République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de
la Recherche Scientifique

المدرسة الوطنية المتعددة التقنيات
Ecole Nationale Polytechnique

Ecole Nationale Polytechnique
Département d'Electronique

Projet de fin d'études

en vue de l'obtention du diplôme

d'Ingénieur d'Etat en Electronique

Thème

Le tatouage des images JPEG

Présenté par :

AROUR Meriem

KASSAB Nassima

Dirigé par :

Pr L. HAMAMI

Melle S. BOUCHAMA

Promotion : Juillet 2010

Projet de fin d’études

Thème :

Le tatouage des images JPEG

DEDICACES

Je dédie ce travail à :

Mes Parents ;
Ma petite sœur ;
Toutes les personnes qui me sont chères;

Nassima

Je dédie ce travail à:

Mes parents ;
Mes chères sœurs : Nora, Taois et Samia ;
Mes frères : Abdelkarim , Fateh et Younes ;
Rayane, Chaima, Eliass ;
Tous les amis ;

Meriem

Remerciements

Nos remerciements s'adressent tout particulièrement à Pr L.HAMAMI notre promotrice à l'Ecole Nationale Polytechnique d'Alger (ENP) et à Melle BOUCHAMA Samira, notre promotrice au Centre de Recherche sur l'Information Scientifique et Technique (CERIST). Tout au long de ce travail, elles ont su nous apporter un soutien constant, une disponibilité, une écoute, une confiance et des conseils précieux et avisés à la hauteur de leurs compétences et de leurs réelles qualités humaines.

Nous remercions sincèrement les membres du jury Mr D. BERKANI et Mr M. HADDADI pour l'attention accordée à notre travail.

Ils s'adressent aussi aux enseignants du Département Génie Electronique de l'Ecole Nationale Polytechnique d'Alger, qui nous ont soutenus et encouragés et auxquels nous devons notre formation d'ingénieur.

Bien évidemment, nous remercions nos familles pour leur encouragement et leur soutien.

Merci à tous ceux qui ont contribué, de près ou de loin, à la réalisation de ce travail.

ملخص

إن الإستخدام المتزايد للمعلومات الرقمية ، يطرح باستمرار مشكل المدة المستغرقة للإرسال ، حجم التخزين وكذا أمن الملفات والوثائق الرقمية ؛ وبذلك يعتبر الضغط والوشم الرقمي من الحلول المقترحة لـهذه الإشكاليات.

الضغط هو تمثيل المعلومات في أصغر حجم ممكن، في حين أن الوشم الرقمي هو إدخال معلومة (إسم ، شعار، أو معلومات حول المصدر, إلخ) في صورة ما من أجل حمايتها من النسخ والإستعمال الغير قانوني.

الهدف من عملنا هو الجمع بين تقنية الوشم الرقمي و الضغط ،وذلك بإدخال علامة خلال عملية الضغط JPEG و بالضبط خلال مرحلة التكميم، بهدف إثبات هوية الصورة.من أجل هذا عالجنا نوعان من الوشم الرقمي الأعمى، الأول غير قابل للعكس، أما الثاني فهو قابل للعكس؛بحيث يسمح باسترجاع تام للصورة المضغوطة JPEG بدون وشم، ويضمن أمن الصورة عبر مفاتيح التشفير.

مفاتيح :JPEGالضغط, الوشم الرقمي الأعمى , الوشم قابل للعكس , هوية الصورة , التشفير

Résumé

Les données numériques, par leur utilisation, non pas croissante mais explosive, posent des problèmes de temps de transmission, du volume de stockage et de la sécurité du document. Ainsi la compression et le tatouage viennent répondre à ces problématiques. La compression consiste à représenter l'information sous sa forme la plus compacte, le tatouage d'images quant à lui, consiste à introduire une marque (un nom, un logo des informations sur un auteur, etc) dans une image dans le but de la protéger contre les copies illégales.

Le but de notre travail est d'associer à la compression *JPEG* un schéma de tatouage numérique. En effet, une marque est introduite après l'étape de quantification de la compression *JPEG,* dans le but d'assurer l'authenticité de l'image. Deux méthodes de tatouage aveugle ont été traitées, la première concerne le tatouage non réversible. La seconde méthode est réversible, elle permet de récupérer une image identique à l'image *JPEG non tatouée*, sa sécurité réside dans la connaissance ou non des clés de cryptage.

Mots clés : compression *JPEG*, tatouage numérique aveugle, authenticité de l'image, tatouage réversible, cryptage.

Abstract

Digital data, by their use not only increasing but explosive, posing problems of transmission time, storage volume and document security. Thus compression and watermarking are responding to these issues. While compressions try to represent the information in its most compact form, the image watermarking consist on introducing a mark (name, logo of information about an author, etc.) in an image in order to protect it from illegal copies.

The aim of our work is to associate a scheme of watermarking to JPEG compression. Indeed, a mark is inserted after the quantization step of JPEG compression in order to ensure the authenticity of the image. Two blind watermarking methods have been studied; the first one concerns the non-reversible watermarking. The second method is reversible, it allows to recover an identical image to the JPEG unwatermarked one, its safety lies in knowing whether the encryption keys.

Key words: JPEG compression, blind watermarking, authenticity of the image, reversible watermarking, encryption.

