الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DR. YAHIA FARES DE MEDEA

FACULTE DES SCIENCES ET DE LA TECHNOLOGIE

**Département du Génie Électrique
et de l'Informatique**



Mémoire de Fin d'Études

**Présenté pour l'obtention du Diplôme
de Master en Génie Électrique**

Option : Systèmes de Télécommunications

THEME

Etude et simulation d'un système de codage d'image sécurisé à base du tatouage numérique

Proposé et dirigé par,

Mr : B**. MIMEN**

Préparé et présenté par,

Mr. **Hicham KALLACHE**

Remerciement

Nous tenons à adresser nos sincères remerciements:

.....

Tous d'abord, le grand merci à notre "Dieu" le plus puissant, pour son aide, sa générosité et pour la patience qu'il nous a donné pour aboutir à ce stade qui est pour nous le point de départ d'une merveilleuse aventure celle de la recherche de remise en cause permanent et de perfectionnement perpétuelle, ainsi mes très chers parents, qui ont toujours été là pour moi, Vous avez tout sacrifié pour vos enfants n'épargnant ni santé ni efforts. Vous m'avez donné un magnifique modèle de labeur et de persévérance. Je suis redevable d'une éducation dont je suis fier.

.....

Nous tenons à remercier tout particulièrement notre promoteur ***Mr. B. MIMEN*** *pour avoir bien voulu nous encadrer, pour tout le temps qu'il nous a octroyé et pour tous les conseils qu'il nous a prodigué. Qu'il trouve ici l'expression de notre profonde gratitude.*

Nos remerciements vont également à Mrs les membres du jury "nous vous sommes très reconnaissants pour avoir accepté de juger ce travail modeste. Qu'il nous soit permis de vous exprimer nos sentiments de respect, d'estime et de gratitude"

Nous aimerions remercier tous les enseignants et éducateurs que nous avons eu la chance et l'honneur de rencontrer durant notre parcours universitaire.

.....

Nos plus vifs et sincères remerciements à tous ceux qui, de près ou de loin, ont apporté leur contribution, aussi modeste soit elle, à la réalisation de ce travail à travers lequel nous voudrions apporter une pierre au grand édifice de la recherche dans ce domaine.

Nous espérons que cette étude qui n'a nullement la prétention d'être exhaustive saura retenir l'attention favorable du jury ainsi que l'intérêt des éventuels lecteurs.

ملخص:

الهدف الرئيسي من هذا المشروع هو تصميم نظام تشفير الصور استنادا على الوشم الرقمي باستعمال التكميم الشعاعي،في دراستنا كان اهتمامنا بشكل خاص على تقنية الوشم الرقمي تسمى التكميم بواسطة تحويل المؤشر QIM المعتمدة على تقسيم القاموس QV .للوصول إلى هذه التقنية بدأنا بتنفيذ التكميم الشعاعي للصور بتطبيق الخوارزمية LBG، الذي يتكون من جزء خاص بمعالجة التكميم الشعاعي من أجل صنع قاموس أمثل وأخر من اجل تشفير وفك الصور ،حيث يكون بعد شعاع الصورة وتدفق التشفير قابلين للتغيير .وبعد، نقوم بتنفيذ نظام وشم الصور بواسطة تطبيق الخوارزمية QIM المعتمدة على تقسيم القاموس QV بواسطة طريقتين عشوائية و متوازنة، وسيتم تقييم دراسة لأداء كلا نظامين وشم الصور وفقا لمعيارين: سعة الإخفاء الممثلة بتدفق إخفاء الصورة المخفية و الشفافية الممثلة بنوعية تشوه الصورة الموشومة .

كلمات المفتاحية : *معالجة الصور، الوشم الرقمي ، التكميم الشعاعي ، تشفير وفك الصور ، الخوارزمية LBG ، تكميم تحويل المؤشر QIM .*

Résumé :

L'objectif principal de ce projet est de concevoir un système de codage d'images à base du tatouage numérique en utilisant la quantification vectorielle (QV). Dans notre étude, on s'est intéressé particulièrement à une technique de tatouage numérique appelée la quantification par modulation d'indice (QIM) basée sur la division du dictionnaire QV. Pour mettre en œuvre cette technique, nous avons commencé d'abord par implémenter un quantificateur vectoriel d'images par application de l'algorithme LBG. Il est composé d'une partie entrainement QV pour la conception du dictionnaire optimal et du codeur/décodeur QV d'images, où la dimension du vecteur d'image ainsi que le débit du codage sont modifiables. Ensuite, nous avons conçu le système de tatouage d'images par application de l'algorithme QIM basée sur la division du dictionnaire QV de manière aléatoire ou équilibrée. Une étude des performances des deux systèmes de tatouage d'images seront évaluées selon deux critères : la capacité de dissimulation représentée par le débit de dissimulation de l'image secrète et l'imperceptibilité (transparence) représentée par la qualité perceptuelle de l'image tatouée.

Mots clés : *Traitement des images, Tatouage numérique, Quantification vectorielle, codage / décodage d'image, Algorithme LBG, La quantification QIM.*

Abstract:

The main objective of this project is to design image coding system based on Digital watermarking using vector quantization (VQ). In our study, we were particularly interested in a watermarking technique called quantization index modulation (QIM) based on the division of QV dictionary. To implement this technique, we started first by implementing a vector quantizer images by applying the LBG algorithm. It is composed of a drive part QV for the design of optimum dictionary and the encoder / decoder QV images, where the dimension of the image vector and the flow rate of encoding are modifiable. Than we designed the image watermarking system by application of QIM algorithm based on the division of QV dictionary random or balanced way. A study of the performance of both image watermarking systems will be evaluated according to two criteria: concealment capability represented by the flow of concealing secret image and imperceptibility (transparency) represented by the perceptual quality of the watermarked image.

Keywords: *image processing, Digital Watermarking, Vector quantization QV, encoding / decoding image, LBG algorithm, Quantification QIM.*

Table de matières

Table de matières…..... I
Liste des figures ……..... V
Liste des tableaux…….……..... VII
Liste des abréviations ……..... VIII
Liste de notations……..... IX

Introduction générale ……..…… 1

Chapitre 1 : Généralité sur le traitement des images :

1.1. Introduction ……...…… 3
1.2. Définition de l'image ……..……..…… 3
1.3. Image numérique ……..……..……... 3
1.4. Les attributs de l'image ……..……...…… 4
1.4.1 Pixel ……..……..……..…… 4
1.4.2. Dimension (définition) ……..……..……...…… 4
1.4.3. Bruit ……..……...…… 5
1.4.4. Résolution ……..…… 5
1.4.5. Contours et Textures ……..…….. 6
1.4.6. Luminance ……...……. 6
1.4.7. Contraste …..... 6
1.4.8. Le poids de l'image ……..…… 7
1.5. Les différents types d'images ……..…… 7
1.5.1. Mode Monochrome ……..…..……... 7
1.5.2. L'image en niveaux de gris ……..….. 7
1.5.3. L'image en couleurs ……..…..... 8
1.6. Les Formats d'image … ……...……..... 9
1.6.1. Les images bitmap ……...…..…. 9
1.6.1.1. Les différents formats d'Images bitmap ……...……..… 9
1.6.1.2. Avantages et inconvénients ..……..……..... 9
1.6.2. Les images vectorielles ……..…..... 9
1.6.2.1. Les différents formats d'images vectorielles ……..…... 10
1.6.2.2. Avantages et inconvénients ……..…… 10

1.7. Domaines d'application ……. 10
1.8. Qualité de l'image numérique ……. 11
1.9. Compression d'image ……. 11
1.9.1. Schéma fonctionnel de la compression des images ……. 11
1.9.2. Classification des méthodes de compression ……. 12
1.10. Conclusion ……. 13

Chapitre 2 : Notions de base sur les systèmes du tatouage :

2.1. Introduction ……. 14
2.2. Historique ……. 14
2.3. Terminologie ……. 15
2.3.1. Stéganographie ……. 15
2.3.2. Tatouage ……. 16
2.3.3. Dissimulation de données et insertion de données ……. 16
2.3.4. Empreintes digitales et étiquetage ……. 17
2.3.5. Tatouages visibles ……. 17
2.4. Formes de données de dissimulation ……. 17
2.5. Tatouage numérique ……. 17
2.5.1. Exigences ……. 18
2.5.1.1. Sécurité de la marque et les clés ……. 18
2.5.1.3. Imperceptibilité ……. 19
2.5.1.2. Robustesse ……. 19
2.5.1.4. Récupération de la marque avec ou sans les données d'origine ……. 20
2.5.1.5. Extraction de la marque ou vérification de sa présence ……. 20
2.5.1.6. Capacité d'insertion ……. 21
2.5.1.7. Le coût ……. 21
2.6. Le codage de la marque ……. 21
2.7. Les méthodes d'insertion ……. 22
2.7.1. Méthode additive ……. 22
2.7.2. Méthodes substitutives ……. 23
2.7.2.1. Tatouage par quantification ……. 23
2.7.2.2. Tatouage par contrainte ……. 25
2.8. Les domaines d'insertion ……. 26
2.8.1. Le domaine spatial ……. 26
2.8.2. Le domaine de Fourier ……. 28

2.8.3. Le domaine de la transformée en Cosinus Discrète (DCT) ……..……. 28
2.8.4. Domaine des ondelettes ……..…… 29
2.8.5. Autres domaines ……..……..…. 30
2.9. Principes de base du tatouage ……...……..... 30
2.10. Domaines d'application du tatouage numérique ……...……..… 32
2.11. Conclusion ……...……... 33

Chapitre 3 : Système de tatouage d'images par la QIM basée sur la QV :

3.1. Introduction ……..... 34
3.2. Quantification ……....…….. 35
3.2.1. Principe de codage par quantificateur scalaire ……...…… 35
3.2.2. Principe de codage par quantificateur vectoriel ……...……..… 36
3.2.2.1. Mesure de performances d'un quantificateur vectoriel ……...……... 37
3.2.2.2. Conception d'un quantificateur vectoriel optimal ……...……... 38
3.2.2.3. Algorithme LBG ……..… 39
3.3. Quantification vectorielle appliquée à l'image ……...……..… 42
3.3.1. Définitions préliminaires et notations de base …… 43
3.3.2. Principe de la quantification vectorielle d'une image ……...……. 43
3.3.3. Procédure de décodage QV d'image ……...…… 45
3.3.4. Mise en œuvre du système QV d'image ……...……..… 46
3.3.4.1. Taille optimale des blocs ……...……. 47
3.3.4.2. Détermination du dictionnaire ……...……..… 47
3.4. Tatouage d'images …… 48
3.5. Systèmes de tatouage d'images à base de la QV ……...… 48
3.5.1. Méthode de tatouage par QIM …… 49
3.5.1.1. Phase de prétraitement …… 50
3.5.1.2. Phase de la dissimulation …… 50
3.5.1.3. Phase de l'extraction ……... 50
3.6. Procédure d'application de la QIM pour le tatouage d'images …… 51
3.6.1. Division du dictionnaire ……...…….. 51
3.6.1.1. Méthodes de division du dictionnaire 52
3.6.2. Procédure de dissimulation ……..53
3.6.3. Procédure d'extraction ……...……. 54
3.7. Conclusion ……..... 55

Chapitre 4 : Simulations et résultats :

4.1. Introduction ……..……. 56
Partie 1 ……...……..…….. 57
4.2. Décomposition des deux images en vecteurs ……..……..… 57
4.3. L'algorithme LBG ……..……. 58
Partie 2 ...……..…..… 62
4.4. La quantification vectorielle d'une image base sur l'algorithme LBG …….……....62
Partie 3 …….…..… 65
4.5. Performances des méthodes de tatouage QIM implémentées …….…….…..... 65
4.5.1. Performances de la QIM par division aléatoire (QIM-DA) …….…….. 66
4.5.2. Performances de la QIM par division équilibrée (QIM-DE) …….…… 68
4.6. Performances de la QIM concernant l'image secrète (la marque) par division aléatoire (QIM-DA) …….……..... 70
4.7. La relation entre le choix de clé K et les performances de la QIM (dans le cas « QIM-DA ») …….…….....… 72
4.8. Evaluation comparative entre les méthodes QIM implémentées ……..…….…… 73
4.9. Exemples de tatouage des images par des marques textes …….…… 74
4.10. Conclusion ……...……..….. 76
Conclusion générale …….....…… 77
Bibliographie …….……....….. 79

Liste des figures

Figure **Page**

Figure 1.1 : Représentation de dimension d'une image …….…….…….. 5
Figure 1.2 : Images avec et sans bruit …….…….…….... 5
Figure 1.3 : Image avec texture ……..…….... 6
Figure 1.4 : Image en mode monochrome …….…... 7
Figure 1.5 : Image en mode niveau de gris …….…….…. 8
Figure 1.6 : Image en mode couleur …….…….…… 8
Figure1.7 : schéma fonctionnel de la compression des images ……11

Figure 2.1: Les différents domaines de la stéganographie …….…….…… 16
Figure 2.2 : Schéma général d'un système de tatouage numérique …….…… 18
Figure 2.3 : L'insertion du message par tatouage additif …….…… 22
Figure 2.4 : un exemple simple de QIM, l'ensemble A et B sont représenté
respectivement par un cercle et une croix ……..…….…… 24
Figure 2.5 : schéma bloc concernant les méthodes d'insertion ……..…….....…….. 25
Figure 2.6 : Découpage de l'image lena en 8 plans …….……..……. 27
Figure 2.7 : Image Lena et son spectre de Fourier …….……..…… 28
Figure 2.8 : Exemple d'insertion dans les fréquences moyennes de DCT …….……..… 29
Figure 2.9 : Schéma d'insertion d'une marque par tatouage numérique …….…….... 31
Figure 2.10. Schéma du principe de l'extraction de la marque ……..……..… 31
Figure 2.11. Classification des technologies du tatouage selon les applications …..…..…. 32

Figure 3.1 : schéma bloc d'un quantificateur vectoriel ...…….…… 37
Figure 3.2 : Partitionnement de l'espace d'entrée en classes bidimensionnelles(k =2).....38
Figure 3.3 : Génération du dictionnaire par l'algorithme LBG…….…….....… 40
Figure 3.4 : Exemple de dictionnaire construit par la méthode LBG……...… 40
Figure 3.5 : Principe de la quantification vectorielle d'une image ……..…..... 42
Figure 3.6 : Procédure de codage QV d'une image ……..… 44
Figure 3.7 : Principe de décodage QV ……...….. 46
Figure 3.8 : Schéma général d'une procédure de tatouage d'image …….....… 48
Figure 3.9 : Principe général de la division du dictionnaire Y ……...……. 49
Figure 3.10 : Schéma de dissimulation par QIM ……...…..… 50

Figure 3.11 : Schéma d'extraction de données par QIM ……..…..…… 51
Figure 3.12 : Exemple de division équilibrée du dictionnaire …….…..…..… 54

Figure 4.1 : Répartition des vecteurs de la source et les Vecteurs-code "Centroïdes" …… 61
Figure 4.2 : Images avec taille du dictionnaire QV différent …….....… 64
Figure 4.3 : Image secrète et images de couverture utilisées dans les simulations ……..... 65
Figure 4.4 : Images couvertures et images tatouées par la QIM-DA ……..... 67
Figure 4.5 : Images de couvertures et images tatouées par la méthode QIM-DE .....… 69
Figure 4.6 : Images de la marque avant et après tatouage …….……..... 71
Figure 4.7 : marques avec tailles différentes des textes..…….……..... 75

Liste des tableaux

tableau **Page**

Tableau 4.1 : Distorsion moyenne obtenu par l'algorithme LBG -VQ pour une source uniforme……..58

Tableau 4.2 : Distorsion moyenne obtenu par l'algorithme LBG-VQ pour une source Gaussienne …….58

Tableau 4.3 : Les variations de la PSNR du Système QV d'image avec taille du dictionnaire QV différent ……..…….……...… 63

Tableau 4.4 : *Comparaison entre les systèmes QV sans tatouage et avec tatouage QIM-DA* ……..…….. 66

Tableau 4.5 : *Comparaison entre les systèmes QV sans tatouage et avec tatouage QIM-DE* ……...…… 68

Tableau 4.6 : Les variations de la PSNR du Système QV d'image secrète avec taille du dictionnaire QV différent ……...…. 70

Tableau 4.7 : Les variations de la PSNR du système QIM-DA pour des clés K différentes ……..…….…….…… 72

Liste des abréviations

ASCII	Code américain normalisé pour l'échange d'information.
bpe	Bit par échantillon.
bpp	Bit par pixel.
dB	Décibel.
EQM	Erreur quadratique moyenne.
GLA	l'algorithme de Lloyd-Max généralisé.
LBG	Algorithme de Linde, Buzo et Gray.
mod	Modulo.
pdf	Fonction densité de probabilité.
pgm	Portable Gray Map.
PSNR	le rapport signal sur bruit de crête.
QIM	Quantification par modulation d'indice.
QIM-DA	Quantification par modulation d'indice par division aléatoire.
QIM-DE	Quantification par modulation d'indice par division équilibrée.
QS	Quantificateur scalaire.
QV	Quantificateur vectoriel.
QV_LBG	Quantificateur Vectoriel à base de l'algorithme LBG.
RSB	Rapport Signal sur Bruit.

Liste de notations

b_j	Le bit à dissimuler.
B	Ensemble des bits à cacher.
b_w	Le débit de codage pour l'image secrète.
$card(R_i)$	Le cardinale des classes.
$d(x, y_i)$	La distance quadratique entre x et y
d×d	Taille des blocs de l'image de couverture.
D	Distorsion moyenne entre la valeur originale et son représentant.
$D(R)$	La fonction distorsion débit.
e	Erreur de quantification.
E	Esperance mathématique.
f_i	La fonction fitness de l'algorithme génétique.
H	Hauteur d'une image.
I	Indice de quantification pour l'image de couverture.
I_w	Les indices obtenus après le codage de l'image secrète.
$I(X,Y)$	Information mutuelle entre X et Y
G_i	Groupe des vecteurs-codes.
k	Dimension des vecteurs pour VQ.
K	La clé utilisée pour la division du dictionnaire et pour la dissimulation.
L	La taille de dictionnaire.
m	Le débit de dissimulation.
M	Nombre de bloc de l'image de couverture.
N	Nombre de groupe des vecteurs-code.
Nb_w	Nombre de blocs de l'image secrète.
R	Le débit de codage pour l'image de couverture.
R_i	Les classes QV.
$R(D)$	La fonction de débit distorsion.
ℓ	La largeur d'une image.
w	La marque à cacher.
w'	Image secrète reconstruite.
x	Vecteur d'image de couverture.
X	Séquence d'apprentissage.
x'	Le vecteur d'image tatouée.

