

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS – SETIF 1–
UFAS (ALGERIE)

MEMOIRE

Présenté à la Faculté de Technologie
Département d'Électronique

Pour l'obtention du Diplôme de

MAGISTER

Option : Communication

par

M. Farouk ZEHDA

THEME

**Tatouage d'images basé sur des transformées discrètes
entières**

Soutenu le : 26 / 11 / 2014

devant la commission d'examen :

Mr. A. FERHAT HAMIDA	Prof à l'université de Sétif 1	Président
Mr. N. AMARDJIA	M.C.C.A à l'université de Sétif1	Examineur
Mr. L. ZIET	M.C.C.A à l'université de Sétif1	Examineur
Mr. S. BOUGUEZEL	Prof à l'université de Sétif 1	Rapporteur

Remerciements

Au terme de ce travail je tiens à remercier au premier lieu le bon dieu miséricordieux qui m'a éclairé le bon chemin pour m'avoir donné le courage et la volonté à amener ce modeste travail à bon terme.

*Mes remerciements sont aussi adressés à mon encadreur le professeur Mr **Saad BOUGUEZEL** qui m'a proposé le thème de ce mémoire pour ces orientations, ses conseils, ses remarques judicieuses et sa disponibilité, je tiens à lui exprimer ma profonde gratitude en vue du bon déroulement du travail durant l'élaboration de ce mémoire.*

*Je tiens à exprimer ma parfaite considération au professeur Mr **Abdelhak FERHAT HAMIDA** de m'avoir fait l'honneur de présider mon jury de soutenance, aux membres de jury : Mr **Nourredine AMARDJIA** et Mr **Lahcen ZIET** maîtres de Conférence à l'université de Sétif¹, de m'avoir fait l'honneur d'évaluer mon travail.*

Je voudrais remercier tous les enseignants qui ont contribué énormément à ma formation de près ou de loin en particulier les enseignants du département d'électronique.

Enfin, mes remerciements vont à l'ensemble des personnes du département d'électronique enseignants et étudiants.

Dédicaces

Je dédie ce modeste travail :

*à l'esprit de mon père suppliant Dieu d'accorder sa miséricorde infinie et éternelle et
ma très chère mère pour leurs sacrifices.*

à ma très chère femme ZEINEB, et mon cher fils LOUAI ABD SAMAD.

à ma chère sœur et mes chers frères.

Je dédie également ce travail à ma grande famille ZEHDA et la famille HALFAVA.

*à mes amis abdelalli Belhamel, sofiane Dehelis, morad Merabette, chabane Djabali,
walid Dairi et fateh Chettibi, ainsi qu'à tous mes amis de l'université de Sétif et de
l'institut national de la formation et de l'enseignement professionnels Kacem Chérif
de Sétif.*

à tous ceux qui m'aime.

Farouk

Table des matières

Liste des figures	
Liste des tableaux	
Liste des abréviations	
Résumé	
Introduction générale.....	1

Chapitre 1

Etat de l'art sur le tatouage d'images

1.1 Introduction	3
1.2 Historique	3
1.3 Concept général du tatouage d'images.....	4
1.4 Contraintes du tatouage d'images	6
1.4.1 Imperceptibilité	6
1.4.2 Robustesse	6
1.4.3 Capacité.....	7
1.4.4 Sécurité.....	7
1.5 Techniques de tatouage d'images	7
1.5.1 Tatouage visible et invisible.....	7
1.5.2 Type de l'algorithme.....	8
1.5.2.1 Types de d'insertion	8
1.5.2.2 Types d'extraction.....	11
1.5.3 Domaine d'insertion.....	12
1.5.3.1 Domaine spatial	12
1.5.3.2 Domaine fréquentiel	12
1.5.4 Méthodes basées sur les modèles du système visuel humain	14
1.5.4.1 Seuil de perception	15
1.6 Mesures perceptuelles de la qualité visuelle de l'image	16
1.6.1 Métriques basées sur les pixels.....	16
1.6.2 Métriques de pondération perceptuelle	17
1.7 Attaques considérées dans le tatouage d'images.....	18

1.7.1 Compression JPEG.....	18
1.7.2 Ajout de bruit	18
1.7.3 Filtrage	19
1.8 Application du tatouage d'images.....	19
1.8.1 Protection des droits d'auteur	19
1.8.2 Authentification.....	19
1.8.3 Gestion des transactions	20
1.8.4 Protection de Copie	20
1.8.5 Information sur le support	21
1.8.6 Indexation.....	21
1.9 Conclusion.....	21

Chapitre 2

Méthode de tatouage d'images basée sur le contenu de l'image

2-1 Introduction.....	23
2.2 Généralités sur les caractéristiques de l'image	23
2.2.1 Texture	23
2.2.2 Contour.....	23
2.2.3 Corner.....	24
2.2.4 Luminance.....	25
2.3 Masque visuel (<i>JND</i>).....	26
2.4 Principe de la méthode [36]	26
2.4.1 Génération du masque visuel	27
2.4.2 Algorithme d'insertion	30
2.4.3 Algorithme d'extraction	31
2.5 Implémentation de la méthode	32
2.5.1 Résultats de simulation.....	33
2.5.2 Discussions des résultats	37
2.8 Conclusion.....	39

Chapitre 3

Nouveau algorithme de tatouage multi-bit à poids variable basé sur la DCT et HVS

3.1 Introduction	40
3.2 Algorithme de tatouage développé dans [9].....	41
3.2.1 Génération de la marque.....	41
3.2.1.1 Mise en forme du message à inséré	41
3.2.1.2 Génération du dictionnaire de codes (codebook)	42
3.2.1.3 Orthogonalité de Gram-Schmidt	42
3.2.1.4 Génération de la marque étendue	42
3.2.2 Masques visuels de Watson.....	43
3.2.3 Insertion de la marque	44
3.2.4 Extraction de la marque.....	45
3.3 Méthode proposée	46
3.3.1 Choix approprié de coefficients DCT pour l'insertion de la marque	47
3.3.2 Masques visuels proposés	48
3.3.3 Réduction du nombre de blocs altérés.....	48
3.3.4 Poids d'insertion variable	49
3.4 Implémentation et comparaison des deux méthodes.....	50
3.4.1 Choix approprié de coefficients DCT pour l'insertion de la marque	50
3.4.2 Masques visuels proposés	51
3.4.3 Réduction du nombre de blocs altérés.....	53
3.4.4 Poids d'insertion variable	54
3.5 Conclusion.....	56

Chapitre 4

Nouvelle Technique de tatouage d'images basée sur DCT-3D et QIM

4-1 Introduction.....	57
4.2 Outils utilisés.....	57
4.2.1 Domaine DCT 2-D	57

4.2.2 Quantification par modulation indexée	57
4.3 Méthode proposée utilisant la DCT-3D et QIM.....	58
4.3.1 Transformation d'Arnold	59
4.3.2 Algorithme d'insertion	61
4.3.3 Algorithme d'extraction	62
4.4 Résultats de simulations	63
4.5 Discussion	72
4.6 Conclusion.....	72
Conclusion générale	73
Bibliographie	75

Liste des figures

Figure 1.1	Nombre annuel des articles publiés dans tatouage par IEEE	4
Figure 1.2	Concept général du tatouage d'images	5
Figure 1.3	Contraintes du tatouage d'images	6
Figure 1.4	Image tatouée: (a) tatouage visible, (b) tatouage invisible	7
Figure 1.5	Quantification par la méthode QIM	10
Figure 1.6	Décomposition DWT à un niveau	14
Figure 1.7	Dégradations fournissant un <i>PSNR</i> similaire	17
Figure 2.1	Extraction des contours par : (a) L'opérateur <i>Canny</i> , (b) Phase Conguency	24
Figure 2.2	Détection des corners utilisant CSS	25
Figure 2.3	Définition des régions DCT	30
Figure 2.4	Images originales de test: (a) Image <i>Lena</i> , (b) Image <i>Boat</i>	32
Figure 2.5	Marque originale de taille 16×16	33
Figure 2.6	Images tatouées en utilisant la DCT : (a) Image <i>Lena</i> , (b) Image <i>Boat</i>	33
Figure 2.7	Images tatouées en utilisant la DCT entière : (a) Image <i>Lena</i> , (b) Image <i>Boat</i>	33
Figure 2.8	Variation <i>wPSNR</i> en fonction du facteur scalaire β	34
Figure 2.9	Les valeurs <i>JND</i> pour <i>Lena</i> (ligne 1)	34
Figure 2.10	Les valeurs <i>JND</i> pour <i>Lena</i> (ligne 32)	35
Figure 2.11	Les valeurs <i>JND</i> pour <i>Boat</i> (ligne 1)	35
Figure 2.12	Les valeurs <i>JND</i> pour <i>Boat</i> (ligne 32)	35
Figure 2.13	Compression JPEG : (a) $q = 35$ (b) $q = 40$ (c) $q = 45$ (d) $q = 50$	37
Figure 2.14	Bruit Gaussien : (a) 1% (b) 2%	37
Figure 2.15	Bruit Salt&Pepper (a) 1% (b) 2% (c) 3% (d) 4%	38

Figure 2.16	Cropping : (a) $1/4$, (b) $1/2$	38
Figure 2.17	Filtrage Gaussien 3×3	39
Figure 3.1	Schéma bloc du système de tatouage	41
Figure 3.2	Masque de luminance de <i>Watson</i> pour l'image de test <i>Lena</i>	44
Figure 3.3	Emplacements des coefficients <i>AC</i> choisis par bloc DCT 8×8	44
Figure 3.4	Processus d'extraction de la marque	45
Figure 3.5	Différents bandes de fréquence dans un bloc DCT 8×8	47
Figure 3.6	Emplacement de coefficients proposés	47
Figure 3.7	de test <i>Lena</i> taouée utilisant : (a) le masque JND_3 , (b) le masque luminance de <i>Watson</i>	53
Figure 3.8	Variation du α_i en fonction des bits b_i dans trois coefficients <i>AC</i> différents	54
Figure 3.9	Image de test <i>Lena</i> taouée utilisant : (a) la méthode [9], (b) la méthode proposée	56
Figure 4.1	Processus d'insertion à base de QIM	58
Figure 4.2	Système du tatouage proposé	59
Figure 4.3	Transformation d' <i>Arnold</i> (a) Image <i>Lena</i> après 1 itération, (b) image <i>Baboon</i> après 1 itération, (c) logo droits d'auteur après 25 itérations	60
Figure 4.4	<i>NC</i> en fonction du nombre d'itérations pour l'image logo droits d'auteur	61
Figure 4.5	Illustration de la transformation DCT pseudo-3D	62
Figure 4.6	Image <i>Lena</i> , image <i>Baboon</i> et logo droits d'auteur	63
Figure 4.7	Images tatouées <i>Lena</i> et <i>Baboon</i>	63
Figure 4.8	Marques extraites <i>Lena</i> et <i>Baboon</i>	64

Liste des tableaux

Tableau 2.1	Evaluation en terme <i>NC</i> l'extraction de la marque	36
Tableau 3.1	Evaluation en terme <i>NC</i> l'extraction de la marque dans deux emplacements différents (Pos1 et Pos2)	50
Tableau 3.2	Evaluation en terme <i>NC</i> l'extraction de la marque pour 4 masques différents	52
Tableau 3.3	Evaluation en terme <i>NC</i> l'extraction de la marque pour 1024 blocs	53
Tableau 3.4	Evaluation en terme <i>NC</i> l'extraction de la marque pour un facteur gain variable	55
Tableau 4.1	<i>NC</i> en fonction du nombre d'itérations	61
Tableau 4.2	<i>PSNR</i> des images tatouées et <i>NC</i> entre W et W^*	64
Tableau 4.3	Ajout de bruit Salt&Pepper	65
Tableau 4.4	Ajout de bruit Gaussien	66
Tableau 4.5	Filtrage Gaussien	67
Tableau 4.6	Filtrage médian	68
Tableau 4.7	Filtrage average	69
Tableau 4.8	Cropping	70
Tableau 4.9	Compression JPEG	71

Liste des abréviations

DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
wPSNR	Weighted Peak Signal to Noise Ratio
NC	Normalized Correlation
BER	Bit Error Rate
CSF	Contrast Sensitive Function
JND	Just Noticeable Distortion
NVF	Noise Visibility Function
CSS	Curvature Scale Space
PC	Phase Conguency
JPEG	Joint Photographic Experts Group
HVS	Humain Visual System
QIM	Quantization Index Modulation
DC	Direct component
AC	Alternative component
IEEE	Institute of Electrical and Electronics Engineers
LSB	Less Significant Bits
PN	Pseudo Noise

QF	Quantization Function
FQ	Facteur de Qualité
CDMA	Code Division Multiple Access
LL	Low Low frequency band
LH	Low High frequency band
HL	High Low frequency band
HH	High High frequency band
DVD	Digital Video Disc
CD	Compact Disc
1-D	1 Dimension
2-D	2 Dimensions
3-D	3 Dimensions
DivX	Le DivX et le XviD sont des codecs de compression vidéo basés sur la norme MPEG-4
MPEG	Moving Picture Experts Group

Résumé

Ce travail considère le tatouage des images fixes en exploitant les masques visuels récemment développées dans la littérature. Le mémoire présente tout d'abord un état de l'art sur le tatouage d'images et une étude bibliographique sur les techniques de tatouage d'images et leurs domaines d'applications. Cette étude nous a permis de développer deux nouveaux algorithmes de tatouage d'images fixes aveugles et robustes. Le premier algorithme est dédiée essentiellement à l'utilisation de la technique d'étalement de spectre dans le domaine de la transformée DCT et la DCT entière, tout en exploitant les caractéristiques locales de l'image pour la conception des masques visuels. Par contre, le deuxième algorithme est dédié pour l'exploitation de la technique de tatouage par quantification basée sur la méthode QIM en utilisant le domaine DCT-3D. Les résultats de simulation pour l'évaluation de la robustesse et les mesures objectives effectuées sur les images tatouées soumises aux différentes attaques, présentés dans ce travail montrent clairement l'efficacité et la robustesse des algorithmes proposés dans ce mémoire. En plus, ces algorithmes proposés présentent un avantage de complexité réduite par rapport à celles des algorithmes de tatouage d'images existants.

Mots clés : Tatouage des images, Transformées DCT et DCT entière, étalement de spectre, quantification QIM.

Introduction générale

Les réseaux numériques de communication sont largement utilisés pour l'échange des informations comme texte, audio, vidéo etc. La sécurité de ces informations échangées est devenue une nécessité primordiale dans beaucoup d'applications des organismes civils ou militaires, citons par exemple, l'internet, la téléphonie mobile, les distributeurs de billets, les abonnements aux chaînes de télévision payantes, le commerce électronique et les cartes à puce, afin d'assurer la confidentialité et d'empêcher toute modification ou exploitation non autorisée des données. L'une des méthodes connues pour la réalisation efficace de cet objectif est le tatouage qui rend la marque insérée complètement illisible et imperceptible. En effet, le tatouage est l'un des moyens technologiques utilisés pour fournir la sécurité et l'authenticité aux données transmises sur des systèmes de communication.

Plusieurs techniques de tatouage ont été développées pour résoudre le problème de sécurité. Elles peuvent être classifiées de différentes manières. On distingue généralement deux types de systèmes de tatouage selon l'apparence ou non de la marque insérée : le tatouage visible et le tatouage invisible. Les systèmes de tatouage invisibles sont largement utilisés, puisque il est difficile de faire la distinction entre l'information originale (image, audio ou vidéo) et l'information tatouée d'une part, et d'autre part, une tentative de suppression de la marque insérée provoque une dégradation de manière significative de la qualité de la donnée tatouée.

Il existe dans la littérature des techniques de tatouage spatiales et fréquentielles. Les algorithmes traditionnels de tatouage comme ceux qui modifient les bits de poids faibles LSB (Least Significant Bit) des pixels de l'image hôte dans le domaine spatial [1], ne sont pas très robustes aux attaques comme la compression et l'ajout de bruit. Pour fournir une meilleure solution au problème de la robustesse des images tatouées, des techniques de tatouage d'images ont été proposées dans [2]-[3], où le tatouage se fait dans le domaine fréquentiel. La marque est insérée dans les coefficients obtenus par l'utilisation d'un processus de transformation sur l'image. Une catégorie de ces techniques est celle qui exploite les transformées discrètes telles que la transformée de Fourier discrète DFT (Discrete Fourier Transform), la transformée en ondelettes discrète DWT (Discrete Wavelet Transform), la transformée en cosinus discrète DCT (Discrete Cosine Transform) etc. Bien que la DCT et la DFT disposent des algorithmes de calcul rapide, la complexité reste encore élevée et ne répond pas aux exigences des applications modernes. Par conséquent, il est préférable d'utiliser des transformées entières dont la complexité est significativement réduite. Cela est dû au fait que ce types de transformées n'exigent que des additions et des décalages de bits, et pas de multiplications. La transformée entière de la DCT est plus attractive par rapport aux autres transformées entières existantes car elle a une bonne capacité de compactage d'énergie.

Les techniques de tatouage peuvent également être classées suivant l'un des deux techniques d'insertion de base suivantes: Type I - est une technique de tatouage par quantification QIM (Quantization Index Modulation) [4], le principe consiste à se munir de jeux de quantificateurs entrelacés et indexés par les codes possibles à tatouer. Dans la littérature, des algorithmes ont été proposées pour le tatouage d'images à base de QIM. Une technique à deux pas de quantification adaptés [5]. La technique angle QIM où la marque est insérée en quantifiant l'angle formé par un système de coordonnées sphérique pour réduire l'effet des attaques du changement d'échelle [6]. Une autre technique qui se base sur la sélection adaptative de la taille du pas de quantification en exploitant des masques visuels est proposée dans [7]. Type II - est une technique de tatouage basé sur l'étalement de spectre (spread spectrum), qui est probablement la technique la plus populaire de tatouage, où la marque ajoutée à l'image hôte est détectée par un corrélateur [2]. Dans quelques applications de tatouage telles que la protection de la propriété, les empreintes digitales et le contrôle d'accès, la robustesse du système de tatouage peut être critique. Moins de 100 bits d'information (par exemple, 60 bits selon [8]), peuvent être suffisants pour représenter l'information de l'auteur, un timbre de temps, les informations de copyright, ou des informations de contrôle. Récemment, une technique de tatouage multi-bit à poids d'insertion fixe basée sur l'étalement de spectre plus efficace que celles proposées par [2]-[3] est développée dans [9]. L'efficacité de cette méthode est due essentiellement à l'utilisation d'un masque perceptuel afin d'améliorer la qualité visuelle de l'image tatouée.

Afin d'améliorer davantage l'efficacité de la technique de tatouage multi-bit et de développer des techniques de tatouage d'images plus robustes et plus rapides que celles mentionnées précédemment, nous proposons dans ce travail une technique de tatouage à poids d'insertion variable tout en exploitant les caractéristiques perceptuelles de l'image à tatouée.

Ce mémoire est composé de quatre chapitres. Le premier chapitre présente des notions générales sur le tatouage et ses applications et une étude bibliographique des différentes techniques de tatouage. Le deuxième chapitre est consacré à l'implémentation d'un algorithme de tatouage basé sur le contenu de l'image. Nous proposons dans le chapitre 3 un nouveau algorithme de tatouage multi-bit à poids d'insertion variable basé sur la DCT en exploitant le masque visuel présenté dans le chapitre 2. Une technique basée sur la quantification est exploitée dans le chapitre 4 pour concevoir un nouveau algorithme de tatouage d'images en utilisant le domaine DCT pseudo-3D et la technique QIM. Afin de tester les performances des méthodes proposées, des expériences d'analyse de la robustesse, des mesures objectives effectuées sur les images tatouées et des attaques par compression, ajout de bruit et filtrage sont réalisées dans les chapitres 2, 3 et 4.

1.1 Introduction

Le tatouage d'images ou *watermarking* est apparu au début des années 1990, dans le but de parer le piratage des documents multimédia.

Le tatouage consiste à insérer une information numérique, éventuellement cryptée, dans une image, une vidéo, une séquence sonore ou même un texte numérisé.

Les applications du tatouage d'images sont vastes. La littérature nous fournit diverses approches de tatouage, tant sur des images monochromes que sur des images couleurs.

Nous allons présenter dans ce chapitre, le concept général du tatouage d'images, nous présenterons les différentes techniques utilisées, un recueil des principales attaques considérées dans le tatouage, et enfin les applications considérées dans le tatouage.

1.2 Historique

Les tatouages du papier sont apparus dans l'art de la fabrication du papier, il y a presque 700 ans. Le plus ancien document tatoué trouvé dans les archives remonte à 1292 et a son origine dans la ville de Fabriano en Italie qui a joué un rôle important dans l'évolution de l'industrie papetière. A la fin du troisième siècle, environ 40 fabricants du papier partageaient le marché du papier.

La concurrence entre ces fabricants était très élevée et il était difficile que n'importe quelle partie maintienne une trace de la provenance du papier et ainsi que son format et sa qualité. L'introduction des tatouages était la méthode parfaite pour éviter n'importe quelle possibilité de confusion.

Après leur invention, les tatouages se sont rapidement étendus en Italie et puis en Europe et bien qu'au commencement utilisé pour indiquer la marque ou le fabricant du papier, ils ont servi plus tard pour indiquer le format, la qualité, et la force du papier, et ont été également employés comme une base pour dater et authentifier le papier [10].

L'analogie entre le tatouage du papier et le tatouage numérique est évidente : les tatouages du papier des billets de banque et de timbres ont inspiré la première utilisation du terme *marque d'eau* dans le contexte de données numériques. Le terme *digital watermarking* a été introduit en 1993, quand Tirkel et al ont présentés deux techniques pour incruster des données dans l'image. Ces méthodes ont été basées sur des modifications du bit le moins significatif (LSB, *Less Significant Bit*) des valeurs de pixels [11].

Les premières publications portant sur le tatouage d'images numériques ont été publiées par [12] en 1990 et par [13] en 1993. L'évolution du nombre de publications à ce sujet (voir figure(1.1)) date de 1995, ce qui s'est concrétisé par la création de l'atelier IHW (*Information Hiding Workshop*) en 1996, d'une conférence spécifique au sein de SPIE (*Society of Photographic Instrumentation Engineers*) en 1999 et de l'atelier IWDW(*International Workshop on Digital Watermarking*) en 2002. Quatre journaux dédiés aux problématiques de sécurité de l'information ont été créés récemment : *IEEE Trans. on Information Forensics and Security* et *IEE Proc. Information Security* en 2005, *LNCS Transactions on Data Hiding and Multimedia Security* et *EURASIP Journal on Information Security* en 2006, ce qui souligne le dynamisme du domaine [14].

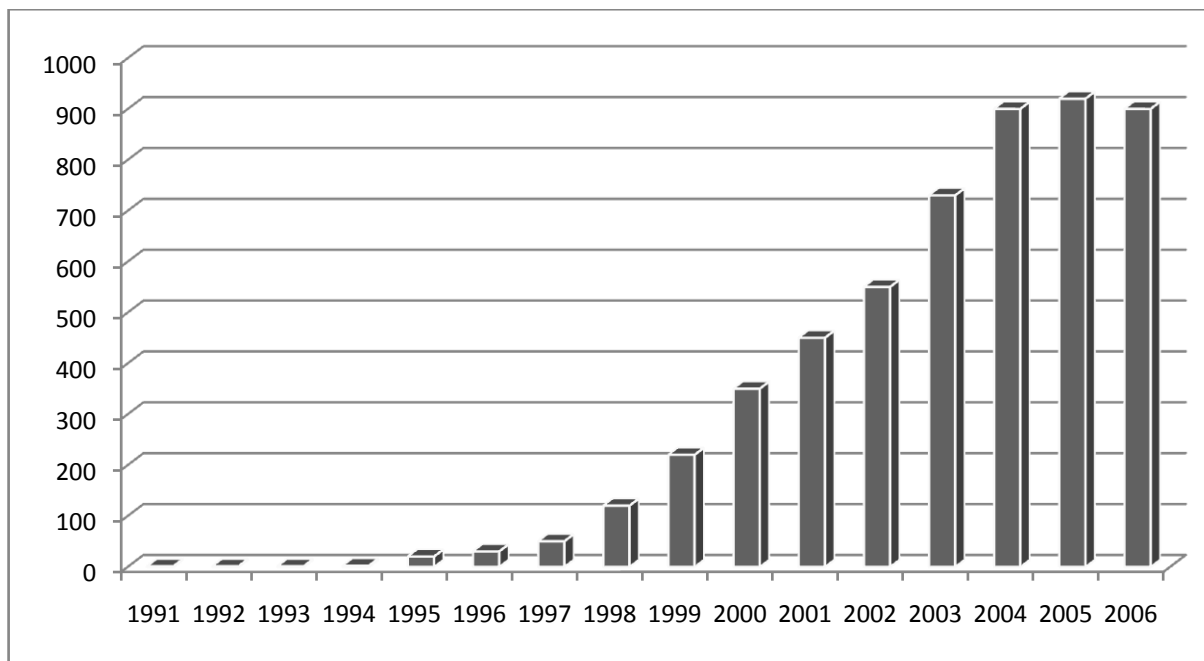


Figure (1.1) : Nombre annuel des articles publiés dans le tatouage par IEEE.