Sommaire

Introduction générale

CHAPITRE 1 : La compression JPEG

1.1 Introduction 1

1.2 Généralités sur la compression d'images 1

1.2.1 Définition 1

1.2.2 Evaluation de la compression 1

1.2.3 La quantité d'information 2

1.2.3.1 Information de source 2

1.2.3.2 Information propre 2

1.2.3.3 L'entropie 3

1.2.3.4 Courbe débit-distorsion 3

1.3 Les méthodes de compression 4

1.3.1 Les méthodes de compression sans pertes 5

1.3.1.1 Les codages statistiques à longueur variable 5

1.3.1.2 Les codages par dictionnaire 7

1.3.1.3 Codages par longueur de plages 7

1.3.2 Les méthodes avec pertes 8

1.3.2.1 La compression par ondelettes 9

1.3.2.2 l'approche fractale 9

1.3.2.3 La quantification scalaire (QS) 10

1.3.2.4 La quantification vectorielle (QV) 11

1.4 *JPEG* et la compression des images 11

1.4.1 Introduction 11

1.4.2 La compression JPEG 12

1.4.2.1 Algorithme de base 12

1.4.2.2 La Transformée en Cosinus Discrète (DCT) 13

1.4.2.3 La quantification 14

1.4.2.4 Le codage entropique 15

1.4.2.5 Transformation des couleurs 17

1.4.3 Modes JPEG 19

1.4.3.1 Progressif_JPEG 19

1.4.3.2 Compression JPEG sans perte. (P-JPEG) 20

1.4.3.3 Mode hiérarchique 20

1.4.4 Les extensions de JPEG 21

1.4.5 Les limites du JPEG 23

1.5 Conclusion 23

CHAPITRE 2 : Les techniques de tatouage

2.1 Introduction 24

2.2 La triade du secret……..……24

2.2.1.La cryptographie..... 25

2.2.2 La stéganographie…….. 26

2.2.3 Le tatouage numérique…… 27

2.3 Processus de tatouage numérique d'image……29

2.3.1 Processus d'insertion……....30

2.3.1.1Schéma général.....30

2.3.1.2 Propriétés de la marque……31

2.3.2 Processus de détection / extraction de la marque…….…..33

2.3.2.1 Schéma général……..……...33

2.3.2.2 Processus de détection privé…….……..……34

2.3.2.3 Processus de détection aveugle…….……..…….34

2.3.3 Propriétés du processus de détection……....35

2.3.4 Les types de tatouage existants……...……..35

2.4 Etat de l'art sur les techniques de tatouage…… 38

2.4.1 Tatouage additif…….38

2.4.2 Tatouage substitutif……41

2.5 Evaluation des algorithmes de tatouage……..……. 44

2.5.1. Les attaques..…….…44

2.5.2 Mesure de la qualité de l'image……..……45

2.5.3 Banc d'essai……...49

2.6 Différentes applications du tatouage numérique…….……49

2.6.1 Protection des droits d'auteur……....49

2.6.2 Traçabilité dans un système commercial……..……...50

2.6.3 Authentification du document…….…..50

2.6.4 Contrôle d'accès…….……....50

2.6.5 Gestion du nombre de copies…….…....51

2.6.6 Contrôle de diffusion audiovisuelle…….…..…51

2.6.7 Indexation des documents…….....51

2.6.8 Autres applications…….....52

2.7 Conclusion…….…..……53

CHAPITRE 3 : Tatouage des images JPEG

3.1 Introduction 54

3.2 Etat de l'art sur les techniques de tatouage appliquées aux images JPEG..... 54

3.3 Application 59

3.3.1 Méthode non-réversible…….. 59

3.3.2 Méthode réversible…….…. 62

3.3.3 Prétraitement de la marque……. 64

3.3.3.1 Algorithme de chiffrement……. .64

3.3.3.2 Fonction de hachage…….. 66

3.4. Conclusions 66

CHAPITRE 4 : Applications

4.1 Introduction 67

4.2 Méthode Non-réversible 67

4.2.1 Résultats et interprétations 68

4.2.1.1 Evaluation perceptuelle 70

4.2.1.2 Evaluation de la capacité d'insertion 78

4.2.1.3 Evaluation du taux de compression..... 81

4.2.4 Avantages et inconvénients..... 82

4.3 Méthodes réversibles..... 84

4.3.1 Résultats et interprétations 84

4.3.2 Intérêts de la méthode réversible..... 86

4.4 Interface graphique..... 86

4.5 Conclusion……..89

Conclusion générale

Annexe A Les attaques

Annexe B Les bancs de tests

Annexe C Les algorithmes

Bibliographie

Liste des figures

Figure 1.1 : Courbe débit –distorsion…… ..….....3
Figure 1.2 : Codage d'Huffman… …….…..... 6
Figure 1.3 : Chaîne de compression avec perte. ……...……..…… 9
Figure 1.4 : Exemple d'homothétie dans une image de scène naturelle…….…..... 10
Figure 1.5 : Principe de quantification vectorielle…….…..... 11
Figure 1.6 : Schéma bloc de la technique de compression *JPEG*……..…..… 12
Figure 1.7 : Application de la DCT sur un bloc 8*8 de l'image…….....…..… 14
Figure 1.8 : Codage des coefficients du bloc 8*8 quantifiés……...……...…… 15
Figure 1.9 : Courbes de scanning : (a) Courbe de Hilbert, (b) Ragazoni (c) Courbe en zigzag (d) Courbe associée à l'ordre lexicographique…….16
Figure 1.10 : Schéma bloc de la décompression *JPEG*…….. 17
Figure 1.11: Principe du codage prédictif se basant sur les valeurs des pixels voisins…..…..20
Figure 1.12 : Illustration de la décomposition en ondelettes…….. 22
Figure 2.1 : Illustration du principe de cryptologie ……..…. 25
Figure 2.2 : Exemple de la stéganographie…….……....27
Figure 2.3 : Nombres de publications sur le watermarking par IEEE ……..…...29
Figure 2.4: Schéma général de tatouage d'image :(a) principe d'insertion, (b) principe d'extraction……...30
Figure 2.5 : Schéma général du processus d'insertion d'une marque…….....31
Figure 2.6 : Spécificité de la marque…….....31
Figure 2.7 : Schéma général du processus de détection/extraction d'une marque……..…33
Figure 2.8 : Schémas privés:(a) schéma privé de type I ;(b) schéma privé de type II ……...34
Figure 2.9: Schémas aveugles : (a) schéma aveugle semi-privé (b) schéma aveugle publique……34

Figure 2.10 : Illustration d'un tatouage: (a) Visible, (b) Invisible…… ..…….....36
Figure 2.11 : Tatouage réversible ……...……...…..... 37
Figure 2.12 : Schéma de tatouage par blocs…….....40
Figure 2.13 : Schéma général d'un algorithme de tatouage substitutif.……...…....41
Figure 2.14 : Modification du bit de poids faible d'un pixel. …….....42
Figure 2.15: Les 8 coefficients sur lesquels on peut insérer un bit. …….....42
Figure 2.16 : Quantification selon le bit à insérer. ……...…….....43
Figure 2.17 : Décomposition en régions de recherche. ……...……44
Figure 2.18 : Comparaison d'images avec le même PSNR …….....47
Figure 2.19 : Evaluation du PSNR comme mesure de qualité visuelle ……..……...47
Figure 2.20 : Evaluation du PSNR comme mesure de qualité visuelle……..….. ..48
Figure 2.21 : Contrôle d'accès par masquage visible d'une image ……....…….50
Figure 2.22 : Application du tatouage pour l'indexation d'image (smart image) ……...52
Figure 3.1 : Schémas génériques pour l'insertion de la marque dans un fichier JPEG ……..55
Figure 3.2 : Distribution des fréquences dans un bloc DCT ……..…….....56
Figure 3.3 : Bloc DCT 8x8 quantifié …….....56
Figure 3.4 : Schéma général d'insertion et d'extraction de la marque de ma méthode de Xuan *et al*…… 58
Figure 3.5 : Illustration de la technique du décalage de l'histogramme……..… 59
Figure 3.6 : Schéma proposé : insertion et extraction de la marque ……..….....60
Figure 3.7 : Schémas de tatouage réversible …….……..……63
Figure 3.8 : Le carré de Vigenère……..……..65
Figure 4.1 : Images tests……...…….....69
Figure 4.2 : Comportement du coefficient DC et AC sur l'image de Lena 512*512 en tatouant un seul bit par bloc…….……...…….73
Figure 4.3 : Comparaison des histogrammes d'une image avant et après tatouage 74
Figure 4.4 : Distorsion introduite sur un bloc 8*8 de l'image de Lena 512*512……...…….77
Figure 4.5 : Insertion d'un bit par bloc dans la zone basses fréquences, moyennes et hautes fréquences respectivement……...… 78
Figure 4.6 : Evaluation de la capacité d'insertion…….....……..……. …80

Figure4.7: Comparaison du taux de compression de différentes insertion d'un bit sur l'image de Lena 512*512…… 81

Figure 4.8 : Comparaison du taux de compression de différentes insertion de deux bits sur l'image de Lena 512*512……..……..……... 81

Figure 4.9 : Illustration du tatouage réversible ……...……85

Figure 4.10 : Interface graphique…….……..…….....……88

Liste des tableaux

Tableau 2.1: Appréciations possibles de la qualité de l'image ……...45
Tableau 3.1: Exemple d'un chiffrement de Vigenère ……...……..65
Tableau 4.1: Insertion de la marque dans le coefficient DC……...…….70
Tableau 4.2: Insertion de la marque dans la zone des moyennes fréquences……..71
Tableau 4.3: Insertion de la marque dans la zone des hautes fréquences……...….71
Tableau 4.4: Insertion de la marque dans le coefficient DC et d'autres coefficients basses fréquences…… 74
Tableau 4.5: Insertion de la marque dans le coefficient DC et d'autres coefficients moyennes fréquences……...……...…….……. 75
Tableau 4.6: Insertion de la marque dans le coefficient DC et d'autres coefficients hautes fréquences…… 75
Tableau 4.7: Tableau récapitulatif de la méthode réversible…….……...…...……84

ABREVIATIONS

CCITT: Consultative Commette for International Telegraph and Telephone;

ITU: International Telecommunication Union;

ISO: Organisation Internationale de Standardisation ;

IEC : International Electrotechnical Commission;

DES : Data Encryption Standard;

SALT 2: Strategic Arms Limitation Talks 2;

LSB: Least Significant Bit;

IHW: Information Hiding Workshop;

SPIE: Société parisienne pour l'industrie électrique ;

IWDW: InternationalWorkshop on Digital Watermarking;

IEEE: Institute of Electrical and Electronics Engineers;

LNCS: Lecture Notes in Computer Science ;

DVD: Digital Versatile Disc ;

JASRAC : Japanese Society for Rights of Authors;

RIAS: Remote Infrared Audible Signage ;

DCT : Discrete Cosine Transform ;

SVH : Systéme Visuel Humain (en anglais HVS) ;

JPEG: Joint Photographic Experts Group ;

TFD Transformée de Fourier Discrète ;

GPS: Global Positioning Satellite;

DFT: Density Functional Theory;

DWT : Discrete Wivelet Transform;

IFS : Iterated Function System ;

MSE :Mean Squared Error / EQM : d'erreur quadratique moyenne ;

SNR: Signal to Noise Ratio;

PSNR: Peak Signal to Noise Ratio;

VHS: Video Home System ;

CCIR : Comité Consultatif International de la Radio Electricité ;

SACEM : Société des Auteurs, Compositeurs et Editeurs de Musique ;

JPEG-LS: lossless and near-lossless;

LOCO-I: LOw COmplexity LOssless COmpression for Images;

JBIG: Joint Bi-level Image Experts Group;

JFIF : JPEG File Interchange Format ;

MPEG : Motion Picture Expert Groups ;

Introduction générale

Si la «révolution industrielle» a bouleversé en son temps le développement de toute une époque, force est de constater que la «révolution numérique» prend actuellement le même chemin. Rares sont les domaines qui n'ont pas succombé au numérique, parmi les premiers fut l'image.