Y	Le dictionnaire conçu par LBG-image.
y_i	Les vecteurs-code.
Δx	L'écart entre l'image QV et l'image tatouée.
Δx_0	Le seuil de l'algorithme LBG.

Introduction générale

L'avènement d'internet à partir des années 1990, a ouvert de larges perspectives à différentes applications dans plusieurs secteurs d'activité. La quantité de données numériques échangées a ainsi connu une augmentation exponentielle, facilitée par la compression de données, l'efficacité des réseaux de communication et l'augmentation constante des débits de transfert de données. La démocratisation des services en ligne et la disponibilité d'ordinateurs à bas coût ont permis l'émergence de nouvelles offres de stockage et de distribution des images numériques notamment dans le domaine du multimédia, des transmissions par satellite ou de l'imagerie médicale… etc.

Cependant, la gratuité d'accès à ces données a facilité leur piratage, grâce notamment aux réseaux peer-to-peer et le téléchargement direct permettant le partage sans contrôle des fichiers. Par conséquent, les demandes de la protection des droits ainsi que l'authentification de données sont devenus de plus en plus empressées. Ceci a fait appel à la conception de systèmes de transmission sécurisés. Conventionnellement, ces systèmes se basaient principalement sur les techniques de cryptographie afin d'assurer une bonne sécurité contre les attaques (passives ou actives) de tout type. Cependant, dans certains environnements hostiles, cacher l'existence d'une communication est nécessaire pour éviter un certain nombre d'attaques de la part d'adversaires malintentionnés.

A l'heure actuelle, la dissimulation des données (Data Hiding) a connu une grande révolution qui a permis le développement de nouvelles techniques de sécurité de l'information dans le domaine des images. Parmi ces techniques figure le tatouage numérique qui est devenue l'un des outils les plus efficaces dans la lutte contre le piratage des images numériques.

L'objectif principal de ce projet est de concevoir un système de tatouage numérique d'images à base de la quantification vectorielle (QV). Dans notre étude, on s'est intéressé particulièrement à une technique de tatouage numérique appelée la quantification par modulation d'indice (QIM) basée sur la division du dictionnaire QV. Pour mettre en œuvre cette technique, nous avons commencé d'abord par implémenter un quantificateur vectoriel d'images par application de l'algorithme LBG. Il est composé d'une partie entrainement QV pour la conception du dictionnaire optimal et du codeur/décodeur QV d'images dont la dimension du vecteur d'image ainsi que le débit de codage sont modifiables. Ensuite, nous avons conçu le système de tatouage d'images par application de l'algorithme de la QIM basée sur la division du dictionnaire QV. Dans notre travail, la division du dictionnaire a été réalisée par deux méthodes : aléatoire et équilibrée. Les performances de nos systèmes de tatouage d'images seront évaluées

selon deux critères : la capacité de dissimulation représentée par le débit de dissimulation de l'image secrète et l'imperceptibilité (transparence) représentée par la qualité perceptuelle de l'image tatouée.

Ce mémoire est divisé en quatre chapitres structurés comme suit :

Dans le premier chapitre, on a essayé de faire un récapitulatif sur les notions élémentaires de traitement d'image.

Dans le deuxième chapitre, nous allons donner une idée générale sur le domaine de la dissimulation de données en définissant les principales techniques employées. On se focalisera particulièrement sur le tatouage numérique et les exigences que doit satisfaire un tel système. Nous citerons, en fin de chapitre, quelques domaines d'application du tatouage numérique.

Le troisième chapitre est consacré à la quantification vectorielle et QIM, un système de QV d'images basé sur l'algorithme LBG sera présenté. Nous commencerons par donner les formulations théoriques développées dans ce contexte. Par la suite, nous décrirons en général les systèmes de tatouage basés sur la QV. Et nous détaillerons le système de tatouage adopté qui est conçu à base de la technique de quantification par modulation d'indice. (QIM) avec ces trois phases : prétraitement, dissimulation et extraction. Les méthodes de division du dictionnaire seront ensuite présentées.

Enfin, le quatrième chapitre regroupe les résultats de simulation de la QV sur l'image qui est basé sur l'algorithme LBG et les résultats de simulation obtenus suite à l'application de la QIM dans le domaine de l'imagerie. Les performances des systèmes de tatouage QIM par division du dictionnaire QV avec les deux méthodes : aléatoire et équilibrée, seront présentées. Des évaluations comparatives entre ces deux méthodes seront présentées en fin de chapitre.

Nous terminons ce mémoire par une conclusion générale et quelques perspectives pour les travaux futurs.

Chapitre 1 :

Généralité sur le traitement des images

1.1. Introduction :

L'image constitue l'un des moyens les plus importants qu'utilise l'homme pour communiquer avec autre. C'est un moyen de communication universel dont la richesse du contenu permet aux êtres humains de tout âge et toute culture de se comprendre.

Le traitement numérique des images trouve des applications dans un nombre croissant de domaines, aussi divers que le tri automatique du courrier, le contrôle industriel, les télécommunications (compression) et la reconnaissance de cibles militaires. La croissance exponentielle des capacités des processeurs est pour une grande part dans le développement du traitement d'images, ce domaine étant, par nature, très gourmand en puissance de calcul. Le traitement d'images, par sa diversité même, est parfois très déroutant pour l'étudiant ou l'ingénieur débutant. Les informations que l'on souhaite extraire d'une image, les applications, les types de données, sont si variés qu'il est difficile, lorsque l'on doit traiter une nouvelle application, de savoir à quel modèle se raccrocher et quelle méthodologie suivre. Le présent ouvrage a pour objectif de donner au lecteur une bonne compréhension des principes de base du traitement d'images, associée à un certain esprit critique. A travers différents domaines applicatifs (restauration d'images, recalage, compression, reconnaissance de formes, etc.) il montre quels sont les raisonnements et méthodes qui permettent d'obtenir le résultat désiré et met en évidence quelques pièges à éviter.

1.2. Définition de l'image :

L'image est une représentation d'une personne ou d'un objet par la peinture, le dessin, la photographie, le film...etc. C'est aussi un ensemble structuré d'informations, qui après affichage sur l'écran, ont une signification pour l'œil humain [1].

Elle peut être décrite sous la forme d'une fonction I (x, y) de brillance analogique continue, définie dans un domaine borné, tel que **x** et **y** sont les coordonnées spatiales d'un point de l'image et **I** est une fonction d'intensité lumineuse et de couleur. Sous cet aspect, l'image est inexploitable par la machine, ce qui nécessite sa numérisation [2].

1.3. Image numérique :

Contrairement aux images obtenues à l'aide d'un appareil photo, ou dessinées sur du papier, les images manipulées par un ordinateur sont numériques (représentées par une série de bits) [2]. L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleur prélevé à

l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter [3].La numérisation d'une image est la conversion de celle-ci de son état analogique (distribution continue d'intensités lumineuses dans un plan (x * y) en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques $I(x, y)$ où: x, y : coordonnées cartésiennes d'un point de l'image. I (x, y) : niveau de gris en ce point.

Pour des raisons de commodité de représentation pour l'affichage et l'adressage, les données images sont généralement rangées sous formes de tableau I de n lignes et p colonnes. Chaque élément I (x, y) représente un pixel de l'image et à sa valeur est associé un niveau de gris codé sur m bits (2^mniveau de gris ; 0 = noir ; 2^m-1 = blanc). La valeur en chaque point exprime la mesure d'intensité lumineuse perçue par le capteur [2].

1.4. Les attributs de l'image :

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants:

1.4.1 Pixel :

Contraction de l'expression anglaise "*Picture Cell* " : éléments d'image, le pixel est le plus petit point de l'image, c'est une entité calculable qui peut recevoir une structure et une quantification. Si le bit est la plus petite unité d'information que peut traiter un ordinateur, le pixel est le plus petit élément que peuvent manipuler les matériels et logiciels d'affichage ou d'impression. La quantité d'information que véhicule chaque pixel donne des nuances entre images monochromes et images couleurs. Dans le cas d'une image monochrome, chaque pixel est codé sur un octet, et la taille mémoire nécessaire pour afficher une telle image est directement liée à la taille de l'image.

Dans une image couleur ($R.V.B$), un pixel peut être représenté sur trois octets : un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B). [1]

1.4.2. Dimension (définition) :

On appelle définition d'une image, le nombre de points (pixel) constituant l'image, c.à.d sa (dimension informatique). Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multiplié par le nombre de colonnes nous donne le nombre total de pixels dans une image. [1]

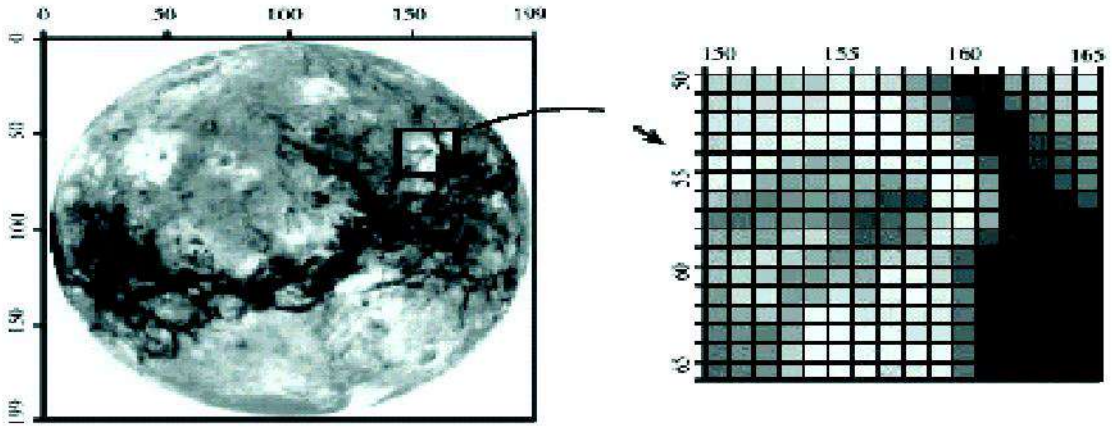
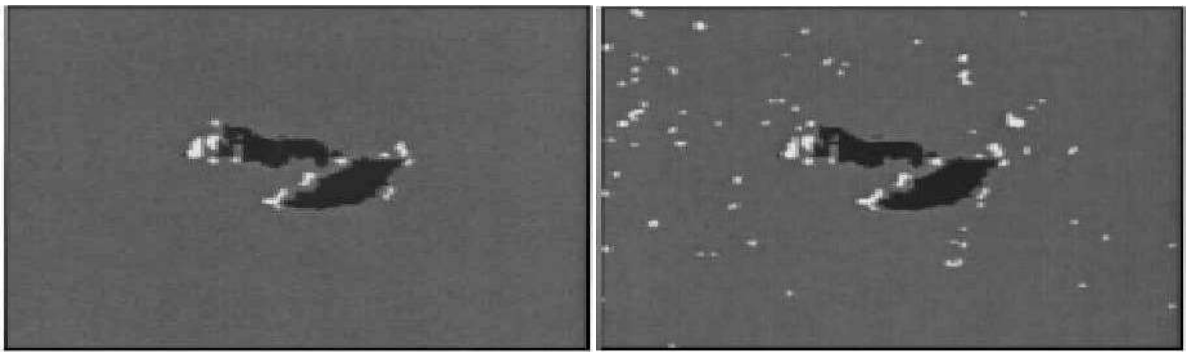


Figure 1.1 : Représentation de dimension d'une image

1.4.3. Bruit :

C'est un signal qui lors de l'acquisition ou la transmission vient s'ajouter à l'image, Il se matérialise par la présence dans une région homogène des valeurs plus ou moins éloignées de l'intensité de la région. Le bruit est le résultat de certains défauts électroniques du capteur et de la qualité de numérisation.



a)-Image sans bruit b)-Image avec bruit

Figure 1.2 : Images avec et sans bruit

1.4.4. Résolution :

C'est la clarté ou la finesse de détails atteinte par un moniteur dans la production d'images .Sur les moniteurs d'ordinateurs, la résolution est exprimée en nombre de pixels par unité de mesure (pouce ou centimètre). On utilise aussi le mot résolution pour désigner le nombre total de pixels affichables horizontalement ou verticalement sur un moniteur ; plus grand est ce nombre, meilleure est la résolution [1].

1.4.5. Contours et Textures :

Les contours représentent la frontière entre les objets de l'image, ou la limite entre deux pixels dont les niveaux de gris représentent une différence significative [4]**.** Les textures décrivent la structure de ceux-ci. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différentes (figure 1.3).

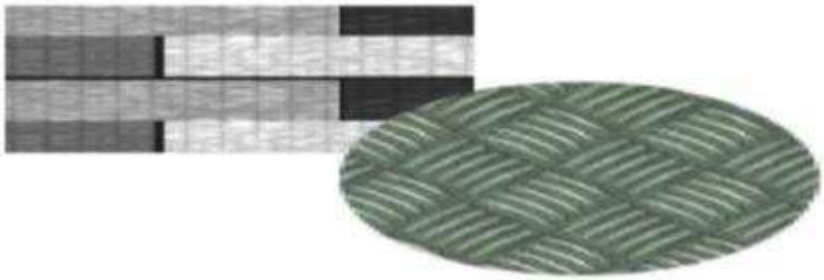


Figure 1.3 : Image avec texture

1.4.6. Luminance :

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance, qui correspond à l'éclat d'un objet. Une bonne luminance se caractérise par : [1]

1. Des images lumineuses (brillantes).
2. Un bon contraste : il faut éviter les images où la gamme de contraste tend vers le blanc ou e noir; ces images entraînent des pertes de détails dans les zones sombres ou lumineuses.
3. L'absence de parasites.

1.4.7. Contraste :

C'est l'opposition marquée entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Le contraste est défini en fonction des luminances de deux zones d'images. Si *L1* et *L2* sont les degrés de luminosité respectivement de deux zones voisines *A*l et *A*2 d'une image, le contraste *C* est défini par le rapport :

$$C = (L1 - L2) / (L1 + L2) \qquad (1.1)$$

1.4.8. Le poids de l'image :

Le poids d'une image se détermine en fonction de ces 3 paramètres : dimensions, résolution et nombre de couleurs. Il se mesure en octets.

1.5. Les différents types d'images :

II existe différentes catégories d'image selon le nombre de bit sur lequel est codée la valeur de chaque pixel.

1.5.1. Mode Monochrome :

Le mode monochrome (figure 1.4) est le plus simple ; chaque pixel *y* est soit allumé [*Blanc*], soit éteint [*Noir*], l'image obtenue n'est pas très nuancée. Alors, pour convertir une image couleur en mode monochrome il faut d'abord passer par le mode à niveaux de gris [4].

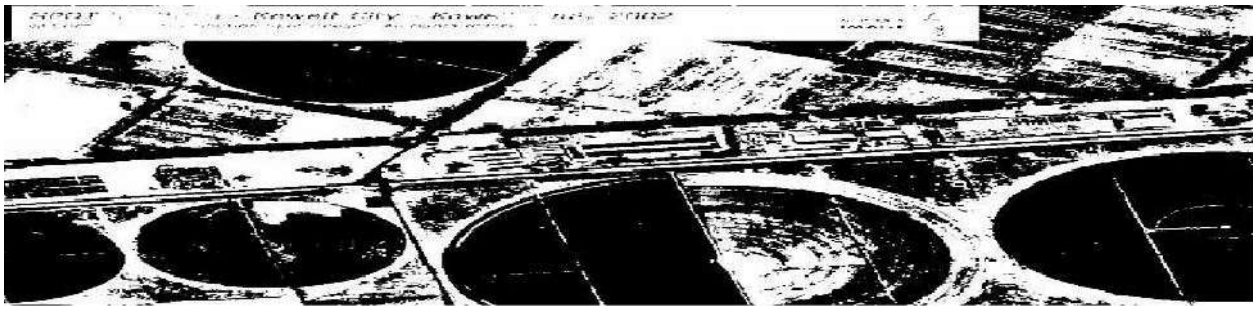


Figure 1.4 : Image en mode monochrome

1.5.2. L'image en niveaux de gris :

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Donc pour représenter les images à niveaux de gris (figure 1.5), on peut attribuer à chaque pixel de l'image une valeur correspondante à la quantité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255. Chaque pixel n'est donc plus représenté par un bit, mais par un octet [3].

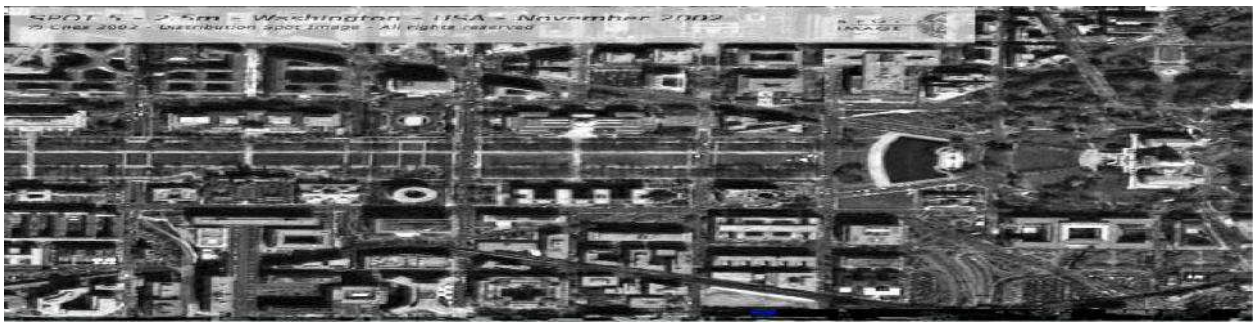


Figure 1.5 : Image en mode niveau de gris

1.5.3. L'image en couleurs :

Même s'il est parfois utile de pouvoir représenter des images en noir et blanc ou en niveau de gris, les applications multimédias utilisent le plus souvent des images en couleurs (figure 1.6).La représentation des couleurs s'effectue de la même manière que les images monochromes avec cependant quelques particularités. En effet, il faut tout d'abord choisir un modèle de représentation.