1.3 Concept général du tatouage d'images

Toutes les méthodes de tatouage se basent sur le même principe général. La figure (1.2.a) illustre ce principe. Un système de tatouage est constitué de deux entités, un bloc d'insertion et un bloc d'extraction de la marque [15].

Pour le schéma de tatouage donné dans la figure (1.2.b), un message m contenant L bits d'information est transformé selon une clé k en une marque w qui est ensuite insérée dans le document x aussi appelé "hôte" peut être une image, un son, ou une vidéo, pour donner un document tatoué y , c'est la phase d'insertion. Ici, w est exprimé sous la forme d'un bruit qui est ajouté au document, la déformation dépendant de la puissance du bruit. k est secrète et spécifique

au tatoueur. y est ensuite copié et attaqué, ce qui est modélisé par la transmission dans un canal soumis à du bruit.

Après déformation, le document reçu est appelé z . La réception d'un document consiste en deux parties, d'une part la détection du tatouage et d'autre part s'il est présent son décodage.

La phase de détection consiste à prouver la présence d'une marque dans z grâce à la clé k . La phase de décodage consiste à calculer une estimation $\hat{m}$ du message m .

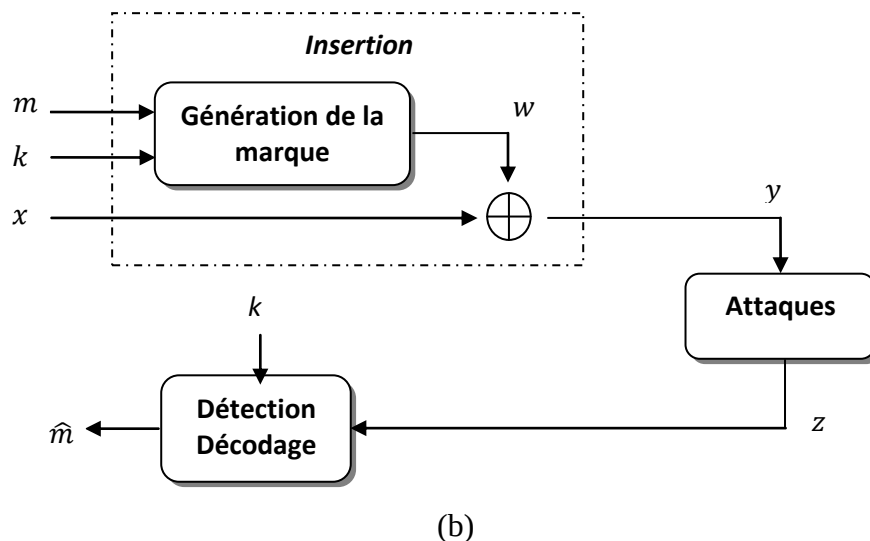
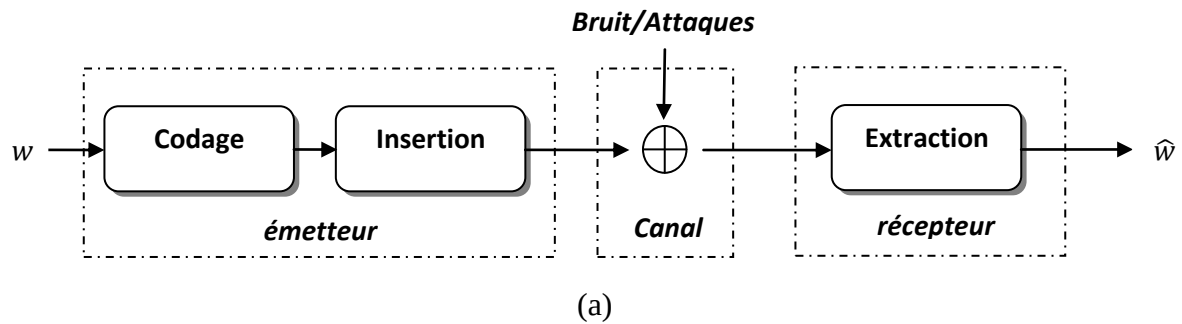


Figure (1.2) : Concept général du tatouage d'images.

Selon l'application, les systèmes de tatouage pourraient généralement être classés en deux groupes, détection et décodage de la marque [16].

Dans le premier groupe, le but principal est de vérifier si la marque insérée dans un document spécifique (par exemple les informations de copyright) est présente ou non.

Dans le second groupe, les informations intégrées sont considérées comme un message caché qui doit être décodé correctement au niveau du décodeur.

1.4 Contraintes du tatouage d'images

En général, il ya quatre facteurs essentiels couramment utilisés pour quantifier la performance d'une technique de tatouage. Ces facteurs sont l'imperceptibilité, robustesse, capacité et la sécurité [17]-[18].

J.Fridrich [19] présente le compromis entre l'imperceptible, robustesse et la capacité par un triangle montré par la figure (1.3).

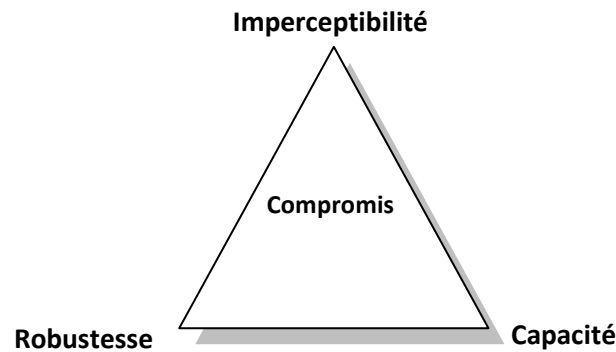


Figure (1.3) : Contraintes du tatouage d'images.

1.4.1 Imperceptibilité

Le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée. Les auteurs [14] définissent l'imperceptibilité en tant que similitude visuelle entre l'image originale et l'image tatouée.

1.4.2 Robustesse

Les méthodes robustes sont utilisées dans la plupart des applications, si ce n'est le contrôle d'intégrité. Les données insérées dans le support doivent donc en général être capables de résister aux attaques, volontaires ou non. Par exemple, dans de nombreux systèmes impliquant stockage et transmission d'images, un mécanisme de compression avec pertes est appliqué afin de réduire la taille des données et ainsi augmenter l'efficacité du système.

La compression constitue alors une attaque de la marque. De plus, les images numériques sont aisément modifiables (zoom, filtrage,...) en utilisant des logiciels extrêmement répandus. Ces modifications entraînent alors un risque de détérioration du tatouage.

Les concepteurs des systèmes de tatouages tentent donc de rendre leur marque résistante face aux nombre d'attaques.

1.4.3 Capacité

La quantité d'information insérée dans le tatouage, ou capacité (*payload*), est très variable selon les algorithmes et applications proposés. Pour l'insertion d'un copyright, on peut par exemple vouloir insérer une information similaire à la norme ISBN (International Standard Book Number ou Numéro international normalisé du livre) utilisée pour les livres, soit de 60 à 70 bits d'information [18]. Un message encore plus long peut être inséré si l'image est considérée comme un canal de communication caché.

A l'inverse, beaucoup d'auteurs proposent d'insérer une information binaire (présence du tatouage ou non), pour une application à la protection de copie. On parle également de signature pour la séquence ainsi générée [20].

1.4.4 Sécurité

La sécurité des techniques de tatouage peut être interprétée de la même manière que la sécurité des techniques de cryptographique. L'hypothèse de *Kerckhoff* suppose que la méthode utilisée pour crypter les données est connue pour le public non autorisé, et que la sécurité doit se situer dans le choix d'une clé. Ainsi, une technique de tatouage est vraiment sûre si la connaissance exacte des algorithmes pour l'insertion et l'extraction de la marque n'aide pas une personne non autorisée d'éliminer ou de détecter la présence de la marque [21].

1.5 Techniques de tatouage d'images

Vu le nombre phénoménal des techniques de tatouage d'images disponibles dans la littérature, nous allons classer les techniques de tatouage d'images en quatre catégories selon : tatouage visible et invisible, types d'algorithmes utilisés dans l'insertion et l'extraction de la marque, domaine d'insertion et tatouage basé sur les modèles du système visuel humain (HVS).

1.5.1 Tatouage visible et invisible

Du point de savoir si la marque insérée peut être vue par l'œil humain ou non, toutes les techniques de tatouage d'images peuvent être classées comme des techniques de tatouage visibles ou invisibles. Par exemple, la figure (1.4.a) montre une image qui contient un logo visible dans son coin supérieur gauche et la figure (1.4.b) montre la même image tatouée par le même logo mais d'une manière invisible.



Figure (1.4) : Image tatouée: (a) tatouage visible, (b) tatouage invisible.

Dans les techniques de tatouage visible, il existe au moins deux inconvénients :

- La marque insérée est facilement enlevée par un simple cropping.
- La visibilité de la marque insérée dégrade la qualité visuelle de l'image l'hôte.

Dans la technique de tatouage invisible, il n'est pas facile de faire la distinction entre l'image originale et l'image tatouée. Ainsi, il est difficile d'enlever ou détruire la marque insérée sans avoir une dégradation de la qualité visuelle de l'image tatouée de manière significative.

1.5.2 Type de l'algorithme

1.5.2.1 Types d'insertion

a. Tatouage additif

Le tatouage additif consiste à ajouter un signal w au signal hôte x suivant l'expression (1.1) sans que le codage amenant à w soit déterminé par x , même si les échantillons w_i peuvent être modulés par un facteur perceptuel dépendant de x_i .

L'extraction se fait en décodant le signal y' reçu, c'est-à-dire en décodant w bruité par l'attaque et par le signal hôte x . De plus, afin de respecter la contrainte d'imperceptibilité, l'énergie de w est très inférieure à celle de x .

$$y = x + w \quad (1.1)$$

La fonction de codage permet d'associer à un message m un signal w avec $\text{codage}(m, c) = w$. De même, la fonction de décodage permet de retrouver un message depuis un signal reçu, c'est-à-dire le message correspondant au signal $\hat{w}$ le plus proche du signal reçu.

Dans le cas où le nombre de symboles du message est important, la recherche du signal le plus proche est en pratique impossible (pour un message binaire de n bits, il faudrait 2^n calculs de distance).

L'étalement de spectre [22] est une solution de communication adaptée à ce type de caractéristiques et utilisable sans difficulté pour des valeurs de symboles importantes. Le principe est de coder les symboles de m séparément, plutôt que de coder le message complet.

Chaque symbole est codé différemment selon son rang dans m . Le vecteur de marque est donné par l'expression (1.2).

$$w = \sum_{j=1}^k SS(j, m_j, c) \quad (1.2)$$

L'extraction du *jème* symbole consiste à rechercher le signal $\widehat{w}_j$ le plus proche de y' parmi les M possibles. Pour un message de n symboles binaires, l'extraction complète se fait en seulement 2^n calculs de distance.

Dans le cas de symboles binaires, une simplification commune [23] consiste à prendre $M = \{-1, +1\}$. La fonction $SS()$ est définie par une matrice G de dimensions $k \times n$ générée pseudo-aléatoirement depuis la clé c . Les w_j sont obtenus grâce à la modulation du *jème* vecteur de G (c'est-à-dire la *jème* porteuse) par le *jème* bit.

$$w_j = SS(j, m_j, c) \Rightarrow m_j \times G(j) \quad (1.3)$$

Le calcul de la distance entre y' et une porteuse $G(j)$ consiste en un calcul de produit de corrélation entre ces deux signaux suivant la formule :

$$\widehat{m}_j = \arg \max \{ \langle y', SS(j, m_j, c) \rangle \} \quad (1.4)$$

Si l'on prend y' (signal marqué non attaqué) donné par l'expression :

$$y' = y = x + \sum_{j=1}^k SS(j, m_j, c) \quad (1.5)$$

Le résultat de ce calcul est séparable en trois composantes.

$$\begin{aligned} \langle y', SS(j, m_j, c) \rangle &= \langle SS(j, m_j, c), SS(j, m_j, c) \rangle + \langle x, SS(j, m_j, c) \rangle \\ &\quad + \sum_{l=1, l \neq j}^k \langle SS(j, m_l, c), SS(j, m_j, c) \rangle \end{aligned} \quad (1.6)$$

On trouve donc :

- L'auto-corrélation de la porteuse. C'est dans ce terme d'espérance non nulle que réside l'énergie de la marque ;
- Le produit de corrélation entre la porteuse et le signal hôte. Malgré son espérance nulle, ce terme est la principale source d'interférence (et donc de potentielles erreurs) ;

– Le produit de corrélation entre la porteuse du *jème* symbole et celle des autres symboles. Bien que dans l'idéal, les porteuses doivent être parfaitement orthogonales afin de s'assurer d'une interférence nulle, leur grand nombre et leur grande longueur rend cette construction quasi impossible. Cela entraîne une interférence résiduelle limitant la performance du canal de transmission.

a.1 Tatouage additif par étalement de spectre

Le principe de l'étalement de spectre (*Spread Spectrum*) consiste à utiliser toutes les composantes fréquentielles du document x . Le terme "étalement" désigne le fait de passer d'un signal possédant un spectre à bande limitée à un signal dont le spectre occupe toute la bande de fréquences.

A partir du modèle de l'équation (1.1), on peut considérer le tatouage comme la transmission d'un signal w dans un canal bruité x (le document). Cette analogie avec les télécommunications est à la base de l'utilisation de la théorie de l'information et des techniques de tatouage par étalement de spectre.

La marque devient alors une mise en forme du message m , suivie d'une modulation. La principale différence avec les télécommunications réside dans l'inversion du rapport Signal/Bruit. Ici la puissance du bruit x est beaucoup plus grande que celle du signal w . Si le tatoueur utilise la connaissance de x à l'insertion, il s'agit d'une transmission avec information adjacente (*side information*).

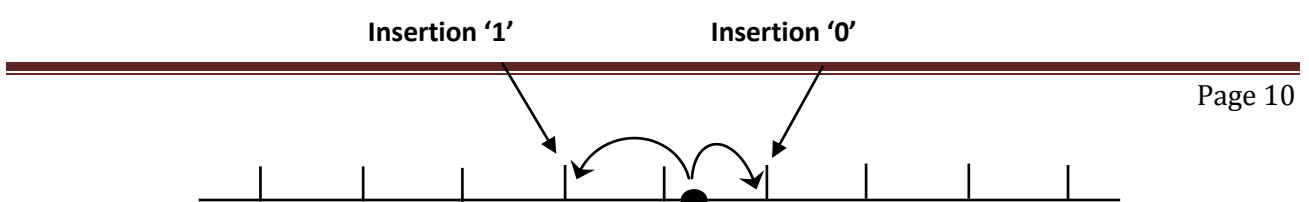
b. Tatouage substitutif

Plutôt que de construire un signal w n'ayant que peu de rapport avec les données hôtes, le tatouage substitutif se propose de modifier ces données afin de les faire correspondre au message que l'on souhaite transmettre. On peut classer dans ces méthodes le tatouage par quantification [24].

b.1 Tatouage substitutif par quantification QIM

Les méthodes de quantification proposées par [25] appartiennent à la classe des schémas substitutifs et consistent à remplacer des blocs de l'image par des blocs d'un dictionnaire prédéfini.

La méthode QIM (Quantification par Modulation Indexée) utilise les fonctions de quantification QF . Le principe d'insertion par quantification consiste d'abord à choisir deux fonctions de quantification $\times$ et 0 . On quantifie alors le signal source x en fonction du message à insérer, si le message à insérer est un 0 on utilisera la fonction $\times$, sinon on utilisera la fonction 0 .



$$\frac{\Delta}{2}$$

Figure (1.5) : Quantification par la méthode QIM.

Δ est le pas de quantification. L'insertion d'un bit b peut se décrire par :

$$\begin{cases} \text{si } b = 0 & s(x, b) = \times(x) \\ \text{si } b = 1 & s(x, b) = o(x) \end{cases} \quad (1.7)$$

où encore

$$\begin{cases} \text{si } b = 0 & s(x, b) = QF_{\Delta}(x) \\ \text{si } b = 1 & s(x, b) = QF_{\Delta}\left(x - \frac{\Delta}{2}\right) + \frac{\Delta}{2} \end{cases} \quad (1.8)$$

La détection est réalisée en évaluant l'inégalité de distance (1.9).

$$|s(x, m) - QF_{\Delta}(s(x, m))| < \left|s(x, m) - QF_{\Delta}\left(s(x, m) - \frac{\Delta}{2}\right) - \frac{\Delta}{2}\right| \quad (1.9)$$

Si celle-ci est vérifiée, alors le bit décodé vaut 0, sinon il vaut 1.

Une forme dérivée de quantification utilise deux vecteurs de dilution d_0 et d_1 rendant le marquage plus robuste. La fonction d'insertion s'écrit alors (1.10).

$$s(x, m) = QF_{\Delta}(s(x, m) - d(m)) - d(m) \quad (1.10)$$

Le vecteur de dilution d utilisé dépend du bit à insérer : d_0 pour un 0 à insérer et d_1 pour un 1. Le décodage procède également, en évaluant la distance :

$$\begin{aligned} |s(x, m) - QF_{\Delta}(s(x, m) - d_0(m)) - d_0(m)| \\ < |s(x, m) - QF_{\Delta}(s(x, m) - d_1(m)) - d_1(m)| \end{aligned} \quad (1.11)$$

Si celle-ci est vérifiée, alors le bit décodé vaut 0, sinon il vaut 1.

1.5.2.2 Types d'extraction

Les schémas de tatouages peuvent être classés suivant les éléments nécessaires pour l'extraction de la marque.

Un schéma aveugle n'a pas besoin du document original pour extraire la marque. Au contraire, un schéma non aveugle nécessite le document original pour pouvoir lire correctement le

message. Dans le schéma semi-aveugle, nous avons besoin d'informations supplémentaires pour aider la détection ou l'extraction. Cette demande est due à la perte de synchronisation à cause de canal bruité ou de la technique d'insertion. La phase d'extraction peut requière la marque ou l'image tatouée [26].

Un dernier point discriminant est l'utilisation des clés. La marque insérée est issue du codage du message à transmettre. Il est dépendant d'une clé. Si cette même clé est nécessaire au décodage (c'est-à-dire à l'extraction du message), le schéma est symétrique et dans le cas contraire, il est asymétrique (systèmes à clé privée K_s et clé publique K_p). N'importe quel utilisateur peut détecter la marque en connaissant K_p , mais seul la connaissance de K_s permet de modifier ou de supprimer la marque. On retrouve cette classification dans les algorithmes de cryptographie [21].

1.5.3 Domaine d'insertion

Les techniques de tatouage courantes décrites dans la littérature peuvent être regroupées selon leurs domaines d'insertion en deux classes, techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

1.5.3.1 Domaine spatial

Dans le domaine spatial, la marque est insérée en modifiant les LSB (bits de poids faible). Les images sont en général manipulées en modifiant un ou plusieurs bits de l'octet constituant les pixels de l'image. Pour une image codée sur 8 bits, une modification du LSB entraîne une variation du niveau de gris de 1 sur une échelle de 256. Cette modification est en pratique invisible.

Cette méthode d'insertion consiste alors à supprimer tous les bits de poids faible de l'image à marquer, puis à y insérer les données voulues. Un bit de donnée est ainsi inséré par pixel de l'image.

Deux techniques LSB sont proposées par [27]. La première remplace les LSB de l'image hôte par une séquence pseudo-bruit (PN) d'amplitude fixe, et la deuxième ajoute la séquence PN aux bits LSB.

En règle générale, le tatouage dans le domaine spatial est facile à mettre en œuvre, mais trop fragile pour résister aux nombreuses attaques, par exemple l'ajout de bruit ou bien la compression avec perte peut facilement dégrader la qualité de l'image ou de supprimer la marque [28]-[29].

1.5.3.2 Domaine fréquentiel

Comme nous venons de le voir, le principal inconvénient des méthodes de tatouage spatial est la faible robustesse face aux attaques et notamment face aux attaques géométriques.

Les techniques de tatouage spatial telles que celles que nous venons de découvrir peuvent tout aussi bien être adaptées aux domaines fréquentiels.

Les domaines transformés les plus fréquemment exploités pour les applications de tatouage d'image sont le domaine de DFT (Transformée de Fourier Discrète), le domaine DCT (Transformée en Cosinus Discrète) et DWT (Transformée en Ondelette Discrète).

a. Domaine de la DFT

Les auteurs [30] ont présenté une méthode de tatouage de la phase de la DFT. Ici, les auteurs ont opté pour la phase du spectre, car l'insertion d'une marque dans les composantes les plus importantes de l'image permet d'accroître la robustesse du schéma.

Une attaque opérant dans la phase du spectre dégraderait rapidement la qualité de l'image. Une seconde raison justifiant le tatouage de la phase du spectre provient de la théorie de la communication ou la modulation de la phase possède une meilleure immunité au bruit que la modulation d'amplitude.

Cependant, plusieurs techniques de tatouage exploitent la modulation d'amplitude de la DFT. L'invariance du spectre en translations ou décalages a motivé certains auteurs à tatouer l'amplitude du spectre de Fourier [31].

b. Domaine de la DCT

La propriété essentielle de la DCT est la décroissance rapide de l'amplitude des coefficients lorsque la fréquence augmente, ce qui la rend utile pour la compression d'images. De plus, la DCT offre une bonne robustesse à des attaques telles que l'ajustement de brillance et de contraste, filtrage, smoothing (lissage) et compression.

Dans l'article fondateur du tatouage d'image par étalement de spectre [2], les auteurs proposent une insertion dans le domaine de la DCT appliquée à l'image complète pour une robustesse à la compression avec perte et au changement d'échelle.

Une méthode assez répandue de tatouage d'images, extensible aux signaux audio voire aux séquences vidéo est celle présentée par [3]. Cette méthode est extensible aux signaux audio et vidéo et applicable dans le domaine DCT ou DFT.

La méthode de [2]-[3] consiste à insérer un bruit dans le contenu fréquentiel de l'image pondérée par une force d'insertion constante.

c. Domaine de la DWT

La théorie des ondelettes est commune à celle des bancs de filtres. L'idée est de séparer le signal original en plusieurs bandes de fréquences (basse-fréquence et haute-fréquence). La partie passe-bas donne une représentation compactée de l'image initiale. Cette partie peut être décomposée plusieurs fois et ces décompositions successives correspondent aux échelles de décomposition. Pour reconstruire le signal, il faut rassembler ces diverses bandes.

La transformée en ondelettes est une description multi-résolution d'une image. Elle décompose une image en plusieurs sous-bandes dans trois directions différentes, horizontale, verticale et diagonale.

La DWT consiste à décomposer le signal x en basses et hautes fréquences en utilisant respectivement des filtres passe-bas et passe-haut qui doivent être orthogonaux.

La décomposition de niveau simple de l'image donne quatre représentations de fréquence. Ces quatre représentations s'appellent les sous-bandes LL, LH, HL, et HH comme montre la figure (1.6).

LL	HL
LH	HH

Figure (1.6) : Décomposition DWT à un niveau.

Plusieurs recherches ont même été faits pour combiner la DWT avec d'autres transformées, on peut citer notamment l'algorithme de [30] qui insère les valeurs singulières de la marque dans celles de l'image hôte, la méthode de [32] qui insère la DCT de la marque dans la bande HH de l'image hôte après décomposition et enfin d'autres méthodes hybrides [33] qui combine les techniques DWT et CDMA (Code Division Multiple Access).

1.5.4 Méthodes basées sur les modèles du système visuel humain

L'utilisation de modèles psycho-visuels permet d'augmenter la force de la marque sans que les dégradations soient visuellement perceptibles. L'objectif de ces techniques est de prendre en défaut le HVS et d'exploiter les différentes propriétés de masquage.

Le masquage a lieu lorsqu'un signal (la signature) est rendu imperceptible par la présence d'un autre signal dit masquant (l'image).

Plusieurs modèles de masque ont été utilisés en tatouage d'image, certains modèles dans le domaine spatial [34], d'autres dans le domaine fréquentiel [35].

Les auteurs [36] ont proposé un masque permettant d'assembler des caractéristiques fréquentielles du HVS et des caractéristiques spatiales de l'image traitée.

La sensibilité du HVS dépend principalement de trois paramètres, la fréquence spatiale, la couleur et l'intensité lumineuse (la luminosité).

La réponse perceptuelle en fonction de la fréquence spatiale correspond à la sensibilité au contraste. Cette réponse définit une fonction notée CSF (Contraste Sensitivity Function), étudiée dans [11].

Le HVS est sensible aux contrastes moyens, et peu stimulé par les contrastes très forts ou très faibles. De plus, la sensibilité varie selon l'orientation de cette fréquence, l'œil est plus sensible aux motifs horizontaux et verticaux, plutôt qu'aux motifs à 45 degrés.