Des applications voient le jour au rythme de l'imagination de leurs concepteurs, créant ainsi un besoin incessant d'innovation et de développement de systèmes déjà existants, afin de répondre à des utilisateurs de plus en plus exigeants.
Mais cette ruée vers le progrès technologique n'est pas de tout repos, car elle a dû être confrontée à de réels problèmes, d'une part à la limitation du stockage de données et l'augmentation drastique des temps de transmission, et d'autre part à la protection de ces données qui sont devenues facilement et illégalement exploitées, ainsi de nouvelles disciplines ont vu le jour, telles que le tatouage numérique, s'associant à des disciplines plus anciennes telles que la cryptographie et la compression, afin d'assurer une fluidité des données numériques sur la toile, en toute sécurité.

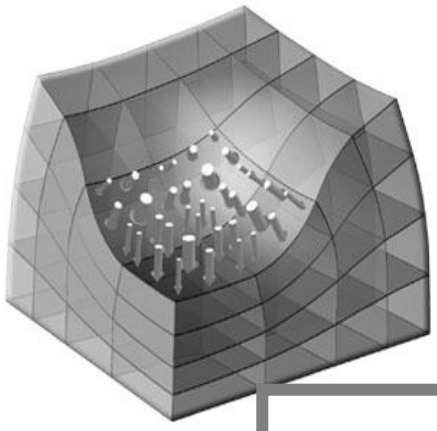
Les progrès technologiques en matière d'intégration, de capacité de stockage et de support de transmission, ne suffisent pas à eux seuls pour absorber les flux de données de plus en plus importants, générés par des applications de plus en plus sophistiquées, notamment l'image qui représente une entité très riche en information. La compression répond à cette problématique, elle a fait l'objet de plusieurs recherches qui ont donné naissance à des standards, dont le plus célèbre est incontestablement le *JPEG,* à la base de la majorité des appareils photos numériques. La compression vise à représenter l'information sous sa forme la plus compacte, en se basant sur les limites du système visuel humain, elle est devenue un passage obligatoire pour tout document numérique. Cette discipline fait l'objet de notre premier chapitre.
Mais il ne s'agit pas uniquement de compresser une image en vue de la transmettre ou de la stocker, mais de lui intégrer une autre chaine de traitement, dans notre cas, c'est le tatouage.

En effet, le pouvoir d'accéder à la donnée très rapidement, de pouvoir la copier, la modifier et même la dupliquer, ne la laisse pas à l'abri des pirates informatiques, à la quête de données, ainsi le tatouage consiste à introduire une information dans un document numérique, sous forme d'une marque, d'une manière invisible et indélébile, s'inscrit dans la protection des droits d'auteur et de la propriété intellectuelle et bien d'autres rôles aussi importants tels que l'authentification, le contrôle d'intégrité, et le suivi des copies illégales, développés dans le deuxième chapitre.

Cependant, compression et tatouage ne font pas bon ménage, puisque l'une tend à réduire l'information et l'autre à ramener de l'information, ce qui fait le défi de nouvelles études s'orientant vers l'association de ces deux disciplines, révélant ainsi un terrain de recherche très prometteur. Un état de l'art de quelques techniques existantes est proposé dans le chapitre trois.

Cette association fait l'objet de notre projet de fin d'études, intitulée «Le tatouage des images *JPEG*». Dans notre travail, nous insérant une marque après l'une des étapes de la compression *JPEG*, qui est la quantification, dans le but d'assurer l'authenticité de l'image. Dans un premier temps, nous effectuons une étude de l'impact de la marque sur la qualité de l'image et sur le taux de compression, à travers l'implémentation d'une méthode de tatouage non réversible.

Une méthode réversible est ensuite proposée, permettant, à qui de droits de récupérer la qualité initiale de l'image *JPEG*. Afin de renforcer la sécurité de ces deux méthodes, on les associe à des outils de cryptographie. Les méthodes sont proposées dans le chapitre trois, les applications et résultats sont traités dans le dernier chapitre.



Chapitre 1

La compression JPEG

1.1 Introduction

Depuis les débuts des technologies de l'information, le problème de l'exploitation optimale des voies de communication et des capacités de stockage est toujours resté un sujet d'actualité. Dans le domaine des applications multimédias, par exemple, la plupart des données traitées sont volumineuses et le domaine de la compression des données est crucial pour leur existence et pour les enjeux économiques sous-jacents, ainsi la compression a fait l'objet de multiples études dans le but de mettre les données sous un format tel qu'elles occupent moins de volume.

Une fois compressées, les données ne sont plus directement accessibles, une opération de décompression est nécessaire pour qu'elles redeviennent intelligibles. La grande variété des domaines d'exploitation, chacun ayant ses contraintes spécifiques (nature des données, capacités de traitement,…), conduit aujourd'hui à un très grand nombre de procédés de compression, qui peuvent être classés en deux grandes familles selon la perte d'information, en méthodes réversibles et méthodes irréversible. Nous traiterons dans ce chapitre les généralités sur la compression avec perte et sans perte, nous nous attarderons sur la compression *JPEG* qui est le pilier de notre travail.

1.2 Généralités sur la compression d'images

1.2.1 Définition

L'objectif principal de la compression d'image est de réduire la quantité d'information (le nombre de bit par pixel) nécessaire à une représentation visuelle fidèle à l'image originale, en exploitant la redondance informationnelle dans l'image, à des fins de stockage ou de transmission.

1.2.2 Evaluation de la compression

Le taux de compression (compression ratio) est utilisé pour évaluer le résultat d'un procédé de compression. Si on peut compresser un fichier de dix fois, on parlera alors d'un taux de 10:1 ce qui signifie que sa taille a été divisée par 10. Ce sera également un critère d'efficacité entre différents algorithmes possédants respectivement un taux de 10:1 contre un taux de 2 :1 par exemple.

Dans la littérature il est représenté sous plusieurs formes, la plus répandue est celle exprimée par la formule (1.1), [1] :

$$\sigma = \frac{nombres\ de\ bits\ utilisés\ par\ l'image\ originale}{nombre\ de\ bits\ utilisés\ pour\ l'image\ compressée} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1.1)$$

1.2.3 La quantité d'information

Les notions d'information propre, d'entropie et la fonction débit/distorsion sont issues de la théorie de l'information à laquelle Schannon a laissé des travaux d'une importance essentielles. Dans ce qui suit on donnera quelques définitions qui ont été à la base de la compression **[1]**.

1.2.3.1 Information de source

La quantité d'information de source d'un signal numérique quelconque est le nombre de bits nécessaires à la représentation binaire des nombres qui lui ont été attribués par le capteur (appareil photo, scanner…).

1.2.3.2 Information propre

On peut dire qu'un signal est la composition d'une information utile (le message) et d'une redondance. L'idéal serait de ne coder que l'information utile. Une première phase est donc d'évaluer, dans un signal, les parts respectives de l'information et de la redondance, chose qui est faisable en modélisant le système par des variables aléatoires.

Dans le cas d'une image, chaque point « n_i » représentant le niveau de gris, est considéré comme variable aléatoire de valeur comprise entre 0 et 255. Chaque niveau de gris aura donc comme information propre celle exprimée par la formule (1.2) :

$$I(n_i) = \log_2 \frac{1}{p(n_i)} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1.2)$$

Où : $p(ni)$ est la probabilité d'apparition du i ième niveau de gris dans l'image.