Figure 1.6 : Image en mode couleur

Pour cela on utilise un espace de couleur à plusieurs dimensions qui consiste à donner suffisamment de composantes numériques pour décrire une couleur. Il y a des différentes représentations des images couleur :

1- La représentation en couleurs réelle sur 24 bits.
2- La représentation en couleurs indexées ; on utilise une table appelée palette pour éviter la redondance de couleur.
3- Le mode *RGB* est idéal pour l'affichage sur écran, une image *RGB* est composée de trois couches *Rouge*, *Vert* et *Bleu*. Chaque pixel est définit par une valeur possible de ces couleurs de [0 à 255]. Une fois combinées, ces couches permettent de générer toutes nuances de couleur. Le mode RGB correspond à l'affichage des moniteurs, où chaque point affiché est décomposé d'un mélange de lumière *RGB*.

1.6. Les Formats d'image :

1.6.1. Les images bitmap :

Les images affichées sur l'écran d'un *PC* sont des images matricielles, encore appelées bitmap, chaque image est en réalité une matrice de pixels.

1.6.1.1. Les différents formats d'Images bitmap :

1- ***Le format GIF (Graphic Interchange Format) :***Créé par Compuserve, utilise aussi le codage *RVB*, mais le format *GIF* n'utilise pas toutes les 16 millions de couleurs. Il prend les 256 couleurs les plus courantes pour réaliser l'image au format *GIF*. Cela permet une bonne compression et un affichage rapide de l'image.

2- ***Le format JPG ou JPEG (Joint Photographique Experts Group):*** Créé par un consortium industriel, ce format très utilisé sur Internet, permet d'afficher les images en mode 16millions de couleurs et donc c'est le mode sans perte. Le codage d'un pixel (point de l'affichage) 3*x*1, byte (*RVB*) soit :(0<*R*<255), (0<*V*<255), (0<*B*<255). Le format *JPG* peut aussi être utilisé pour compacter les images, il utilise un algorithme de compression qui réduit énormément la taille des images.

3- ***Le format PCX (Picture Exchange Image Bitmap Zsoft)*** **:** a été créé à l'origine par *ZSoft* pour un programme de dessin (paint bruch)

1.6.1.2. Avantages et inconvénients :

1- **Avantages :**
   - Format proche du hardware (sauf processeur dédié).
   - Adaptable aux images complexes.

2- **Inconvénients :**
   - Modification spatiales difficile, transformation par réduction => perte d'information, transformation par agrandissement => grossissement des points.
   - Encombrement important.

1.6.2. Les images vectorielles :

L'image vectorielle est définie par une fonction mathématique. Pour définir par exemple la silhouette de la lettre *"d"*, on dira à l'ordinateur de dessiner un anneau, à la droite de la quelle est accolé un rectangle vertical et allongé de même couleur, positionné de manière spécifique par rapport à l'anneau. Mais pour afficher à l'écran ou imprimer, ces images vectorielles sont en fait

automatiques traduites en images bitmap, car c'est le seul format directement affichable par ordinateur [1].

1.6.2.1. Les différents formats d'images vectorielles :

1- ***Le format EPS (Postscript / Encapsulated Postscript)***: Le Postscript est un langage de description de page conçu pour imprimer des documents indépendamment du périphérique utilisé. Il contient toutes les commandes nécessaires pour dessiner l'image sauvegardée.

2- ***Le format CGM (Computer Graphics Metafile)*** : Les fichiers graphiques *CGM* restent un moyen privilégié d'échange de dessins vectoriels entre applications, mais il ne traite pas les images bitmaps.

1.6.2.2. Avantages et inconvénients :

1- **Avantages :**
   - Adaptable à chaque périphérique (car ajustable, coordonnées relatives, adaptable aux drivers intelligents, ...).
   - Stockage moins encombrant (la taille ne dépend que de la complexité du document lui-même).
   - Adapté aux objets mathématiques et leur extension (voiture, avion,...).

3- **Inconvénients :**
   - Mal adapté aux images quelconques.
   - La difficulté de traitement d'une partie de l'image.

1.7. Domaines d'application :

Parmi les domaines d'application de traitement d'images on peut citer :

1- ***Imagerie aérienne et spatiale:*** dans laquelle les traitements concernent l'étude des images satellites, l'analyse des ressources terrestres, la cartographie automatique, les analyses météorologiques.

2- ***imagerie médicale :*** on trouve des utilisations de cette technique dans l'échographie, la résonance magnétique nucléaire, ainsi que dans le domaine de la reconnaissance automatique des cellules ou de chromosomes.

3- ***La robotique:*** qui connaît actuellement le plus grand développement et dont les tâches suant de l'imagerie sont principalement l'assemblage (pièce mécanique, composants électroniques,…), le contrôle de la qualité, ainsi que la robotique mobile.

4- ***Simulation et contrôle de processus :*** on trouve des utilisations de cette technique dans les cours de pilotage et le contrôle des Panneaux [5].

1.8. Qualité de l'image numérique :

Elle dépend, d'une part, de la qualité des images d'origine, et d'autre part, des moyens mis en œuvre pour convertir un signal analogique en signal numérique. Elle dépend aussi de :

1- La qualité des périphériques de numérisation de l'image, du nombre de niveaux de gris ou de couleurs enregistrées, etc.

2- La qualité de l'affichage à l'écran : définition de l'écran, nombre de teintes disponibles simultanément, calibrage de l'écran, etc.

Les critères d'appréciation de la qualité d'une image, tels que cités succinctement ci-dessus, dépendent largement de la structure même de l'image réaliste ou conceptuelle et de son mode de représentation (bitmap ou vectorielle) [1 ; 6].

1.9. Compression d'image :

Les méthodes de compression et de codage réduisent le nombre de bits par pixel à stocker ou à transmettre, en exploitant la redondance informationnelle dans l'image [7].

Les principaux critères d'évaluation de toute méthode de compression sont :

- La qualité de reconstitution de l'image.
- Le taux de compression.
- La rapidité du codeur et décodeur (codec).

1.9.1. Schéma fonctionnel de la compression des images :

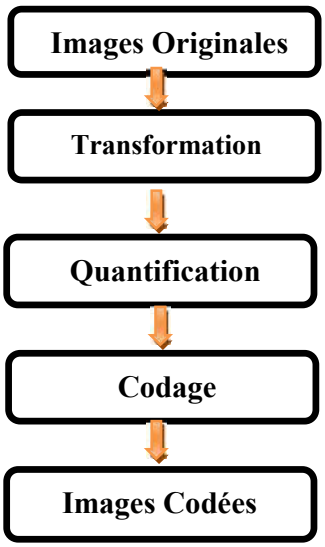


Figure1.7 : schéma fonctionnel de la compression des images

Le schéma fonctionnel de la compression est présenté dans la figure1.7 :

A partir de ce schéma, nous allons revoir chacune de ses étapes à fin de préciser leur rôle.

1. **Transformation :**

La dépendance existante, entre chacun des pixels et ses voisins (la luminosité varie très peu d'un pixel à un pixel voisin), traduit une corrélation très forte sur l'image. On essaie donc de tirer partie de cette corrélation, pour réduire le volume d'information en effectuant une opération de décorrélation des pixels.

Le décorrélation consiste à transformer les pixels initiaux en un ensemble de coefficients moins corrélés, c'est une opération réversible.

2. **Quantification :**

La quantification des coefficients a pour but de réduire le nombre de bits nécessaires pour leurs représentations. Elle représente une étape clé de la compression. Elle approxime chaque valeur d'un signal par un multiple entier d'une quantité q, appelée quantum élémentaire ou pas de quantification. Elle peut être scalaire ou vectorielle. Un des résultats fondamentaux des travaux de Shannon concernant la relation : (débit /distorsion) montrent que l'on obtient de meilleures performances en utilisant la quantification vectorielle.

3. **Codage :**

Une fois les coefficients quantifiés, ils sont codés. Un codeur doit satisfaire a priori les deux conditions suivantes :

- Unicité : deux messages différents ne doivent pas être codés de la même façon.
- Déchiffrabilité : deux mots de codes successifs doivent être distingués sans ambiguïté.

1.9.2. Classification des méthodes de compression :

La plupart des méthodes de compression visent à enlever la redondance présente dans l'image de manière à diminuer le nombre de bits nécessaires à sa représentation [8].Plusieurs types de redondance en termes de corrélation peuvent être considérés :

- La redondance spatiale entre pixels ou blocs voisins dans l'image.
- La redondance temporelle entre images successives dans une séquence vidéo.

Les méthodes de compression peuvent se regrouper, en deux classes :

- Les méthodes sans perte d'informations (sans distorsion ou réversible).
- Les méthodes avec perte d'informations (avec distorsion ou irréversible).

Les expérimentations menées montrent que généralement les méthodes qui atteignent des taux de compression très élevés sont les méthodes avec distorsion. Par contre, les méthodes sans

distorsion engendrent des taux de compression très faibles et ne sont utilisées que dans des applications sensibles telles que les images médicales et les images satellites.

1.10. Conclusion :

Dans ce chapitre, on a essayé de faire un récapitulatif sur les notions élémentaires de traitement des images.

On a porté aussi sur les problèmes de taille rencontrée lors de la manipulation de l'image et le besoin de compression, transformation, quantification, codage, comme solutions à ces problèmes.

Chapitre 2 :

Notions de base sur les systèmes du tatouage

2.1. Introduction :

Faciliter l'accès à l'information, développer et créer de nouveaux moyens de communication, promouvoir l'interactivité, sécuriser les échanges …tels sont les enjeux industriels et commerciaux de ces dernières années et de celles à venir. Les techniques de dissimulation de données, favorisées par l'avènement des documents sous format numérique, offrent des possibilités innovantes dans ce domaine : un document hôte (en particulier une image numérique) peut cacher une information numérique aux applications diverses et servir de nouveau support de transmission. Les techniques de dissimulation sont alors appelées stéganographie ou tatouage numérique.

Une marque numérique est une information insérée au document hôte ou de couverture en toute imperceptibilité et robustesse de façon à ne jamais pouvoir l'en accéder. Elle contient généralement une information concernant son origine. L'information cachée sert à différents intérêts en fonction de l'application à laquelle elle est destinée. Les fortes demandes industrielles en matière de protection de la propriété intellectuelle la conduisent souvent à devenir une signature ineffaçable même face à un utilisateur malveillant, appelé pirate, qui mettrait tout en œuvre pour la supprimer. En parallèle de ce contexte sécuritaire particulier, cette information permet également d'augmenter le contenu du document hôte, de lui apporter une valeur ajoutée.

Ce chapitre se propose de spécifier les contraintes à satisfaire par un système de tatouage au regard de l'application envisagée. Il présente aussi les différentes applications gravitant autour du tatouage, et les raisons pour les quelles le tatouage numérique et ces techniques intelligentes sont significatifs pour donner des solutions aux problèmes du monde digital courant et de définir les deux systèmes de codage de base que sont la quantification scalaire et vectorielle dont on va exposer les étapes fondamentales des algorithmes correspondants, et nous décrironsle principe de conception d'un système à base du quantificateur vectoriel qui sera appliqué au codage d'images.

2.2. Historique :

Le tatouage numérique est une discipline très récente, dont on fait remonter la naissance en 1990 sur une méthode pour cacher de l'information dans une image.

Le terme digital watermark (tatouage numérique) fut pour la première fois employé en 1992 par Andrew Tirkel et Charles.

Paul Levinson parle également de tatouage numérique en embarquant dans chaque élément technologique une puce électronique qui donnerait la liste des inventeurs.

Ingemar Cox popularisa les techniques d'étalement de spectre pour le tatouage numérique. L'invention des systèmes de re-synchronisation en 1998 marqua la disciplie de même que le tatouage avec information adjacente en 1999.

2.3. Terminologie :

A l'heure actuelle, nous sommes face à la communication numérique. Comme dans la communication analogique classique, la communication numérique s'intéresse aux méthodes qui tolèrent la transmission d'une information dissimulée ou insérée dans une autre donnée. Bien que ces techniques partagent souvent des principes similaires et des idées basiques, cependant ils existent aussi d'importants éléments distinctifs, principalement en termes de robustesse contre les attaques. Des appellations multiples ont été forgées pour de telles techniques, quoique les termes sont souvent confus ; d'où la nécessité de clarifier les différences.

2.3.1. Stéganographie :

Elle consiste en l'altération d'un contenu d'une manière indétectable dans le but d'insérer un message (voir [9] pour plus de détails). En effet, la stéganographie est l'art de la dissimulation d'un message privé ou secret dans un support [10]. Elle sert généralement à communiquer secrètement à travers des réseaux publics. Ainsi, elle est souvent utilisée dans le domaine militaire ou le contre-espionnage.

La figure 2.1 montre comment la dissimulation de l'information peut être implémentée dans différents domaines. La stéganographie peut être utilisée pour dissimuler un message destiné pour une récupération ultérieure par un individu ou groupe spécifique. Dans ce cas le but est de priver la détection de n'importe quelle autre partie [11].

Un autre domaine majeur de la stéganographie est le marquage pour la protection des droits, où le message à insérer est utilisé pour assurer la protection des droits à travers le document. Ce cas peut être représenté par un tatouage et des empreintes digitales qu'on va aborder dans ce qui suit [11].

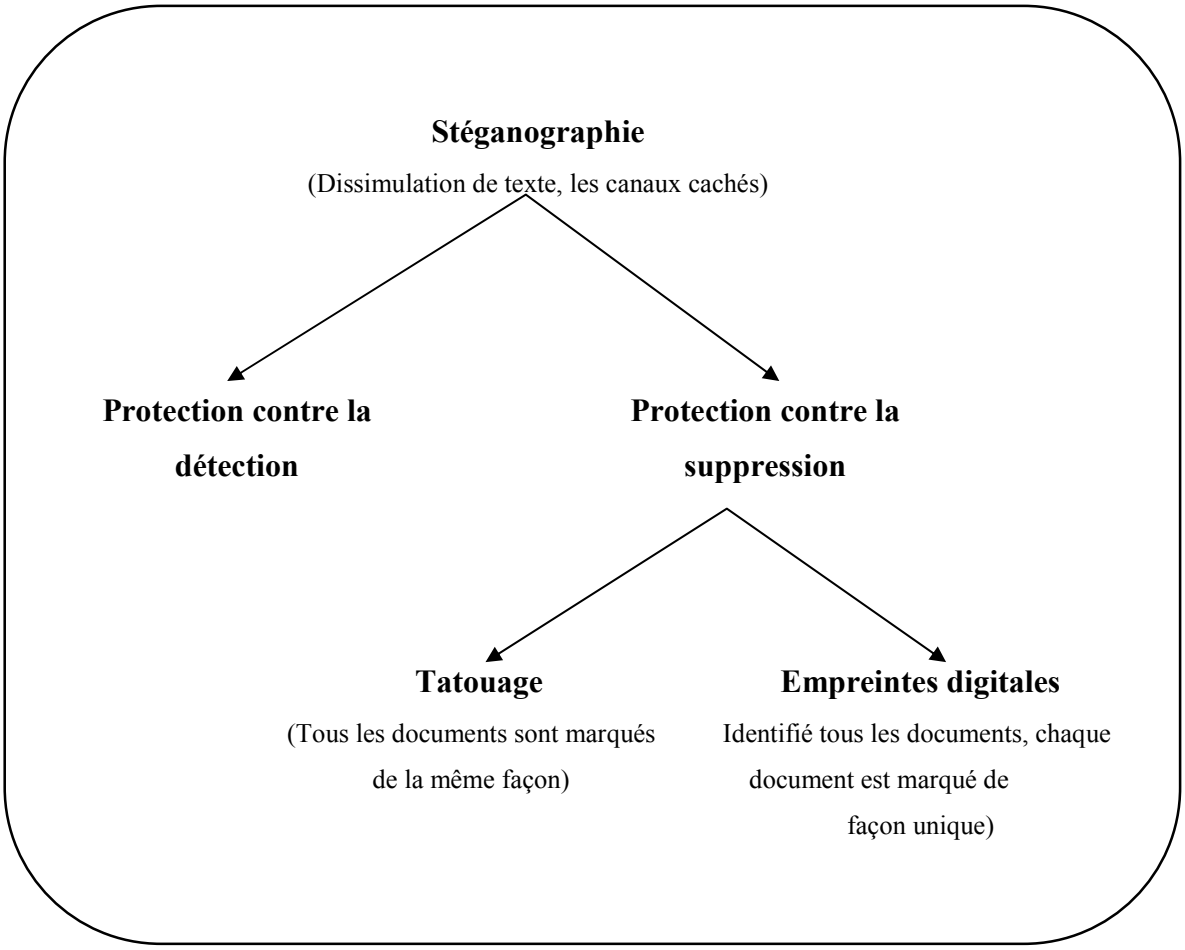


Figure 2.1 : Les différents domaines de la stéganographie

2.3.2. Tatouage :

Le tatouage fait souvent référence à l'insertion d'une information dans un contexte sécuritaire, notament de protection contre le piratage. L'information dissimulée, qui est souvent associée à une signature ou une marque, est liée au contenu même du document. Elle régit la propriété, l'authenticité et les droits d'utilisation du document.

Contrairement à la stéganographie, la technique de tatouage suppose que la communication est connue d'une tierce personne, le pirate. En effet, le tatouage vise justement à adapter le marquage en fonction de l'action de ce pirate sur le document : la signature doit être ineffaçable si l'on souhaite lutter contre le piratage des documents ; à l'inverse, elle doit disparaitre dès que le pirate modifie le document si l'on souhaite garantir l'intégrité du document [12].

2.3.3. Dissimulation de données et insertion de données :

Ceux sont des termes utilisés dans divers contextes [12], mais ils représentent généralement soit la stéganographie ou des applications " entre " la stéganographie et le tatouage, ce qui

signifie que les applications où l'existence des données insérées sont publiquement connus, mais ce n'est pas nécessaire de les protéger. C'est typiquement le cas d'une transmission dans laquelle on ajoute des informations ou des services auxiliaires qui sont accessibles au public et ne portent pas sur la protection des droits d'auteur ou de fonctionnalités d'accès conditionnel.

2.3.4. Empreintes digitales et étiquetage :

Ceux sont des termes qui dénotent des applications spéciales de tatouage [12]. Ils portent sur les applications de protection des droits d'auteur où l'information sur l'émetteur et le récepteur des données numériques est insérée comme tatouage. Les tatouages individuels, qui sont des codes uniques sur une série de codes, sont appelés "empreintes digitales" ou "étiquettes".

