءا على خوارزميات هجينة تجمع بين اثنين من المحو لات المشتركة DCT-SVD و DCT-TWD و تشغيل النظام البصري للإنسان لتوضيح مناطق انخفاض معدل المعلومات عن طريق حساب الانتروبية و مستويات الانتروبية، والسماح بالاختيار الدقيق لمواقع الإدراج و ذلك لضمان التسوية بين المتانة و الخفاء.

النتائج تؤكد أمانة النظام المقترح و وجهات النظر المتانة و الإخفاء وجها لوجه ضد الـهـجمات المـبـرمـجـة وساهمنا بعـمل ثاني باستخدام التحويلات الرقمية الوسائطية . المذكرة تعرض أولا دراسة مكتبية عن تقنيات الوشم الرقمي للصور و التحويلات الرقمية المألوفة و الحالة التقنية للتحولات بالوسائط و أساليب تطويرها. ثم استخدمنا تقنيات التحويل الوسيطي انطلاقا من تحويل ROP. هذه الدراسة سمحت لنا باستخدام التحويلات الرقمية الوسائطية عن طريق القوالب ورؤية مدى نجاعة استعمال الوسائط كمفاتيح سرية للزيادة في صلابة الوشم الرقمي أكدت النتائج التجريبية فعالية التحويلات الوسيطية اتجاه الهجمات وبالتحديد الهجمات المقصودة باستغلال الوسائط على شكل مفاتيح سرية إضافية إن هذه التقنيات أثبتت ايجابيتها في قلة التعقيد بالنسبة لتقنيات الوشم الرقمي المعهودة كلمات مفتاحية: تقنيات الوشم الرقمي للصور, الوسائط, التحويلات بالوسائط.

كلمات مفتاحيه: الوشم الرقمي، المحولات المشتركة ، النظام البصري للإنسان SVH.

Résumé :

Un nouveau formulaire de dissimulation d'information, appelé tatouage numérique, pour traiter le problème de la vie privée et du droit d'auteur et pour assurer l'authenticité des produits multimédias. Le tatouage numérique est une technique pour la protection numérique et doit satisfaire le compromis : robustesse, invisibilité et capacité. Les approches proposées dans ce travail présentent un schéma de tatouage d'image robuste basé sur les algorithmes hybrides par la combinaison de deux transformées DCT-SVD pour la première DCT-DWT pour la deuxième et par l'exploitation du système visuel humain HVS pour la localisation des zones à faible taux d'information par le calcul de l'entropie et l'edge entropie, et le gradient qui est une dérivée spatial ce qui donne une carte topologique de l'image. Cette étape est importante pour localiser les régions où les perturbations sont intenses et permet également d'évaluer la douceur moyenne de l'image, ce qui permet un choix judicieux des endroits d'insertion pour assurer le compromis robustesse et imperceptibilité.

Ce travail traite aussi par une autre approche le tatouage des images en exploitant les transformées discrètes paramétriques. On a présenté un état de l'art des transformées non paramétriques comme la transformée de Walsh Hadamard et la transformée paramétrique orthogonale ROP et sa méthode de développement et de construction. Vu que la ROP se propose comme une nouvelle transformée. Et son exploitation dans notre travail comme une méthode de tatouage d'images par blocs et l'utilisation de ces paramètres indépendants comme des clés secrètes pour renforcer la robustesse et consolider notre tatouage, à donner des résultats expérimentaux, très satisfaisants Spécialement l'analyse des attaques malicieuses, montrent clairement l'efficacité de la paramétrisation et la robustesse des méthodes proposées. En plus, ces méthodes présentent un avantage de complexité réduite par rapport à celles des méthodes de tatouage d'images existantes.

Mots clés : Tatouage numérique, combinaison de transformées, SHV, ROP.

Abstract

A new information concealment form, called Digital Watermarking, to address the privacy and copyright issue and to ensure the authenticity of multimedia products. Digital watermarking is a technique for digital protection and must satisfy the trade-off: robustness, invisibility and capacity. The approaches proposed in this work present a robust image watermarking scheme based on hybrid algorithms by the combination of two DCT-SVD transforms for the first and DCT-DWT for the second one by exploiting the HVS human visual system. for the localization of low information rate zones by calculating entropy and edge entropy, and the gradient which is a spatial derivative which gives a topological map of the image. This step is important for locating regions where disturbance is intense and also for evaluating the average softness of the image, which allows for a judicious choice of insertion locations to ensure the compromise robustness and imperceptibility.

This work also deals with the watermarking of images using discrete parametric transforms. A state of the art of non-parametric transforms such as the Walsh Hadamard transform and orthogonal parametric ROP and its method of development and construction has been presented. Since the ROP proposes itself as a new transformation. And its exploitation in our work as a watermarking method of block images and the use of these independent parameters as secret keys to strengthen the robustness and consolidate our watermarking, to give experimental results, very satisfactory Specially the analysis of malicious attacks, clearly show the efficiency of the parameterization and the robustness of the proposed methods. In addition, these methods have a reduced complexity advantage over existing tattooing methods.

Key words: watermarking, combining transforms, HVS,ROP