1.2.3.3 L'entropie

A chaque niveau de gris *ni* d'une source *S* est associée une quantité d'information propre *I*(*ni*). La valeur moyenne de *I*(*ni*) définit l'entropie de *S*, ou la surprise moyenne apportée par la source *S* d'où :

$$H(S) = \sum_{i=1}^{m} p(ni).I(ni) \dots\dots\dots\dots\dots\dots\dots\dots (1.3)$$

1.2.3.4 Courbe débit-distorsion

La courbe présente deux zones bien distinctes. Celle sous l'entropie où le décodage a toutes les chances de ne pas se faire correctement. Il est synonyme de dire que de la distorsion a été introduite et que la compression est plus importante, cette zone concerne la compression irréversible. Par contre la zone en dessus de l'entropie n'introduit pas de distorsion, mais au prix d'une efficacité (diminution du débit) souvent très réduite. La figure (1.1) nous illustre cette courbe.

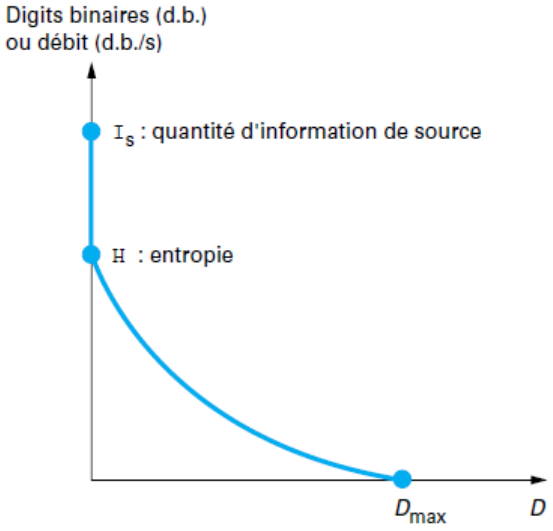


Figure 1.1 : Courbe débit - distorsion

1.3 Les méthodes de compression

Il existe plusieurs méthodes de compression qui peuvent être distinguées par plusieurs critères, qui sont:

- ✓ *Méthodes symétriques et asymétriques*

Une méthode de compression symétrique utilise le même algorithme, et demande la même capacité de calcul, aussi bien pour la compression que pour la décompression. Pour les méthodes asymétriques, l'étape de compression demande beaucoup plus de temps et de ressources systèmes que l'étape de décompression, c'est valable pour les bases de données où les données seront compressées une seule fois mais décompressées un grand nombre de fois.

- ✓ *Codage adaptatif et non-adaptatif*

La compression adaptative est capable de s'adapter à n'importe quelles données d'entrées et de retourner une sortie avec le taux de compression le meilleur possible. C'est une des principales différences avec les compressions non-adaptatives qui sont capables d'avoir des codages efficaces uniquement avec un type de données d'entrées très restreint pour lequel ils ont été conçus.

- ✓ *Méthodes avec et sans distorsion*

Elles représentent le critère le plus important sur lequel se base la majorité des classifications des algorithmes de compression.

Une compression est dite « sans perte » signifie qu'après décompression l'information originale est préservée. Quant à la compression « avec perte », elle élimine de façon sélective quelques données de l'image pour améliorer le taux de compression. En effet, en tenant compte des limitations de l'œil humain, il est possible de réduire les informations de chrominance et de luminance difficilement perceptible par la plupart des gens.

Expérimentalement les méthodes sans distorsion offrent un très faible taux de compression se qui intéresse particulièrement les applications qui ne peuvent souffrir de décoder un signal non exactement identique à l'original, plus particulièrement les images médicales. Par contre les méthodes avec distorsion engendrent des taux de compression très élevés est sont destinées aux données multimédia.

1.3.1 Les méthodes de compression sans pertes

La compression sans perte, codage entropique ou codage réversible, tous ces termes désignent une compression sans distorsion. Le processus consiste à créer des "mots-codes" c'est-à-dire accorder un nombre de bits différents à chaque symbole, de façon que les plus fréquents soient représentés par un nombre minimum de digits binaires. Ces processus s'appuient sur des informations statistiques de l'image [2]. Le but est de tendre vers l'entropie.
Les contraintes étant d'ordre pratique : faisabilité, complexité, coûts et temps de calcul. Nous citerons dans ce qui suit les méthodes de codage les plus répondues.

1.3.1.1 Les codages statistiques à longueur variable

Elle repose sur le fait qu'un flux de données peut être compacté en utilisant un code de longueur variable, *VLC* (Variable Length Code), pour représenter les différents octets ou séquences d'octets. Les symboles les plus fréquents sont codés sur de courtes séquences de bits tandis que les symboles les plus rares sont codés sur davantage de bits. Avec cette méthode de stockage le taux avoisine les 50%. Parmi les algorithmes les plus usités [1]:

- ✓ ***Algorithme de Shannon-Fano***

L'algorithme de Shannon-Fano permet la détermination d'un *VLC* préfixé[1]. L'idée est de classer les symboles par ordre de probabilités décroissantes, ensuite les répartir en deux groupes de valeur à peu près équivalente, cette valeur étant la somme, dans chaque groupe, des probabilités d'apparition des symboles qu'il contient.

Le groupe de gauche est appelé 0, celui de droite 1 (ce choix est arbitraire). Les groupes sont à nouveau subdivisés et nommés 0 ou 1 jusqu'à ce que la subdivision ne contienne plus qu'un symbole. L'arbre binaire ainsi obtenu est formé de segments ou branches et de feuilles. Chaque branche représente un bit d'information (0 ou 1), Chaque feuille contient un caractère simple. Pour déterminer le code numérique d'un caractère donné, il faut partir du sommet de l'arbre et suivre les branches jusqu'à atteindre la feuille qui le représente. Les caractères les plus fréquents se trouvent le plus près du sommet et requièrent donc moins de bits dans leurs transcriptions compressées.

[1] Un code est dit préfixé s'il n'est le début d'aucun autre.

Le fait d'être à longueur variable présente l'avantage de pouvoir vérifier le théorème de Schannon c'est-à-dire de nécessité un nombre global de bits minimum proche de l'entropie. Le fait d'être préfixé, il préserve la synchronisation mais on lui préfère l'algorithme d'Huffman détaillé dans ce qui suit.

- ✓ ***Codage d'Huffman***

L'algorithme de Huffmann a été décrit pour la première fois en 1952, son idée de base est d'inverser le raisonnement de Shannon et Fano. Ainsi plutôt que de subdiviser une liste indéfiniment avec pour effet de développer un arbre à partir de son sommet, pourquoi ne pas le construire en partant d'en bas. Les symboles sont d'abord triés et classés en fonction de leur fréquence (occurrence).

Un graphe est alors construit de la manière suivante: A partir des deux symboles présentant la fréquence la plus faible, un nœud est créé. Il lui est affecté un poids égal à la somme des fréquences des deux symboles. Le nœud créé remplace désormais les deux symboles dans la suite du processus. A ces derniers sont affectés respectivement les chiffres binaires 0 pour le plus fréquent et 1 pour le plus rare, (ou l'inverse, il s'agit d'une convention totalement arbitraire).

La même démarche est reprise en considérant les deux symboles ou nœuds de poids le plus faible. Elle est renouvelée tant qu'il reste plus d'un nœud libre. La figure 1.2 nous illustre ce principe en prenant comme exemple la suite de symbole A, B, C, D, E avec une fréquence respective d'apparition de: 7, 6, 5, 14, 4.