2.3.5. Tatouages visible :

Comme leur nom l'indique, les tatouages visibles sont des motifs visuels (comme des logos) qui sont insérés dans (ou superposées sur) les images ou les vidéos [12]. Ils sont très semblables aux tatouages visibles sur un papier. Le tatouage visible est principalement appliqué aux images, par exemple, pour tatouer visiblement les images de prévisualisation disponibles dans les bases de données d'images ou sur le World Wide Web afin d'empêcher les gens de l'utilisation commerciale de ces images. Une méthode de tatouage visible conçue par Braudaway et al [13] combine l'image représentant le tatouage avec l'image d'origine en modifiant la luminosité de l'image originale en fonction du tatouage et une clé secrète. La clé secrète détermine les valeurs pseudo-aléatoires de mise à l'échelle utilisées pour la modification de la luminosité, afinde rendre difficile pour les attaquants de supprimer la marque visible [12].

2.4. Formes de données de dissimulation :

La dissimulation de données [12] peut être classée de différentes manières en fonction de :

- L'importance relative des signaux de couverture et de messages à dissimuler,
- La nature du contenu de la couverture,
- L'exigence du signal de couverture non modifié pour l'extraction de la marque,
- Le type de communication subliminale asynchrone ou synchrone,
- Le type d'attaques pour éliminer les messages dissimulés : les gardiens actifs et passifs.

2.5. Tatouage numérique :

C'est l'application la plus connue du ***data-hiding***. D'ailleurs, le tatouage numérique est souvent utilisé comme le terme générique qui désigne tout les systèmes de data-hiding. Il est défini comme l'ensemble des modifications robustes et invisibles dans un document hôte. Ces

modifications permettent d'insérer une information qui concerne directement le document tatoué, copyright par exemple, ou indirectement, tel que les droits de l'utilisateur sur le contenu (pour plus d'informations voir par exemple les références suivantes [14], [15], [16]).

La plupart des algorithmes de tatouage reposent sur le même modèle et diffèrent seulement par la stratégie spécifique à certains niveaux du processus d'insertion ou d'extraction/ détection de la marque. Il est possible donc de présenter d'une façon générique un système tatouage comme le montre la figure suivante.

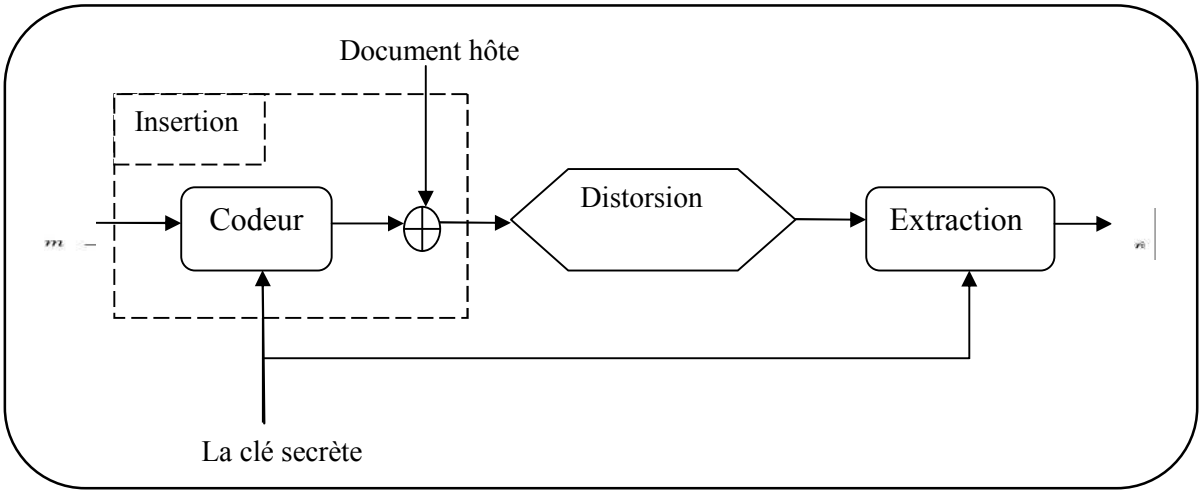


Figure 2.2 : Schéma général d'un système de tatouage numérique

2.5.1. Exigences :

Les exigences de base en tatouage s'appliquant à tous les médias sont mentionnées ci-dessous [17] :

2.5.1.1. Sécurité de la marque et les clés :

Si la sécurité des informations insérées est exigée, une ou plusieurs clés secrètes doivent être utilisées pour les procédures d'insertion et d'extraction. Il existe dans ce contexte deux niveaux de sécurité :

- Dans le premier niveau, un utilisateur non autorisé ne peut ni lire ni décoder une marque insérée et ne peut détecter si un ensemble de données contient une marque.
- Le deuxième niveau permet aux utilisateurs non autorisés de détecter si des données sont tatouées. Cependant, les informations insérées ne peuvent pas être lu sans avoir la clé secrète. Ces systèmes peuvent, par exemple, insérer deux marques, l'une avec une clé publique et l'autre avec une clé secrète.

Lors de la conception un système de protection des droits d'auteur, des problèmes comme la génération des clés secrètes, la distribution et la gestion (éventuellement par des tiers

de confiance), ainsi que d'autres aspects des systèmes d'insertion doivent être considérés.

2.5.1.2. Robustesse :

Dans la conception d'un système de tatouage, la robustesse de la marque est généralement l'un des principaux problèmes, du moment où la robustesse contre les distorsions des données introduites suite à un traitement standard ainsi que les attaques est une importante exigence. Le traitement standard de données comprend toute manipulation et/ou modification que les données pourraient subir dans la chaîne de diffusion habituelle, telles que l'édition de données, l'impression, l'amélioration, et la conversion de format. Le mot "Attaque" désigne la manipulation des données dans le but d'affecter, détruire ou enlever les marques insérées. Bien qu'il soit possible de concevoir des techniques de tatouage robustes, il convient de noter que la marque est uniquement robuste tant qu'elle n'est pas publique ; c.-à-d, tant qu'elle ne peut pas être lue par tout le monde. Si le principe de détection de la marque et la clé sont publiques, et même si seulement un détecteur de marque en " boîte noire "est public, la marque est alors vulnérable aux attaques. Par conséquent, les marques publiques, comme celles parfois proposées dans la littérature, ne sont pas robustes à moins que chaque récepteur utilise une clé différente. Ce qui est cependant difficile en pratique et donne lieu à des attaques de collusion.

2.5.1.3. Imperceptibilité:

L'une des principales exigences pour un tatouage est la transparence perceptuelle. Le processus d'intégration de données ne doit pas présenter aucun effet artificiel perceptible dans les données hôtes. Ainsi, la conception d'un procédé de tatouage implique toujours un compromis entre l'imperceptibilité et la robustesse. Il serait optimal d'insérer une marque juste au-dessous du seuil de perception. Toutefois, ce seuil est difficile à déterminer dans le cas des images du monde réel, vidéo et signaux audio. Plusieurs mesures pour déterminer objectivement la distorsion perçue et le seuil de perception ont été proposées pour les médias mentionnés. Cependant, la plupart de ces mesures ne sont pas encore assez parfaites pour remplacer les téléspectateurs ou auditeurs humains qui jugent la fidélité visuelle ou audio grâce à des tests aveugles. Le second problème apparait en combinaison avec le post-traitement de tatouage, ce qui pourrait entraîner une amplification de la marque intégrée et qui va la rendre perceptible .Un exemple est le zoom d'images tatouées, qui rend souvent la marque intégrée visible ; ou l'amélioration du contraste, qui peut amplifier les configurations très fréquentes de la marque qui sont autrement invisibles.

2.5.1.4. Récupération de la marque avec ou sans les données d'origine :

La récupération de la marque est généralement plus robuste si les données originales sans marque sont disponibles. En outre, la disponibilité de l'ensemble de données d'origine dans le processus de récupération permet la détection et l'inversion des distorsions qui changent la géométrie des données. Cela aide, par exemple, si une image tatouée a été tournée par un attaquant. Cependant, l'accès aux données originales n'est pas possible dans tous les cas, comme par exemple, dans la surveillance ou le suivi des données. Pour d'autres applications, comme le tatouage vidéo, il peut être difficile d'utiliser les données d'origine en raison de leur grand volume, même si elles sont disponibles. Il est, cependant, possible de concevoir des techniques de tatouage qui ne nécessitent pas l'original pour l'extraction de la marque.

La plupart des techniques de tatouage effectuent une sorte de modulation, dans laquelle la base de données initiale est considérée comme une distorsion. Si cette déformation est connue ou peut être modélisée dans le processus de récupération, les techniques désignées explicitement vont permettre sa suppression sans connaitre l'original. En fait, la plupart des méthodes récentes n'ont pas besoin de la donnée originale pour la récupération de la marque. Dans certaines publications [16], ces techniques sont appelés techniques "aveugles" de tatouage.

2.5.1.5. Extraction de la marque ou vérification de sa présence :

Dans la littérature, deux types différents de systèmes de tatouage peuvent se présenter [16]: les systèmes qui insèrent des informations connues ou un motif spécifique et vérifient après l'existence de l'information dans la phase de récupération de la marque (en utilisant généralement des techniques de test par hypothèses), et les systèmes qui insèrent des informations arbitraires dans les données de l'hôte.

Dans le premier type, la vérification de la présence d'une marque connue est suffisante pour la plupart des applications de protection des droits d'auteur.

Dans le second type, l'insertion de l'information arbitraire est utile, par exemple, pour le suivi d'une image sur Internet par des agents intelligents où il pourrait non seulement être d'intérêt de découvrir des images, mais aussi de les classer. Dans de tels cas, la marque insérée peut servir comme un numéro d'identification d'une image. Un autre exemple où des informations arbitraires insérés sont des applications pour la distribution vidéo où, par exemple, le cas où le numéro de série du récepteur doit être inséré.

Bien que la plupart des méthodes présentées soient conçus pour l'extraction de la marque ou la vérification de présence d'une marque, il convient de noter qu'en faite, les deux approches

sont fondamentalement équivalentes. Un système de récupération de marque peut être considéré comme un système de vérification de marque en supposant que l'information insérée est connue.

2.5.1.6. Capacité d'insertion :

La capacité d'insertion est la quantité maximale d'information pouvant être transmise pour une probabilité d'erreur quasi nulle. Le débit d'insertion exigé par le système de tatouage est fortement dépendant de l'application envisagée. Par exemple, dans le contexte de marquage pour la protection des droits d'auteurs, la capacité n'est pas primordiale. L'insertion d'un numéro d'identification codé sur 64 bits suffit dans ce contexte tandis que le débit d'insertion vaut un millier de bits pour des applications de réduction de bruit. Dans la plupart des cas, il convient de choisir un système de tatouage permettant une capacité d'insertion la plus grande possible [18].

2.5.1.7. Le coût :

Certaines applications étant destinées à fonctionner en temps-réel, le coût en termes de temps de calcul peut être alors un critère déterminant dans le choix d'une technique de tatouage.

Satisfaire ces objectifs définit la notion de performance d'un système de tatouage. Différents critères d'évaluation doivent être alors mis en œuvre pour juger la performance de ce système [18].

2.6. Le codage de la marque :

Souvent, en tatouage numérique, la signature à insérer est un message binaire {0,1}, un logo (une image binaire ou de même nature que l'image originale). La marque est générée de façon pseudo aléatoire à partir de la signature. Le nombre utilisé dans cette génération constituera la première clé KI de l'algorithme du tatouage. Ce nombre permet par la suite de déterminer le message. Par exemple, **Li** et $\mathbf{C_{ox}}$ brouillent (randomiser) l'information binaire à insérée de façon pseudo aléatoire afin d'améliorer la performance de la détection.

Les codes correcteurs d'erreur sont potentiellement utilisés en tatouage numérique pour coder et protéger la marque des erreurs de transmission ou de stockage (attaques), et ainsi augmenter les performances en termes de la robustesse des algorithmes de tatouage.

Différents codes dérivés des codes correcteurs d'erreur sont alors proposés, Chen et al proposent l'utilisation des codes cycliques dans l'authentification de visages photographiques par tatouage d'images, ce sont des codes linéaires utilisés en raison de leurs bonne adaptation à la détection des erreurs indépendantes et à la détection possible par paquets, Schönfeld et Winkler propose l'insertion de watermark en utilisant le codage BCH.

2.7. Les méthodes d'insertion :

Nous avons cité ci-dessus que la phase d'insertion désigne l'opération qui consiste à passer d'une image original *I* et d'un watermark w à une image tatouée *Iw*.

On classe les techniques de tatouage, suivant la phase d'insertion, en deux catégories : l'insertion additive et substitutive.

2.7.1. Méthode additive :

La Figure (2.3) présente le schéma de la méthode additive pour l'insertion du message. Le tatouage est ajouté aux composantes du document.

Le signal hôte *x* peut cependant intervenir dans la génération de w, soit par l'emploi d'un masque perceptuel, soit dans une adaptation au tatouage : $w = g(m, KI, x)$.

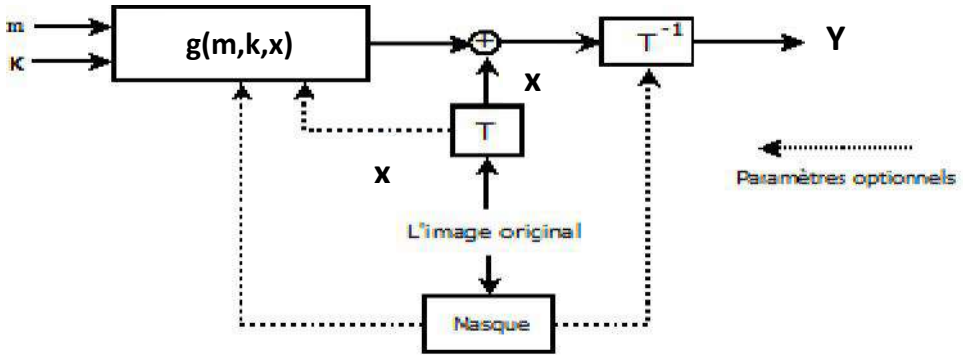


Figure 2.3 : L'insertion du message par tatouage additif

La prise en compte de critères psycho-visuels et de caractéristiques propres à l'image permet d'avoir un bon compromis entre la robustesse et l'invisibilité.

La technique la plus populaire pour ce type de schéma est l'étalement de spectre. Cette technique a été utilisée pour la première fois en tatouage numérique d'image par Cox. Le principe consiste à coder les symboles de m séparément en utilisant une modulation par des séquences pseudo-aléatoire (appelées porteuses). Cette technique permet d'assurer un cryptage du message, de fait que la détection nécessite la connaissance de la porteuse utilisée qui dépend d'une clé secrète. La détection est effectuée par l'exploitation des caractéristiques statistiques de la marque insérée avec le document tatoué.

Souvent un calcul de corrélation permet de détecter l'existence de la marque.

L'avantage de cette méthode de modulation est qu'elle a une grande robustesse aux déformations et bruit pouvant perturber l'image tatoué.

Le principal inconvénient par contre, est la capacité de tatouage très réduite pour ce genre de méthode. En effet, le document hôte est considéré comme source d'interférences et une partie de la capacité est perdue pour résister à ces interférences. De plus, l'encodage se fait de manière indépendante de l'hôte (le vecteur x). Du point de vue visuel, le résultat est assez efficace, car la modulation par une séquence proche d'un bruit blanc passe bien inaperçue à peu près par tout, sauf dans les sections uniformes. Pour cela, Malvar et Florêncio ont introduit l'étalement de spectre amélioré (ISS) qui permet de prendre en compte le vecteur x dans le codage de message (l'information adjacente).

2.7.2. Méthodes substitutives :

A l'inverse des méthodes additives, le tatouage substitutif se propose de substituer un élément de l'image originale par un autre tatoué. Le watermark à insérer est obtenue en appliquant une contrainte (une mesure de similarité, une propriété géométrique, un critère d'ordre …) afin de le faire correspondre au message que l'on souhaite transmettre.

On distingue dans ces méthodes le tatouage par quantification et le tatouage par contrainte.

2.7.2.1. Tatouage par quantification :

Appelé aussi tatouage substitutif avec dictionnaire. Le principe est de substituer le signal hôte par des états de quantification correspondant à différents messages à cacher.

L'extraction se fait en prenant l'état le plus proche des données reçues z, et donc le message correspondant. Contrairement à l'étalement de spectre vu au-dessus, l'avantage de schéma par quantification est qu'il est possible de définir un ensemble de quantificateurs tel qu'il n'y ait aucune erreur pour un niveau de bruit donné. Ainsi, si le bruit ajouté est inférieur à la distance minimale (le pas de quantification) entre deux états de quantification ($\Delta/2$ dans le cas présenté dans la Figure 2.4), l'extraction est sans erreur. De ce fait, il est possible de développer une résistance absolue à une attaque parfaitement (par exemple: JPEG).Cependant, L'inconvénient majeur réside dans la résistance aux changements d'échelle du canal lors de l'attaque ($y = \alpha * x$) et à l'ajout de bruit non blanc. Les quantificateurs seront décalés et l'extraction sera mise en défaut.

Un autre point délicat est qu'il faut que les états de quantification, utilisés lors de l'insertion, soient transmis au décodeur d'une manière sécurisée (pour les cas les plus simples, cela se résume au pas de quantification).

La technique la plus populaire pour ce type de schéma est la quantification par la modulation d'index (QIM) de Chen et Wornell, En effet, les travaux de Chen et Wornell en 2001 marquent

le début des recherches sur les fonctions d'insertion par quantification, qualifiés par la suite de codage informée. Le principe consiste à quantifier le vecteur *x* en utilisant un ensemble de quantificateurs indexés par le message à transmettre. Ainsi, à chaque symbole du message *m(i)* est associé un quantificateur différent, et le tatouage s'effectue par quantification du vecteur x avec le quantificateur correspondant au message à transmettre.

La Figure (2.4) illustre un exemple simple de quantification par QIM, considérons le cas où *m=0* ou *1*. Le vecteur *x* est divisé en deux ensembles de points disjoints A et B en utilisant d'une fonction de quantification *Q(x, m)* avec un pas de quantification Δ. L'ensemble A correspond à *m=0* et B correspond à *m=1*. En suite, en fonction de bit à cacher, chaque élément de vecteur *x* est quantifié au plus proche point, c'est à dire *Q(x, 0)* ou *Q(x, 1).*

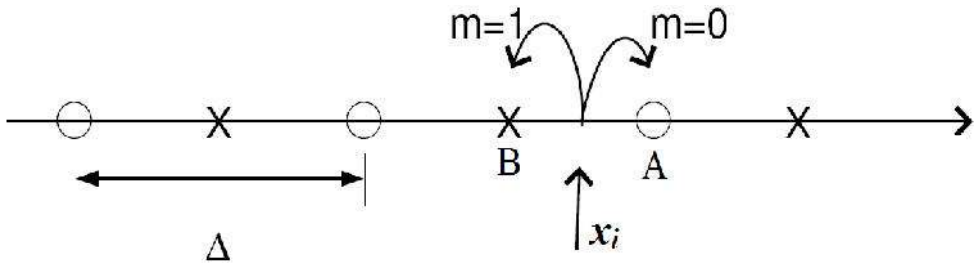


Figure 2.4 : un exemple simple de QIM, l'ensemble A et B sont représenté respectivement par un cercle et une croix

A la détection, le message $m\hat{}$ est estimé en faisant correspondre chaque valeur du vecteur tatoué reçu z, à la valeur d'un quantificateur la plus proche. Ainsi, à chaque valeur est associée un quantificateur, et donc un index correspondant qui est le message tatoué. Il est alors nécessaire que les quantificateurs soient connus et fixés pour l'encodeur et le décodeur. Par exemple dans le cas précédent, si le vecteur reçu est plus proche de l'ensemble A alors le bit extrait est 0 sinon c'est 1.