Le second paramètre est la fréquence spectrale, c'est-à-dire la couleur. Le HVS n'est en effet pas sensible de la même manière aux différentes longueurs d'onde du spectre visible.

Dans le cas d'une représentation de la couleur sous la forme de trois canaux rouge, vert et bleu, le canal bleu est celui qui a le moins d'importance (le HVS y est moins sensible).

Enfin, le dernier paramètre est la luminosité. L'œil est moins sensible aux changements dans les régions sombres et claires [37].

1.5.4.1 Seuil de perception

Une autre façon de prendre en compte le système perceptuel humain est d'utiliser des seuils de perception. Ce type de seuil ne mesure pas une distorsion, mais indique la distorsion maximale autorisée sans que la modification soit visible.

Au dessous de ce seuil, la modification ne pourra pas être remarquée, mais au dessus, elle pourra être perçue. Ce niveau de distorsion maximal est noté *JND* (*Just Noticeable Difference*) pour différence juste perceptible [36].

Selon le modèle de Watson, le seuil de perception est l'amplitude maximale d'une altération invisible d'un coefficient donné de la DCT. Il est calculé à partir des fréquences spatiales associées à chaque coefficient, qui dépendent de la taille d'un pixel sur l'écran et de la distance de vision.

Leur influence perceptuelle a été déterminée par des expériences psycho-visuelles effectuées à partir de mires sinusoïdales d'une fréquence et d'une orientation donnée, qui ont par la suite été utilisées dans la norme JPEG [35].

Le seuil est pondéré pour chaque bloc par l'intensité du coefficient DC (composante continue). Le masque de contraste détermine le contraste maximum au sein d'un motif lorsqu'il est superposé de façon invisible à un autre motif masquant d'un contraste, d'une fréquence spatiale et d'une orientation donnée.

1.6 Mesures perceptuelles de la qualité visuelle de l'image

La définition même du tatouage indique que les modifications apportées au document hôte doivent rester imperceptibles. Afin de respecter cette condition, ou de pouvoir mesurer de façon efficace la distorsion introduite par le tatouage, il est nécessaire d'introduire un critère perceptuel basé sur une modélisation de la perception des signaux multimédia.

En général, deux types de métriques peuvent être utilisées pour l'évaluation de l'imperceptibilité, métriques basées sur les pixels et métriques de pondération perceptuelle [38].

1.6.1 Métriques basées sur les pixels

Ces mesures sont basées sur le calcul de la différence (mesures de distances) entre l'image originale et l'image tatouée (attaquée ou non attaquée).

La mesure habituellement utilisée pour quantifier la distorsion entre un signal original x et un signal modifié y est le *PSNR* (Peak Signal-to-Noise Ratio). Elle est basée sur l'erreur quadratique moyenne *MSE* (Mean Square Error), définie par :

$$MSE = \frac{1}{n} \sum_{i=1}^n (x_i - y_i)^2 \quad (1.12)$$

où n est la dimension commune aux deux vecteurs considérés. Quant au *PSNR*, il est calculé par :

$$PSNR(x, y) = 10 \log_{10} \left[\frac{(\max(x))^2}{MSE} \right] \quad (1.13)$$

On considère généralement en tatouage d'images qu'un tatouage est imperceptible pour un *PSNR* supérieur à 36 dB, et plus il est élevé, moins la distorsion est importante [39].

Comme nous le constatons sur la figure (1.7), pour deux images dont le rapport signal à bruit (*PSNR*) est similaire, les dégradations occasionnées sont très différentes.

Malgré l'utilisation courante du *PSNR* pour mesurer la qualité des images tatouées, celui-ci, n'est pas bien adapté au système visuel humain HVS.

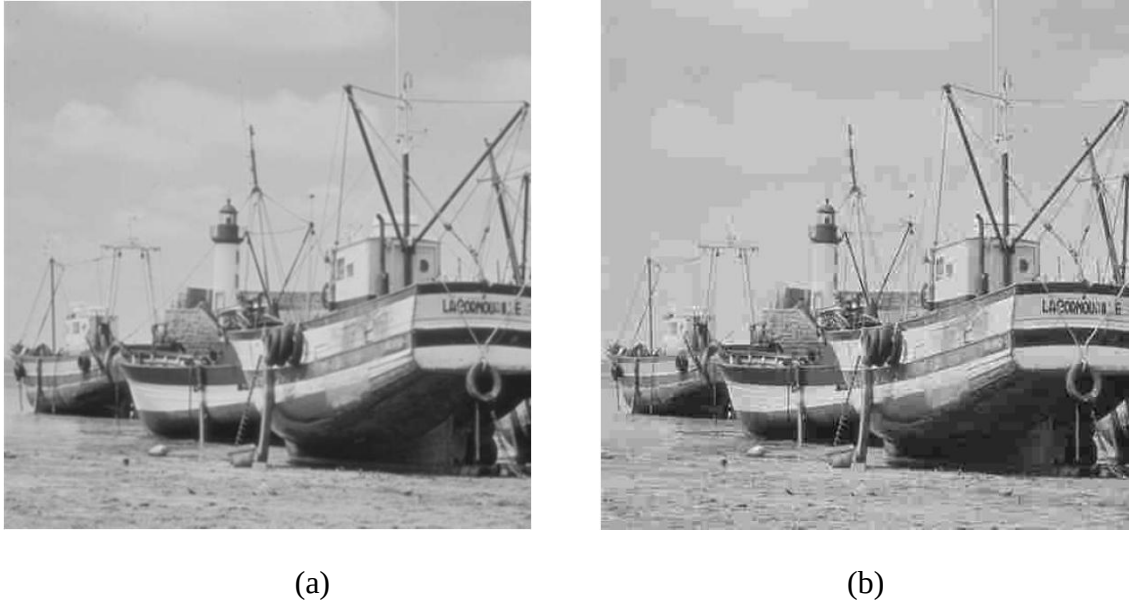


Figure (1.7) : Dégradations fournissant un *PSNR* similaire.

L'image (1.7.a) a subi un filtrage passe bas fournit un *PSNR* de 33,75 dB, alors que l'image (1.7.b), qui a subi un codage JPEG de facteur de qualité $q = 10\%$ fournit un *PSNR* de 32,76 dB présente des dégradations perceptuelles plus gênantes.

Le *PSNR*, bien que fréquemment utilisé ne semble donc pas être approprié pour juger de façon fiable la qualité des images tatouées.

Les métriques de corrélation (par exemple corrélation normalisée *NC*) sont légèrement plus complexes, elles permettent de calculer la corrélation entre les deux images. De telles métriques ne mesurent plus la différence entre deux images, mais plutôt la ressemblance des images.

$$NC = \frac{\sum_{i,j}^{MN} (x(i,j) \cdot y(i,j))}{\sqrt{\sum_{i,j}^{MN} x(i,j)^2 \cdot \sum_{i,j}^{MN} y(i,j)^2}} \quad (1.14)$$

Si ces métriques représentent grossièrement une mesure de dégradation des images, elles ne sont cependant pas adaptées au système visuel humain.

1.6.2 Métrique de pondération perceptuelle

L'approche la plus pratique pour prendre en compte les caractéristiques vues précédemment est l'introduction d'une pondération perceptuelle au sein de la mesure classique du *PSNR* ou *MSE* l'erreur quadratique moyenne.

De nombreuses pondérations ont été proposées, telles que celles citées par [36]. Ce type de mesure, noté $wPSNR$ (*weighted PSNR*), est défini par :

$$wPSNR(x, y) = 10 \log_{10} \left[\frac{(\max(x))^2}{wMSE} \right] \quad (1.15)$$

$$wMSE = MSE \times NVF^2 \quad (1.16)$$

L'œil humain est moins sensible au bruit dans les régions fortement texturées [34]. La NVF (*Noise Visibility Function*) est une fonction utilisée pour estimer la quantité de texture contenant dans n'importe quelle partie de l'image.

$$NVF(i, j) = \frac{1}{1 + \sigma_x^2(i, j)} \quad (1.17)$$

où $\sigma_x^2(i, j)$ désigne la variance locale de l'image dans une fenêtre centrée sur le pixel de coordonnées (i, j) .

1.7 Attaques considérées dans le tatouage d'images

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors de son extraction.

On distingue plusieurs types d'attaques telles que les attaques intentionnelles, ces dernières ne visent pas forcément à attaquer le tatouage. Parmi ces attaques classiques nous retrouvons :

- Les transformations géométriques (décalage, rotation, zoom, ...);
- La compression avec pertes, essentiellement le JPEG;
- L'addition d'un bruit;
- Le filtrage.

Il faut noter que nous n'allons pas utiliser les attaques géométriques puisque les techniques de tatouage basées sur la DCT (adoptée dans notre travail) sont fragiles contre ce type d'attaques.

1.7.1 Compression JPEG

La compression JPEG est une technique de compression avec pertes qui supprime les informations redondantes des images dont le but de diminuer la taille du fichier image. L'avantage de cette méthode réside dans les taux importants de compression que l'on puisse obtenir. Plus celui-ci va être élevé, plus l'on va supprimer une gamme de fréquences importantes et plus l'image va être dégradée.

1.7.2 Ajout de bruit

Le bruit est une altération de l'image : toute l'information pertinente dans l'image n'est pas simplement accessible. Des exemples de bruit artificiel peuvent être :

- Le bruit gaussien qui consiste à un ajout successif de valeurs générées aléatoirement à chaque pixel de l'image.
- Le bruit Salt&Pepper (sel et poivre) qui transforme aléatoirement des pixels de l'image en pixels noir ou blanc.

1.7.3 Filtrage

Le bruitage d'une image ayant utilisation particulièrement limité, voyons à présent les différents type de filtre servant justement à récupérer une certaine compréhension de l'image en y filtrant les bruits.

Les filtres les plus utilisés sont : filtre médian, filtre Gaussien et filtre average.

1.8 Applications du tatouage d'images

Les applications du tatouage d'images sont nombreuses ; leur diversité fait que les contraintes qu'elles imposent varient selon l'application envisagée. Les contradictions existantes entre ces contraintes rendent impossible la création d'un algorithme universel adaptable à toutes les applications.

La littérature relative au tatouage décrit abondamment les utilisations possibles du marquage [6]-[40]. On distingue généralement la protection de la propriété individuelle, le suivi de document, la prévention de la redistribution non autorisée, la protection des droits de copie, l'indexation, l'information sur le support et l'intégrité du contenu du document.

1.8.1 Protection des droits d'auteur

L'objectif du tatouage pour la protection du copyright est d'introduire dans une image originale une marque invisible contenant un code de copyright. L'image ainsi marquée ou tatouée peut alors être distribuée, elle portera toujours la marque de son propriétaire. Cette image est susceptible de subir diverses transformations. Ces transformations peuvent être licites (comme la compression) ou illicites, elles ont alors pour but de détruire le marquage.

1.8.2 Authentification

La marque permet de s'assurer que le contenu du document est authentique, il s'agit d'une marque fragile, qui subit des distorsions si le document a été altéré.

Le concept de robustesse est ici différent : à l'inverse des autres applications du tatouage, la marque est conçue de manière à se détériorer dès que le document est modifié.

Seules les modifications agressives doivent être prises en compte, la marque idéale en terme d'intégrité n'est pas affectée par des opérations de compression ou par l'ajout de bruit inhérent à la transmission des données.

Un exemple d'utilisation est l'authentification de conversations téléphoniques ou de vidéos afin de permettre leur utilisation lors de procès, la marque montrerait si le signal a subi des coupes permettant de vérifier si le sens premier de la conversation a été respecté.

1.8.3 Gestion des transactions

L'objectif est de détecter les possesseurs licites d'un document qui sont à l'origine de sa distribution illicite. Les exemples les plus courants de telles distributions sont les copies (gravées) de CD audio, ou encore la mise à disposition de fichier audio au format mp3 sur les pages web personnelles.

Une solution au problème de la redistribution non autorisée consiste à identifier séparément les acheteurs, en leur attribuant un numéro de série personnel.

La principale difficulté de conception d'un tel algorithme est qu'il faut générer autant de clefs qu'il existe d'acheteurs sans pour autant diminuer la robustesse du système.

Un exemple concret d'application est le paiement à la séance sur les chaînes numériques et Internet. L'acheteur peut avoir l'intention de copier le document (film ou musique) pendant sa lecture pour le mettre ensuite à disposition sur sa page personnelle par exemple. Savoir que le document est tatoué d'un numéro de série unique permettant aux possesseurs des droits de remonter jusqu'à lui pourra éventuellement le dissuader de le pirater.

Une application du tatouage transactionnel a été déployée par la société DivX. L'une des mesures de sécurité mises en œuvre dans le matériel DivX est un tatouage qui pourrait être utilisé pour identifier une tentative de piratage. Si des copies illégales d'un film DivX apparues sur le marché noir, DivX pourrait utiliser le tatouage pour les suivre jusqu'à la source [41].

1.8.4 Protection de Copie

Le cryptage d'un document ne suffit pas à assurer la protection de la copie. La sécurité est assurée le long du canal de transmission qui relie le vendeur à l'acheteur sous certaines hypothèses de robustesse, mais une fois décrypté le document n'est plus protégé et rien n'empêche le client de le copier. Le tatouage peut s'appliquer à cette famille de problèmes.

Des informations relatives à la copie et à l'utilisation sont encodées dans la marque, il peut s'agir d'autorisations du type pas de copies, 'une seule copie', 'plus de copies disponibles', ou encore 'copie sans restriction' [41].

Le dispositif chargé de la lecture et/ou de la copie interroge le support en refusant de le lire ou de le copier si les données encodées ne le permettent pas.

Ce dispositif suppose la construction d'une nouvelle génération de lecteurs audio. Les lecteurs DVD de seconde génération (permettant de graver des données vidéo) devraient être équipés d'un tel système de tatouage [11].

1.8.5 Information sur le support

La marque peut contenir des données publiques informatives sur l'œuvre, de type auteur, titre, date, adresse électronique etc. Dans l'éventualité (très probable) où cette application interviendrait en complément d'une protection de la propriété, il s'agirait non pas d'une seconde marque, mais d'informations supplémentaires insérées dans la première marque.

On peut aussi envisager l'insertion d'une seconde marque entièrement publique, ce qui autoriserait le client à supprimer ces informations supplémentaires pour minimiser la taille des données stockées. Cette technique a été développée par *Digimarc* sur les images numériques [11] qui sont alors appelées 'smart images'.

Ces images contiennent des adresses de pages Internet permettant d'obtenir des renseignements de nature publicitaire sur l'image.

1.8.6 Indexation

On peut envisager l'utilisation du tatouage afin de faciliter l'accès à des banques de données. La marque n'a pas besoin d'être robuste à de nombreux types d'attaque, puisqu'il ne s'agit plus de protection mais d'identification.

Par exemple, un médecin peut inclure dans une radiographie, de façon discrète afin de ne pas la dénaturer, le nom du patient traité, son diagnostic et ses observations. Ce cas est le plus simple, puisqu'une attaque visant à détruire la marque ne présente aucun intérêt et n'est donc a priori pas à craindre.

Selon [9], ce type de documents est appelé documents auto-indexé, car la marque contient sa propre description, afin de permettre son stockage dans une base de données sans problème de changement de format.

1.9 Conclusion

Dans ce chapitre, nous avons présenté le concept général du tatouage d'images. Nous avons aussi présenté une classification des techniques du tatouage selon différents critères tel que la visibilité ou non de la marque insérée, le type de l'algorithme utilisé dans la phase d'insertion et la phase d'extraction, l'utilisation des modèles du système visuel humain et le domaine d'insertion.

Selon ce dernier critère les techniques du tatouage peuvent être regroupées en deux catégories ; ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel.

Dans cette dernière catégorie, plusieurs transformées peuvent être utilisées telles que la DFT, DWT et DCT et c'est cette dernière transformée qui est utilisée dans le reste des chapitres.

Dans le chapitre suivant, nous allons implémenter une technique de tatouage d'images qui exploite les caractéristiques perceptuelles du système visuel humain.

2-1 Introduction

Beaucoup de recherches dans les techniques de tatouage d'images basées sur les propriétés de perception du système visuel humain (HVS) ont été réalisées pour améliorer la robustesse et la capacité des données à dissimuler [42]-[43]-[44]-[45]. Le développement et l'amélioration de la précision des modèles visuels humains aident à la conception et la croissance des masques perceptuels qui sont utilisés pour mieux dissimuler la marque à insérer dans l'image originale (hôte) ainsi en augmentant sa sécurité.

Les auteurs [36] ont proposés une méthode de tatouage aveugle qui est capable de dissimuler les informations de la marque d'une manière imperceptible dans l'image hôte. Cette imperceptibilité est obtenue en considérant les propriétés du HVS qui rend le système de tatouage plus robuste aux diverses attaques.

Dans ce chapitre, nous présentons le système de tatouage proposé par *Parthasarathy et Kak* [36] qui exploite la sensibilité en fréquence du HVS et les caractéristiques locales de l'image obtenues à partir du domaine spatial. L'idée est de générer un masque visuel basé sur la perception du HVS du contenu de l'image. Ce masque est exploité dans la phase d'insertion de la marque dans l'image hôte.

2.2 Généralités sur les caractéristiques de l'image

2.2.1 Texture

Dans une image la texture est définie comme la qualité visuelle de la surface de l'objet exposée dans l'image par des écarts dans le ton, la profondeur et la forme. Après l'obtention des coefficients DCT, premièrement nous extrairons l'information de texture directement par l'analyse de ces coefficients.

A partir du model visuel de l'image, chaque bloque DCT de taille 8×8 (64 coefficients) est analysé et comme les régions fortement texturées ou bien le long des contours l'énergie du signal est concentrée dans les composantes de hautes fréquences tandis que dans les régions où l'image est uniforme l'énergie du signal est concentrée dans les composantes de basses fréquences [36].

2.2.2 Contour

L'œil humain est plus sensible aux changements dans les zones ayant plusieurs contours comparées à ceux qui ont moins de contours (les zones lisses) et par conséquent nous allons utiliser les informations des contours pour offrir un poids d'insertion adapté [36].

Ces informations des contours sont extraites du domaine spatial (pixel) et elles sont utilisées pour déterminer la quantité d'information qui peut être insérée dans l'image hôte.

Il existe de nombreuses méthodes pour déterminer les contours. Ces méthodes basées soit sur le gradient de l'image ou bien le passage par zéro après filtrage de l'image par un filtre Gaussien ou Laplacien.

L'un des meilleurs algorithmes qui retournent plus de contours avec une bonne précision est l'algorithme Phase Conguency (PC) mis en œuvre par *Peter et Kovesi* [46] qui a prouvé une meilleur extraction de contours par rapport à d'autres algorithmes [36]. Cette méthode est invariante au changement du contraste de l'image.

Les contours de l'image *Lena* présentés par les figures (3.1.a) et (3.1.b) sont détectés par deux méthodes différentes.



Figure (2.1) : Extraction des contours par : (a) L'opérateur *Canny*, (b) Phase Conguency

On constate à partir de ces deux images que le nombre de contours détectés par Phase Conguency est beaucoup plus grand que celui détecté par l'opérateur de *Canny*.

2.2.3 Coins

Une autre caractéristique importante de l'image extraite dans le domaine spatial, est l'information relative aux coins.

Un coin représente le point où deux contours se rencontrent, et l'œil humain est sensible aux changements réalisés dans ces zones. Les coins sont mieux localisés que les contours, et ils

définissent mieux les formes des objets dans l'image, comme le contour peut fournir l'information locale dans une seule direction perpendiculaire au contour [47].

Les systèmes de tatouage perceptuel considèrent l'uniformité comme un facteur important dans la perception humaine. Les auteurs [42] ont utilisés l'opérateur de *Moravec* pour extraire les régions uniformes. Il s'agit essentiellement d'un détecteur de coin qui utilise une méthode à fenêtre glissante pour détecter le lissage dans un bloc à l'aide de la variation de l'intensité. L'opérateur de *Moravec* en raison de sa sensibilité aux bruits est utilisé pour identifier les faux coins en particulier les pixels isolés [48].

Il existe plusieurs algorithmes utilisant différentes approches pour détecter les vrais coins, un de ces algorithmes amélioré est basé sur Curvature Scale Space (CSS) [49]-[50].

La figure (3.2) montre la détection des coins de l'image de test *Lena* basée sur CSS.



Figure (2.2) : Détection des coins utilisant CSS

2.2.4 Luminance

La luminance est définie comme la manière dont l'œil humain perçoit la luminosité de différentes couleurs. Cette propriété influe sur la perception de l'image par l'œil humain.

La luminance est déterminée dans deux domaines différents, le domaine des pixels et le domaine fréquentiel où la composante continue *DC* est utilisée.

Dans un bloc DCT, la composante continue *DC* comporte des informations importantes en ce qui concerne la luminance, elle représente la moyenne de la luminance du bloc.

2.3 Masque visuel (*JND*)

Le *JND* est défini comme une mesure référant la capacité d'un observateur humain pour détecter un bruit ou une distorsion dans l'image. La plupart des systèmes de tatouage d'images considère l'insertion de la marque comme l'ajout d'un bruit à l'image hôte [36].

Une image peut être déformée que dans certaine limite sans faire la différence entre l'image tatouée et l'image originale [10]. La limite à laquelle nous pouvons modifier la valeur d'un pixel sans que la distorsion soit perceptible est nommée *JND*.

Il y a plusieurs caractéristiques définissant le *JND*, dont on considère textures, la luminance, coins et contours pour estimer un masque visuel qui est le poids d'insertion attribué à un bloc particulier. Ce poids est utilisé pour moduler la marque en maintien ainsi l'amplitude du signal au-dessous la sensibilité à la distorsion causé par un bruit de chaque pixel.

Plusieurs études sur le système visuel humain ont montrées que dans les zones fortement texturées la visibilité de la distorsion est faible. Il est préféré de dissimuler les informations de la marque dans ces zones et donc les valeurs du *JND* correspondantes à ces zones sont grandes.

Les valeurs des coins, contours et luminances, générées dans le domaine spatial, sont considérées aussi comme des caractéristiques importantes qui influent sur la perception humaine [45]. Les blocs de l'image hôte ayant plusieurs contours ou coins ont des valeurs *JND* plus basses parce que dans ces blocs la marque est facilement localisée [36].

2.4 Principe de la méthode [36]

La méthode de tatouage proposé dans [36] utilise les informations perceptuelles de l'image pour donner plus d'imperceptibilité de la marque insérée dans le domaine fréquentiel DCT.

Ce système de tatouage de l'image est divisé en trois étapes :

- Génération du masque basé sur les propriétés perceptuelles de l'image ;
- L'insertion de la marque par l'étalement d'une séquence pseudo-aléatoire dans le domaine fréquentiel ;
- Extraction de la marque par la méthode de corrélation.

2.4.1 Génération du masque visuel

L'image originale $f(x, y)$ est segmentée en blocs B_n de taille 8×8 qui ne chevauchent pas suivant l'expression (2.1), où $n = 1, 2, \dots, N - 1$.

$$f(x, y) = \bigcup_{n=0}^{N-1} B_n = \bigcup_{n=0}^{N-1} f_n(i, j), \quad \text{ou } 0 \leq i, j < 8 \quad (2.1)$$

La transformée DCT de image $f(x, y)$ de taille $N \times N$ est définie par :

$$F(u, v) = \frac{2}{N} C(u) C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{(2x+1)u\pi}{2N} \times \cos \frac{(2y+1)v\pi}{2N} \quad (2.2)$$

$$C(i) = \begin{cases} \frac{1}{\sqrt{2}} & \text{pour } i = 0, \\ 1, & \text{pour } i > 0 \end{cases}$$

et la transformée inverse est donnée par :

$$f(x, y) = \frac{2}{N} C(x) C(y) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u, v) \cos \frac{(2x+1)u\pi}{2N} \times \cos \frac{(2y+1)v\pi}{2N} \quad (2.3)$$

Alors, la matrice de la DCT de taille 8×8 est donnée par T .

$$T = \begin{bmatrix} 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 \\ 0.4904 & 0.4157 & 0.2778 & 0.0975 & -0.0975 & -0.2778 & -0.4157 & -0.4904 \\ 0.4619 & 0.1913 & -0.1913 & -0.4619 & -0.4619 & -0.1913 & 0.1913 & 0.4619 \\ 0.4157 & -0.0975 & -0.4904 & -0.2778 & 0.2778 & 0.4904 & 0.0975 & -0.4157 \\ 0.3536 & -0.3536 & -0.3536 & 0.3536 & 0.3536 & -0.3536 & -0.3536 & 0.3536 \\ 0.2778 & -0.4904 & 0.0975 & 0.4157 & -0.4157 & -0.0975 & 0.4904 & -0.2778 \\ 0.1913 & -0.4619 & 0.4619 & -0.1913 & -0.1913 & 0.4619 & -0.4619 & 0.1913 \\ 0.0975 & -0.2778 & 0.4157 & -0.4904 & 0.4904 & -0.4157 & 0.2778 & -0.0975 \end{bmatrix};$$

Par contre, la matrice de la DCT entière, en anglais integer DCT (intDCT), de taille 8×8 est donnée par T_i .

$$Ti = \begin{bmatrix} 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \\ 10 & 9 & 6 & 2 & -2 & -6 & -9 & -10 \\ 10 & 4 & -4 & -10 & -10 & -4 & 4 & 10 \\ 9 & -2 & -10 & -6 & 6 & 10 & 2 & -9 \\ 8 & -8 & -8 & 8 & 8 & -8 & -8 & 8 \\ 6 & -10 & 2 & 9 & -9 & -2 & 10 & -6 \\ 4 & -10 & 10 & -4 & -4 & 10 & -10 & 4 \\ 2 & -6 & 9 & -10 & 10 & -9 & 6 & -2 \end{bmatrix};$$

L'avantage de la intDCT par rapport à la DCT est qu'elle n'exige dans son implémentation que des additions et des décalages de bits. La transformation bidimensionnelle d'un bloc B de taille 8×8 de l'image par la DCT où la intDCT est exprimée comme :

$$F = T * B * T^{-1} \text{ ou } Fi = Ti * B * Ti^{-1}$$

Dans ce qui suit, toutes les discussions qui considèrent la DCT sont également valable pour intDCT.