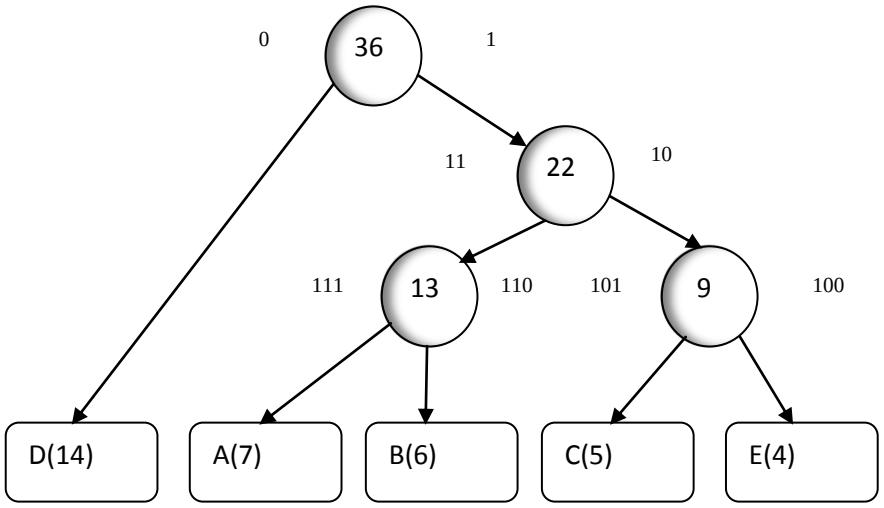


Figure 1.2 : codage d'Huffman

1.3.1.2 Les codages par dictionnaire

Les codages par dictionnaire sont fondés sur la constitution d'une suite de motifs, apparaissant dans le flux du message. Ces motifs remplissent un dictionnaire, où ils sont indexés, et lorsque les motifs réapparaissent, ils sont simplement codés par leur index dans ce dictionnaire. Ils seront efficaces pour les sources longues, codés sur des alphabets restreints, ce qui permet d'envisager la présence de motifs récurrents. La seule manière pour un algorithme à dictionnaire d'être efficace est d'utiliser un dictionnaire dynamique ou adaptatif, c'est-à-dire construit selon la source à coder. C'est le principe de l'algorithme LZ et de ses variantes, nous détailleront l'algorithme LZW, le plus utilisé [2].

- ✓ ***Algorithme LZW***

Son principe repose sur le repérage de séquences qui se répètent dans une suite complète de niveaux de gris d'une image. L'idée est alors, au moment du codage, de ranger en mémoire ces séquences, dès qu'on les découvre pour la première fois. Cette mémoire, ou partie de mémoire affectée à cette tâche est appelée table de traduction. Si dans la suite, au cours de l'analyse, il apparaît une chaîne de caractères déjà présente dans la table de traduction, plutôt que de remplacer (coder) chacun des symboles qui la composent par un mot binaire, le codeur, code l'ensemble de la chaîne par son adresse dans la table de traduction.

On le trouve par exemple dans : les fichiers ayant l'extension Z, zip; les formats PDF[2]. Dans le format TIFF, les données pixels sont empaquetées en deux bits avant d'être présentées au compresseur LZW. Pour le format GIF permet des profondeurs d'images allant de 1 à 8 bits, il y a entre 2 et 256 valeurs de codes d'entrées possibles pour le dictionnaire de LZW, donc le dictionnaire est initialisé en conséquence.

1.3.1.3 Codages par longueur de plages

Dans la pratique, il est rare que l'on prenne directement les niveaux de gris d'une image comme symboles à coder, un bel exemple est le codage par plage ou encore le codage RLE (Run Length Encoding), son principe est de regrouper les points voisins ayant les mêmes niveaux de gris. Chaque groupement définit d'une façon unique une paire de nombres $P=(plage,n)$ en changeant le support d'information dans laquelle :

[2] Portable Document Format

Plage est le nombre de points voisins possédants le même niveau de gris et *n* est le niveau de gris commun entre les points voisins.

C'est une méthode très simple si l'image comporte de nombreuses « plages » de valeurs identiques : il est alors avantageux de coder la longueur (le nombre de symboles identiques) et la valeur de chaque plage. C'est particulièrement vrai dans le cas d'images avec « aplats[3] » où le codage des coefficients DCT quantifiés dans l'algorithme de type *JPEG*.

1.3.2 Les méthodes avec pertes

Les images se prêtent à la compression avec pertes, car l'œil agit comme un filtre et élimine d'lui-même certaines informations. La chaîne de compression avec perte la plus répandue est représentée par la figure (1.3). Elle comporte trois étapes essentielles : une étape de transformation des données, de façon à les représenter de manière plus compacte, suivie d'une étape de quantification et d'une étape de codage pour éliminer les dernières redondances. Nous noterons que la quantification peut être scalaire ou vectorielle [3].

On distingue trois approches selon le contenu de la première étape :

- ✓ l'approche fréquentielle, telle qu'elle est utilisée dans JPEG à travers la transformée en cosinus discrète. Nous nous attarderons sur ce concept puisqu'il est à la base de notre mémoire, dans la section (1.4).

- ✓ L'approche spatio-fréquentielle, qui a été retenue dans JPEG2000, basée en particulier sur la transformée en ondelettes dont l'efficacité a été prouvée pour coder des signaux non stationnaires tels que les images;

- ✓ L'approche par fractales ou plus récemment par ondelettes «géométriques» visant à améliorer la prise en compte de l'information géométrique des contours dans l'image.

[3] Surface d'une seule couleur ou de couleur uniforme exemples : logos, images graphiques

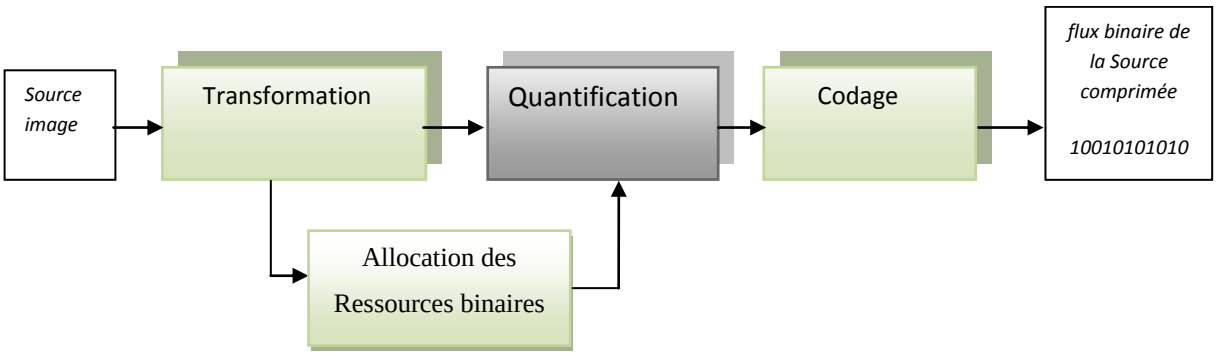


Figure 1.3: Chaîne de compression avec perte.

1.3.2.1 La compression par ondelettes

La transformée en ondelettes discrète est un outil efficace utilisé largement en traitement du signal. Elle est la base du standard de compression JPEG2000. La transformée en ondelettes d'une image consiste à la décomposer en plusieurs bandes de fréquences et en différentes orientations et échelles. Cette décomposition permet de localiser les grandeurs des fréquences de l'image (fréquences hautes, moyennes et basses) et leurs orientations (fréquences horizontales, verticales et diagonales).

La compression d'images par ondelettes est une méthode "destructrice", c'est à dire que lors de la compression, des informations sont définitivement perdues par rapport à l'image originale. Son fonctionnement est similaire à celui du jpeg (voir section 1.4) à la seule différence que la transformée utilisée est la DWT (Discret Wavelet Transform) ou la transformation en ondelettes discrète.

1.3.2.2 l'approche fractale

La théorie des fractales modélise la nature de certaines courbes, et plus généralement, de certains objets, en y reconnaissant, entre autre, une homothétie [4] interne. Une fractale : est une structure géométrique qui se reproduit, dans une boucle infinie, par transformation affine

[4] L'existence d'une similarité de forme, par exemple pour un arbre : on peut distinguer des branches maîtresses qui, globalement, ressemblent à l'arbre lui-même, on constate aussi qu'une branche maîtresse est elle-même constituée de branches qui ressemblent à nouveau à l'arbre mais en dimensions réduites et selon des directions variées.

(translation, rotation et mise à l'échelle). Cette structure se refait à toutes les échelles de forme réduite et légèrement déformée.

La compression par fractale exploite les récurrences des motifs qui, après quelques traitements, peuvent permettre une compression. La figure 1.4 présente un exemple d'exploitation des motifs. L'idée étant qu'une image est stockée sous la forme d'un ensemble de formules plutôt que d'un ensemble de points (ou bien de transformations d'ensembles de points).

Figure 1.4 : Exemple d'homothétie dans une image de scène naturelle

Les contenus des deux encadrés A1 et A2 ainsi que des encadrés B1 et B2 sont presque identiques à des transformations linéaires près. Ces dernières peuvent intervenir sur les niveaux de gris.