Le pas de quantification Δ conditionne les distorsions introduites dans l'image tatouée et la robustesse. Il est donc important de choisir un bon pas de quantification Δ suivant les besoins nécessaires (en termes d'imperceptibilité et robustesse). Pour coder un nombre plus m portant de bits, il est possible d'utiliser un nombre élevé de quantificateurs. Ceci a pour problème de diminuer considérablement la distance minimale, et donc la robustesse. Pour augmenter la robustesse, il est aussi possible de coder des groupes de valeurs du vecteur x(dans notre cas chaque bloc dominant) plutôt que chaque valeur indépendamment. Cela rajoute donc une redondance dans l'information, mais diminue sensiblement la capacité.

Dither-modulation QIM (DM-QIM) est l'implémentation de QIM la plus utilisée par le comité de tatouage numérique. Cela consiste à insérer avant quantification un signal permettant de réduire les artefacts visuels entre les données quantifiées puis reconstruites et les données originales. Il peut de plus servir de clef nécessaire à l'extraction (i.e. Appliquer un décalage aux quantificateurs). Les décalages sont représentés classiquement par des vecteurs pseudo-aléatoires appelés « *dither vectors* ». Il suffit de moduler le dither vector par le message à transmettre, c'est-à-dire faire correspondre à chaque symbole de message *m(i)* un unique dither vector *d (m(i))*. En plus, le dither vector peut être utilisé comme une clé afin d'améliorer la sécurité de la méthode. Cette clé doit être partagée entre le tatoueur et le décodeur.

Une propriété intéressante du tatouage quantitatif est que les données hôtes n'interfèrent pas dans la phase d'extraction (Décodage). En l'absence d'attaque, on est certain de décoder correctement le message inséré, contrairement au tatouage additif.

2.7.2.2. Tatouage par contrainte :

Le principe est de substituer le watermark à des caractéristiques de l'image. Ces caractéristiques sont extraites en appliquant une contrainte ***cc***(une mesure de similarité, une propriété géométrique ou un critère d'ordre…) sur les composantes de l'image de telle sorte que, à la détection, l'image est considérée comme tatouée si cette contrainte est vérifiée. Un exemple de méthode illustrant ce principe est celle proposée par Koch et Zhao Cette méthode consiste à fixer une contrainte entre *mmet* une variable booléenne calculée à partir d'une comparaison entre les zones des coefficients DCT. L'extraction est effectuée en comparant les valeurs des coefficients DCT afin de déterminer si le bit concerné du message était un 0 ou un 1.

- Le schéma bloc suivant présente les méthodes de tatouage par insertion :

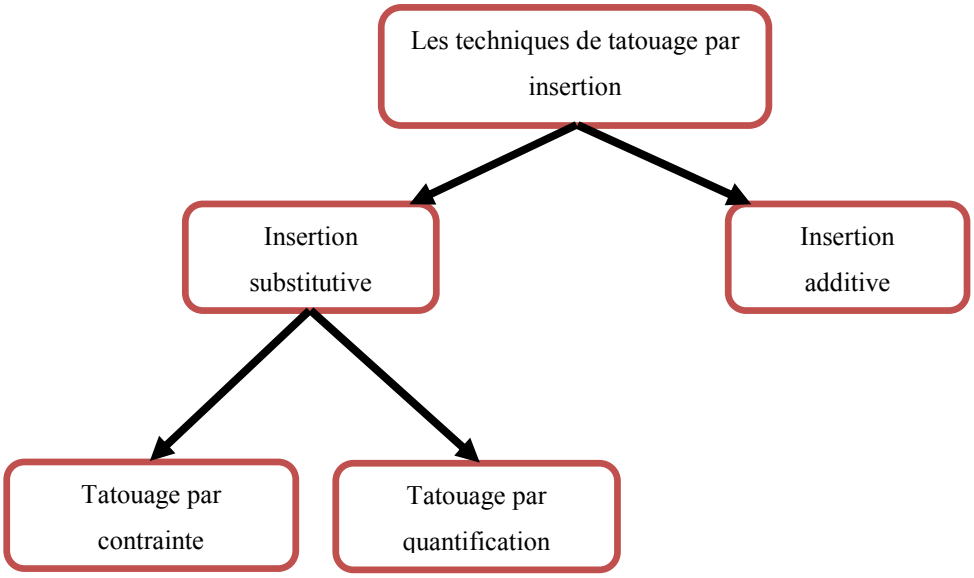


Figure 2.5 : schéma bloc concernant les méthodes d'insertion

2.8. Les domaines d'insertion :

L'insertion de la marque est effectuée dans un domaine d'une transformation inversible. Le choix du domaine d'insertion est une étape délicate dans la conception du système de tatouage. Différents critères régissent le choix d'un domaine adapté, ce domaine peut :

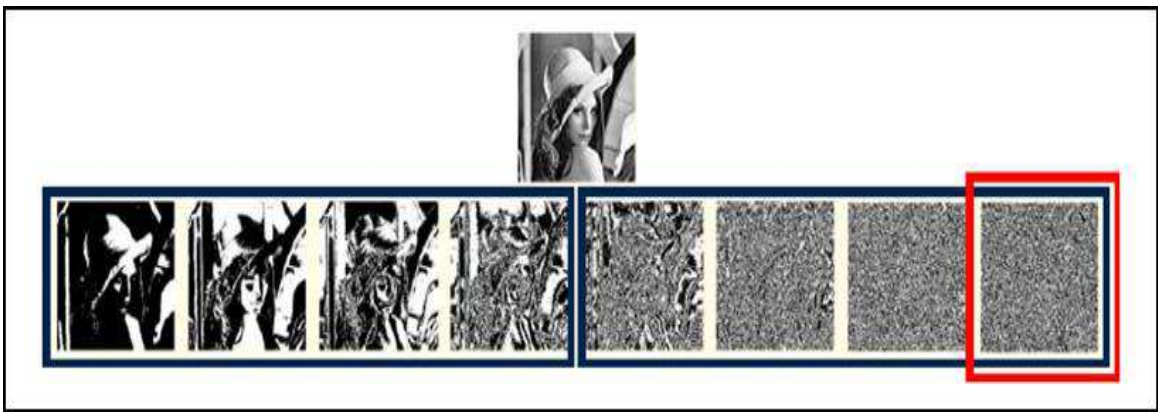
- Permettre de décorréler le signal hôte (l'image) du signal de tatouage. Cette décorrélation tente de ramener le système de tatouage à avoir des performances optimales.
- Rendre la distorsion d'insertion moins faible. En effet, permettre une altération importante de certaines composantes de l'image sans modifier la perception de celui-ci peut faciliter la détection du tatouage.
- Etre invariant à certaines perturbations subies par l'image ; ce critère est fréquemment utilisé lorsque les perturbations désynchronisantes sont considérées. Cette invariance facilite la conception de systèmes robustes aux perturbations. La littérature propose les différents domaines respectant au moins l'un de ces critères (mais jamais les trois). Nous présentons dans les sous sections suivantes les domaines d'insertion es plus utilisés. Ainsi, nous présentons quelques exemples des méthodes de tatouage pour chaque domaine :

2.8.1. Le domaine spatial :

L'insertion de la marque est effectuée en modifiant directement les valeurs des pixels de l'image. L'avantage principal de ce domaine est le faible coût, ce qui permet de l'utiliser dans les applications du tatouage en temps réel.

Parmi les exemples des méthodes opérantes dans le domaine spatiales, nous citons :

La technique de substitution de plan LSB qui constitue l'une des premières méthodes proposées dans la littérature. En effet, les valeurs des pixels de l'image sont codées sur 8 bits. Ce qui permet de découper l'image en 8 plans comme illustré dans la Figure 2.6. La méthode de tatouage du LSB consiste donc à forcer le poids faible de chaque pixel à 0 ou 1, suivant la valeur du bit de la séquence contenue dans le watermark. Cette méthode est très simple, l'image marquée n'est pas visiblement dégradée parce que les données contenues dans les bits LSB sont visuellement insignifiantes. Cette simplicité se paye par une très faible robustesse : n'importe quel traitement, même peu important, suffit à modifier les LSB et donc à rendre l'extraction impossible. D'où elle peut être utilisée pour véhiculer des informations ou pour concevoir un schéma de tatouage fragile,



Bits de poids Forts Bits de poids Faible

Figure 2.6 : Découpage de l'image lena en 8 plans

Afin de gagner des performances au niveau de la robustesse, ils ont proposé une méthode renommée par Patchwork, qui repose sur la différence de luminance observée entre deux ensembles de pixels, déterminés à l'aide d'une clé. Ainsi, l'insertion consiste à modifier les pixels du premier ensemble d'une quantité *c* et l'on diminue les pixels de l'autre de la même quantité *c*.

L'extraction de la marque se fait alors par un calcul de la somme des différences entre les positions des bits donnés par la clé. Ce type d'algorithme résiste mieux que LSB à certaines manipulations de l'image. Mais, il n'est toujours pas satisfaisant face à une compression JPEG.

Une amélioration de la méthode précédente, Cette amélioration adapte la marque à l'image en utilisant sur critères visuels élémentaires. Il s'agit d'un tatouage par blocs de 8×8. La marque est incrustée dans ces blocs afin d'avoir une certaine résistance à la compression JPEG. En suite, chaque bloc est divisé en catégorie A ou B suivant une grille prédéfinie et choisie par le biais d'une clé secrète. L'insertion des bits dans les blocs est effectuée en utilisant un ensemble de règles basées sur l'analyse statistique de chaque bloc.

Récemment, des algorithmes robustes à quelques attaques géométriques sont proposés dans le domaine spatial.

Néanmoins, les marquages dans le domaine spatial résistent très mal à tout type d'attaque, géométrique ou fréquentiel. Cet inconvénient a dirigé les chercheurs vers l'utilisation d'autres domaines robustes à ce type d'attaques comme DFT, DCT et DWT.

2.8.2. Le domaine de Fourier :

La théorie de Fourier permet de décomposer une image en une série de sinusoïdes à différentes fréquences. La Figure (2.7) représente l'image Lena et le spectre de sa transformée de Fourier.

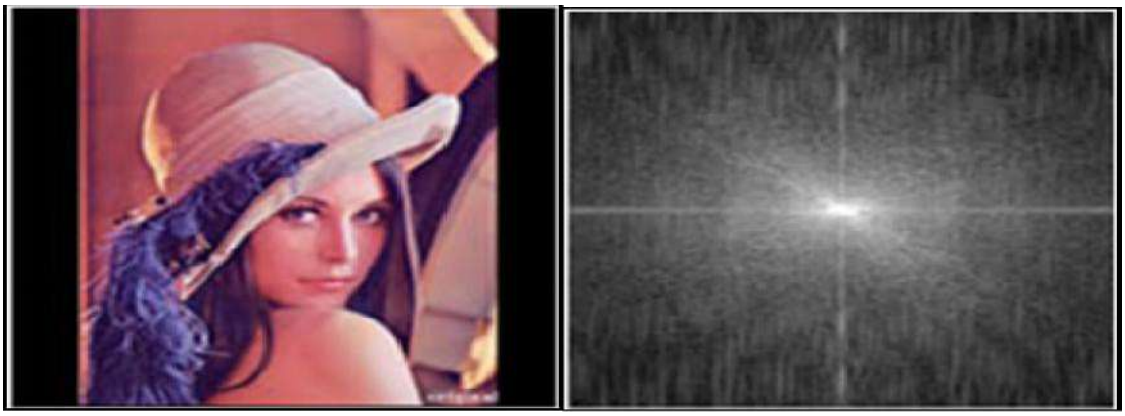


Figure 2.7 : Image Lena et son spectre de Fourier

Cette transformation permet de contrôler les fréquences du signal. Elle permet de choisir adéquatement les zones adéquates à l'insertion de la marque, de telles sortes à obtenir un bon compromis robustesse-invisibilité. Aussi, le principal avantage de ce domaine est qu'il est invariant à la translation et au changement d'échelle. Piva et al, ont présenté une approche de tatouage d'images basée sur la transformée de Fourier discrète (DFT). Malgré sa faible robustesse, elle est intéressante pour la compréhension du tatouage d'image dans le domaine de Fourier. La marque est générée d'une manière pseudo aléatoire à moyenne nulle. L'insertion se fait dans les bandes moyennes de fréquence.

2.8.3. Le domaine de la transformée en Cosinus Discrète (DCT) :

La transformée en cosinus discrète DCT afin d'anticiper et de rendre le watermark plus robuste à une compression JPEG, puisqu'elles utilisent le même espace qui sert au codage de l'image. Elle permet entre autres de réduire la corrélation spatiale entre les pixels d'une image.

Un autre avantage en faveur de l'utilisation de DCT est la possibilité de bénéficier des études psycho-visuelles déjà menées en codage de source .En effet, elles se proposent de prendre en compte les phénomènes connus comme la représentation de la couleur, la sensibilité au contraste et les effets de masquage.

De nombreuses méthodes ont été développées dans ce domaine, Cox et al présentent un schéma non aveugle de tatouage par l'étalement de spectre dans le domaine de DCT. La marque est insérée par une modification de 1000 coefficients DCT plus grandes amplitudes, de façon à

ce que le watermark soit inséré dans les zones visuellement significatives. Le calcul la DCT sur toute l'image prendrait un temps très long. Pour éviter cela, on applique la DCT sur des blocs de longueur fixe. Généralement, la taille des blocs DCT utilisée est de 8 x 8 pixels : ce choix donne un meilleur compromis entre la qualité et le temps de calcul. La Figure 2.8 présente une technique non-aveugle mais ne travail pas sur l'image complète.

L'image est préalablement découpée en blocs. Le message, constitué d'une séquence aléatoire, est inséré dans les fréquences moyennes de chaque bloc.

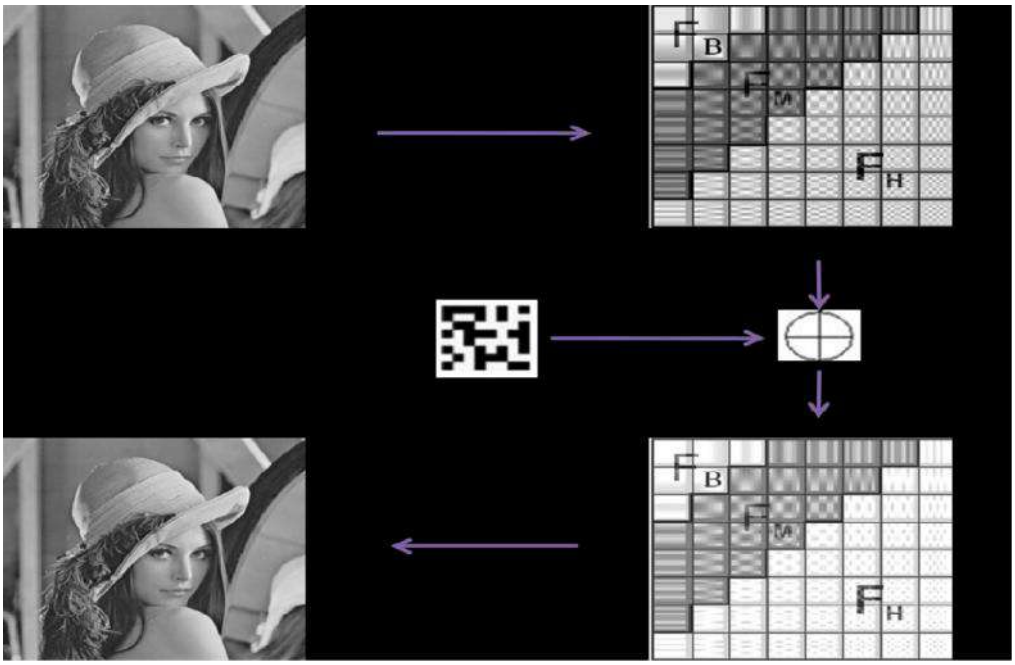


Figure 2.8 : Exemple d'insertion dans les fréquences moyennes de DCT.

2.8.4. Domaine des ondelettes :

L'utilisation de la transformée en ondelette discrète DWT est intéressante pour le tatouage numérique grâce à son utilisation dans l'algorithme de la compression JPEG2000.

De plus, cette transformée peut être interprétée comme une décomposition de l'image en sous bandes fréquentielles ce qui permet de développer facilement des masques psycho-visuels. En plus de la robustesse commune avec la DCT, le tatouage dans le domaine d'ondelettes est robuste à un changement d'échelle de facteur. De plus, les masque perceptuels sont plus fins et il y a moins d'effets de blocs.

2.8.5. Autres domaines :

Outre les FFT, DCT et DWT précédemment cité, d'autres transformations inversibles classiques en traitement d'images ont été aussi envisagées, sans apporter en pratique une amélioration significative des performances ou des invariances géométriques. Nous citons par exemple, l'utilisation de la décomposition en valeurs singulières (SVD).

2.9. Principes de base du tatouage :

L'idée de base du tatouage est d'ajouter une marque aux données du document hôte de telle sorte que la marque soit discrète et sécurisée dans le document tatoué [17]. Par ailleurs, la marque peut être partiellement ou totalement récupérée plus tard à partir du document tatoué si la clé secrète correcte nécessaire pour la récupération est utilisée.