Une mesure pour les informations de textures à l'intérieur de chaque bloc basée sur l'énergie des coefficients AC , est donnée par :

$$P_T = \log \left(\sum_{i=1}^{63} v_i^2 - v_0^2 \right) \quad (2.4)$$

où

$$v_i = 0, 1, \dots, 63 \quad \text{sont les 64 coefficients DCT d'un bloc } 8 \times 8.$$

Il faut noter que v_0 est la valeur de la composante continue des coefficients DCT et qu'elle n'est pas prise en compte lors du calcul de la valeur de texture. Nous avons calculé les valeurs de P_T normalisées pour chaque bloc par la formule suivante :

$$M_T = \frac{64 \times P_T}{\max(P_T)} \quad (2.5)$$

Ainsi pour une image de taille 512×512 , nous aurons une matrice de taille 64×64 où chacune de ces valeurs corresponde aux informations de texture de chaque bloc 8×8 .

Nous avons utilisé l'algorithme de *Peter Kovesi* donné dans [37] pour extraire les informations des contours à partir du plan binaire des contours, les informations normalisées des contours pour chaque bloc sont calculées par :

$$M_E = \frac{64 \times P_E}{\max(P_E)} \quad (2.6)$$

où P_E est le cardinal d'un ensemble de pixels formant le contour dans chaque bloc, tandis que $\max(P_E)$ est la valeur maximale de P_E .

Nous allons utiliser le même l'algorithme de *Peter Kovesi* pour calculé les informations normalisées des coins pour chaque bloc de l'image en utilisant la formule suivante :

$$M_C = \frac{64 \times P_C}{\max(P_C)} \quad (2.7)$$

où P_C est le cardinal du groupe de pixels déterminent les coins de chaque bloc.

$\max(P_C)$ est la valeur maximale de P_C de tous les blocs dans l'image et M_C est la valeur normalisée de l'information des coins.

Dans le domaine DCT, la valeur de la luminance dans un bloc est estimée par :

$$D_L = \left\{ \frac{DC_b}{DC_{mean}} \right\}^\alpha \quad (2.8)$$

où DC_b est la composante continue DC du bloc b .

DC_{mean} la moyenne des coefficients DC de tous les blocs.

α est le paramètre qui est utilisé pour contrôler la sensibilité à la luminance.

La valeur de α est égale à 0,649 selon le model utilisé par les auteurs [23].

Dans le domaine spatial, nous allons calculer la luminance des pixels pour chaque bloc 8×8 par la formule suivante :

$$M_L = \frac{P_L}{64} \quad (2.9)$$

où P_L est la somme de toutes les valeurs de pixels dans le bloc.

M_L est la moyenne des valeurs de pixels à l'intérieur du bloc considéré.

Après l'obtention des quatre valeurs qui correspondent aux informations de textures, contours, coins et luminance, nous allons générer le masque initial du *JND* en utilisant l'expression suivante :

$$J_I = M_T - \frac{1}{2}(M_E + M_C) \quad (2.10)$$

Le système visuel humain est plus sensible aux changements de l'intensité dans la région mi-gris. Cette sensibilité diminuée paraboliquement aux deux extrémités de l'échelle de gris [36]. Une correction de la valeur initiale du masque initial J_I est introduite d'où la valeur finale du *JND* pour chaque bloc est donnée par :

$$J_F = J_I + (128 - M_L)^2 \quad (2.11)$$

J_I est la valeur initiale du paramètre JND .

J_F est la valeur finale du paramètre JND .

Une autre méthode pour calculer le masque final du J_F consiste à multiplier le facteur de la luminance D_L avec la valeur du masque initial J_I générée au-dessus et le coefficient DCT, au moment de l'insertion de la marque [36].

2.4.2 Algorithme d'insertion

L'insertion de la marque est effectuée dans le domaine DCT en modifiant les coefficients DCT sélectionnés, qui embarque une séquence pseudo-aléatoire pour chaque bloc en fonction de la marque. La valeur du JND contrôle la force d'insertion de la marque pour chaque bloc.

Les résultats expérimentaux ont montrés que l'insertion de la marque dans les composantes de hautes fréquences portant l'information est moins perceptible, résulte l'élimination de la marque à travers les attaques de compression et de bruit. Tandis que l'ajout de la marque dans les composantes de basses fréquences, qui porte une perception importante de l'information, entraîne des changements visibles dans l'image tatouée [39].

Dans le système proposé par [36], les coefficients DCT qui se trouvent dans la bande de fréquences moyennes sont uniquement sélectionnés et modifiés. La localisation de ces coefficients dans un bloc 8×8 est représentée par la figure (2.3).

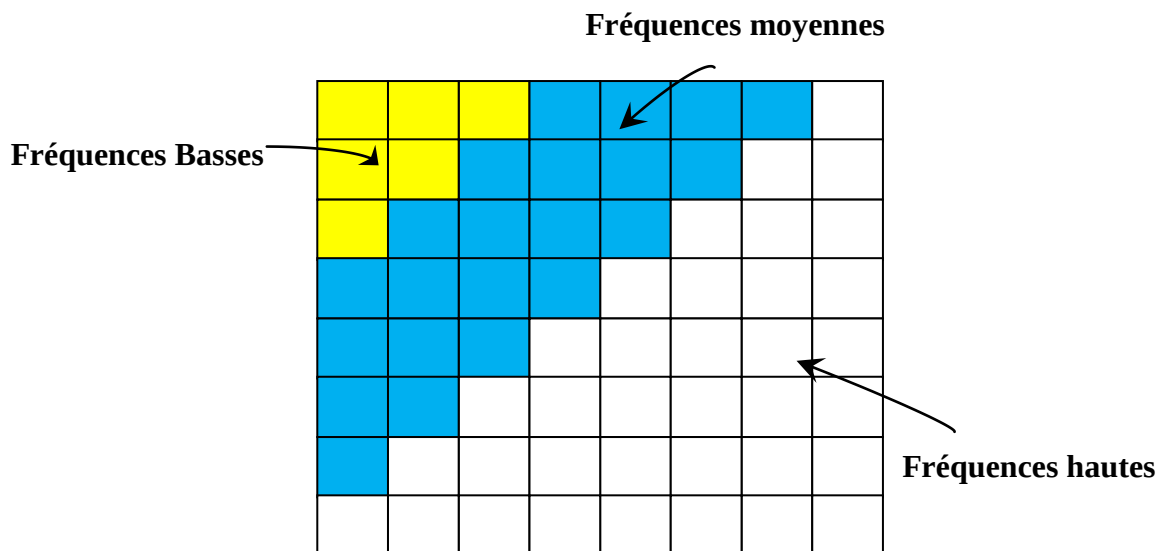


Figure (2.3) : Définition des régions DCT

Pour chaque bloc DCT de taille 8×8 , la séquence pseudo-aléatoire est multipliée par un facteur scalaire et le masque JND est ajouté aux composantes moyennes fréquences tandis que les coefficients de basses et hautes fréquences restent inchangés.

Le facteur scalaire indique la force d'insertion de la marque et il peut être utilisé pour contrôler la robustesse et la qualité de l'image.

Lors de la transformation DCT inverse la marque sera dispersée sur toute l'image et on obtient l'image tatouée. L'insertion de la marque est réalisée en utilisant les formules (2.12) et (2.13).

Marque bit = '0'

$$I_w(u, v, b) = \begin{cases} I(u, v, b) + (\beta \times J_F(b) \times d) & u, v \in F_{mid} \\ I(u, v, b) & u, v \notin F_{mid} \end{cases} \quad (2.12)$$

Marque bit = '1'

$$I_w(u, v, b) = \begin{cases} I(u, v, b) - (\beta \times J_F(b) \times d) & u, v \in F_{mid} \\ I(u, v, b) & u, v \notin F_{mid} \end{cases} \quad (2.13)$$

où

$I_w(u, v, b)$ est le coefficient DCT modifié dans un emplacement (u, v) de bloc b ;

$I(u, v, b)$ est le coefficient DCT dans un emplacement (u, v) de bloc b ;

β est le facteur scalaire ;

$J_F(b)$ est la valeur du *JND* généré pour le bloc b ;

d est la séquence pseudo-aléatoire ;

F_{mid} est la bande de fréquences moyennes du bloc DCT de taille 8×8 .

Enfin, nous obtenons l'image finale tatouée en appliquant la transformée DCT inverse.

2.4.3 Algorithme d'extraction

Afin de récupérer la marque, un système de détection de la marque basé sur la corrélation est utilisé. Premièrement l'image est transformée en DCT et décomposée en blocs de même taille 8×8 comme c'est fait dans la phase d'insertion. Les valeurs des coefficients DCT moyennes fréquences ainsi obtenues sont comparées avec la séquence pseudo-aléatoire générée.

$$\text{Correlation } C(b) = \frac{1}{N} (I^*(b) \times d(b)) \quad (3.12)$$

$$\text{Marque bit détecté} = \begin{cases} 0 & \text{si } C(b) > T \\ 1 & \text{si } C(b) < T \end{cases} \quad (3.13)$$

où T est le niveau de seuil ;

$C(b)$ est la valeur de corrélation du bloc b ;

I^* est le coefficient DCT de l'image tatouée supposé avoir été modifié par une attaque ou un traitement ;

$d(b)$ est la séquence pseudo-aléatoire générée dans la phase d'insertion.

Il faut être conscient que la détermination de la présence d'une marque à travers la corrélation est un test statistique et par conséquent il est possible d'avoir des erreurs de détection.

Les erreurs peuvent être de deux types '0' détectés comme '1' et '1' détecté comme '0'. Le réglage du seuil T est considéré comme une décision nécessaire pour minimiser les erreurs, telles que celles mentionnées ci-dessus, dans la détection de la marque.

Les résultats du schéma de tatouage sont présentés dans la partie suivante. Certaines attaques de tatouage sont appliquées afin de tester les performances du système de tatouage présenté.

2.5 Implémentation de la méthode

Nous allons implémenter la méthode de tatouage sous MATLAB . Nous allons utiliser deux images de test aux niveaux de gris de taille 512×512 qui sont l'image *Lena* et *Boat* présentées dans la figure (2.4).



(a)



(b)

Figure (2.4) : Images originales de test: (a) Image *Lena*, (b) Image *Boat*

Le facteur scalaire β choisi expérimentalement est égale à 0,1 pour l'image *Lena* et 0,4 pour *Boat*. La marque à insérer dans les images hôtes est de taille 16×16 illustrée dans la figure (2.5).

Figure (2.5) : Marque originale de taille 16×16

2.5.1 Résultats de simulation

Nous avons effectué la simulation sur deux images de test présentées précédemment. Les images tatouées sont données dans les figures (2.6) et (2.7).



(a)



(b)

Figure (2.6) : Images tatouées en utilisant la DCT : (a) Image *Lena*, (b) Image *Boat*

(a)



(b)

Figure (2.7) : Images tatouées en utilisant la DCT entière : (a) Image *Lena*, (b) Image *Boat*

Nous avons utilisé les métriques données par les expressions (1.12)-(1.16) pour évaluer la méthode de tatouage.

La figure (2.8) montre la variation du $wPSNR$ en fonction du facteur scalaire β pour les images *Lena* et *Boat*.

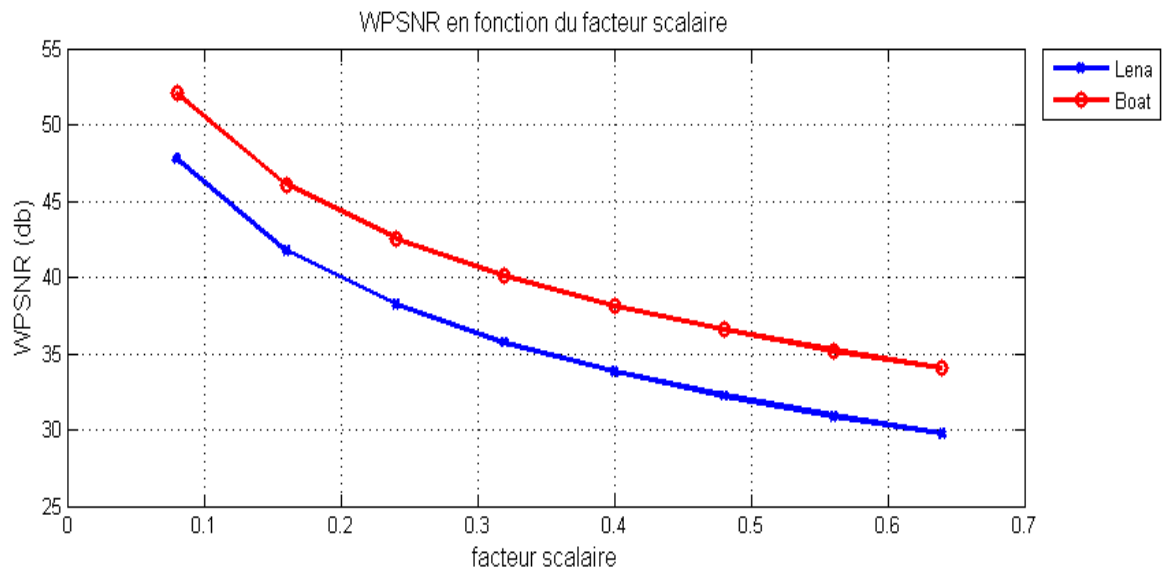


Figure (2.8) : Variation $wPSNR$ en fonction du facteur scalaire β

D'après la figure (2.8), nous constatons que l'écart entre les deux courbes est presque constant. La valeur de l'écart est traduite par la différence dans les valeurs du JND due au contenu des deux images. Pour un facteur scalaire donné, le $wPSNR$ de l'image *Boat* tatouée est de 35,54 db, mais pour la même valeur du facteur scalaire β l'image *Lena* tatouée est énormément déformée.

Les valeurs du masque JND pour deux lignes sélectionnées de façon aléatoire pour l'image *Lena* sont représentées aux figures (2.9) et (2.10). Ces figures indiquent les valeurs maximales des poids d'insertion de la marque qui doivent être ajoutées à l'image hôte sans avoir des distorsions visibles.

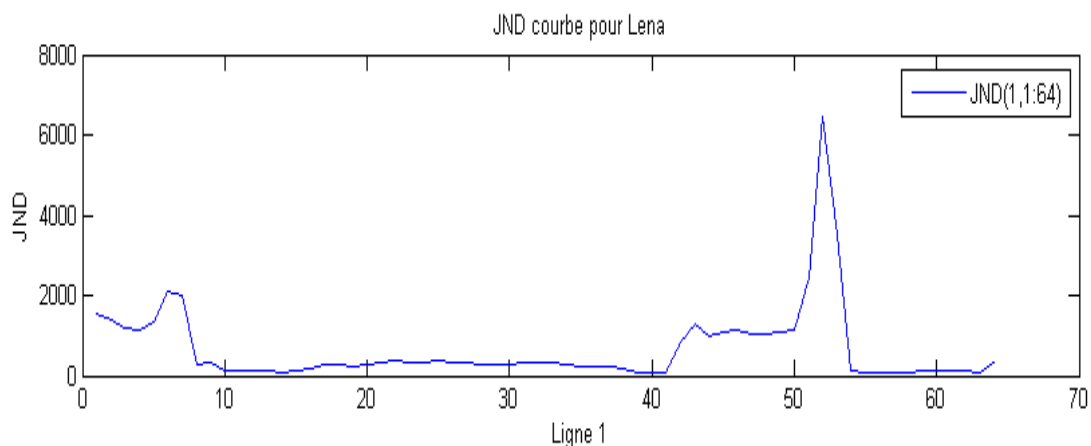
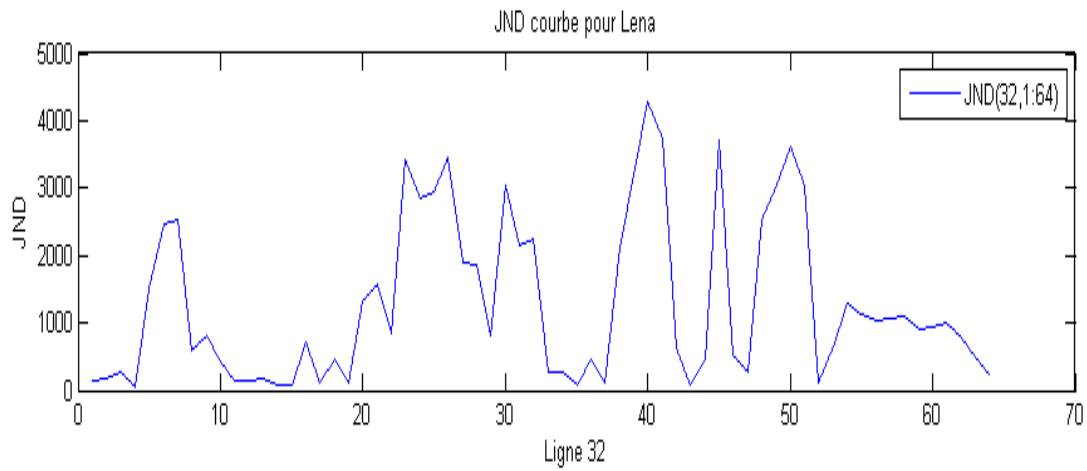
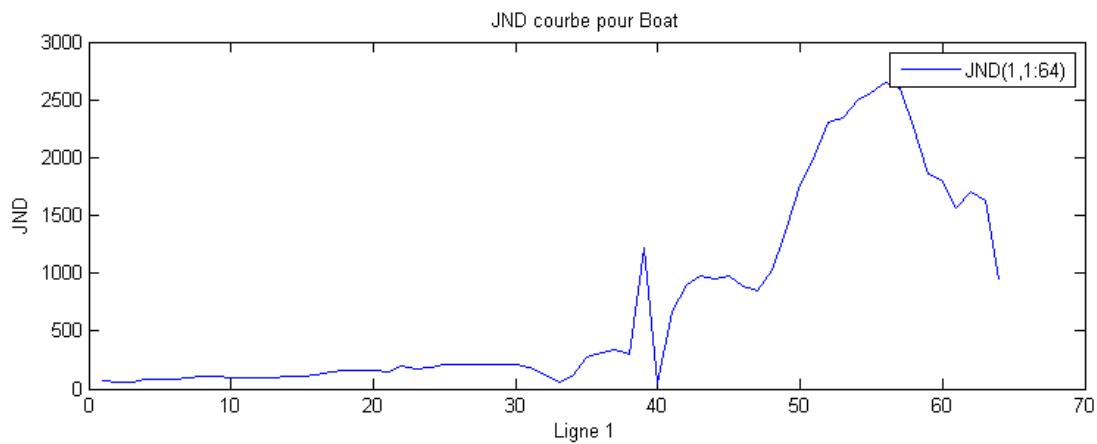
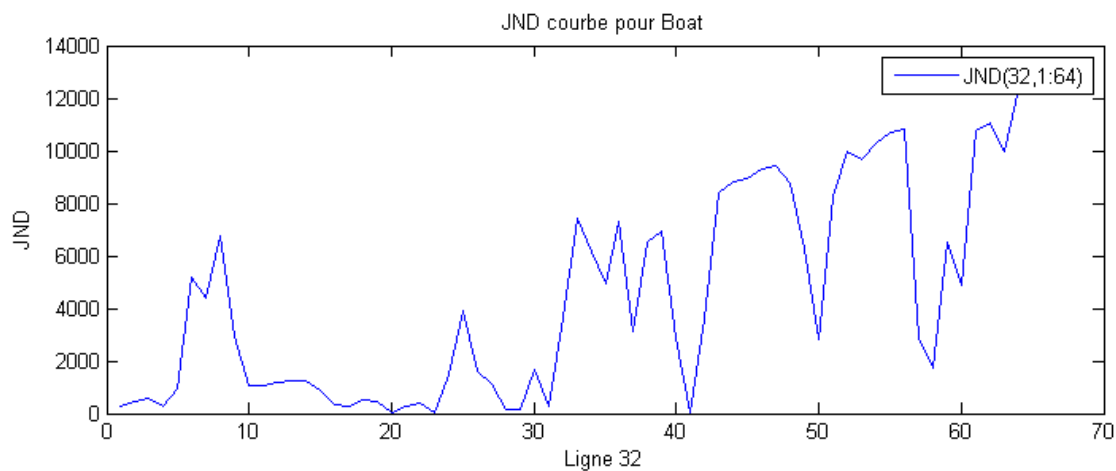


Figure (2.9) : Les valeurs JND pour *Lena* (ligne 1)

Figure (2.10) : Les valeurs JND pour *Lena* (ligne 32)

Une courbe similaire pour les deux lignes de l'image *Boat* est représentée par les figures (2.11) et (2.12). Il est clair que les valeurs du JND sont grandes pour *Lena* et *Boat* à la ligne 32 et donc on peut insérer plus d'informations de la marque dans ces régions.

Figure (2.11) : Les valeurs JND pour *Boat* (ligne 1)Figure (2.12) : Les valeurs JND pour *Boat* (ligne 32)

Pour tester la robustesse de la méthode implémentée, nous avons appliqué sur l'image *Lena* taouée plusieurs attaques telles que la compression, l'ajout de bruit, filtrage et cropping.

Le tableau (2.1) montre les résultats de l'évaluation en terme de *NC* de la marque extraite pour le cas de l'image de test *Lena*.

Tableau (2.1) : Evaluation en terme *NC* de la marque extraite

Attaques	Paramètres	<i>NC</i>
Bruit Salt&Pepper	1%	0.9962
	2%	0.9808
	3%	0.9692
	4%	0.9421
Bruit Gauss	0.5%	0.9923
	1%	0.9554
	1.5%	0.9405
	2%	0.8808
	2.5%	0.8882
Filtre median	3x3	0.7805
	5x5	0.7238
	7x7	0.7224
Filtre Average	3x3	0.8460
	5x5	0.7079
	7x7	0.7049
Filtre Gauss	3x3	0.8830
	5x5	0.7166
	7x7	0.7049
Cropping	1/8	1
	1/4	0.9925
	1/2	0.8965
Compression JPEG	35%	0.9708
	40%	0.9887
	45%	0.9962
	50%	0.9962
	55%	0.9962
	60%	1

2.5.2 Discussions des résultats

L'image tatouée compressée par différents facteurs de qualité q allant de 35% à 50% sont représentés dans la figure (2.13) avec la marque extraite. On constate que ce système de tatouage est robuste contre la compression JPEG pour des facteurs de qualité supérieurs à 40%.