1.3.2.3 La quantification scalaire (QS)

La quantification scalaire est réalisée indépendamment pour chaque élément. D'une manière générale, on peut la définir comme étant l'association de chaque valeur réelle, à une autre valeur q qui appartient à un ensemble fini de valeurs. La valeur q peut être exprimée en fonction de la troncature utilisée. La différence entre la vraie valeur et le niveau de quantification le plus proche, constitue une erreur ou distorsion qui nuit à la qualité du signal restitué en bout de chaîne. On parle de bruit de quantification.

1.3.2.4 La quantification vectorielle (QV)

En réalité, il n'y a qu'une quantification et elle est vectorielle, la QS n'étant qu'un cas particulier de la QV lorsque la dimension est de 1. Plutôt que de quantifier les échantillons les uns après les autres, la QV les quantifie par blocs. La figure (1.5) nous illustre ce principe.

La QV s'effectue sur une image successivement de la façon suivante : Découpage de l'image en blocs, ici de taille 4 × 4. Un bloc donné de l'image est comparé à l'ensemble des M blocs prédéfinis de ce que l'on appelle le dictionnaire. On remplace le bloc donné original par le bloc le plus ressemblant. On perd alors l'image au profit d'un tableau de nombres. Cet ensemble de nombres constitue le codage de l'image [1].

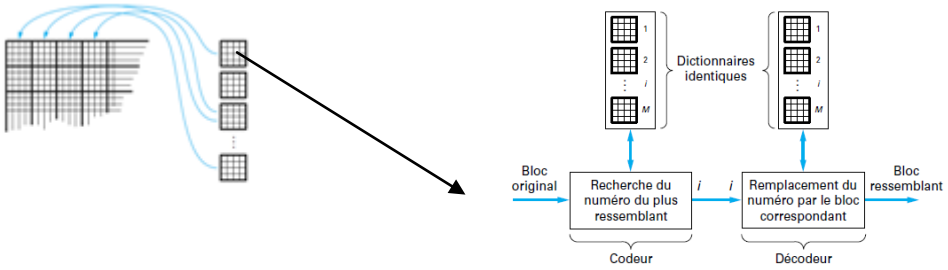


Figure 1.5 : Principe de quantification vectorielle

2.1

2.2 1.4 *JPEG* et la compression des images

1.4.1 Introduction

Le CCITT (Aujourd'hui appelé l'ITU) et l'ISO, ont travaillé ensemble pour élaborer une norme internationale commune pour la compression d'images fixes, devenue nécessaire pour faciliter l'échange des images dans divers domaines.

Officiellement, *JPEG* (*Joint Picture Expert Group)* est la norme 10918-1 de ISO / IEC internationale standard de la compression numérique et le codage des images fixes, ou bien la Recommandation T.81 de l'ITU-T. Le JPEG est devenu une norme internationale en 1992, il comprend des spécifications pour un codage sans perte qui permet une restitution de l'image identique à elle-même à la suite d'un codage ou bien un codage avec perte qui modifie légèrement l'image pendant le cycle de compression.

Le *JPEG* est aujourd'hui largement utilisé dans les secteurs de l'informatique et de la communication (appareils photo numériques, scanners, imprimantes, télécopieurs...). Dans ce qui suit, nous nous intéresserons plus au codage avec perte qui est le plus utilisé.

1.4.2 La compression JPEG

La compression JPEG est une méthode de compression qui permet d'altérer une image d'une manière à éliminer des informations que l'œil humain a de la peine à voir en offrant des taux de compression considérable jusqu'à 20-25 fois la taille de l'image sans qu'elle subisse de détérioration notable.

Selon la norme posée par le *CCITT*, il existe quatre formes pour le *JPEG* ainsi il offre un éventail d'utilisation très large, mais l'algorithme séquentiel avec perte reste le plus prisé des quatre.

1.4.2.1 Algorithme de base

La figure 1.6 résume le processus de compression avec perte pour des images en niveau de gris. Il s'agit essentiellement de compression d'un flux de bloc 8x8 d'échantillons de l'image. En effet le format *JPEG*, comme le font généralement les algorithmes de compression à perte, commence par découper l'image en blocs carrés de 64 coefficients (8 × 8).

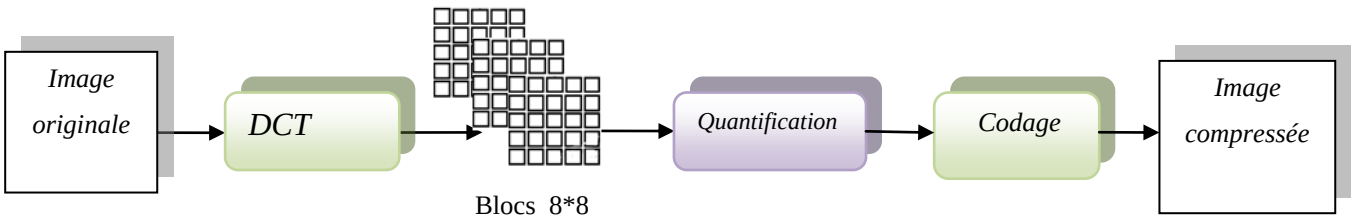


Figure 1.6 : schéma bloc de la technique de compression *JPEG*

L'étape suivante est la transformée en effet, la plupart des algorithmes de compression avec perte opèrent sur une transformation de l'image qui projette les données dans un espace plus propice à la quantification et au codage entropique. L'idée est d'obtenir un ensemble de coefficients moins corrélés et plus compact c'est-à-dire que le signal est concentré sur un nombre restreint de composante au lieu d'être uniformément réparti [4].

1.4.2.2 La Transformée en Cosinus Discrète (DCT)

On appliquera donc sur chaque bloc 8*8 la Transformée en Cosinus Discrète (DCT) exprimée par la formule (1.4) qui décrira une carte de fréquences et d'amplitudes plutôt que de pixels et de couleurs. La valeur d'une fréquence reflète l'importance et la rapidité d'un changement de couleur, tandis que la valeur d'une amplitude correspond à l'écart associé à chaque changement de couleur.

$$C(u,v) = \alpha(u)\alpha(v)\left[\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j)\cos\left(\frac{(2i+1)u\pi}{2N}\right)\cos\left(\frac{(2j+1)v\pi}{2N}\right)\right] \quad \text{.....(1.4)}$$

$$\alpha(u)=\begin{cases} 1 \ pour\ u = \ 1,\dots,N-1 \\ \frac{1}{\sqrt{2}} \ pour\ u = 0 \end{cases}$$

avec : N=8

$$\alpha(v)=\begin{cases} 1 \ pour\ u = \ 1,\dots,N-1 \\ \frac{1}{\sqrt{2}} \ pour\ u = 0 \end{cases}$$

A la sortie de la matrice DCT, la valeur de la position (0,0) est appelée le *coefficient continu(DC).* Cette valeur représente une moyenne d'ensemble de la matrice d'entrée, le *DC* est plus important en ordre de grandeur que les autres coefficients nommés *AC*. Plus on s'éloigne du coefficient continu plus l'ordre de grandeur tend à diminuer. Ce qui signifie que la DCT concentre la représentation de l'image en haut à gauche de la matrice de sortie, les coefficients en bas et à droite de cette matrice contient moins d'information utile, voir figure1.7. Le calcul de la DCT est l'étape qui coûte le plus de temps et de ressources dans la compression *JPEG*, mais c'est l'étape la plus importante car elle permet de séparer les basses fréquences (représentants les zones uniformes de l'image) des hautes fréquences (représentants le changement brusque d'intensité dans l'image). Cette étape ne compresse pas réellement l'image, c'est à partir de l'étape suivante qui est la quantification qu'il y a réellement perte d'information.