Il existe trois éléments principaux dans la conception d'un système de tatouage :

1) La conception d'une marque W pour être dissimulée dans le signal hôte. Généralement, le signal de la marque est une fonction (f_0) d'une clé K et de l'information de son contenu I:

$$W = f_0(I, K) \tag{2.1}$$

Il est possible qu'il dépende aussi de l'information originale hôte notée X dans laquelle il sera dissimulé :

$$W = f_0(I, K, X) \tag{2.2}$$

2) La conception de la méthode d'insertion elle-même qui va insérer la marque dans l'information hôte donnant une information tatouée :

$$Y = f_1(X, W) \tag{2.3}$$

3) La conception de la méthode d'extraction correspondante qui va extraire l'information de la marque de l'information tatouée en utilisant la clé et l'information originale :

$$\tilde{I} = g(X, Y, K) \tag{2.4}$$

Ou sans l'information originale :

$$\tilde{I} = g(Y, K) \tag{2.5}$$

Concernant les deux premiers éléments, la conception de la marque à insérer ainsi que l'insertion de ce document, sont souvent considérés comme un seul élément, spécifiquement pour les méthodes où la marque insérée est adaptée au document hôte. Les Figures 2.9 et 2.10 illustrent ce concept

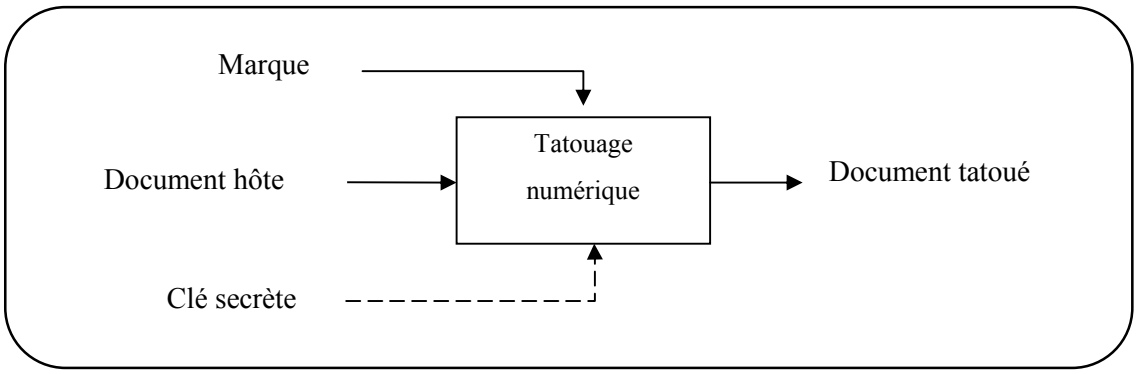


Figure 2.9 : Schéma d'insertion d'une marque par tatouage numérique

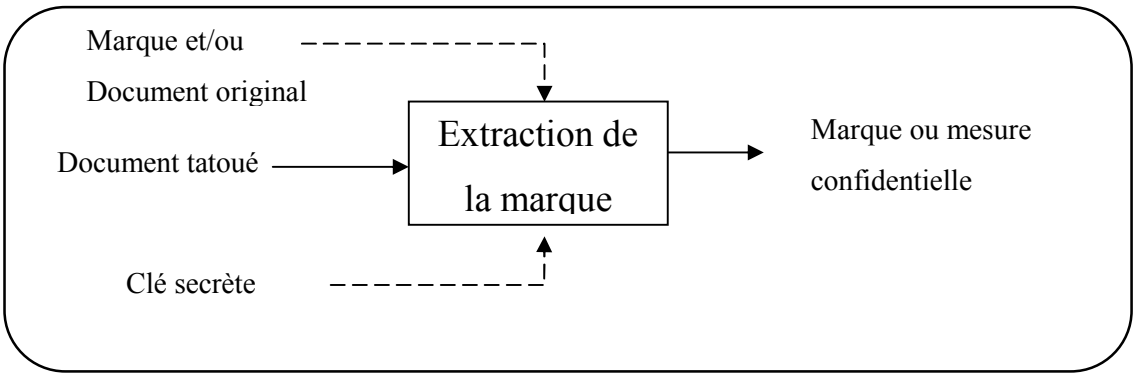


Figure 2.10 : Schéma du principe de l'extraction de la marque

La figure 2.9 montre le schéma de principe du tatouage pour le processus d'insertion [17]. L'entrée du dispositif est la marque, le document hôte et une clé publique ou secrète. Selon l'application, les données hôtes peuvent être non compressées ou compressées. La marque peut être de toute nature, par exemple un numéro, un texte ou une image. Si la marque ne doit pas être lue par des parties non autorisées, une clé doit être utilisée pour protéger la marque. En se référent à la nature de la clé (secrète ou publique), les techniques de tatouage sont secrètes ou publiques, respectivement. La sortie du schéma de tatouage est le document tatoué.

Le processus d'extraction de la marque est représenté dans la figure 2.10. Les entrées du dispositif sont les données tatouées ou à tester, la clé secrète ou publique et les données d'origine et la marque suivant la méthode. La sortie du dispositif est soit la marque récupérée ou une sorte de mesure de confiance indiquant quelle est la probabilité de présence de la marque à l'entrée dans le document sous contrôle.

2.10. Domaines d'application du tatouage numérique :

Le tatouage numérique a été proposé comme un outil dans divers applications. Les quatre principales applications du tatouage numérique sont :

- Protection des droits.
- Authentification d'images.
- Dissimulation de données.
- Les communications couvertes.

La figure 2.11montre les différentes applications du tatouage avec quelques exemples pour chacune de ces applications.

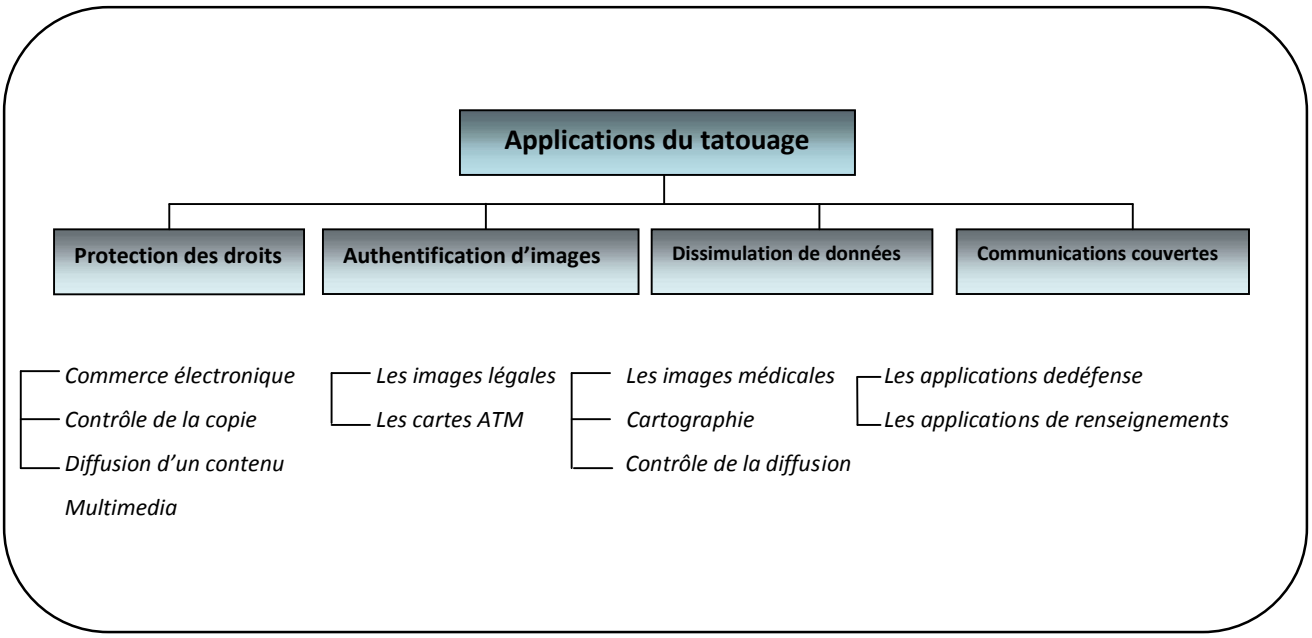


Figure 2.11 : Classification des technologies du tatouage selon les applications

2.11. Conclusion :

Dans ce chapitre, on a vu que les principales exigences d'un système de dissimulation de données doivent satisfaire l'imperceptibilité et la robustesse.

Le tatouage numérique doit être invisible de sorte que sa présence n'affecte pas la qualité des données dans lesquels il est inséré. D'autre part, il faut qu'il soit résistant contre les manipulations, appelant à la nécessité d'insertion avec une aussi grande force que possible. La disponibilité des modèles précis décrivant les phénomènes régissant la vision humaine peut donner un grand avantage pour satisfaire aux exigences citées précédemment.

Parmi les applications qu'on a citées à la fin de ce chapitre, le tatouage numérique est proposé pour les images afin de parer à leur distribution illicite. Cette application fait l'objet de notre étude dans le cadre du tatouage d'images dans le domaine de compression. Donc, avant d'entamer la procédure de tatouage, il faut appliquer une technique de compression efficace. Nous avons opté pour la quantification qui fera l'objet du chapitre suivant.

Chapitre 3 :

Système de tatouage d'images par la QIM basée sur la QV

Chapitre 4 :

Simulations et résultats

4.1. Introduction :

Dans ce chapitre, nous allons présenter les résultants suivant trios partie :

Dans la première partie, nous allons décrire les paramètres permettant de définir le débit de dissimulation, précisément le choix de la dimension des blocs de chacune des deux images ainsi que le débit de codage de l'image secrète par l'algorithme LBG. Des résultats de simulation obtenus lors du codage de sources sans mémoire seront présentés. Et nous décrirons le principe de conception d'un système à base du quantificateur vectoriel qui sera appliqué au codage d'images. Des évaluations des performances de ce système de codage.

Dans la deuxième partie nous présentons les résultats de l'implémentation d'une technique de tatouage numérique que nous avons adoptée et appliquée à l'image. Il s'agit de la technique QIM basée sur la division du dictionnaire de la quantification vectorielle (QV). Cette technique a été mise au point en utilisant une clé secrète correspondante à chacune des méthodes de division étudiées. L'objectif principal est de dissimuler une image secrète codée par un système QV dans une autre image de couverture qui va être codée pendant l'étape de dissimulation. Les performances des méthodes que nous avons implémentées seront évaluées selon deux critères :

- la capacité de dissimulation représentée par le débit de dissimulation de l'image secrète.
- l'imperceptibilité (transparence) représentée par la qualité perceptuelle de l'image tatouée.

Dans la troisième partie nous évaluons les performances de notre système de tatouage QIM conçu par deux méthodes de division du dictionnaire QV: la division aléatoire et la division équilibrée. Une évaluation comparative des performances des deux méthodes est présentée pour un même débit de dissimulation qui est de un bit par indice. Les évaluations sont effectuées à base du critère d'imperceptibilité PSNR avec présentation des images originales et tatouées.

Partie 1:

4.2. Décomposition des deux images en vecteurs :

Cette partie est relative au choix des paramètres de la phase de quantification : dimensions de l'image secrète et de couverture, le nombre de vecteurs suite à la décomposition de chacune ainsi que le débit de codage. En effet, nous avons constaté durant les expériences que le choix de ces paramètres ne doit pas être arbitraire car tous ces paramètres définissent le débit de dissimulation que nous allons décrire dans ce qui suit.

Rappelons que, pour une image de taille $h \times \ell$, le nombre de blocs (vecteurs) est donné par:

$$NB_{bloc} = \frac{h \times \ell}{d \times d} \tag{4.1}$$

Où $d \times d$ est la dimension en pixels d'un seul bloc de l'image.

Dans nos simulations, nous avons utilisé une image secrète de taille 128×128 et des images de couverture de taille 512×512 avec des blocs de tailles 2 × 2 et 4 × 4, respectivement. Par conséquent :

$$M = \frac{512 \times 512}{16} = 16384 \text{ vecteurs} \quad \text{et} \quad Nb_w = \frac{128 \times 128}{4} = 4096 \text{ vecteurs.}$$

Où M et Nb_w sont respectivement les nombres de vecteurs de l'image de couverture et de l'image secrète à dissimuler.

➢ Le débit de dissimulation :

Le débit (ou la capacité) de dissimulation est en relation directe avec le nombre d'indices QV des deux images codées (couverture et secrète) et le débit de codage de l'image secrète. Il est définit par :

$$m = \frac{Nb_w \times b_w}{M} (bits/indice) \tag{4.2}$$

Où Nb_w est le nombre d'indices QV (ou de vecteurs) utilisés pour coder l'image secrète, b_w est le débit de codage de l'image secrète et M est le nombre d'indices QV (ou de vecteurs) de l'image de couverture codée.

Ainsi, le choix adéquat des paramètres de codage va nous permettre de réaliser un tatouage d'image à un débit de dissimulation de :

$$m = \frac{4096 \times 4}{16384} = 1 \text{ bit / indice.}$$

4.3. L'algorithme LBG:

➢ Performances de l'algorithme LBG :

Nous donnons à présent les performances des VQ optimaux que nous avons conçu par implémentation de l'algorithme LBG (noté LBG-VQ). Nous avons utilisé la méthode de Katsavounidis lors de l'initialisation des dictionnaires. Les résultats présentés dans les tableaux 4.1 et 4.2 ont été obtenus par quantification de sources sans mémoire (Uniforme et Gaussienne), de variance unité, pour des débits entiers et des dimensions variables. Rappelons que dans les cas ou la dimension des vecteurs est égale à un (k = 1), la QV se réduit à la QS.

Tableau 4.1. : Distorsion moyenne obtenu par l'algorithme LBG -VQ pour une source uniforme.

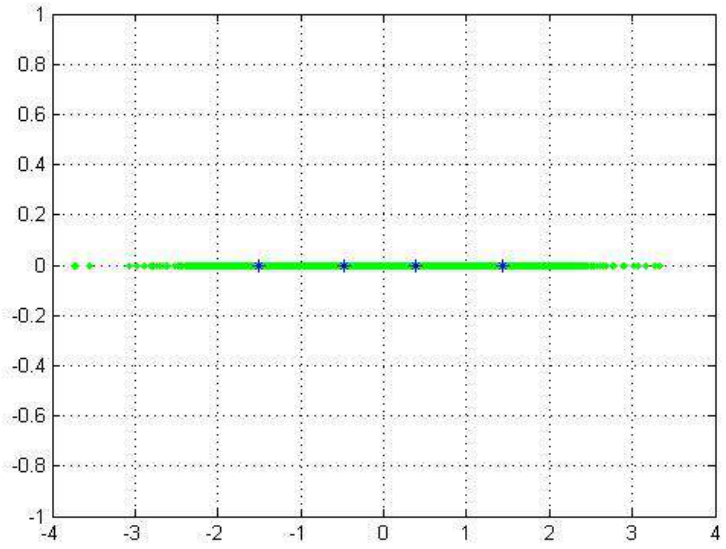
Dimension k Débit (bpe)	*D(R)*					
	1	2	3	4	5	6
1	0.0207	0.0518	0.0650	0.0688	0.0714	0.0745
2	0.0050	0.0209	0.0389	0.0503	0.0568	0.0620

Tableau 4.2. : Distorsion moyenne obtenu par l'algorithme LBG-VQ pour une source Gaussienne.

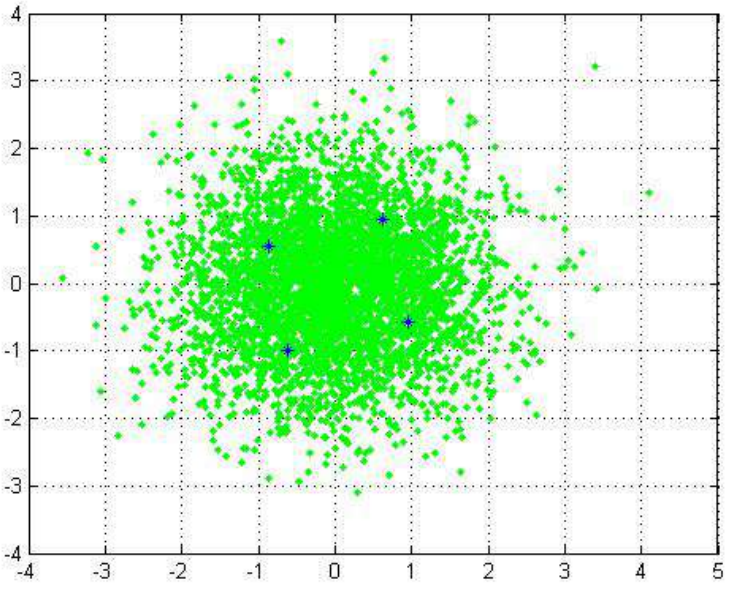
Dimension k Débit (bpe)	*D(R)*					
	1	2	3	4	5	6
1	0.9992	0.9830	1.0016	1.0107	0.9923	0.9988
2	0.1230	0.3614	0.5157	0.6425	0.6984	0.7633

Les résultats de simulation, donnés dans les tableaux 4.1 et 4.2 montrent clairement que le LBG-VQ offre de meilleurs performances que le SQ. Pour un même débit de codage, plus la dimension k augmente, plus les performances deviennent meilleures.

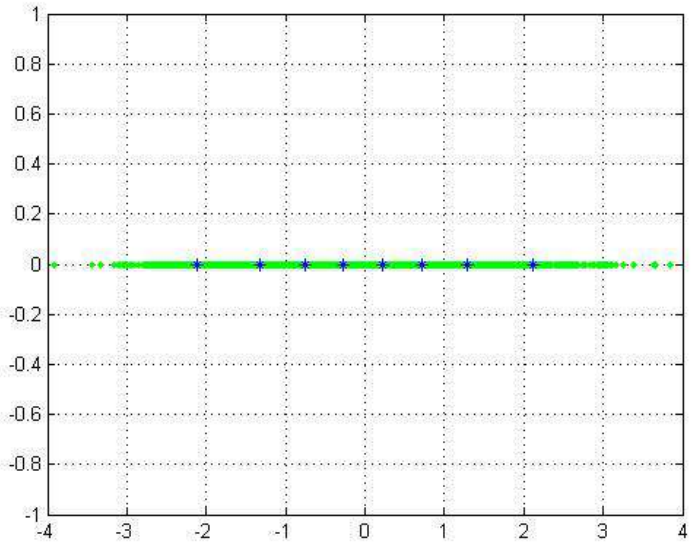
Les figures ci-dessous illustres un exemple de répartition des vecteurs de la source et les vecteurs code "Centroïdes" d'un dictionnaire conçu par l'algorithme LBG.