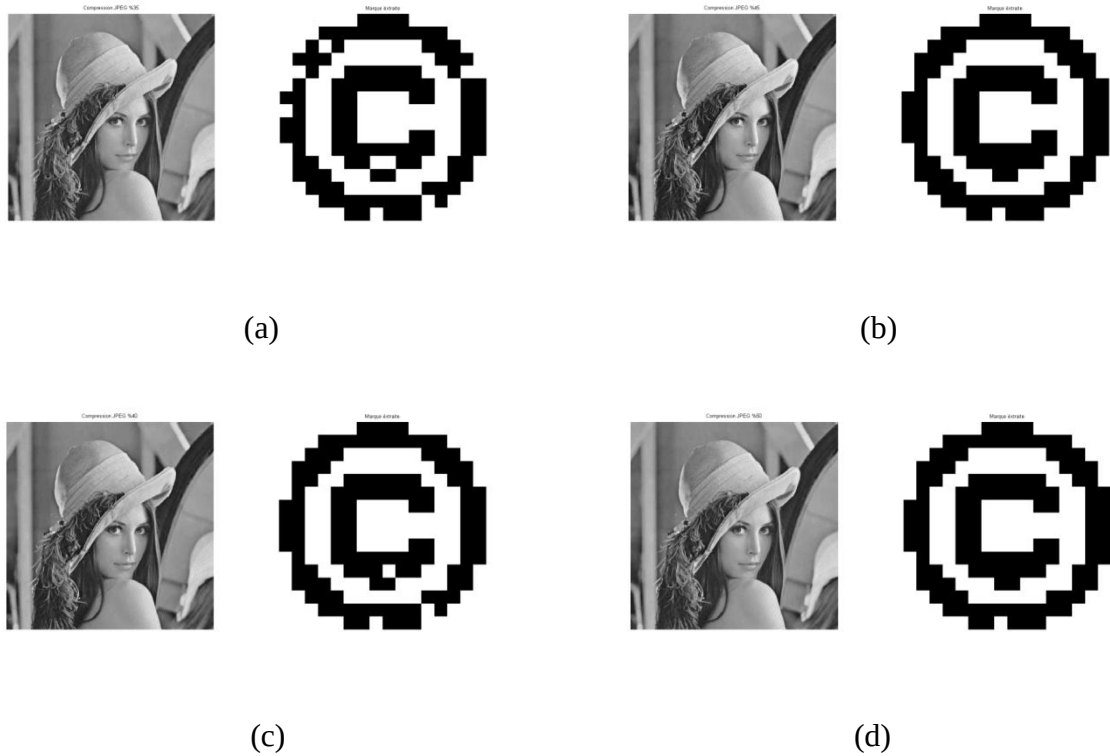


Figure (2.13) : Compression JPEG : (a) $q = 35$ (b) $q = 40$ (c) $q = 45$ (d) $q = 50$.

Nous avons ensuite introduit deux types de bruit, le premier est de type gaussien de moyenne nulle et le deuxième est de type bruit Salt&Pepper dans l'image tatouée pour vérifier à quel point le système est robuste. D'après les résultats représentés dans les figures (2.14) et (2.15), nous pouvons observer que pour un bruit gaussien de 2%, la récupération de la marque est moyenne, et pour un bruit gaussien de 1% la récupération est bonne avec très peu d'erreurs de détection. Concernant l'ajout du bruit Salt&Pepper, la récupération de la marque est très bonne pour 1% et 2% et acceptable pour 3% et 4%.

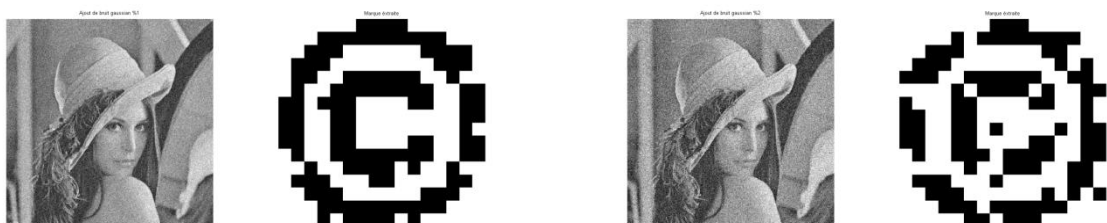


Figure (2.14) : Bruit Gaussien : (a) 1% (b) 2%.

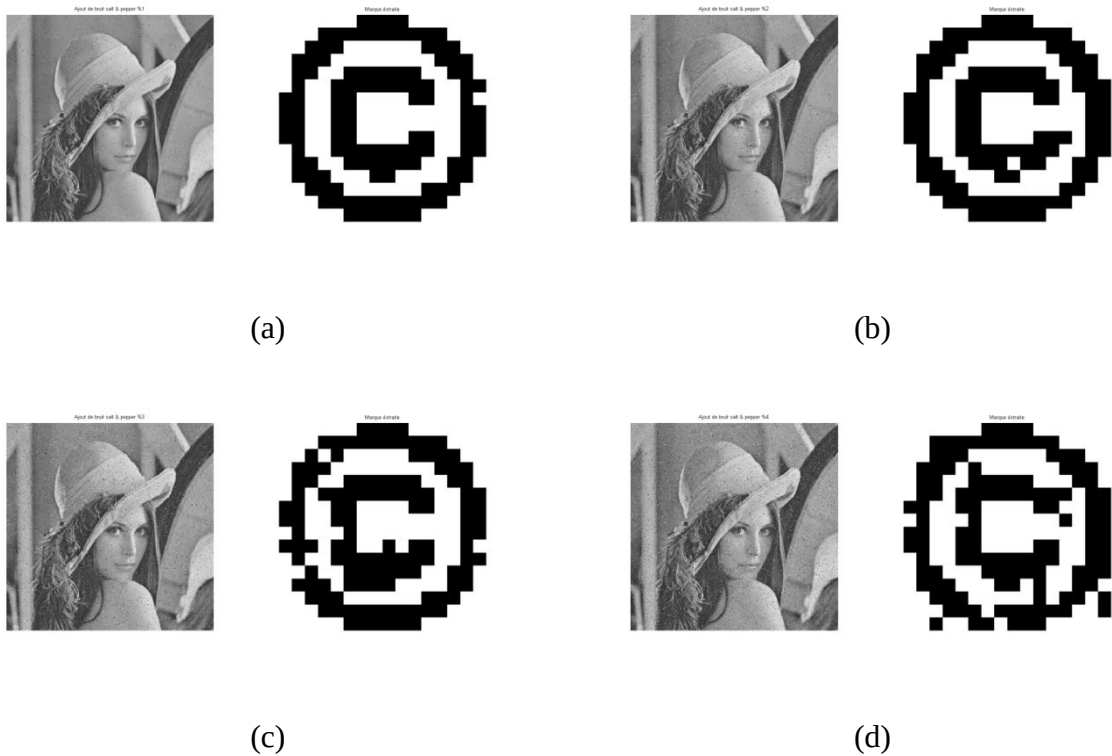


Figure (2.15) : Bruit Salt&Pepper (a) 1% (b) 2% (c) 3% (d) 4%

Nous avons appliqué une autre attaque sur l'image tatouée qui est le cropping. Comme nous pouvons le voir, la marque a été récupérée parfaitement pour un facteur de cropping $\frac{1}{4}$ et moins bonne pour $\frac{1}{2}$ à l'exception de quelques erreurs de détection, voir la figure (2.16).

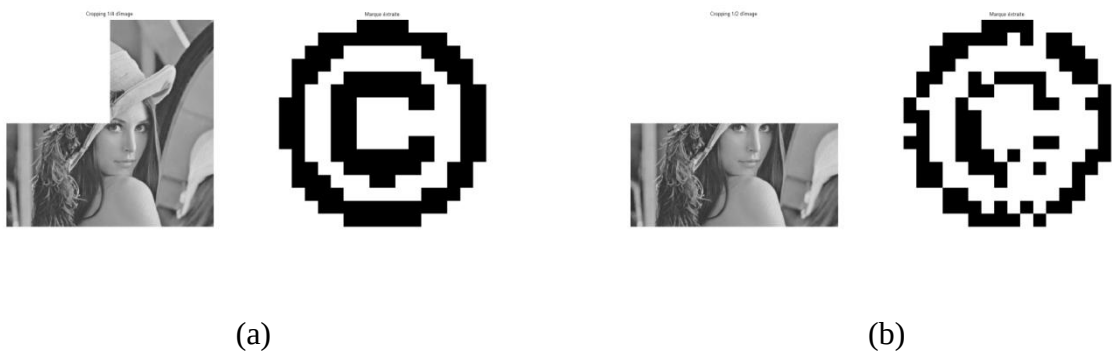


Figure (2.16) : Cropping : (a) $\frac{1}{4}$, (b) $\frac{1}{2}$

Nous avons appliqué une dernière attaque sur l'image tatouée qui est le filtrage. Nous avons testé la robustesse du système de tatouage par trois types de filtre, Gauss, médian et moyenneur (average).

La figure (2.17) montre l'extraction de la marque pour l'image tatouée filtrée par le filtre de Gauss. Comme nous pouvons le voir, le système implémenté est moins robuste au filtrage.



Figure (2.17) : Filtrage Gaussien 3×3 .

2.8 Conclusion

Dans ce chapitre, nous avons implémenté un système de tatouage existant basé sur le contenu de l'image. Nous avons aussi analysé l'image hôte dans le domaine spatial et fréquentiel afin d'obtenir les propriétés de l'image telles que textures, coins, contours et luminance. Ces propriétés sont exploitées, dans ce travail, dans la détermination d'un masque visuel de valeur inférieure à la distorsion juste perceptible (*JND*). Cette valeur qui dépend du contenu de l'image hôte détermine le poids d'insertion de la marque dans l'image hôte.

En se basant sur le *wPSNR* pour évaluer avec précision la qualité perceptuelle de l'image tatouée en tenant compte de l'effet du HVS. Les résultats de simulation montrent que le système implémenté globalement présente un bon compromis entre la robustesse et l'imperceptibilité.

Les performances de ce système de tatouage sont obtenues grâce à l'utilisation du masque visuel, alors nous allons exploiter ce masque dans le chapitre suivant pour développer un nouveau algorithme de tatouage multi-bit plus efficace.

3.1 Introduction

Selon des recherches récentes, l'un des méthodes importantes du tatouage d'images est l'étalement du spectre dans le domaine fréquentiel.

Le tatouage d'images par étalement du spectre est proposé pour la première fois par Cox et Kilian [2]. Les auteurs proposent une insertion dans le domaine de la DCT appliquée à l'image complète pour une robustesse à la compression avec perte et au changement d'échelle. Leur algorithme a cependant recours à une comparaison avec l'image originale pour extraire la marque, il est non aveugle. Les auteurs [9] ont proposés une méthode de tatouage similaire à celle de [2] mais de type aveugle et l'insertion est appliquée dans le domaine de la DCT par bloc 8×8 . Ce type d'insertion permet donc une meilleure résistance à la compression JPEG.

Dans [51], les auteurs ont proposé une méthode d'insertion et d'extraction de la marque dans le domaine fréquentiel avec information adjacente. Ils ont utilisé la méthode de codage en treillis pour avoir une marque étendue vise à obtenir des performances meilleures, mais le nombre de vecteurs utilisés dans le dictionnaire de code est supérieur à la longueur de chaque vecteur. Ils ne peuvent pas éliminer directement les corrélations entre les différents vecteurs, c'est l'un des raisons à laquelle l'algorithme proposé est inefficace.

Les auteurs de [52]-[53] ont utilisé la technique d'étalement de spectre pour concevoir et réaliser d'autres nouveaux algorithmes de tatouage. Dans leurs travaux, un message multi-bits est élargi à un autre type d'étalement de spectre, le message élargi est inséré dans un vecteur caractéristique extrait du domaine spatial de l'image, l'essentiel du travail qu'ils ont fait est de calculer le poids d'insertion de manière adaptative dans toutes les positions. L'inconvénient de cette méthode est la grande complexité de calcul pour obtenir la matrice inverse utilisée pour calculer les poids d'insertion. D'ailleurs, cette matrice inverse peut parfois, voire inexistante, dans ce cas, l'algorithme va échouer.

Les auteurs de [9] ont proposé une méthode de tatouage multi-bit dont l'insertion de la marque est basée sur l'étalement de spectre dans le domaine de la DCT. Ils ont proposé de placer des clés privées pour déterminer les positions de la marque ou bien pour générer un dictionnaire de code aléatoire. Pour améliorer l'imperceptibilité de la marque, ils ont proposé aussi d'utiliser un masque perceptuel afin d'améliorer les performances de l'algorithme.

Dans ce chapitre, nous proposons un nouveau système de tatouage d'images afin d'améliorer davantage le système proposé par Guan [9]. Alors, nous décrivons premièrement l'algorithme de [9].

3.2 Algorithme de tatouage développé dans [9]

Dans cette section, nous décrivons en détail l'algorithme d'insertion et d'extraction de la marque présenté par [9]. La figure (4.1) illustre le schéma bloqué de l'algorithme de tatouage.

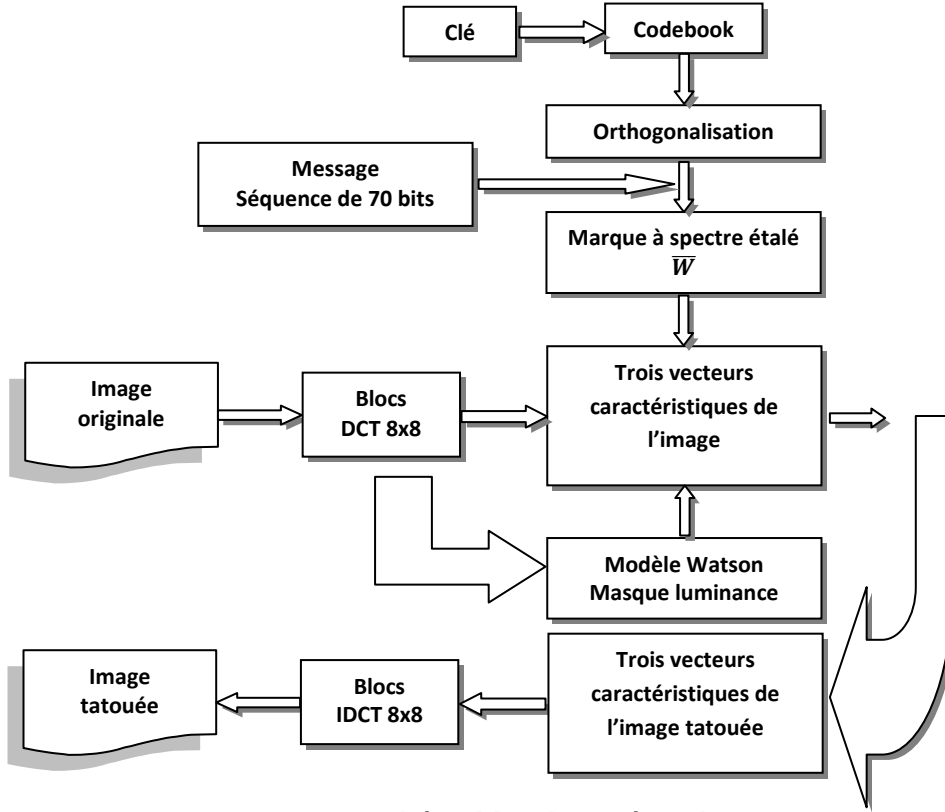


Figure (3.1) : Schéma bloc du système de tatouage

3.2.1 Génération de la marque

3.2.1.1 Mise en forme du message à inséré

Considérant un message m codé par une séquence multi-bit B de longueur N

$$B = [b_1, b_2, \dots, b_N], \quad b_i \in \{0,1\} \quad (3.1)$$

La séquence multi-bit B est transformée à une séquence antipodale $\bar{B}$

$$\bar{B} = [\bar{b}_1, \bar{b}_2, \dots, \bar{b}_N], \quad \text{avec} \quad \bar{b}_i = (2 \times b_i) - 1 \quad (3.2)$$

Ce qui résulte que $\bar{b}_i \in \{-1, +1\}$, c'est cette séquence qui va être étalée dans le spectre de l'image originale.

3.2.1.2 Génération du dictionnaire de codes (codebook)

Comme le montre la figure (3.1), pour obtenir le vecteur de la marque $\bar{W}$ de longueur M portant le message $\bar{B}$ de N bits, nous construisons un dictionnaire de codes (codebook) P de N codes.

$$P = [\bar{P}_1, \bar{P}_2, \dots, \bar{P}_N], \quad \bar{P}_i \in \{0,1\} \quad (3.3)$$

Chaque code $\bar{P}_i$ est une séquence de nombres pseudo-aléatoires de longueur M .

Premièrement, un dictionnaire qui possède N codes de longueur M tel que $(M > N)$ est généré à l'aide d'une clé privée.

Comme c'est mentionné ci-dessus, N a la même valeur que la longueur du message original m . La longueur M peut être calculé selon la taille de l'image originale $f(x, y)$.

3.2.1.3 Orthogonalité de Gram-Schmidt

D'après [53], la non orthogonalité entre les séquences pseudo-aléatoires générées pour former le codebook est due aux interférences inter-symboles. Cette non-orthogonalité peut influencer sur l'efficacité du système de tatouage dans la phase de détection de la marque.

Pour remédier à ce problème on fait appel à l'algorithme d'orthogonalité de *Gram-Schmidt*, de cette manière la corrélation entre une paire de codes choisis aléatoirement est éliminée.

Procédé d'orthogonalisation de Gram-Schmidt

Soit $\mathcal{E}$ un espace vectoriel euclidien de dimension finie ($n > 0$) et $E = \{e_1, e_2, e_3, \dots, e_n\}$ une base de $\mathcal{E}$. On construit une base orthogonale $V = \{v_1, v_1, v_1, \dots, v_n\}$ de $\mathcal{E}$ par récurrence, selon un procédé appelé le procédé d'orthogonalisation de *Gram-Schmidt*, comme suit :

- On pose $v_1 = \frac{e_1}{\|e_1\|}$

- On définit alors v_{j+1} par :
$$v_{j+1} = \frac{e_{j+1} - \sum_{k=1}^j \langle e_{j+1}, v_k \rangle \cdot v_k}{\|e_{j+1} - \sum_{k=1}^j \langle e_{j+1}, v_k \rangle \cdot v_k\|} \quad (3.4)$$

3.2.1.4 Génération de la marque à spectre étalé

Suivant l'équation (3.5) la séquence $\bar{B}$ de N bits est étalé dans une séquence de M dimensions qui correspond au vecteur de la marque finale $\bar{W}$ à insérée. Le facteur gain α détermine l'amplitude de la marque $\bar{W}$.

$$\bar{W} = \alpha \cdot \sum_{i=1}^N \bar{B}_i \cdot \bar{P}_i \quad (3.5)$$

où $\bar{P}_i$ est le vecteur i -ème du codebook.

α est la force d'insertion globale.

3.2.2 Masques visuels de Watson

Deux caractéristiques majeures du système visuel humain sont exploitées par le modèle de Watson, le masque de luminance et le masque de contraste [54].

Le masque de luminance se réfère au fait qu'un coefficient DCT peut tolérer plus de changement avant d'être remarqué si l'intensité moyenne du bloc 8×8 est plus lumineuse. Cet effet de masque de luminance est décrit par

$$T^k(x, y) = T^*(x, y) \cdot \left(\frac{I^k(0,0)}{\bar{I}_{0,0}} \right)^{0.649} \quad (3.6)$$

où

T^* est la table de sensibilité de fréquence ;

$I^k(0,0)$ est la composante continue DC du k -ème DCT bloc ;

$\bar{I}_{0,0}$ est la moyenne des composantes continues de tous les blocs DCT.

La table de sensibilité de fréquence T^* est donnée par

$$T^* = \begin{bmatrix} 9.6 & 9.6 & 4.2 & 4.7 & 6.6 & 10.1 & 15.9 & 24.9 \\ 11.3 & 8.0 & 5.0 & 5.4 & 7.3 & 11.0 & 16.9 & 26.1 \\ 4.3 & 5.2 & 6.2 & 7.3 & 9.5 & 13.5 & 20.0 & 30.0 \\ 4.4 & 5.2 & 7.3 & 9.8 & 13.0 & 17.9 & 25.5 & 36.9 \\ 5.9 & 6.7 & 9.2 & 12.9 & 17.8 & 24.4 & 33.7 & 47.3 \\ 8.7 & 9.6 & 12.4 & 17.2 & 23.9 & 32.9 & 45.1 & 62.1 \\ 13.2 & 14.2 & 17.5 & 23.4 & 32.1 & 44.1 & 60.2 & 81.8 \\ 20.0 & 21.3 & 25.3 & 32.5 & 43.6 & 59.1 & 79.9 & 107.6 \end{bmatrix} \quad (3.7)$$

Le masque de contraste se réfère à la réduction de la visibilité d'un changement d'une fréquence en raison de l'énergie présente dans cette fréquence. La valeur du masque global $M^k(x, y)$ est donnée par l'expression

$$M^k(x, y) = \max(|T^k(x, y)|^{0.7} \cdot T^k(x, y)^{0.3}) \quad (3.8)$$

où $M^k(x, y)$ mesure la perceptibilité du HVS à des changements dans des formulations individuelles de k -ième bloc DCT.

Le masque de Watson calculé par (3.6) pour l'image *Lena* est illustré dans la figure (3.2).



(a)

Figure (3.2) : Masque de luminance de Watson pour l'image de test *Lena*.

3.2.3 Insertion de la marque

Le niveau de gris des pixels pour l'image originale de taille $N_1 \times N_1$ est exprimé par une fonction à deux dimensions $f(x, y)$ tel que : $x, y = 0, 1, 2, \dots, N_1 - 1$. L'image $f(x, y)$ est divisée en blocs $f_q(i, j)$ avec $0 \leq i, j \leq 7$ et $q = 1, 2, \dots, (N/8)^2$.

Après la génération de la marque $\bar{W}$ à spectre étalé, $\bar{W}$ est insérée dans les coefficients de la DCT. Premièrement, l'image originale est divisée en blocs de taille 8×8 ensuite chaque bloc est transformé par la DCT. Deuxièmement, trois vecteurs caractéristiques de l'image originale, de longueur M (la même que la longueur des vecteurs du dictionnaire de codes), constitués de coefficients AC dans des emplacements spécifiques (voir la figure (3.3)) sont extraits.

DC		3					
	2						
1							

Figure (3.3) : Emplacements des coefficients AC choisis par bloc DCT 8×8

L'auteur [46] a calculé les paramètres visuels perceptifs V de *Watson* en utilisant la méthode décrite dans la section (3.2.3), avec la même taille que l'image originale, pour ajuster la force d'insertion de manière adaptative dans différentes positions afin d'avoir une meilleur invisibilité.

La marque est insérée dans les trois vecteurs caractéristiques de l'image par l'expression

$$C' = C + \alpha \times V^* \times \bar{W} \quad (3.9)$$

où

V^* est la valeur du paramètre perceptuel de *Watson* dans la position où le coefficient AC est choisi.

α est la force d'insertion globale de la marque, une valeur appropriée est choisie en fonction du balance de robustesse et imperceptibilité de la marque.

C est le vecteur caractéristique de l'image originale.

C' est le vecteur caractéristique de l'image tatouée.

Troisièmement on obtient l'image taouée par la transformation inverse IDCT appliquée sur les trois vecteurs caractéristiques.

3.2.4 Extraction de la marque

Dans cette section nous décrivons le processus d'extraction de la marque proposé. La figure (3.4) illustre le schéma bloque de l'algorithme d'extraction.

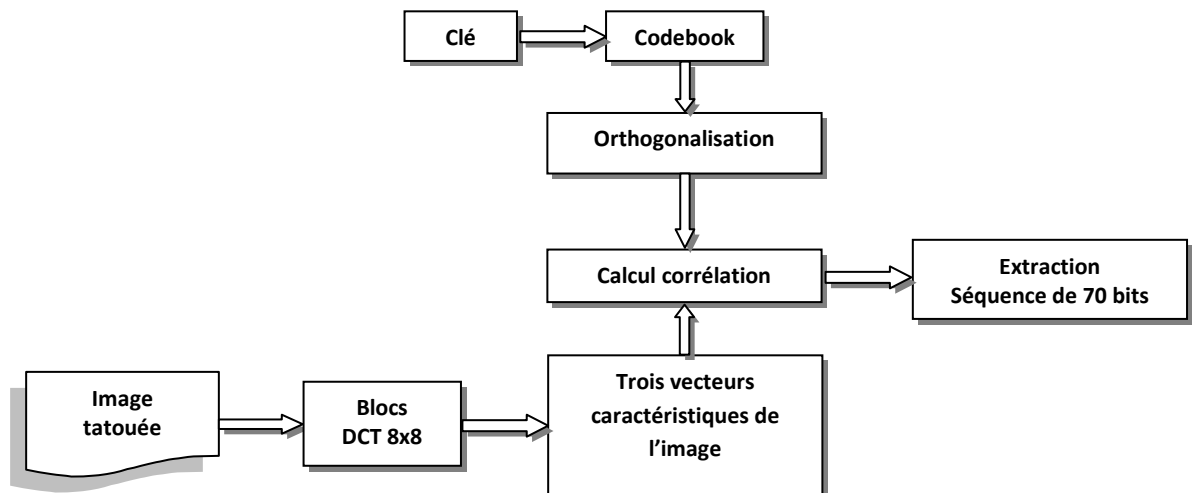


Figure (3.4) : Processus d'extraction de la marque

Le processus d'extraction est similaire au processus d'insertion. Un dictionnaire de code est généré avec la même taille et de la même clé utilisée dans le processus d'insertion, suivi par l'opération d'orthogonalisation de *Gram-Schmidt*.

De la même manière et avec les mêmes positions, trois vecteurs caractéristiques différents sont extraits à partir de l'image tatouée. Ces trois vecteurs sont mentionnés dans le système d'équations (4.4) par C_1 , C_2 et C_3 .

L'opération la plus importante dans le processus d'extraction est le calcul de la corrélation pour obtenir la marque extraite.

$$\begin{cases} N_{1i} = NC(C_1, \bar{P}_i) \\ N_{2i} = NC(C_2, \bar{P}_i) \\ N_{3i} = NC(C_3, \bar{P}_i) \end{cases} \quad i = 1, 2, \dots, N \quad (3.10)$$

où NC est la corrélation entre le vecteur caractéristique de l'image et le vecteur P_i du codebook.