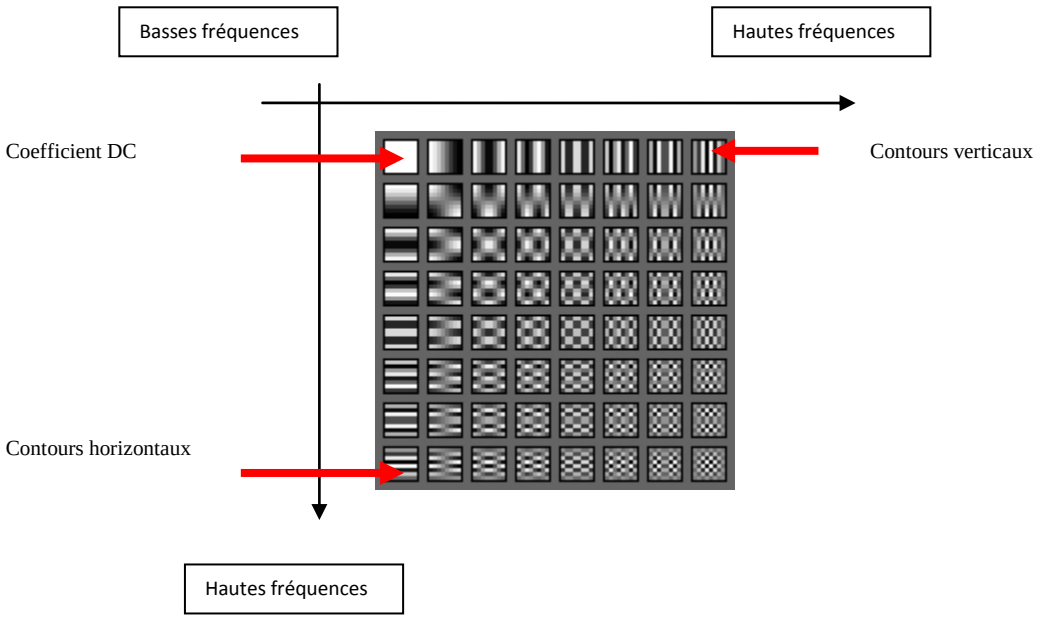


Figure1.7 : Application de la DCT sur un bloc 8*8 de l'image

La quantification est l'étape où l'on gagne beaucoup d'espace mémoire contrairement à la DCT qui ne compresse pas. Il s'agit dans notre cas d'une quantification scalaire uniforme qui consiste à diviser la matrice retournée par la DCT par une autre, appelée matrice de quantification Q (*i*,*j*), et qui contient 8×8 coefficients, le résultat obtenu sera amené à l'entier le plus proche.

Bien que la spécification de la communauté *JPEG* n'impose aucune contrainte sur la matrice de quantification, l'organisme de standardisation ISO a développé un ensemble de standard de quantification utilisable par les programmeurs *JPEG*. Ce choix a été rendu possible grâce aux tests intensifs des matrices via des observateurs mais elle n'est pas toujours appropriée. Pour ce fait et afin de perdre l'information d'une manière "astucieuse", la quantification dont dépend la précision de l'image restituée, va dépendre de la position de la valeur dans la matrice. En prenant un pas relativement petit pour les valeurs importantes (en haut à gauche) et en prenant un pas de plus en plus grand au fur et à mesure qu'on va vers le bas et la droite de la matrice, les hautes fréquences seront atténuées, c'est-à-dire celles auxquelles l'œil humain est très peu sensible. Ces fréquences ont des amplitudes faibles, et elles sont encore plus atténuées par la quantification (les coefficients sont même ramenés à 0). De cette manière une matrice de quantification peut être fabriquée grâce à la formule (1.5), [5]:

$$Q(i,j) = (1 + i + j) \times Fq \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1.5)$$

Où Fq : est le facteur de qualité.

De nombreux tests réalisés ont conduit à retenir en pratique des facteurs de qualité compris entre 1 (l'image reste excellente) et 25 (dégradation encore acceptable).

1.4.2.4 Le codage entropique

L'étape suivante consiste à rendre compact les valeurs retournées par la quantification. Pour ce faire, l'algorithme *JPEG* utilise les techniques classiques de compression sans perte.

Un codage *RLE* est utilisé pour les séquences formées essentiellement de 0, pour les autres valeurs, des ensembles sont compressées avec le codage de *Huffman*. Mis à part le coefficient *DC* qui sera codé d'une manière différente de tous les autres, par un codage différentiel vu qu'il y a corrélation entre le coefficient DC d'un bloc et celui du bloc précédent (voir figure 1.8). En effet pour le coefficient DC l'amplitude est codée par la différence entre deux coefficients voisins. Ils sont hautement prédictibles. La valeur des composantes DC est importante (rarement nulle) et variée, mais est souvent très proche de celle de ses voisins. La seule valeur qui est donc encodée est la différence DIFF entre le coefficient DC_i quantifié du bloc courant i et le précédent DC_{i-1}. Les blocs sont lus de la gauche vers la droite, ligne par ligne : DIFF = $DC_i - DC_{i-1}$. Il s'agit d'un codage appelé « Differential Pulse Code Modulation » (DPCM) ou codage de type prédictif (voir section 1.4.3.2).

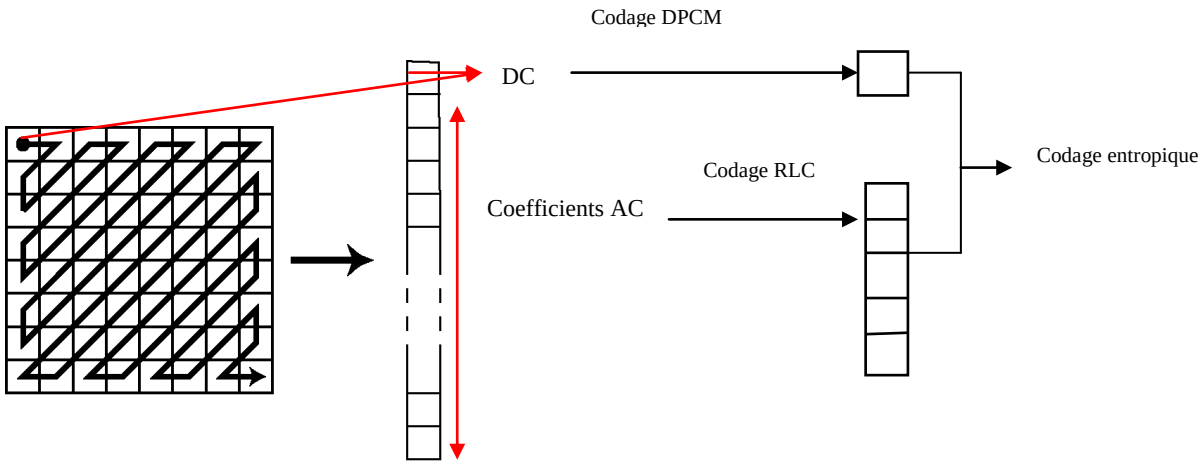


Figure 1.8 : codage des coefficients du bloc 8*8 quantifiés

Avec le codage *RLE*, la manière de balayer l'image pour coder les séquences répétitives est très importante, si on se contentait de lire ligne par ligne, de gauche à droite et de haut en bas, le résultat obtenu serait insatisfaisant, dans la mesure où la fin d'une ligne et le commencement de la suivante ne sont pas en continuité. Pour cela il existe une panoplie de courbe de balayage dite « courbe de scanning » rapportée dans la littérature [5]. La figure 1.9 nous illustre les courbes les plus utilisées.

Le comité *JPEG* a donc préféré un système de parcours en zigzag, c'est justifié par les valeurs proches des coefficients le long des diagonales ascendantes. Elle a pour but de rapprocher des valeurs identiques et de reporter le maximum de valeurs nulles vers la fin de la séquence. Cette méthode est sans doute meilleure mais pas optimale, de nombreux spécialistes estiment qu'un parcourt en courbe de Hilbert (Figure 1.9.a) aurait été un choix plus judicieux, puisqu'il aurait considéré la proximité des points de manière plus efficace, dans plusieurs directions.