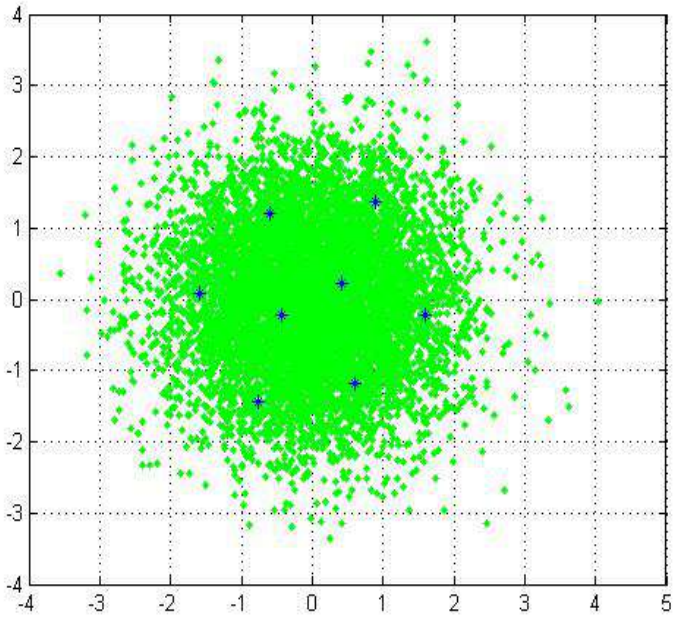
Une dimension (K=1) pour un dictionnaire de taille (L=4)



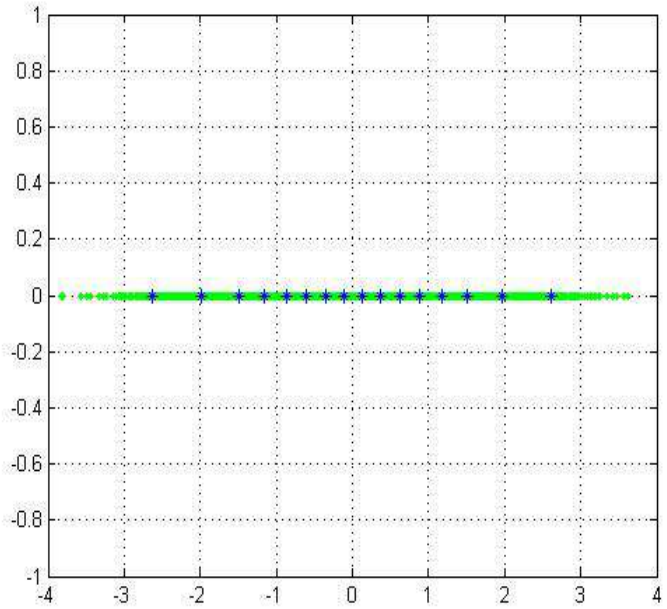
Une dimension (K=2) pour un dictionnaire de taille (L=4)



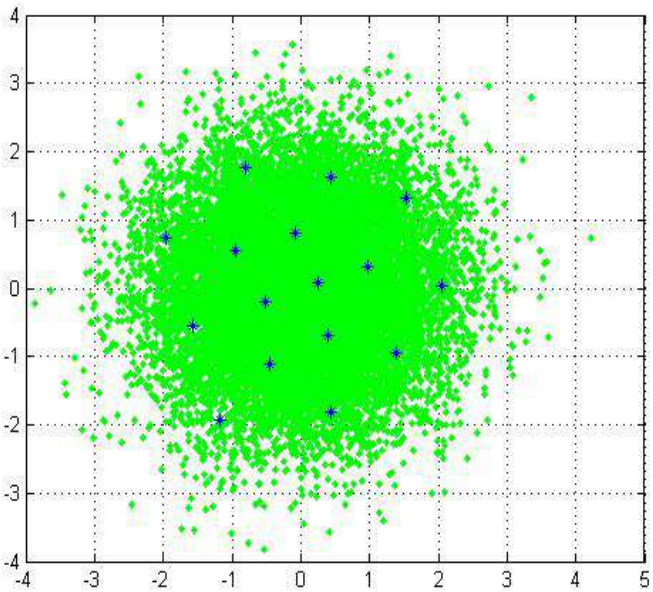
Une dimension (K=1) pour un dictionnaire de taille (L=8)



Une dimension (K=2) pour un dictionnaire de taille (L=8)



Une dimension (K=1) pour un dictionnaire de taille (L=16)



Une dimension (K=2) pour un dictionnaire de taille (L=16)

Figure 4.1 : Répartition des vecteurs de la source et les Vecteurs-code "Centroïdes"

Partie 2:

4.4. La quantification vectorielle d'une image base sur l'algorithme LBG:

Dans cette section, nous présentons les résultats expérimentaux portant sur les performances de l'implémentation de l'algorithme LBG, appliquée à la quantification vectorielle d'image. Mais avant d'exposer ces résultats, on définit d'abord le choix de la base d'apprentissage.

➢ Choix de la séquence d'apprentissage :

Il est évident que la meilleure séquence d'apprentissage possible serait celle formée des blocs de l'image à traiter [27].Mais, le dictionnaire de codage devant être connu du décodeur, celui-ci doit pouvoir le reconstruire. il doit donc connaitre la séquence d'apprentissage, c'est-à-dire l'image qu'il doit justement décoder.

La solution pratique la plus raisonnable est en fait de travailler à partir de séquence d'apprentissage standard , longuement mises au point en laboratoire à partir de statistiques sur très grand nombre d'images .Cela permet de créer des séquences universelles (acceptables pour la plupart des images , mais donc forcément sous optimales) , ou des séquences plus spécifiques pour traiter par exemple des portraits , des paysages , des images radar, des images médicales … La sélection de la bonne séquence se faisant alors soit à la main soit automatiquement par des considérations statistiques sur l'image (histogramme, variance…)[27].

Par la suite, une base detest, composée de 5 images standards de format "*png* " et de taille 512×512 pixels et 256 niveaux de gris ,a été utilisée pour nos simulations.

Afin de mesurer les performances du système QV d'image, nous avons utilisé le rapport signal sur bruit de crête PSNR (peak signal-to-noise ratio), qui est définit par:

$$PSNR = 10log_{10}\left[\frac{(2^n-1)^2}{EQM}\right]dB \qquad (4.3)$$

Où n est le nombre de bits codant un pixel de l'image, dans notre cas n = 8 bits (images test en niveaux de gris).
L'erreur quadratique moyenne d'une image de taille M est donnée par:

$$EQM=\frac{1}{M}\sum_{i=1}^{M}(pi-\widetilde{pi})^2, \quad (4.4)$$

Où M est le nombre de pixels que contient l'image, pi est le $i^{ème}$ pixel dans l'image originale et $\widetilde{pi}$ est le $i^{ème}$ pixel dans l'image reconstruite.

En utilisant une par une les images test cités précédemment comme entrée du codeur ainsi que le dictionnaire obtenu par l'algorithme LBG, on a pu évaluer les performances de notre codage en calculant à chaque fois le PSNR entre l'image originale et reconstituée.

Tableau 4.3. Les variations de la PSNR du Système QV d'image avec taille du dictionnaire QV différent :

Les variations de la (PSNR) du Système QV d'image avec taille du dictionnaire QV différent				
Taille du dictionnaire / Images (.png)	**L=16**	**L=64**	**L=256**	**L=512**
Lena	32.80	33.74	34.64	35.16
Barbara	31.13	32.10	33.20	33.86
Peppers	33.14	34.58	35.84	36.52
Einstein	31.74	32.43	33.21	33.65
Mandrill	32.29	33.74	35.18	35.93

Selon ces résultats, on voit que la valeur du PSNR varie d'une image à une autre, et cela est relatif au choix des images de la base d'apprentissage, cependant, ces valeurs sont proches de ceux données dans la littérature [26] pour les mêmes images utilisées. On peut voir aussi qu'au fur et à mesure qu'en fait augmenter la taille du dictionnaire QV, on obtient de meilleures performances.

La figure 4.2 présente les images résultantes lors du codage QV sans tatouage par une augmentation la taille du dictionnaire L.



Image de couverture:"lena"



Image avec QV: (L=16)



Image avec QV: (L=64)



Image avec QV: (L=256)



Image avec QV: (L=512)

Figure 4.2 : Images avec taille du dictionnaire QV différent

Partie 3:

4.5. Performances des méthodes de tatouage QIM implémentées :

Dans nos simulations, nous avons utilisé des images de couverture en niveau de gris de taille 512×512 pixels. Et la marque en niveaux de gris et de taille 128×128 pixels a été utilisée comme image secrète. Un dictionnaire QV généré par l'algorithme LBG avec un débit de codage de 0.5 bit/pixel (bpp) est donc de taille $L = 256$. Ce dictionnaire été utilisé pour mettre en œuvre la procédure de tatouage QIM par division de dictionnaire. L'image secrète a été codée avec un débit de 1 bit/pixel par un autre dictionnaire LBG approprié, autrement dit, chaque vecteur-code est de dimension 2×2 pixels qui est la même dimension de chaque vecteur de l'image secrète. La figure 4.3 présente les images originales (avant codage et décodage QV) utilisées dans les simulations, à savoir l'image secrète et les trios images de couverture.

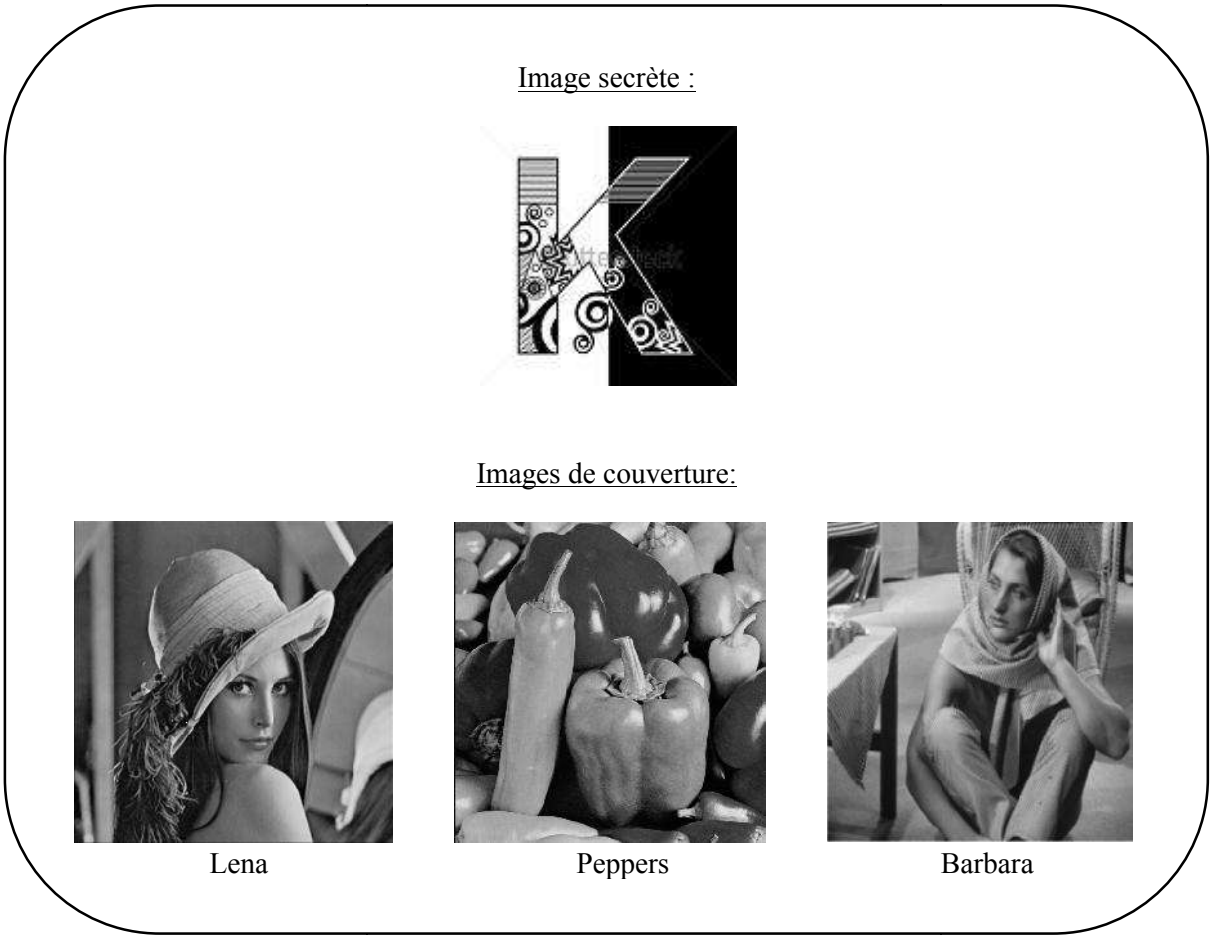


Figure 4.3 : Image secrète et images de couverture utilisées dans les simulations

Nous présentons, ci-dessous, les performances des différentes méthodes implémentées de tatouage QIM par division de dictionnaire en termes de PSNR. Pour les évaluations comparatives entre les méthodes, nous utilisons un paramètre δ qui mesure l'écart entre le PSNR de l'image de couverture codée (sans tatouage) X et celui de l'image codée et tatouée X', *plus* ce paramètre est petit plus la performance de la méthode est élevée. Ce paramètre que nous avons nommé "dégradation" ou "écart", est donné par :

$$\delta = PSNR(X) - PSNR(X') \tag{4.5}$$

4.5.1. Performances de la QIM par division aléatoire (QIM-DA) :

Les performances de la QIM-DA avec dissimulation de 1 bit/indice sont données dans le tableau 4.4.Pour une évaluation perceptuelle, la figure 4.4 présente les images de tests codées par la QV (sans tatouage) et celles codées et tatouées par la technique QIM-DA dans le cas de dissimulation de 1 bit/indice.

Tableau 4.4: *Comparaison entre les systèmes QV sans tatouage et avec tatouage QIM-DA :*

	Performance système QV (sans tatouage)		**Performance système QV (avec tatouage QIM-DA)**		**δ (dB)**
Noms des images	**Débit de codage (*bpp*)**	**PSNR (dB)**	**Débit dissimulation (bit/indice)**	**PSNR (dB) Image tatouée**	
Lena	0.5	34.64	1	33.45	1.19
Peppers	0.5	35.84	1	34.15	1.69
Barbara	0.5	33.20	1	31.86	1.34

Les résultats du tableau 4.4, nous remarquons que les PSNR des trois images tatouées présentent une certaine diminution par rapport aux PSNR des images codées QV sans tatouage .Un écart maximal de 1.69 (dB) a été obtenu lors de l'utilisation de l'image " Peppers " comme

couverture. On remarque donc une légère dégradation perceptuelle de la qualité de cette image (figure 4.4). La qualité des deux autres images est un peu meilleure.



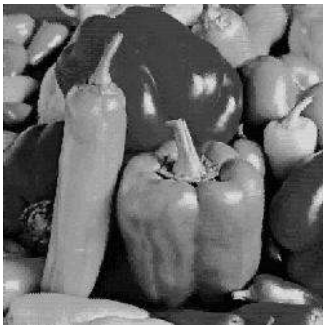
PSNR (VQ) = 34.64 dB



PSNR (QIM-DA) = 33.45 dB



PSNR (VQ) = 35.84 dB



PSNR (QIM-DA) = 34.15 dB



PSNR (VQ) =33.20 dB



PSNR (QIM-DA) =31.86 dB

Figure 4.4 : Images couvertures et images tatouées par la QIM-DA.

4.5.2. Performances de la QIM par division équilibrée (QIM-DE):

Nous donnons, ci-dessous, les résultats de simulation portant sur les performances de la méthode de tatouage QIM par division équilibrée du dictionnaire QV.

Dans le tableau 4.5, nous présentons les performances de cette méthode en termes du PSNR et du taux de sa dégradation par rapport au PSNR QV pour chaque image. La figure 4.5 présente les trois images résultantes lors du codage QV sans et avec tatouage par QIM-DE.

Tableau 4.5*: Comparaison entre les systèmes QV sans tatouage et avec tatouage QIM-DE :*

	Performance système QV (sans tatouage)		**Performance système QV (avec tatouage QIM-DE)**		δ **(dB)**
Noms des images	**Débit de codage (bpp)**	**PSNR (dB)**	**Débit dissimulation (bit/indice)**	**PSNR (dB) Image tatouée**	
Lena	0.5	34.64	1	33.50	1.14
Peppers	0.5	35.84	1	34.24	1.60
Barbara	0.5	33.20	1	32.03	1.17

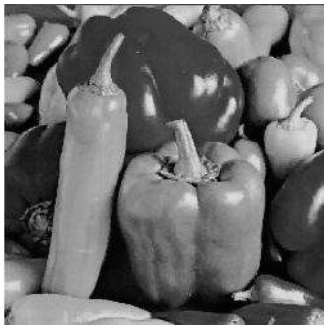
Les résultats donnés dans le tableau 4.5 montrent que les écarts des PSNR des images tatouées par QIM-DE par rapport aux images non tatouées sont aussi faibles avec un maximum de 1.60 dB atteint dans le cas du tatouage de l'image " Peppers ". Ces écarts notés semblent aussi ne pas influencer sur la qualité des images tatoués dont les dégradations ne sont pas vraiment perceptibles surtout pour les deux dernières images de couverture (figure 4.5).



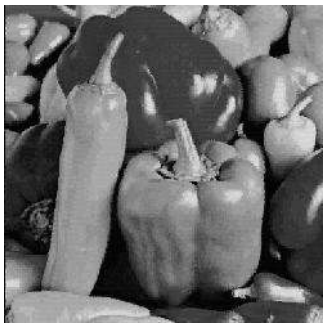
PSNR (VQ) = 34.64 dB



PSNR (QIM-DE) = 33.50 dB



PSNR (VQ) = 35.84 dB



PSNR (QIM-DE)= 34.24 dB



PSNR(VQ) = 33.20 dB



PSNR QIM-DE = 32.03 dB

Figure 4.5 : Images de couvertures et images tatouées par la méthode QIM-DE

4.6. Performances de la QIM concernant l'image secrète (la marque) par division aléatoire (QIM-DA) :

Les performances de la QIM-DA avec dissimulation sont données dans le tableau 4.6. Pour une évaluation perceptuelle, la figure 4.6 présente les images **secrètes** de tests codées par la QV et avec la tatouage par la technique QIM-DA ,pour des tailles du dictionnaire QV différent L dans le cas ou la taille du dictionnaire de la marque est constant e (Lm=16) .