L'auteur [36] a choisi une méthode statistique pour décider sur les valeurs des bits extraits un par un. Le procédé de calcul est donné par les systèmes d'équations (3.11).

Les bits estimés du message $\hat{m}$ est obtenue à l'aide du système d'équations donné par (3.12).

$$\begin{cases} \bar{w}_{-1i} = 1 \text{ si } N_{1i} \geq 0, \\ \bar{w}_{-1i} = 0 \text{ si } N_{1i} < 0, \end{cases} \quad \begin{cases} \bar{w}_{-2i} = 1 \text{ si } N_{2i} \geq 0, \\ \bar{w}_{-2i} = 0 \text{ si } N_{2i} < 0, \end{cases} \quad \begin{cases} \bar{w}_{-3i} = 1 \text{ si } N_{3i} \geq 0, \\ \bar{w}_{-3i} = 0 \text{ si } N_{3i} < 0, \end{cases} \quad (3.11)$$

$$\begin{cases} b'_i = 1, & \bar{w}_{-1i} + \bar{w}_{-2i} + \bar{w}_{-3i} \geq 2 \\ b'_i = 0, & \bar{w}_{-1i} + \bar{w}_{-2i} + \bar{w}_{-3i} \leq 1 \end{cases} \quad i = 1, 2, \dots, N \quad (3.12)$$

où b'_i représente le i -ème bit extrait.

3.3 Méthode proposée

Malgré que la méthode développée par [9] présente une robustesse contre les attaques telles que la compression JPEG, l'ajout de bruit et le filtrage, elle expose une claire dégradation de l'image tatouée. Pour remédier à cet inconvénient, nous proposons d'introduire des modifications intéressantes dans la méthode [9].

Dans cette section, nous présentons le principe de la méthode de tatouage proposée. Dans le processus d'insertion, l'image originale $f(x, y)$ de taille 512×512 est divisée en blocs $f_q(x, y)$ de taille 8×8 , $q = 1, 2, \dots, 4096$. Chaque bloc est transformé en DCT.

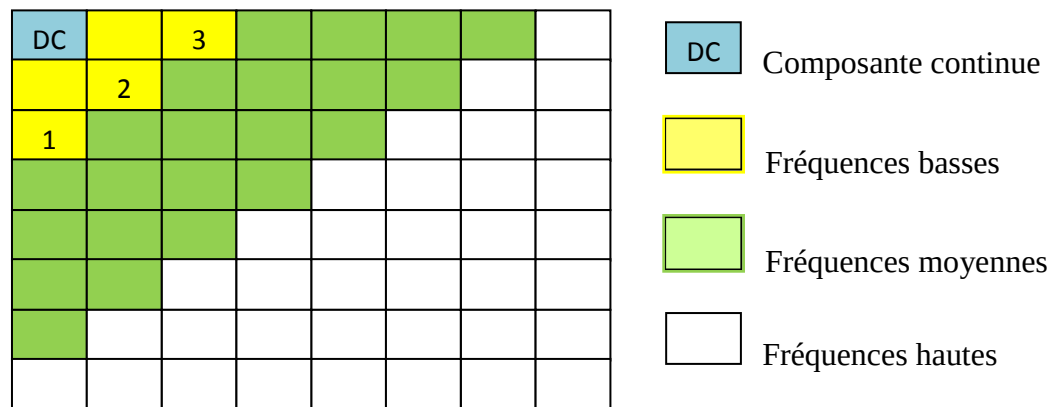


Figure (3.5): Différentes bandes de fréquences dans un bloc DCT 8x8

3.3.1 Choix approprié des coefficients DCT pour l'insertion de la marque

Les résultats expérimentaux présentés dans la littérature montrent que les composantes à basses fréquences représentent les informations des zones uniformes de l'image. L'insertion de la marque dans les composantes à basses fréquences dans un bloc DCT 8×8 va provoquer une distorsion évidente dans l'image tatouée.

Les composantes à moyennes fréquences portent les informations des régions hautes texturées, et l'insertion dans ces zones n'affecte pas la qualité de l'image, et la marque ne sera pas éliminée par la compression JPEG.

Les composantes à hautes fréquences portent les informations sur les détails de l'image, et la marque insérée dans ces régions sera généralement éliminée par les attaques comme la compression JPEG, l'ajout du bruit et le filtrage [35].

Dans la méthode [9] (voir figure (3.5)), la marque est insérée dans trois composantes basses fréquences. Dans notre méthode (voir figure (3.6)), nous proposons d'utiliser une composante basse fréquence afin de garder certaine robustesse et deux composantes moyennes fréquences pour améliorer la qualité visuelle de l'image tatouée.

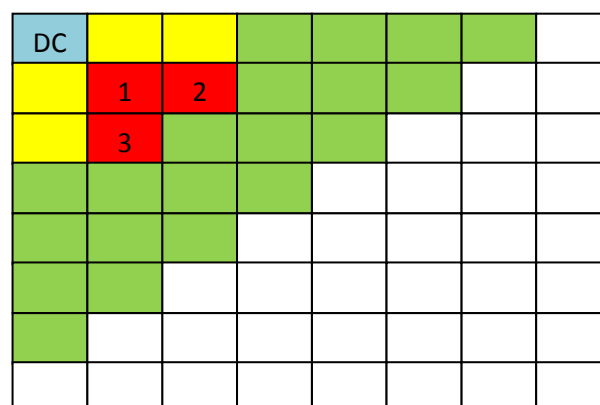


Figure (3.6) : Emplacement des coefficients AC proposés

Les emplacements des composantes DCT choisis sont montrés par la figure (3.6).

Note : Dans ce qui suit ; *Pos1* indique l'emplacement des trois coefficients *AC* d'après la méthode [9] et *Pos2* l'emplacement des trois coefficients *AC* utilisés par notre méthode.

3.3.2 Masques visuels proposés

D'après l'expression d'insertion (3.6) utilisée par [9], on constate qu'il a pris une seule caractéristique qui est la luminance dans la conception du masque visuel, chose qui est insuffisante pour mieux adapter la marque à l'image tatouée.

Un masque visuel utilisé dans la phase d'insertion doit prendre en considération les propriétés suivantes du HVS:

- L'œil est moins sensible au bruit dans les zones fortement texturées;
- L'œil est très sensible aux modifications autour des contours et coins;
- L'œil est moins sensible au bruit dans les zones à haute et faible luminosité [34]-[36].

Dans cette section, nous proposons de changer le masque visuel utilisé par [9] et de le remplacer par un masque qui va prendre en charge les informations de luminance, textures, coins et contours, à partir des expressions (2.10) et (2.11) données au deuxième chapitre. Afin de renforcer l'invisibilité de la marque, les caractéristiques du HVS peuvent être exploitées pour adapter la marque à l'image qui doit d'être tatouée.

3.3.3 Réduction du nombre de blocs altérés

Dans une image, les blocs constituant cette dernière ne comportent pas les mêmes informations perceptuelles, autrement dit la quantité d'informations de textures, contours, coins et luminance change d'un bloc à l'autre. L'algorithme développé par [9] altère tous les blocs pour insérer la marque, ce qui influe gravement la qualité visuelle de l'image.

Donc, nous proposons de sélectionner seulement X blocs parmi les q pour les utilisés dans la phase d'insertion. Mais la question à poser, sur quel critère on va sélectionner ces X blocs ?

Pour répondre à cette question, nous prendrons les blocs qui ont plus d'informations perceptuelles, autrement dit qui ont les valeurs du seuil de perception JND les plus grandes.

3.3.4 Poids d'insertion variable

L'approche du tatouage par étalement du spectre donnée par la formule (3.9) est insuffisante parce qu'elle est limitée à utiliser un seul facteur gain α pour ajuster l'énergie de tous les codes $\bar{P}_i$ constituant la marque $\bar{W}$.

Donnant un facteur gain α fixe, plusieurs codes $\bar{P}_i$ peuvent être introduits avec une d'énergie supérieure à l'énergie minimale nécessaire pour satisfaire les contraintes robustesse et fidélité [52].

Par conséquent, nous proposons de remplacer le facteur gain α fixe par un facteur gain variable α_i . Alors, l'expression pour l'insertion de la marque (3.9) devient :

$$C' = C + (\alpha_i \times \bar{W} \times V^*) \quad (3.17)$$

$$C' = C + \sum_{i=1}^N \alpha_i \cdot B_i \cdot \bar{P}_i \otimes V^* \quad (3.18)$$

$\otimes$ dénote le produit élément par élément des matrices.

Dans la phase d'extraction de la marque, le bit b_i est détecté comme zéro '0' si la décision $d_i < 0$ et vice versa.

La variable de décision d_i est calculée en évaluant la fonction de covariance croisée donnée par (3.19).

$$d_i = \langle \bar{P}_i, C' \rangle \quad (3.19)$$

En substituant C' de (3.18) dans (3.19) on obtient :

$$d_i = \langle \bar{P}_i, C \rangle + \langle \bar{P}_i, \sum_{j=1}^N \alpha_j \cdot B_j \cdot j_i \otimes V^* \rangle \quad (3.20)$$

$$d_i = R_i^C + \sum_{j=1}^N \alpha_j \cdot R_{ij} \quad (3.21)$$

où $R_i^C = \langle \bar{P}_i, c \rangle$ et $R_{ij} = B_j \langle \bar{P}_i, \bar{P}_j \otimes V^* \rangle$.

R_i^C est la corrélation de $\bar{P}$ avec l'image hôte C , et R_{ij} la corrélation croisée entre $\bar{P}_i$ et $\bar{P}_j$ multiplié élément par élément par le masque V^* .

Nous pouvons garantir un niveau de détection spécifique $d_i = \beta b_i$, pour $i = 1, \dots, N$, en résolvant le système d'équations linéaires (3.22), nous obtenons les valeurs du facteur de gain optimal α_j qui assurent l'insertion efficace.

$$\begin{bmatrix} R_{11} & R_{1N} \\ R_{21} & R_{2N} \\ \vdots & \vdots \\ R_{N1} & R_{NN} \end{bmatrix} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} \beta b_1 - R_1^C \\ \beta b_2 - R_2^C \\ \vdots \\ \beta b_N - R_N^C \end{bmatrix} \quad (3.22)$$

où β est la valeur que nous voulons attribuer à la variable de décision d_i .

3.4 Implémentation et comparaison des deux méthodes

Pour évaluer concrètement la qualité de la méthode proposée par rapport à la méthode développée dans [9], nous utilisons deux métriques, le *PSNR* pour estimer la distorsion de l'image hôte tatouée et le coefficient de corrélation normalisés *NC* calculé en utilisant la marque originale et celle extraite, ce coefficient permet de juger l'existence et l'exactitude de la marque extraite.

3.4.1 Choix approprié des coefficients DCT pour l'insertion de la marque

Afin de montrer l'amélioration portée par ce changement d'emplacement, nous avons fixé le $\alpha = 20$ et *PSNR* à 37 db pour les deux positions. Les résultats de simulation sont montrés au tableau (3.1) pour l'image de test *Lena* soumise à diverse attaques.

D'après le tableau (3.1), il est clair que les résultats obtenus confirment l'amélioration portée par le changement de l'emplacement *Pos2* des coefficients DCT choisis pour l'insertion de la marque.

Tableau (3.1) : Evaluation en terme de *NC* pour les deux emplacements *Pos1* et *Pos2*.

Masque de luminance de <i>Watson</i>			
Attaques	Paramètres	<i>Pos1</i>	<i>Pos2</i>
		$\alpha = 20$	$\alpha = 20$
Bruit Salt&Pepper	4%	1	1
	5%	1	1
	6%	0.9867	1
	7%	0.9863	1
Bruit Gauss	2%	1	1
	3%	0.9867	1
	4%	0.9729	1
	5%	1	1
	6%	1	1
Filtre médian	3x3	1	1
	5x5	0.9867	1
	7x7	0.9499	0.9213
Filtre Average	3x3	1	1
	5x5	0.9867	1

	7x7	0.8318	0.8892
Filtre Gauss	3x3	1	1
	5x5	0.9867	1
	7x7	0.9213	0.9867
Cropping	1/8	1	1
	1/4	1	1
	1/2	1	1
Compression Jpeg	7%	1	0.9867
	8%	1	1
	9%	1	1
	10%	1	1
	11%	1	1
	12%	1	1

3.4.2 Masques visuels proposés

Nous proposons quatre masques visuels. Le premier et le deuxième sont des masques de luminance dans le domaine fréquentiel et le domaine spatial respectivement. Le troisième masque va prendre les informations de textures, contours et coins. Le quatrième masque ce n'est que le troisième masque plus le deuxième masque.

$$JND_1 = \left\{ \frac{DC_b}{DC_{mean}} \right\}^{0.649} \quad (3.13)$$

$$JND_2 = (128 - M_L)^2 \quad (3.14)$$

$$JND_3 = M_T - \frac{(M_E + M_C)}{2} \quad (3.15)$$

$$JND_4 = \left(M_T - \frac{(M_E + M_C)}{2} \right) + (128 - M_L)^2 \quad (3.16)$$

où DC_b est la composante continue DC du bloque b .

DC_{mean} la moyenne des coefficients DC de l'image.

Les résultats de simulation pour l'image de test *Lena* sont donnés dans le tableau (3.2) où le $PSNR$ est fixé à 37.7 db.

Tableau (3.2) : Evaluation en terme de NC pour les 4 masques

Attaques		Masque luminance de <i>Watson</i>				Masque JND_3		Masque JND_4	
		JND_1		JND_2		JND_3		JND_4	
		$\alpha = 20$		$\alpha = 0.05$		$\alpha = 2.2$		$\alpha = 0.05$	
		$Pos1$	$Pos2$	$Pos1$	$Pos2$	$Pos1$	$Pos2$	$Pos1$	$Pos2$
Bruit Salt&Pepper	4%	1	1	1	1	1	1	0.9867	1
	5%	1	1	1	1	1	1	1	1
	6%	0.9867	1	1	1	1	1	1	1
	7%	0.9863	1	0.9863	1	1	1	1	0.9867
Bruit Gauss	2%	1	1	1	1	1	1	1	1
	3%	0.9867	1	1	1	1	1	1	1
	4%	0.9729	1	0.9867	0.9863	1	1	0.9867	0.9867
	5%	1	1	0.9867	0.9740	1	1	1	0.9726
	6%	1	1	0.9334	1	1	1	0.9867	0.9448
Filtre median	3x3	1	1	1	1	1	1	1	1
	5x5	0.9867	1	0.9617	0.9863	1	0.9863	0.9617	0.9863
	7x7	0.9499	0.9213	0.8424	0.8000	0.9097	0.9067	0.8577	0.8108
Filtre Average	3x3	1	1	1	1	1	1	1	1
	5x5	0.9867	1	0.9499	0.9863	0.9740	1	0.9617	0.9863
	7x7	0.8318	0.8892	0.7538	0.7225	0.8273	0.8950	0.7538	0.7225
Filtre Gauss	3x3	1	1	1	1	1	1	1	1
	5x5	0.9867	1	0.9617	0.9863	0.9867	1	0.9740	0.9863
	7x7	0.9213	0.9867	0.8215	0.9304	0.9477	0.9729	0.8318	0.9304
Cropping	1/8	1	1	1	1	1	1	1	1
	1/4	1	1	1	1	1	1	1	1
	1/2	1	1	1	1	1	1	1	1
Compression Jpeg FQ	7%	1	0.9867	0.9600	1	0.9740	1	0.9600	1
	8%	1	1	1	1	0.9867	1	1	1
	9%	1	1	0.9867	1	1	1	0.9867	1
	10%	1	1	1	1	1	1	1	1
	11%	1	1	1	1	1	1	1	1
	12%	1	1	1	1	1	1	1	1

D'après les résultats portés au tableau (3.2), nous constatons que l'utilisation du masque visuel JND_3 qui prend en charge trois caractéristiques de l'image hôte donne des meilleurs résultats en termes de robustesse et imperceptibilité face aux attaques telles que la compression et le filtrage par rapport au premier masque qui prend juste la luminance en charge. La figure (3.7) montre que les dégradations portées sur l'image de test *Lena* tatouée en utilisant le masque JND_3 sont minimales par rapport à l'image *Lena* tatouée par le masque de luminance de *Watson*.



(a)



(b)

Figure (3.7) : Image de test *Lena* taouée en utilisant : (a) le masque JND_3 , (b) le masque de luminance de *Watson*.

3.4.3 Réduction du nombre de bloc altérés

Le nombre de blocs sélectionnés pour insérer la marque étalée est égal à 1024 blocs, et les masques visuels sur lesquels nous avons testé notre méthode sont donnés par les expressions (3.13)-(3.16). Les résultats de simulation pour l'image de test *Lena* sont donnés dans le tableau (3.3) où le *PSNR* est fixé à 39 db.

Tableau (3.3) : Evaluation en terme de *NC* pour 1024 blocs

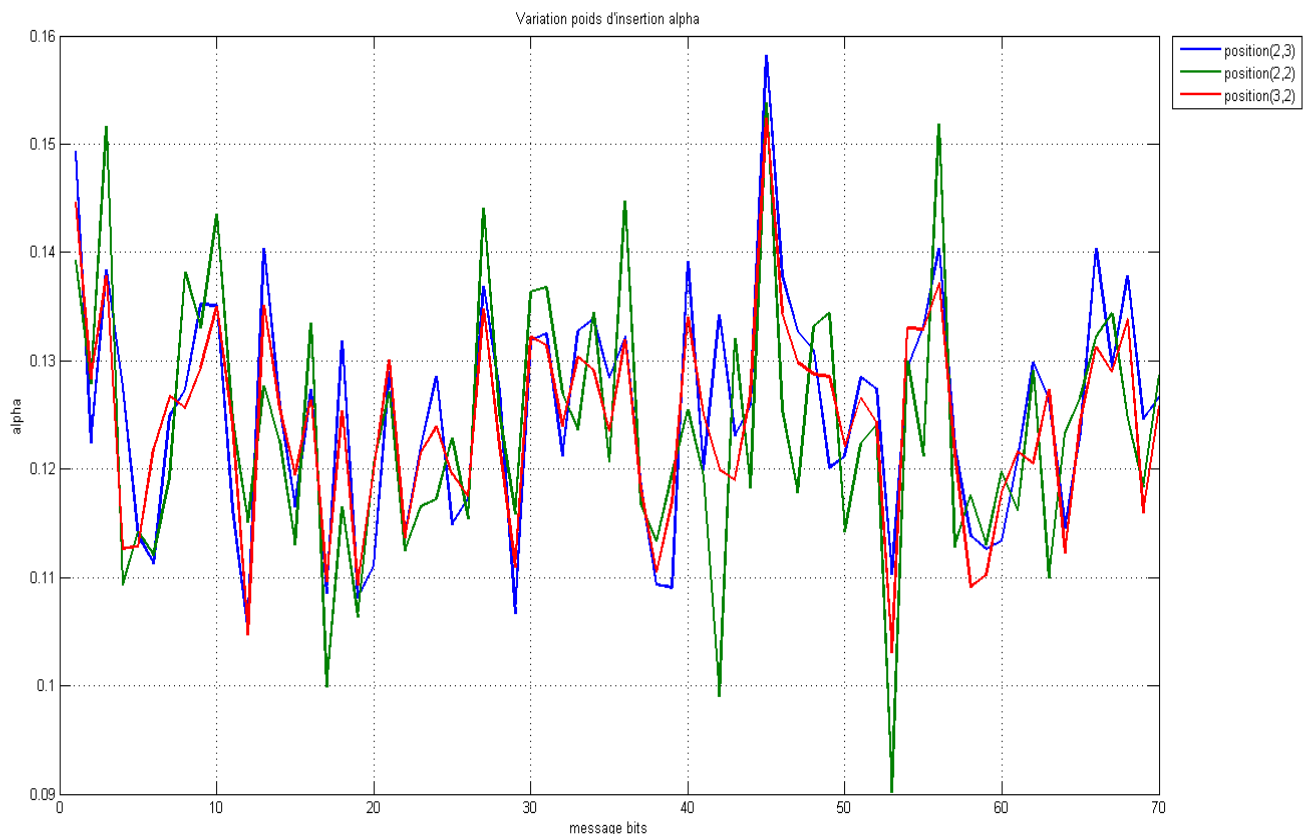
Attaques		Masque luminance de <i>Watson</i>				Masque JND_3		Masque JND_4	
		JND_1		JND_2		JND_3		JND_4	
		<i>Pos1</i>	<i>Pos2</i>	<i>Pos1</i>	<i>Pos2</i>	<i>Pos1</i>	<i>Pos2</i>	<i>Pos1</i>	<i>Pos2</i>
Bruit Salt&Pepper	4%	1	1	1	1	1	1	1	1
	5%	0.9863	1	1	1	1	1	1	1
	6%	1	1	0.9867	1	1	1	0.9867	1
	7%	1	1	0.9863	1	1	1	0.9863	1
Bruit Gauss	2%	1	1	1	1	1	1	1	1
	3%	0.9740	1	1	1	1	1	0.9867	1
	4%	0.9863	0.9863	1	1	0.9867	1	1	0.9729
	5%	0.9863	0.9617	0.9315	0.9589	1	0.9867	0.9863	0.9863
	6%	0.9863	0.9863	0.9729	0.9729	1	0.9726	0.9448	1
Filtre median	3x3	1	1	1	1	1	1	1	1
	5x5	0.9867	1	0.9863	0.9867	1	1	0.9863	0.9863
	7x7	0.8950	0.7726	0.9022	0.8108	1	0.9586	0.9334	0.8318
Filtre Average	3x3	1	1	1	1	1	1	1	1
	5x5	0.9726	1	1	1	0.9589	1	0.9459	1
	7x7	0.7972	0.8058	0.7780	0.8336	0.8648	0.9740	0.7124	0.8267
Filtre Gauss	3x3	1	1	1	1	1	1	1	1

	5x5	0.9726	1	1	1	1	1	0.9729	1
	7x7	0.8547	0.9863	0.9459	0.9448	0.8918	1	0.8267	0.9334
Cropping	1/8	1	1	1	1	1	1	1	1
	1/4	1	1	1	1	1	1	1	1
	1/2	1	1	1	1	1	1	1	1
Compression Jpeg FQ	7%	0.9867	1	0.9589	0.9867	1	0.9867	1	1
	8%	1	1	0.9863	1	1	1	1	1
	9%	1	1	0.9867	1	1	1	1	1
	10%	1	1	1	1	1	1	1	1
	11%	1	1	1	1	1	1	1	1
	12%	1	1	1	1	1	1	1	1

Les résultats portés au tableau (3.3) montrent que la réduction du nombre de bloc altérés donne toujours une robustesse meilleur en utilisant le masque visuel JND_3 .

3.4.4 Poids d'insertion variable

La figure (3.8) montre la variation du facteur gain α_i dans les trois coefficients AC choisis pour l'insertion en fonction des bits b_i du message m .



La figure (3.8) : Variation du α_i en fonction des bits b_i dans trois coefficients AC différents.

Les résultats de simulation pour l'image de test *Lena* sont donnés dans le tableau (3.3) où le *PSNR* dépasse 41db.

D'après les résultats portés sur le tableau (3.4), nous constatons que le système de tatouage à facteur gain variable α_i est toujours robuste aux attaques, et qu'il y a une amélioration du *PSNR* presque de 3 db ce qui va donner une imperceptibilité meilleur par rapport à l'utilisation du facteur de gain fixe.

La figure (3.9) présente l'image de test *Lena* tatouée par deux méthodes. La figure (3.9.a) montre l'image tatouée par la méthode [39], cette méthode se repose sur le masque visuel de la luminance du modèle de Watson et un facteur de gain α fixe, le *PSNR* est égal à 37.08 db . La figure (3.9.b) montre l'image tatouée par la méthode proposée, où nous avons proposé de générer un masque visuel basé sur les caractéristiques locales de l'image hôte et un facteur gain α_i variable selon le coefficient *AC* choisi pour l'insertion de la marque $\bar{W}$, le *PSNR* est égal à 41.76 db.