Tableau 4.6. Les variations de la PSNR du Système QV d'image secrète avec taille du dictionnaire QV différent :

Les variations de la PSNR du Système QV d'image secrète avec taille du dictionnaire QV différent				
Taille du dictionnaire / Images secrète (.png)	**L=16**	**L=64**	**L=128**	**L=256**
Marque 1	45.56	45.56	45.56	45.56
Marque 2	50.93	50.93	50.93	50.93
Marque 3	43.27	43.27	43.27	43.27

Selon ces résultats, on voit que la valeur du PSNR varie d'une image à une autre, et cela est relatif au choix des images de la base d'apprentissage et on obtient de meilleures performances (par exemple la marque2 sa valeur du **PSNR** = 50.93 dB). On peut voir aussi qu'au fur et à mesure qu'en fait augmenter la taille du dictionnaire QV on obtient des valeurs du PSNR constantes, alors la marque est dépend de taille du dictionnaire interne, propre et spécial (Lm).

La figure 4.6 présente les images secrètes (la marque) avant et après tatouage.



La marque avant tatouage



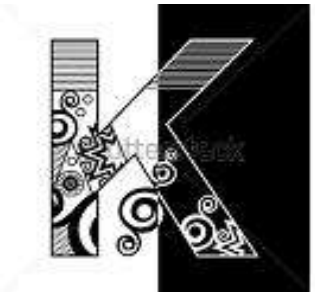
La marque après tatouage



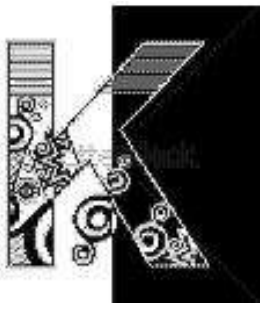
La marque avant tatouage



La marque après tatouage



La marque avant tatouage



La marque après tatouage

Figure 4.6 : Images de la marque avant et après tatouage

4.7. La relation entre le choix de clé K et les performances de la QIM (dans le cas « QIM-DA ») :

Dans le tableau 4.7, nous présentons les performances de cette méthode (*QIM-DA)* en termes du PSNR et les clés différentes K et leurs l'effet sur PSNR, avec les tailles du dictionnaire fixe (L=Lm=16).

Les clés K :

```
K1=[0,0,0,0,1,1,0,0,1,1,0,1,0,0,0,0].
K2=[1,1,0,0,1,1,0,0,1,1,0,1,0,1,0,1].
K3=[1,1,1,1,0,1,0,0,1,1,0,1,0,1,0,0].
K4=[1,1,0,0,1,1,0,0,1,1,0,0,0,1,1,1].
K5=[0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,1].
K6=[1,0,1,0,1,0,1,0,1,0,1,0,1,1,0,1].
```

Tableau 4.7*: Les variations de la* ***PSNR*** *du système* ***QIM-DA*** *pour des clés K* différentes *:*

Les clés K / Noms des images	K1	K2	K3	K4	K5	K6
lena	30.58	30.03	30.39	29.95	28.09	29.13
Peppers	31.09	30.01	30.67	29.72	27.79	28.49
Barbara	31.09	29.26	30.45	29.78	28.49	28.58

Dans le tableau 4.7, On voit que la valeur du PSNR varie d'une image à une autre, et cela est relatif au choix des clés K.

4.8. Evaluation comparative entre les méthodes QIM implémentées :

Pour une même méthode de tatouage (QIM-DA par exemple), si on a une l'augmentation du nombre de bits dissimulés par indice provoque une plus grande de gradation en termes d'imperceptibilité. Ce qui influence négativement sur la qualité perceptuelle de l'image tatouée comparé au cas de dissimulation de moins de bits par indice.

D'autre part, pour un même débit de dissimulation, les résultats ont montré que la méthode de tatouage QIM-DA provoque une plus grande dégradation des performances comparée a une autre méthode de division QIM-DE. Les résultats de simulation ont montré aussi que la méthode QIM-DE assure des performances meilleures que la méthode QIM-DA.

Prenons, par exemple le cas de l'image de couverture "Peppers", on remarque que la division aléatoire donne un écart de 1.69 dB, la division équilibrée donne 1.60 dB. D'où, de gain de 0.09 dB ont été obtenus par la méthode de dissimulation avec division équilibrée comparée au autre méthode, Ainsi, la qualité perceptuelle de l'image tatouée par QIM-DE présente peu d'imperfections comparée à l'image codée par QV.

4.9. Exemples de tatouage des images par des marques textes :

image de couverture originale (512x512)



la marque taille (128x128)



image tatouée



l'extraction de la marque

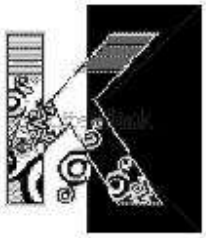


image de couverture originale (512x512)



la marque taille (128x128)



image tatouée



l'extraction de la marque



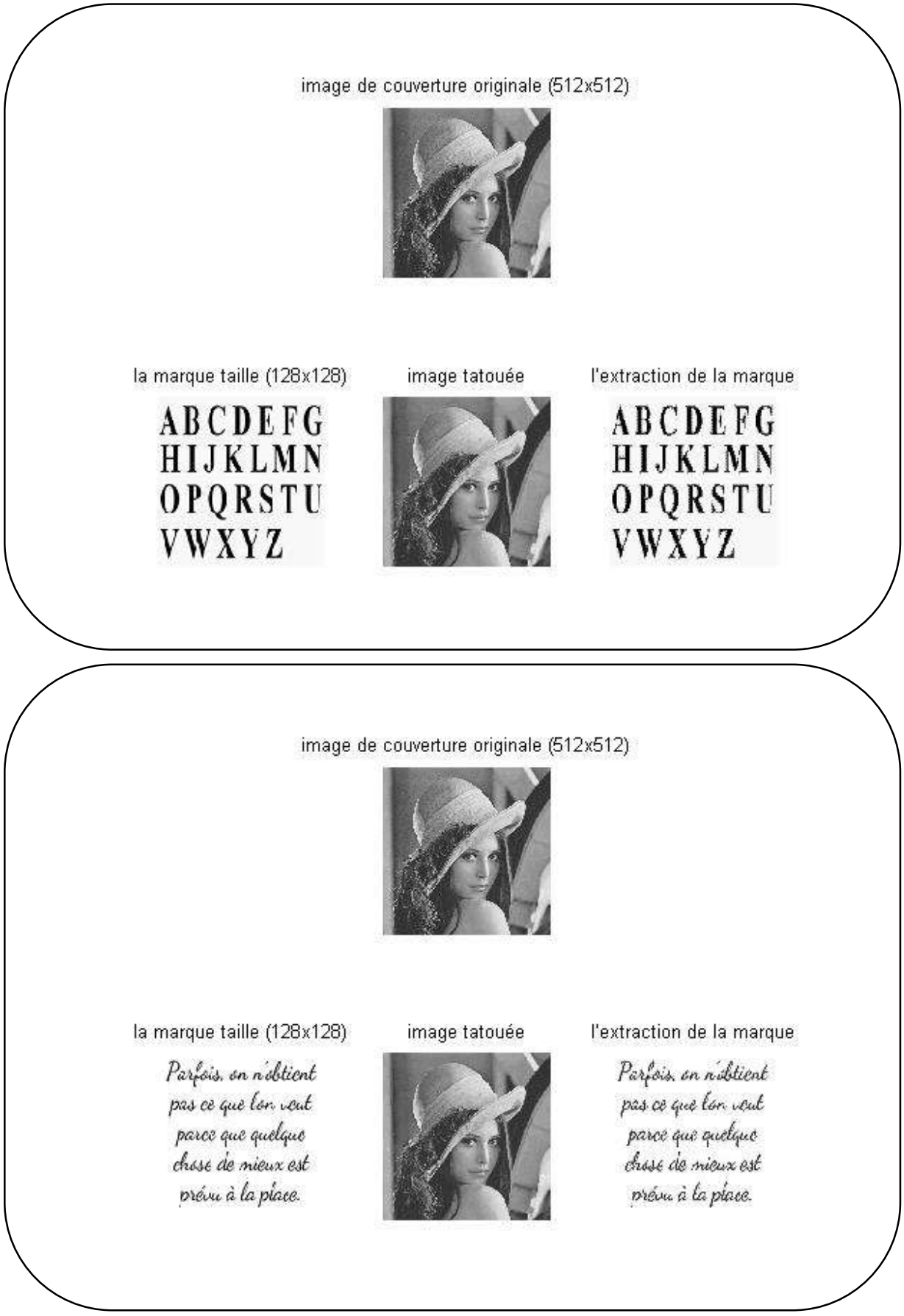


Figure 4.7 : Exemples de tatouage par des marques textes

4.10. Conclusion :

Dans ce chapitre, nous avons montré que la quantification vectorielle à base de l'algorithme LBG présente une meilleure performance évaluée par l'approche de la limite théorique de Shannon *D(R)* en mesure que la dimension du vecteur à quantifier augmente.

Nous avons pu s'apercevoir au cours du test notre système de QV d'image effectué par codage de cinq images connues et utilisées fréquemment dans la littérature, de la performance évaluée par le *PSNR* en se référent à la littérature ainsi que la simplicité de décodage.

Nous avons implémenté un système de tatouage d'image par la technique QIM basée sur la division du dictionnaire QV. Pour mettre en ouvre cette technique, nous avons effectué la division du dictionnaire QV par deux méthodes différentes qui sont la méthode aléatoire et équilibrée. Par la suite, la technique QIM, mise en ouvre par ces deux méthodes, a été appliquée pour un débit de dissimulation d'un bit par indice.

Concernant la méthode QIM-DA, les résultats expérimentaux ont montré que le gain en capacité de dissimulation se paye par une plus grande dégradation des performances, ce qui affecte l'imperceptibilité du système. D'autre part, l'évaluation comparative a montrée que la méthode QIM-DE est la technique qui assure la plus faible dégradation compare à l'autre méthode. Ceci est dû au faite qu'elle assure une dégradation minimale locale (entre les vecteurs-code du dictionnaire) lors de la procédure de division.et le choix de la clé secrète donnant le plus grand PSNR; donc la plus petite distorsion globale entre l'image originale et tatouée. La dégradation est celle provoquée par les méthodes QIM-DE et QIM-DA car le choix de la clé est complètement aléatoire qui n'est pas basé sur un critère.

Malgré que la dégradation soit un peu perceptible dans certains cas, cependant il est théoriquement impossible d'extraire l'image secrète sans avoir la clé secrète appropriée ainsi que le dictionnaire QV de l'image de couverture, ce qui constitue un avantage majeur de la méthode de tatouage QIM.

Conclusion générale:

Ce travail traite du tatouage des images numériques dans le contexte particulier de la transmission de données cachées qui prend de plus en plus d'importance dans le monde des télécommunications modernes. Cette classe applicative permet notamment d'augmenter le contenu de l'image en l'utilisant comme un canal de transmission sécurisé. L'objectif de ce projet était la conception d'un tel système de tatouage.

Pour développer ce système, nous avons étudié une technique de tatouage basée-QV qui est la quantification par modulation d'indice (QIM). Dans notre travail, nous nous sommes intéressé par la mise en œuvre de cette technique en utilisant la méthode de division du dictionnaire QV. Deux méthodes de division de dictionnaire ont été adoptées : aléatoire et équilibrée. Pour atteindre cet objectif, on a tout d'abord conçu un système de compression efficace qui est le quantificateur vectoriel par l'algorithme LBG qu'on a appliqué ensuite à des images de test. Les résultats de simulation obtenus ont montré la performance du système suite à leur compatibilité avec les résultats mentionnés dans la littérature. La procédure d'implémentation de la QIM était ensuite appliquée par division du dictionnaire QV du codeur de l'image de couverture selon les deux méthodes envisagées.

Des évaluations des performances selon les critères d'imperceptibilité et de débit de dissimulation ont montré que notre système de tatouage QIM pour chacune des deux méthodes (méthode de division en exemple) peut assurer une bonne imperceptibilité lorsque la capacité de dissimulation est faible.Ainsi, une augmentation de la capacité de dissimulation se paye par une dégradation perceptuelle de l'image.

D'autre part, l'évaluation comparative entre les deux méthodes de division QIM implémentées, nous a permis de conclure que la méthode de division équilibrée est celle qui assure les meilleures performances. Ceci est dû forcement à sa procédure de minimisation locale de distorsion (entre les vecteurs-code du dictionnaire QV) pour concevoir la clé secrète. La méthode de division équilibrée assure des performances légèrement inférieures puisque sa procédure de conception de la clé secrète est basée sur la minimisation globale de la distorsion en calculant à chaque itération le PSNR de l'image tatouée selon une clé de test et retenir à la fin la clé qui a conduit vers le meilleur PSNR.Enfin, la méthode aléatoire était la moins performante car le choix de la clé aléatoire n'est basé sur aucun critère.

Deux perspectives sont envisageables pour enrichir davantage ce travail. Une première extension concerne l'étude de la robustesse de chaque système contre les attaques et les bruits des canaux de transmission. La deuxième est de travailler avec des images en couleurs ainsi que des vidéos comme support de communication sécurisée.

Bibliographie

[1] K. Chakib, "*La Compression des Images Fixes par les Approximations Fractales Basée sur la Triangulation de Delaunay et la quantification Vectorielle"*, mémoire de fin d'étude, 1999.

[2] J. Fruitet, *"Outils et méthodes pour le traitement des images par ordinateur*", Université de Murne-la-vallée, France 2000.

[3] A.d'hardancourt, "fou du multimédia", Sybex, 1995

[4] F. Devaux, "*Filtrage d'image par réseau de neurones",* thèse de maîtrise, Université de Paris 8, France 1997.

[5] T.T. Alföldi, *"Introduction aux images numériques et aux techniques d'analyse numérique*", Centre canadien de télédétection, 1996.

[6] F. Davoine, "*Compression D'images par Fractales Basée sur la Triangulation de Delaunay"*, Thèse L'INPG, Institut National polytechnique de Grenoble, Décembre 1995.

[7] S. Bres, J-M Jolion et F. Lebourgeois, "Traitement et analyse des images numériques", Edition Lavoisier, 2003.

[8] E. Incerti, "Compression d'images, algorithmes et standards", Edition Vuibert, Paris, 2003.

[9] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker :"Digital watermarking and steganography". Morgan Kaufmann, 2008.

[10] Ali Mohammad Al-Haj :"Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications", IGI Global, 2010.

[11] J.Cummins, P.Diskin, S. Lau and R. Parlett: "steganography and watermarking ". School of Computer Science, The University of Birmingham, 2004.

[12] Husrev T Sencar**,** M.Ramkumar, Ali N. Akansu: "Data hiding fundamentals and applications". ELSEVIER Academic Press, Chapter1, pp 2-8, 2004.

[13] G. W. Braudaway, K. A. Magerlein, and F. C. Mintzer, "Color correct digital watermarking of images" .U.S. Patent ,June 1996.

[14] F.Y Shih : "Digital watermarking and steganography". CRC Press, Taylor & Francis Group, 2008.

[15] M. Barni and F. Bartolini :"Watermarking systems engineering". Signal processing and communications series, 2004.

[16] B. Furht and D. Kirovski :"Multimedia watermarking techniques and applications". Auberbach publications, Taylor & Francis Group, 2006.

[17] Hartung and Kutter:"Multimedia watermarking techniques", proceeding of the IEEE Signal Processing, vol. 87, N°. 7, pp. 1079-1084,July 1999.

[18] Cléo BARAS, Thèse de doctorat :"Tatouage informé des signaux audio numériques ", Ecole Doctorale d'Informatique, Télécommunications et Electronique de Paris, Décembre 2005.

[19] A. Gersho & R. M. Gray:"Vector quantization and Signal compression", Kluwer Academic Publishers, 1992.

[20] S. P. Lloyd:"Least squares quantization in PCM", IEEE Trans. Information Theory, Vol. IT-28, pp. 129-136, Mar. 1982.

[21] B. Laskar, mémoire de Magister : "Système de transmission sécurisé de la parole basé sur la stéganographie". Université des Sciences et de la Technologie Houari Boumediene, 2013.

[22] F. H. Wang, J.S. Pan, and L.C. Jain: "Innovations in Digital Watermarking Techniques".SCI 232, pp. 83–107. Springer-Verlag Berlin Heidelberg, 2009.

[23] Cheng-Hsing Yang et al :"Grouping strategies for promoting image quality of watermarking on the basis of vector quantization", journal of Visual Communication and Image Representation. pp. 49–55, 2009.

[24] I. Katsavounidis, C. Kuo& Z. Zhang:"A new initialization technique for generalized Lloyd iteration", IEEE Signal Proc. Letters, Vol. 1, pp. 144-146, October 1994.

[25] Chin-Chen Chang, Pei-Yu Lin, and Hsin-Chi Wang :" Distortion-Free Steganography Mechanism with Compression to VQ Indices " , International Journal of Signal Processing, Image Processing and Pattern RecognitionVol. 2, No. 2, pp 39 - 41, June 2009.

[26] E.Guzmán Ramírez, Miguel A. Ramírez and O. Pogrebnyak:" Applied Extended Associative Memories to High-Speed Search Algorithm for Image Quantization " .Search Algorithms and Applications, Prof. Nashat Mansour (Ed.), InTech, Vol. 8, PP. 157-160, 2011.

[27] J. P. Guillois:" Compression de données, Compression des images ", Technique de l'ingénieur, E5340, Novembre 1998.

[28] F.-H. Wang,J.-S.Pan, and L.C. Jain: "Innovations in Dig.Watermark "Chapter 6, Tech., SCI 232, pp. 83–107. Springer-Verlag Berlin Heidelberg,2009.

[29] Xing He :"Signal Processing, Perceptual Coding and Watermarking of Digital Audio: Advanced Technologies and Models", SRS Labs Inc, 2012.

[30] Lu, Z.M., Sun, S.H.:"Digital image watermarking technique based on vector quantisation", IEE Electronics Letters 36(4), pp 303–305, 2000.

[31] Langelaar, G.C., Setyawan, I., Lagendijk, R.L.: "Watermarking digital image and video data: A state-of-the-art overview". IEEE Signal Processing Magazine vol. 17, pp. 20–46, 2000.

[32] Cheng-Hsing Yang et al :"Grouping strategies for promoting image quality of watermarking on the basis of vector quantization", journal of Visual Communication and Image Representation. pp. 49–55, 2009.

[33] F. H. Wang, J.S. Pan, and L.C. Jain: "Innovations in Digital Watermarking Techniques".SCI 232, pp. 83–107. Springer-Verlag Berlin Heidelberg, 2009.

[34] B. Laskar, mémoire de Magister : "Système de transmission sécurisé de la parole basé sur la stéganographie". Université des Sciences et de la Technologie Houari Boumediene, 2013.