Tableau (3.4) : Evaluation en terme de *NC* pour un facteur gain variable

Attaques	Paramètres	Alpha variable		Alpha fixe	
		<i>JND</i> ₃	<i>JND</i> ₄	<i>JND</i> ₃	<i>JND</i> ₄
		<i>Pos2</i>	<i>Pos2</i>	<i>Pos2</i>	<i>Pos2</i>
		41.14 db	41.76 db	39 db	39 db
Bruit Salt&Pepper	4%	1	1	1	1
	5%	1	1	1	1
	6%	1	1	1	1
	7%	1	1	1	1
Bruit Gauss	2%	1	1	1	1
	3%	1	1	1	1
	4%	1	1	1	0.9729
	5%	0.9867	1	0.9867	0.9863
	6%	0.9589	0.9334	0.9726	1
Filtre médian	3x3	1	1	1	1
	5x5	1	1	1	0.9863
	7x7	0.9304	0.8058	0.9586	0.8318
Filtre Average	3x3	1	1	1	1
	5x5	1	0.9867	1	1
	7x7	0.9739	0.8219	0.9740	0.8267
Filtre Gauss	3x3	1	1	1	1
	5x5	1	1	1	1
	7x7	1	0.9334	1	0.9334
Cropping	1/8	1	1	1	1
	1/4	1	1	1	1
	1/2	1	1	1	1
Compression Jpeg	7%	0.9600	1	0.9867	1
	8%	0.9867	1	1	1
	9%	1	1	1	1
	10%	1	1	1	1
	11%	1	1	1	1
	12%	1	1	1	1



(b)



(b)

Figure (3.9) : Image de test *Lena* taouée en utilisant : (a) la méthode [9], (b) la méthode proposée.

3.5 Conclusion

Dans ce chapitre, nous avons proposé un nouveau système de tatouage d'images multi-bit à poids d'insertion variable basé sur un masque visuel déterminé par les propriétés de l'image telles que textures, coins, contours et luminance. Ce masque est exploité, dans ce travail, dans la sélection des blocs qui ont des valeurs du *JND* les plus grandes.

Nous avons implémenté le système proposé et celui présenté dans [9] et nous avons utilisé le *PSNR* et le *NC* pour évaluer et comparer les performances des deux systèmes. Les résultats de simulation montrent clairement que le système proposé présente un excellent compromis entre la robustesse et l'imperceptibilité. Les performances du système proposé sont obtenues principalement grâce à l'utilisation d'un facteur gain variable et du masque visuel.

Dans le chapitre suivant, nous allons exploiter le deuxième type de tatouage qui est basé sur la quantification pour développer un autre nouveau algorithme de tatouage.

4-1 Introduction

En général, les systèmes de tatouage d'images adoptent un des deux méthodes d'insertion de base, méthodes basées sur l'étalement de spectre et les méthodes basées sur la quantification. *Chen et Wornell* [4] ont proposé des méthodes de tatouage basées sur la quantification comme la quantification par modulation indexée QIM et la distorsion compensée DC-QIM pour l'insertion de la marque. *Soe et al* [5] ont proposé un schéma de tatouage à base de QIM avec deux pas de quantification adaptés. Basé sur la QIM, *Ourique et al* [6] ont proposé l'utilisation de la méthode angle QIM pour réduire les effets des attaques du changement d'échelle (scaling), la marque est insérée en quantifiant l'angle formé par un système de coordonnées sphérique. *Li et Cox* [7] ont proposé un model perceptuel pour sélectionner d'une manière adaptative la taille du pas de quantification pour améliorer la fidélité du tatouage. Plusieurs techniques de tatouage basées sur QIM ont été proposées dans [40].

Dans ce chapitre, nous allons proposer une nouvelle technique de tatouage d'images basée sur QIM dans le domaine de la DCT.

4.2 Outils utilisés

Dans cette section, nous présentons les outils utilisés dans l'algorithme de tatouage proposé pour l'insertion et l'extraction de la marque.

4.2.1 Domaine DCT

L'image originale $f(x, y)$ est segmentée en blocs B_n de taille 8×8 , et chaque bloc est transformé en coefficients DCT.

4.2.2 Quantification par modulation indexée

La méthode QIM est brièvement décrite dans [4], [5]. Cette méthode intègre un signal qui dépend de la marque utilisant une technique de quantification. Le message à insérer représente un indice pour la sélection d'un quantificateur particulier à partir d'un ensemble de quantificateurs possibles. Le quantificateur sélectionné est appliqué sur les composantes AC de l'image hôte pour coder le message m à insérer.

On suppose qu'on a un bit $m \in \{0, 1\}$ à insérer dans l'image hôte désignée par s . Deux quantificateurs $Q_i(s)$, $i = 0, 1$ seront générés et la valeur du bit détermine la sélection du quantificateur $Q_i(s)$ avec un pas de quantification de taille Δ , où peut être formulé comme (4.1).

$$Q_i(s) = Q(s - d_i) + d_i, \quad i = 0, 1 \quad (4.1)$$

où

$$Q(s) = \Delta \times \text{round}(s/\Delta), \quad d_0 = -\Delta/4, \quad d_1 = \Delta/4$$

L'image tatouée s' est calculée à base des deux quantificateurs $Q_0(s)$ et $Q_1(s)$ en utilisant l'expression (4.2). La figure (4.1) illustre le processus d'insertion d'un bit à base de QIM.

$$s' = \begin{cases} Q_0(s), & m = 0 \\ Q_1(s), & m = 1 \end{cases} \quad (4.2)$$

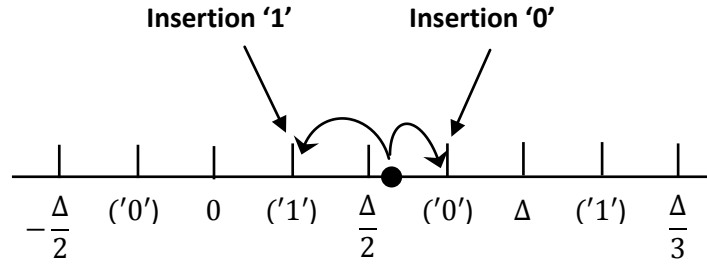


Figure (4.1) : Processus d'insertion à base de QIM

Le signal détecté est $y' = y + n = (s + m) + n$, où n représente le bruit introduit par le canal (par exemple une attaque), ce signal est quantifié par les deux quantificateurs, le bit décodé m correspond à la distance minimale, le décodeur doit choisir le point de reconstitution le plus proche du signal y' . Le bit m décodé est défini par l'expression (4.3).

$$\hat{m} = \arg \min_{m \in \{0,1\}} \|y' - Q_m(y')\| \quad (4.3)$$

4.3 Méthode proposée en utilisant la DCT-3D et QIM

L'objectif de notre travail est l'élaboration d'un algorithme de tatouage aveugle et robuste. Nous optons pour l'insertion de la marque la modification des modules des coefficients DCT en utilisant la quantification QIM. La figure (4.2) montre le système de tatouage proposé. Le détail de la technique proposée est décrit dans la section (4.3.1).

Le système du tatouage proposé se compose de deux processus, le processus d'insertion et le processus d'extraction de la marque. Tout d'abord, nous utilisons la technique d'insertion de la marque pour atteindre le mécanisme de la protection des droits d'auteur. En plus, pour améliorer la sécurité de la marque, la marque est permutée par la transformation d'*Arnold* pour disperser sa corrélation.

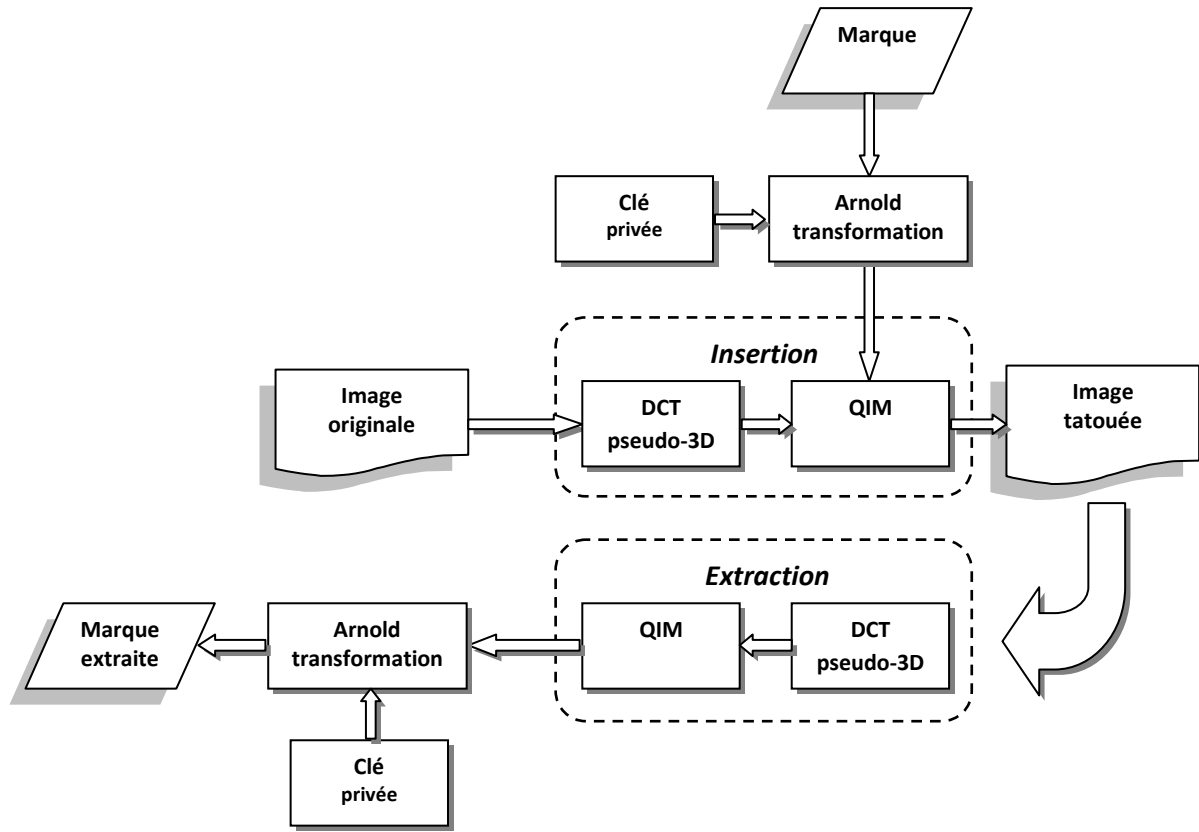


Figure (4.2) : Système du tatouage proposé

4.3.1.1 Transformation d'Arnold

La transformation d'un point (x, y) dans un bloc carré de taille $N \times N$, à un autre point (x', y') suivant l'expression (4.6) est appelée transformation d'Arnold à deux dimensions.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad x, y \in \{0, 1, 2, \dots, N-1\} \quad (4.6)$$

où $\pmod{N}$ représente l'opérateur modulo N .

L'image numérique est considérée comme une matrice à deux dimensions de taille $N \times N$, (x, y) sont les coordonnées du pixel de l'image, (x', y') sont les coordonnées modifiées du même pixel. Cette transformation rend l'image numérique comme un bruit.

La formule itérative de la transformation d'Arnold est donnée par :

$$p_{xy}^{n+1} = A \cdot p_{xy}^n \pmod{N} \quad n = 0, 1, 2, \dots, N-1 \quad (4.7)$$

où

$$p_{xy}^n = (x, y) \text{ et } A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

A est la matrice de transformation ;

n est le nombre d'itérations.

Le nombre de permutation est considéré comme une clé de sécurité du système de tatouage.

Pour récupérer l'image originale on doit appliquer la transformation inverse d'*Arnold* suivante :

$$p_{xy}^{n+1} = B \cdot p_{xy}^n \pmod{N} \quad n = 0, 1, 2, \dots, N - 1 \quad (4.8)$$

où

$$p_{xy}^n = (x, y) \text{ et } B = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$$

B est la matrice inverse de la matrice A ;

n est le nombre d'itérations.

La figure (4.3) montre la transformation d'*Arnold* appliquée sur les images *Lena*, *Baboon* et la marque utilisées dans le processus d'insertion.

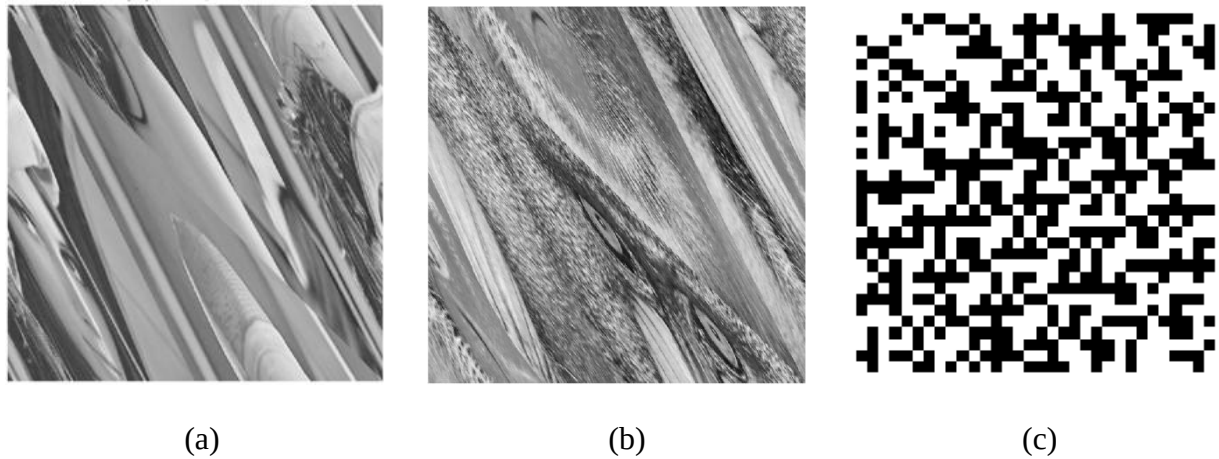


Figure (4.3) : Transformation d'*Arnold* (a) Image *Lena* après 1 itération, (b) image *Baboon* après 1 itération, (c) logo droits d'auteur après 25 itérations.

Pour déterminer la périodicité de la transformée d'*Arnold* appliquée sur le logo droits d'auteur, on a utilisé 64 itérations (deux fois la taille de la marque). La figure (4.4) montre la variation de la corrélation normalisée NC en fonction du nombre d'itérations.

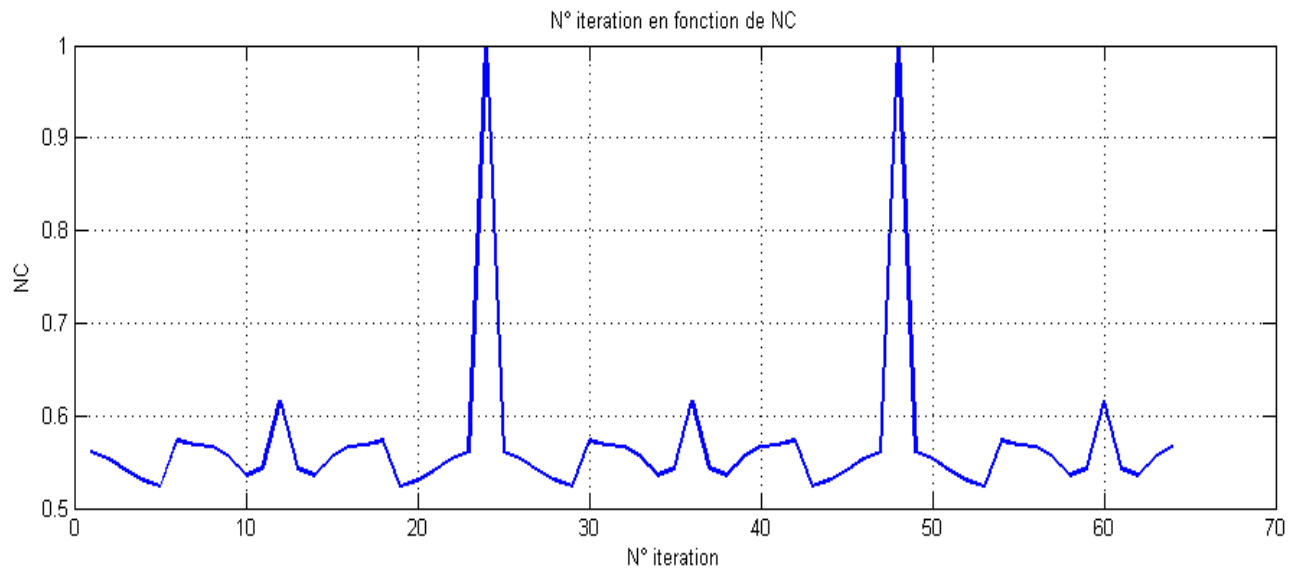


Figure (4.4) : NC en fonction du nombre d'itérations pour l'image logo droits d'auteur

D'après la figure (4.3), il est clair que le cycle itératif reprend chaque 24 itérations, et que la valeur du NC est minimale pour 5 et 19 itérations suivant le tableau (4.1).

Tableau (4.1) : NC en fonction du nombre d'itérations

N° itération	1	2	3	4	5	6	7	8	9	10	11	12
NC	0,56	0,55	0,54	0,53	0,52	0,57	0,56	0,56	0,55	0,53	0,54	0,61
N° itération	13	14	15	16	17	18	19	20	21	22	23	24
NC	0,54	0,53	0,55	0,56	0,56	0,57	0,52	0,53	0,54	0,55	0,56	1

4.3.1.2 Algorithme d'insertion

Dans le processus d'insertion, d'abord nous divisons l'image originale en blocs de taille 8×8 qui seront transformés dans le domaine DCT, en suite nous prenons quatre blocs successifs en tant que groupe. Puis, nous allons choisir les composantes continues DC de chaque bloc de même groupe (pour former un vecteur de quatre valeurs) et de les transformer à nouveau dans le domaine DCT.

Après le processus de transformation, nous pouvons obtenir une nouvelle composante continue DC et trois composantes alternatives AC_1 , AC_2 et AC_3 . Un schéma simple de cette transformation est représenté dans la figure (4.5). En répétant les étapes ci-dessus pour le reste des groupes.

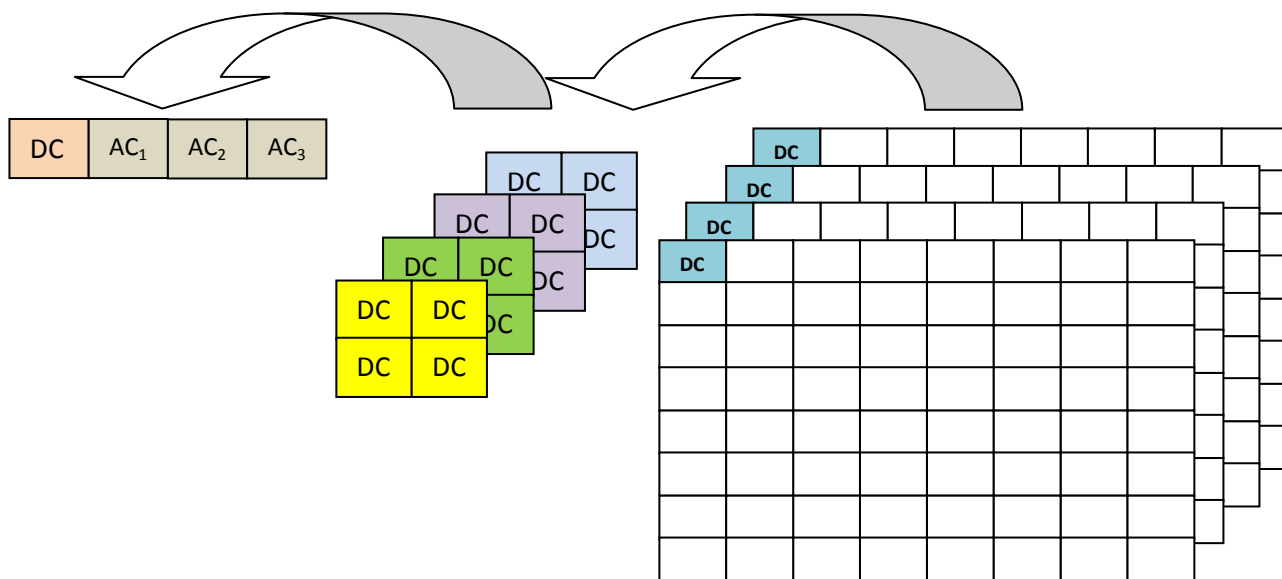


Figure (4.5) : Illustration de la transformation DCT pseudo-3D

Comme décrit ci-dessus, la transformation DCT est prise deux fois. La première DCT effectuée une transformation 2-D par rapport au plan de l'image. La deuxième transformation DCT peut être considérée comme une transformation 1-D. Dans ce contexte, nous considérons la méthode du tatouage proposée comme DCT pseudo-3D.

Afin d'insérer les bits de la marque, la méthode QIM sera utilisée pour effectuer le tatouage. Sur la base de l'algorithme QIM, le domaine d'insertion est divisé en plusieurs régions.

L'intervalle de chaque région est le même, ce qui correspond au pas de quantifications $\Delta/2$, et un index i est attribué à chaque région. Chaque région représente le signal d'un bit (0 ou 1) de la marque. Selon le bit à insérer, nous allons modifier la valeur de la troisième composante continue AC_3 .

4.3.1.3 Algorithme d'extraction

Le processus d'extraction est l'inverse du processus d'insertion. Premièrement, l'image tatouée est divisée en blocs de taille 8x8 qui seront transformés dans le domaine DCT, en suite nous prenons quatre blocs successifs en tant que groupe. Puis, nous allons choisir les composantes continues DC de chaque bloc du même groupe (pour former un vecteur de quatre valeurs) et de les transformer à nouveau dans le domaine DCT. Après le processus de transformation, nous pouvons obtenir une nouvelle composante continue DC et trois composantes alternatives AC'_3 .

Le signal reçu $y' = AC'_3 = (AC_3 + n)$, où n représente le bruit introduit par le canal (par exemple une attaque), est quantifié par les deux quantificateurs $Q_0(y')$ et $Q_1(y')$, enfin on

détermine la valeur du bit détecté m' en jugeant quel signal entre les deux a une distance minimale par rapport au signal reçu y' . Le décodage du bit est défini par l'expression (4.10).

$$\hat{m} = \arg \min_{m \in \{0,1\}} \|y' - Q_m(y')\| \quad (4.10)$$

4.4 Résultats de simulation

Dans la suite, nous appliquons l'algorithme décrit ci-dessus à deux images hôtes présentées dans la figure (4.6). La première est l'image *Lena* figure (4.6.a) et la deuxième est l'image *Baboon* figure (4.6.b). le pas de quantification $\Delta = 80$.

Pour la marque qui est le logo des droits d'auteur © figure (4.6.c) qui sera utilisée pour tatouer les deux images. Les images tatouées f_w de *Lena* et *Baboon* sont respectivement présentées par les figures (4.7.a) et (4.7.b).

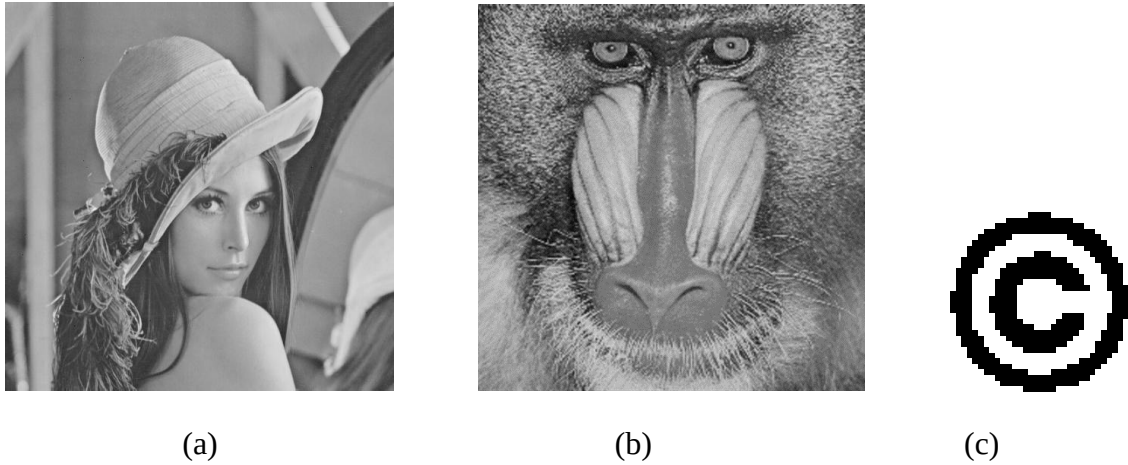


Figure (4.6) : (a) Image *Lena*, (b) image *Baboon* et (c) logo droits d'auteur.

Afin de tester la propriété d'imperceptibilité de notre méthode de tatouage, plusieurs images de taille 512×512 sont tatouées avec le logo droits d'auteur © de taille 32×32 .



Figure (4.7) : Images tatouées (a) *Lena*, (b) *Baboon*

A partir de ces figures, on peut voir qu'il est difficile de différencier entre les images originales et leurs images tatouées.

Les marques extraites à partir des images f_m sont illustrées par les figures (4.8.a) et (4.8.b).

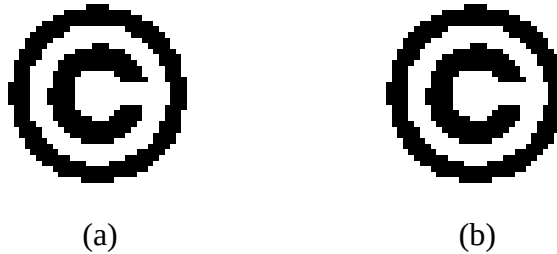


Figure (4.8) : Marques extraites (a) *Lena*, (b) *Baboon*

Pour évaluer concrètement les performances de notre méthode, on utilise deux métriques le *PSNR* pour estimer la distorsion des images tatouées et *NC* pour juger l'exactitude de la marque extraite.

Ces deux métriques sont présentées dans la section (1.7.1). Les valeurs du *PSNR* et du *NC* entre W et W^* sont présentées dans le Tableau (4.2).

Tableau (4.2) : *PSNR* des images tatouées et *NC* entre W et W^* .

Image hôte	<i>PSNR</i> (db)	<i>NC</i>
<i>Lena</i>	44,9263	1
<i>Baboon</i>	44,8521	1

Afin d'évaluer la robustesse de notre nouvelle technique de tatouage, plusieurs types d'attaques involontaire et volontaire telles que les attaques de bruit (bruit Salt&Pepper, bruit Gaussien), les attaques de filtrage (filtre Gaussien, filtre médian, filtre average), les attaques de cropping et la compression JPEG, ont été implantées.

Les tableaux (4.3) à (4.9) illustrent les résultats expérimentaux.

Tableau (4.3) : Ajout de bruit Salt&Pepper

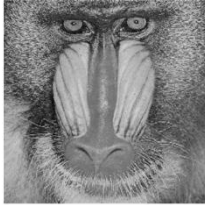
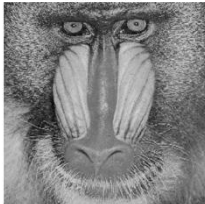
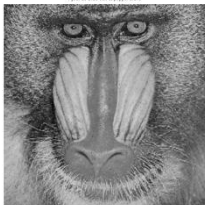
Bruit Salt&Pepper	<i>Lena</i>		<i>Baboon</i>	
0.1%	 		 	
	$NC = 0,9982$		$NC = 0,9982$	
0.2%	 		 	
	$NC = 0,9902$		$NC = 0,9971$	
0.3%	 		 	
	$NC = 0,9821$		$NC = 0,9721$	

Tableau (4.4) : Ajout de bruit Gaussien

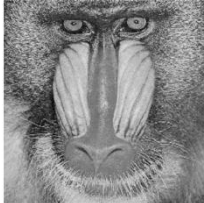
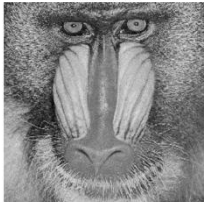
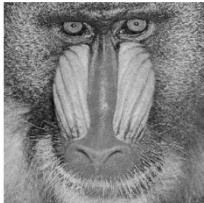
Bruit Gaussien	<i>Lena</i>		<i>Baboon</i>	
0.1%	Après de bruit gaussien(0.1%)  Marque extraite 	Après de bruit gaussien(0.1%)  Marque extraite 	$NC = 0,9642$	$NC = 0,9741$
0.2%	Après de bruit gaussien(0.2%)  Marque extraite 	Après de bruit gaussien(0.2%)  Marque extraite 	$NC = 0,9029$	$NC = 0,8977$
0.3%	Après de bruit gaussien(0.3%)  Marque extraite 	Après de bruit gaussien(0.3%)  Marque extraite 	$NC = 0,8265$	$NC = 0,8439$

Tableau (4.5) : Filtrage Gaussien

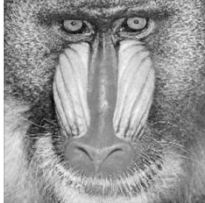
filtrage Gaussien	<i>Lena</i>		<i>Baboon</i>	
3×3	 	$NC = 0,9337$	 	$NC = 0,9331$
5×5	 	$NC = 0,8059$	 	$NC = 0,7272$
7×7	 	$NC = 0,7317$	 	$NC = 0,6219$

Tableau (4.6) : Filtrage médian

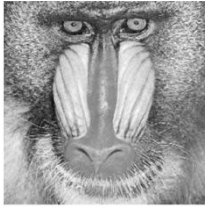
filtrage médian	<i>Lena</i>		<i>Baboon</i>	
3×3				
	$NC = 0,9955$		$NC = 0,9758$	
5×5				
	$NC = 0,9370$		$NC = 0,7680$	
7×7				
	$NC = 0,8354$		$NC = 0,6260$	

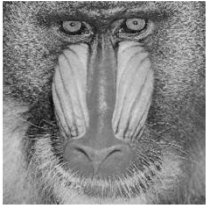
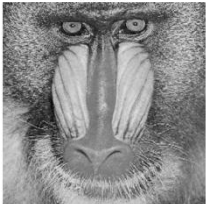
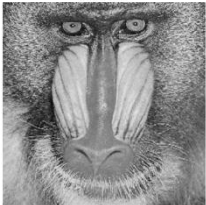
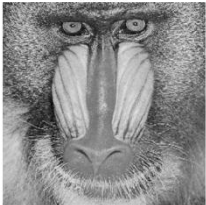
Tableau (4.7) : Filtrage average

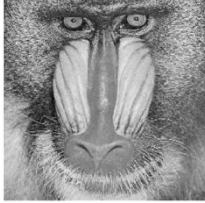
filtrage average	<i>Lena</i>		<i>Baboon</i>	
3×3				
	$NC = 0,9292$		$NC = 0,9294$	
5×5				
	$NC = 0,7885$		$NC = 0,7223$	
7×7				
	$NC = 0,5960$		$NC = 0,7208$	

Tableau (4.8) : Cropping

cropping	<i>Lena</i>		<i>Baboon</i>	
$1/16$	Cropping 1/16 image  Marque extraite 	Cropping 1/16 image  Marque extraite 	$NC = 0,9843$	$NC = 0,9843$
$1/8$	Cropping 1/8 image  Marque extraite 	Cropping 1/8 image  Marque extraite 	$NC = 0,9589$	$NC = 0,9589$
$1/4$	Cropping 1/4 image  Marque extraite 	Cropping 1/4 image  Marque extraite 	$NC = 0,9068$	$NC = 0,9068$

Tableau (4.9) : Compression JPEG

Compression JPEG	<i>Lena</i>		<i>Baboon</i>	
20%				
	$NC = 0,8306$		$NC = 0,8208$	
30%				
	$NC = 0,9688$		$NC = 0,9653$	
40%				
	$NC = 0,9875$		$NC = 0,9828$	
50%				
	$NC = 0,9982$		$NC = 0,9973$	

60%	 Compression jpeg 60%  Marque extraite  Compression jpeg 60%  Marque extraite $NC = 1$ $NC = 1$
-----	--

4.5 Discussion

Les résultats expérimentaux qui ont été présentés ci-dessus montrent que :

Pour la fidélité, la méthode proposée présente une très bonne qualité visuelle et les valeurs de *PSNR* des images de test tatouées sont supérieures à 44,80 db.

Pour la robustesse, nous avons appliquée des attaques de natures diverses sur les deux images tatouées *Lena* et *Baboon* et nous avons évalué l'efficacité de notre nouvelle technique de tatouage et son aptitude à détecter la marque insérée. Les images tatouées sont compressées avec divers facteurs de qualité pour tester la robustesse de notre méthode contre la compression JPEG. D'après le tableau (4.9), notre système de tatouage peut efficacement résister à la compression JPEG, les valeurs de *NC* sont supérieures à 0,96 pour un facteur de qualité supérieur à 20%.

Les tableaux (4.5) à (4.7) présentent les images tatouées attaquées par divers types de filtres (Gauss, médian et average) ainsi que les marques extraites. D'après les résultats portés sur le tableau (4.6), on peut déduire que notre méthode est moins robuste aux attaques de filtrage. Par contre, les tableaux (4.3) à (4.4) montrent que notre méthode est capable de détecter la marque insérée pour les images tatouées qui ont subis des modifications après l'ajout de divers types de bruit (Salt&Pepper et Gaussien). En plus, il est évident d'après le tableau (4.8) que notre méthode a une bonne capacité de résister aux attaques de cropping pour différent taux.

4.6 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle technique de tatouage d'images basée sur la méthode QIM et le domaine DCT-3D. D'après les résultats de simulation obtenus, il est clair que cette nouvelle méthode peut effectivement résister aux attaques comme la compression, l'ajout de bruit et cropping et assurer une bonne efficacité en termes d'imperceptibilité et robustesse.

Conclusion générale

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes de la sécurité des images fixes. La sécurisation des images stockées ou transmises est généralement effectuée par des techniques de tatouage dont leur développement est devenu un grand challenge dans ces dernières années. Après une étude bibliographique des techniques de tatouage d'images basées sur les transformées fixes, nous avons constaté qu'elles ne sont pas très robustes aux attaques et leurs vitesses d'exécution restent insuffisantes pour les applications en temps réel. Le projet que nous a été proposé a pour objectif de renforcer la robustesse des techniques de tatouage basées sur les transformées fixes, d'améliorer la qualité visuelle des images tatouées et de réduire leurs complexité de calcul en utilisant des transformée entières.

Au cours de ce travail de recherche, nous avons réalisé l'objectif ci-dessus en proposant deux nouveaux algorithmes de tatouage aveugle d'images basés sur les transformées DCT et DCT entière. Notre premier algorithme adopte la technique d'étalement de spectre pour l'insertion de la marque en utilisant deux masques visuels qui prennent en considération dans leurs conception les caractéristiques locales de l'image originale telles que la texture, contour, corner et luminance, et de calculer le poids d'insertion de la marque de façon adaptative. Par contre, notre deuxième algorithme est dédié pour l'exploitation de la technique de tatouage par quantification basée sur la méthode QIM en utilisant le domaine DCT pseudo-3D. Dans nos deux algorithmes, nous avons utilisé avec succès l'extraction de la marque de manière aveugle pour des images tatouées soumises aux différentes attaques.

Les résultats de simulation pour l'évaluation de la robustesse et les mesures objectives effectuées sur les images tatouées soumises aux différentes attaques obtenus dans ce travail, montrent clairement l'efficacité et la robustesse des algorithmes proposés dans ce mémoire. En plus, dû au fait que la transformée DCT entière utilisée dans les algorithmes proposés possède une complexité de calcul très réduite comparée à celle de la transformée DCT, nos algorithmes ont l'avantage de haute vitesse d'exécution, en particulier ils n'exigent que des additions et des décalages de bits, par conséquent, ils sont plus attractives pour les transmissions sécurisées des images en temps réel sur les réseaux de communication.

Dans ce travail, nous avons considéré le cas des images fixes. Alors, nous suggérons en perspectives l'exploitation des idées développées dans ce mémoire pour concevoir des nouveaux algorithmes appropriés pour le tatouage des vidéos.

Bibliographie

[1]	V. Martin, "Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique," Thèse PhD, Ecole doctorale : Informatique et Télécommunications, Spécialité : Signal, Image, Acoustique et Optimisation, 2006.
[2]	I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia. Image Processing," <i>IEEE Transaction on image processing</i> , Vol. 6, No. 12, pp. 1673–1687, December 1997.
[3]	I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," <i>Proceedings of the International Conference on Image Processing</i> , pp. 243–246, 1996.
[4]	B. Chen and G. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," <i>IEEE Transaction on information theory</i> , vol. 47, no. 4, pp. 1423–1443, May 2001.
[5]	Y. S. Seo, W. G. Kim, Y. H. Huh, W. G. Oh, and C. J. Hwang, "QIM watermarking for image with tow adaptive quantizaion step-sizes," in <i>Proc. The 9th International Conference on Advanced Communication Technology</i> , pp.997–800, 2007.
[6]	F. Ourique, V. Kicks, R. Jordan, and F. P. Gonzalez, "Angle QIM: A novel watermark embedding scheme robust against amplitude scaling distortions," in <i>Proc. IEEE International Conference on Accustics, Speech, and Signal Processing</i> , pp. 797–800, 2005.
[7]	Q. Li and I. J. Cox, "Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking," <i>IEEE Trans. Inf. Forensics Security</i> , vol. 2, no. 2, pp. 127–139, Jun 2007.
[8]	X. Kang, J.Huang, and W. Zeng "Improving Robustness of Quantization Based Image Watermarking via Adaptive Receiver," <i>IEEE Trans. On multimedia</i> , vol. 10, no. 6, pp. 953–959, October 2008.
[9]	H. Guan, Z. Zeng, S. Zhang. "A new dct-based digital image watermarking algorithm", <i>International Conference on Automatic Control and Artificial Intelligence, ACAI</i> , pp.166–169, March 2012.
[10]	N. Golea, "Tatouage numérique des images couleurs RGB," thèse magister, département d'informatique, université Batna, Algérie, 2010.
[11]	C. Lu, "Multimedia Security : Steganography and Digital Watermarking Techniques for Protection of Intellectual Property," <i>Idea Group publishing</i> , 2005.
[12]	K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding Secret Information into a Dithered Multilevel Image," In <i>IEEE Military Communications Conference</i> , Vol. 1,

	pp. 216–220,1990.
[13]	A. Tirkel, G. Rankin, R. Schyndel, W. Ho, N. Mee, and C. Osborne, “Electronic Watermark,” <i>Digital Image Computing, Technology and Applications</i> , pp. 666–672, 1993.
[14]	J. Cox, L. Miller, A. Bloom, J. Fridrich and T. Kalker, “Digital Watermarking and Steganography,” 2 nd edition, <i>Morgan Kaufmann Publishers</i> , USA, 2008.
[15]	S. Katzenbeisser, A. Fabien , and P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking,” <i>Artech House</i> , Boston, London, 2000.
[16]	A. Valizadeh and Z. J. Wang, “Correlation-and-Bit-Aware Spread Spectrum Embedding for Data Hiding,” <i>IEEE Transactions on image processing</i> , Vol. 6, no. 2, pp. 267–282, June 2011.
[17]	R. Smitha, A. Jyothsna, and P. Pinaka , “Digital Watermarking: Applications, Techniques and Attacks,” <i>International Journal of Computer Applications</i> . Vol. 44, no. 7, pp. 29–34, April 2012.
[18]	G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking Digital Image and Video Data A State of the Art Overview,” <i>IEEE signal processing magazine</i> , , Vol. 17, Issue. 5, pp. 20–46, September 2000.
[19]	J. Fridrich, “Applications of data hiding in digital images,” <i>Tutorial for the ISSPA, Conference in Melbourne, Australia</i> , November 1998.
[20]	M. L. Miller, G. J. Doërr, and I. J. Cox, “Applying informed coding and embedding to design a robust high-capacity watermark,” <i>IEEE Transactions on image processing</i> , Vol. 13, no. 6, pp. 792–807, June 2004.
[21]	T. Furon and P. Duhamel, “An asymmetric watermarking method,” <i>IEEE Transactions on image processing</i> , Vol. 51, no. 4, pp. 981–995, April 2003.
[22]	R. L. Pickholtz, J. M. Winograd, and L. B. Milstein, “Theory of spread spectrum communications : a tutorial,” <i>IEEE Transaction on Communications</i> , Vol. 30, no. 5, pp. 855–884, May 1982.
[23]	G. Csurka, F. Deguillaume, J. J. K. ‘O Ruanaidh, and T. Pun, “A Bayesian approach to affine transformation resistant image and video watermarking,” <i>In Proceeding. Int. spring link, LNCS 1768</i> , pp. 270-285, 2000.
[24]	J. Eggers, R. Buml, R. Tzschoppe, and B. Girod, “Scalar Costa Scheme for Information Embedding,” <i>IEEE Transactions on Signal Processing</i> , Vol. 51, no. 4, pp. 1003–1019, April 2003.
[25]	B. Chen and G. W. Wornell, “Quantization index modulation : a class of provably good methods for digital watermarking and information embedding,” <i>IEEE Transaction on information theory</i> , Vol. 47, No. 4, pp 1423–1443, May 2001.

[26]	F. H. Wang, J. S. Pan, and L. C. Jain, "Innovation in Digital Watermarking Techniques," <i>Springer, Series: Studies in Computational Intelligence</i> , Vol. 232, 2009.
[27]	R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," <i>In IEEE International Conference on Image Processing. ICIP</i> , Vol. 2, pp. 86–90, 1994.
[28]	D. Singh, N. Choudhary, and M. Agrawam, "Spatial and Frequency Domain for Grey level Digital Images," <i>Special Issue of International Journal of Computer Applications (0975 – 8887) on Communication Security</i> , No.4, pp 16–20, Mar.2012.
[29]	V. Tomar, D. Mehrotra and A. Choudhary, "A Statistical Comparison of Digital Image Watermarking Techniques," <i>Special Issue of International Journal of Computer Applications (0975 – 8887) 3rd International IT Summit Confluence</i> , 2012.
[30]	T. Chirawat, C. Somsak, and L. Attasit, "A Robust Image Watermarking Using Multiresolution Analysis of Wavelet," <i>Proceedings of ISCIT2005</i> , pp. 603–606, 2005.
[31]	S. Pereira, J. J. K. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of fourier-based watermarks using log-polar and log-log maps," <i>IEEE International Conference on Multimedia Computing and Systems</i> , pp 870–874, June 1999.
[32]	M. Jiansheng, L. Sukang, and T. Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT," <i>Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)</i> , pp. 104-107, May 2009.
[33]	R. Y. Kuraz and A. H. Modar, "Improve Watermark Security via Wavelet Transform and CDMA Techniques," <i>Al-Rafidain Engineering</i> , Vol. 6, pp. 39-49, 2008.
[34]	S. Belkacem, Z. Dibi, and A. Bouridane, "A Masking model of HVS for image watermarking in the DCT domain," <i>IEEE International Conference on Electronics, Circuits and Systems</i> , pp. 330–334, 2007.
[35]	A. B. Watson, "Visually Optimal DCT Quantization Matrices for Individual Images," <i>Data Compression Conference</i> , pp. 178–187, 1993.
[36]	A. K. Parthasarathy and S. Kak, "An Improved Method of Content Based Image Watermarking," <i>IEEE Transaction on Broadcasting</i> , vol. 53, no. 2, pp. 468–479, June. 2007.
[37]	[site kovesi] [Online]: http://www.csse.uwa.edu.au/~pk/Research/MatlabFns/ .
[38]	J. L. Mannos and J. J. Sakrison, "The effects of avisual fidelity criterion on the encoding of images," <i>IEEE Transaction on Information Thyory</i> , Vol. 20, no. 4, pp. 525-536, July 1974.

[39]	M. Kutter and F. Petitcolas, "Fair evaluation methods for image watermarking Systems," <i>SPIE Journal of Electronic Imaging</i> , Vol. 9, No. 4, pp. 445–455, October 2000.
[40]	P. Moulin and A. Briassouli, "A stochastic QIM algorithm for robust, undetectable image watermarking," in <i>Proceeding IEEE International Conference on ImageProcessing</i> , vol. 4, pp. 1173–1176, 2004.
[41]	I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking Applications and Their Properties," In <i>IEEE International Conference on Information Technology : Coding and Computing</i> , pp. 6–10, 2000.
[42]	S. Kay and E. Izquierdo, "Robust content based image watermarking," in <i>Proc. Workshop on Image Analysis for Multimedia Interactive Services</i> , Tampere, Finland, May 2001.
[43]	R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in <i>Proc. 1996 Int. Conference on Image Processing</i> , Lausanne, Switzerland, vol. 3, pp. 219–222, September 1996.
[44]	M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data embedding and watermarking technologies," <i>Proceedings of the IEEE</i> , vol. 86, no. 6, pp. 1064–1087, June 1998.
[45]	I. Cox and M. Miller, "A review of watermarking and the importance of perceptual modeling," in <i>Proceedings of the SPIE/IST& T Conference on Human Vision and Electronic Imaging II</i> , SPIE, San Jose, CA, vol. 3016, pp. 92–99, February 1997.
[46]	P. Kovesi, "Phase congruency detects corners and edges," in <i>Proceedings DICTA</i> , pp. 10–12, December 2003.
[47]	T. L. Arnow and A. C. Bovik, "Finding corners in images by foveated search," in <i>Proceedings of SPIE—Visual Communications and Image Processing</i> , vol. 6077, 2006.
[48]	[Online]: http://www.cim.mcgill.ca/~dparks/CornerDetector/moravec.html .
[49]	X. C. He and N. H. C. Yung, "Curvature scale space corner detector with adaptive threshold and dynamic region of support," in <i>Proceedings of the 17th International Conference on Pattern Recognition</i> , August 2004, vol. 2, pp. 791–794, Composed by He XiaochenHKU EEE Dept. ITSr, April. 2005.
[50]	[Online]: http://www.ee.surrey.ac.uk/CVSSP/demos/corners/index.html .
[51]	M. L. Miller, G. J. Doerr, I. J. Cox. "Dirty-paper trellis codes for watermarking", <i>IEEE International Conference on Image Processing, ICIP</i> , vol. 2, pp. 129-132, (2002).

[52]	J. Mayer, J. C. M. Bermudez. "Multi-bit informed embedding watermarking with constant robustness", <i>IEEE International Conference on Image Processing, ICIP</i> , vol. 1, pp. 669-672, 2005.
[53]	J. Mayer, R. A. Silva. "Efficient informed embedding of multi-bit watermark", <i>IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP</i> , vol. 1, pp. 389-392, 2004.
[54]	G. Xie, M. N. S. Swamy, M. O. Ahmad. "Perceptual shaping comparison of DWT-based pixel-wise masking model with DCT-based Watson model", <i>IEEE International Conference on Image Processing, ICIP</i> , vol. 2, pp. 1381-1384, (2006).
[55]	N. Mehra and M. Shandilya, "Imprecise reversible visible watermarking," <i>Link Springer, CSIT</i> , Vol. 1, Issue. 4, pp. 355–365, December 2013.

ملخص

يتناول هذا العمل وشم الصور من خلال استغلال أفقعة البصرية وضعت مؤخرا. المذكرة تعرض أولا دراسة مكتبية عن وشم الصور، تقنياتها، أساليب تطويرها، بناؤها وتطبيقاتها. وقد سمحت لنا هذه الدراسة بتطوير نوعين جديدين من خوارزميات لو شم الصور. ندرس الخوارزمية الأولى أساسا لاستخدام تقنية الطيف المنتشر بإستعمال تحويلات الـ DCT و DCT الصحيحة مع الإستغلال المناسبة للخصائص المحلية للصورة لتصميم أفقعة البصرية. أما الخوارزمية الثانية كرسست لإستغلال تقنية QIM في مجال DCT-3D. لتقييم متانة الخوارزميات نفذت على الصور الموشومة عدة هجمات مختلفة و من خلال نتائج المحاكاة المعروضة في هذا العمل، تبين لنا بوضوح كفاءة و متانة الخوارزميات المقترحة في هذه المذكرة. وعلاوة على ذلك، تقدم لنا هذه الخوارزميات المقترحة ميزة انخفاض في التعقيد بالمقارنة مع تقنيات وشم الصورة الموجودة.

كلمات مفتاحية : وشم الصور، DCT و DCT الصحيحة، انتشار الطيف، QIM.

Résumé

Ce travail considère le tatouage des images en exploitant les masques visuels récemment développés dans la littérature. Le mémoire présente tout d'abord un état de l'art sur le tatouage d'images et une étude bibliographique sur les techniques de tatouage d'images et leurs domaines d'applications. Cette étude nous a permis de développer deux nouveaux algorithmes de tatouage d'images fixes aveugles et robustes. Le premier algorithme est dédiée essentiellement à l'utilisation de la technique d'étalement de spectre dans le domaine de la transformée DCT et la DCT entière, tout en exploitant les caractéristiques locales de l'image pour la conception des masques visuels. Par contre, le deuxième algorithme est dédié pour l'exploitation de la technique de tatouage par quantification basée sur la méthode QIM en utilisant le domaine DCT-3D. Les résultats de simulation pour l'évaluation de la robustesse et les mesures objectives effectuées sur les images tatouées soumises aux différentes attaques, présentés dans ce travail montrent clairement l'efficacité et la robustesse des algorithmes proposés dans ce mémoire. En plus, ces algorithmes proposés présentent un avantage de complexité réduite par rapport à celles des algorithmes de tatouage d'images existants.

Mots clés : Tatouage des images, Transformées DCT et DCT entière, étalement de spectre, quantification QIM.

Abstract

This work considers image watermarking by exploiting the visual masks recently developed in the literature. The thesis firstly presents the state of the art on image watermarking techniques and their applications. This study has allowed us to develop two new robust blind image watermarking algorithms. The first algorithm is essentially dedicated for using the spread spectrum technique in the DCT and integer DCT domains along with an appropriate exploitation of the local features of the image to design the visual masks. However, the second algorithm is dedicated for exploiting the QIM watermarking technique in the 3D-DCT domain. The simulation results to evaluate the robustness and the objective measures carried out on the watermarked images attacked with different attacks, presented in this work show clearly the efficiency and robustness of the algorithms proposed in this thesis. Moreover, these proposed algorithms present an advantage of reduced complexity compared to those of the existing image watermarking techniques.

Key words: Image watermarking, DCT and integer DCT, spread spectrum, QIM.