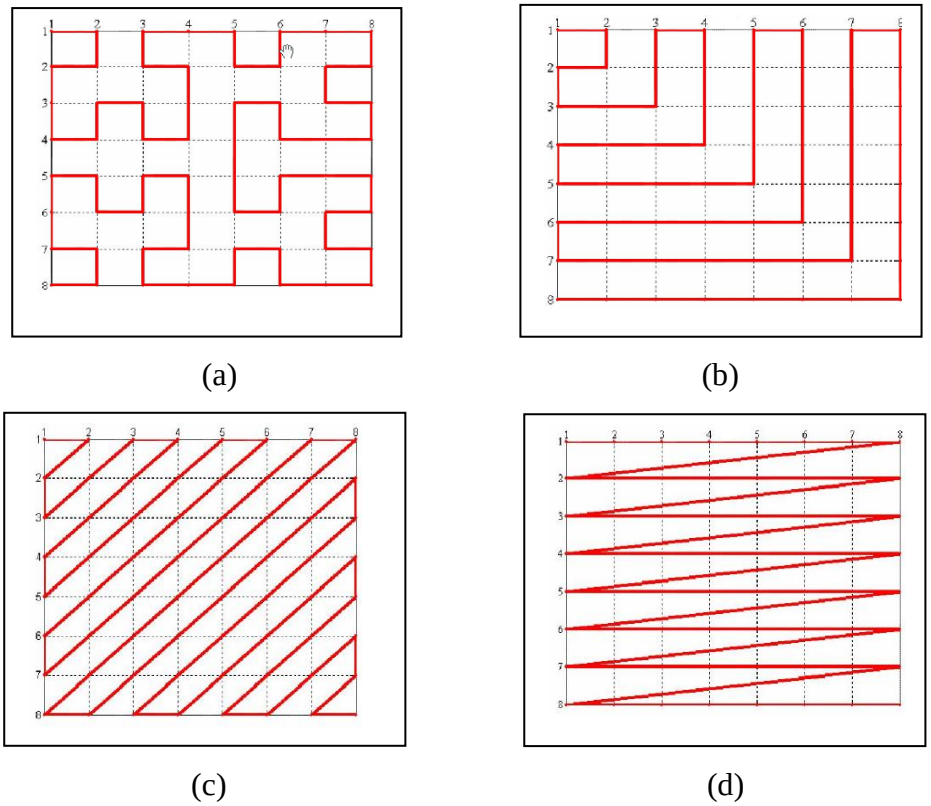


Figure 1.9 : courbes de scanning : (a) Courbe de Hilbert, (b) Ragazoni (c) courbe en zigzag (d) Courbe associée à l'ordre lexicographique

Ultérieurement lors de la restitution de l'image c'est-à-dire la décompression illustrée par la figure 1.10, il suffira de réaliser les opérations inverses.

Figure 1.10 : Schéma bloc de la décompression *JPEG*

Après décodage, on réalise la déquantification en multipliant chaque valeur de la matrice quantifiée par le quantum correspondant pour retrouver la matrice DCT déquantifiée, à partir de laquelle sera établie la matrice de pixel de sortie en appliquant la formule de DCT inverse donnée par l'équation 1.6.

$$f(x,y)=\left[\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left(\frac{(2i+1)u\pi}{2N}\right)\cos\left(\frac{(2j+1)v\pi}{2N}\right)\right] \quad (1.6)$$

1.4.2.5 Transformation des couleurs

Concernant les images couleurs, il y a deux étapes préliminaires qui n'existes pas dans la compression des images aux niveaux de gris, en effet la compression d'image couleur peut être considérée comme la compression de plusieurs images en niveaux de gris, qui sont soit comprimés une à la fois, ou alternativement comprimées (entrelacement des blocs de 8x8 d'échantillon).

Après que l'image est été découpée en bloc 8*8 une transformation lui sera appliquée. *JPEG* est capable de coder les couleurs sous n'importe quel format RGB, HSI ou CMY, toutefois les

meilleurs taux de compression sont obtenus avec des codages de couleur de type luminance/chrominance tels que YUV, YCbCr car l'œil est assez sensible à la luminance mais peu à la chrominance. Nous citerons les formats les plus utilisés [6].

- ✓ **Format RGB**

Le système RGB (Red, Green, Blue) représente chaque pixel comme étant un triplé de valeur, chacune représentant la quantité d'une couleur de base de Rouge, de vert et de bleu.
C'est un système additif dans lequel on varie la quantité des trois couleurs en les additionnant pour produire de nouvelles couleurs, ainsi le triplé (0,0,0) représente le noir alors que le (255,255,255) représente le blanc. Si les trois valeurs sont les même, on obtient un ton gris.

- ✓ **Format YUV (Y-signal, U-signal, and V-signal)**

C'est une transformation linéaire de RGB très utilisée dans le codage des couleurs pour les transmissions, et en télévision. Y spécifie la luminance (information de luminosité) alors que les composantes U et V correspondent à la chrominance (information de couleur). D'autres modèles sont basés sur YUV tels que : YCbCr ou YPbPr donnés respectivement par les relations 1.7 et 1.8.

Où :

$$\begin{cases} \mathrm{Y} = 0.299\mathrm{R} + 0.587\,\mathrm{G} + 0.114\,\mathrm{B} \\ Cb = B - Y \\ Cr = R - Y \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1.7)$$

$$\begin{cases} Y = 0.2122\mathrm{R} + 0.7013\mathrm{G} + 0.0865\mathrm{B} \\ Pb = -0.1162R - 0.3838G + 0.5000B \\ Pr = 0.5000R - 0.4451G - 0.0549B \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1.8)$$

L'étape qui suit et le sous échantillonnage. La façon la plus simple d'exploiter la faible sensibilité de l'œil à la chrominance est simplement de sous-échantillonner les signaux de chrominance. Généralement, on utilise un sous-échantillonnage de type 2h1v ou 2h2v. Dans le premier cas (le plus utilisé), on a un sous-échantillonnage 2:1 horizontalement et 1:1 verticalement ; dans le deuxième cas, on a un sous-échantillonnage 2:1 horizontalement et verticalement. Ces sous-échantillonnages sont utilisés pour les chrominances seulement, la luminance on n'utilise jamais de sous-échantillonnage.

Les étapes qui suivent sont les mêmes que celles décrites précédemment, à savoir, application de la DCT, quantification et codage entropique.

1.4.3 Modes JPEG

Jusqu'à maintenant nous avons étudié les bases de la spécification JPEG, c'est-à-dire le mode séquentiel avec pertes, diverses extensions ont été rajoutées au standard pour améliorer soit la qualité, soit la compression. Nous citerons dans ce qui suit les trois autres modes JPEG [4].

1.4.3.1 Progressif_JPEG

Une image JPEG de base ne peut être affichée qu'après que toutes les données aient été reçues et décodées. Mais certaines applications qui reçoivent des données JPEG par flots comme les browsers Internet (navigateur internet) nécessitent, pour obtenir une impression d'attente moins longue, que l'image soit affichée après seulement qu'une partie des données soit arrivée ce qui défini le mode progressif.

Pour cela les étapes de DCT et de quantification sont les mêmes que pour le mode séquentiel (citées précédemment), la différence réside dans le codage, en effet l'image n'est pas codée d'un coup mais traitée par paquets de lignes. Ainsi dès qu'un paquet est codé, on peut l'envoyer, le décoder et l'afficher pendant que le reste de l'image est en train d'arriver. De la sorte, on verra l'image s'afficher par petits bouts à la fois.

L'idée est de construire une succession d'images approximatives à partir de l'original et les envoyer au fur et à mesure, pour cela il existe deux méthodes : soit la méthode de sélection spectrale, elle consiste à transmettre d'abord les coefficients DC et quelques coefficients AC, soit la méthode d'approximations successives, qui transmet d'abord des coefficients grossièrement quantifiés, puis les quantifie plus finement et transmet cette nouvelle information.

La première image envoyée sera une représentation vraiment grossière (basse qualité, grande compression) de l'original. Les images suivantes auront leur facteur de qualité amélioré. Ce qui visuellement va se traduire par en premier lieu une image grotesque mais reconnaissable, affichable très rapidement vu qu'elle ne prend pas beaucoup de place, puis au fur et à mesure que les images arriveront, la netteté de l'image affichée s'affinera petit à petit.

1.4.3.2 Compression JPEG sans perte. (P-JPEG)

Pour répondre aux exigences d'un mode sans perte, la communauté *JPEG* a choisi une méthode simple de prédiction qui est totalement indépendant de la transformation *DCT* décrite précédemment (vu que la DCT est par nature une approximation entachée de pertes). Elle exploite les redondances que présentent les images en adoptant un algorithme de prédiction de pertes utilisant un code de modulation d'impulsion différentielle bidimensionnelle (DPCM : Differential Pulse Code Modulation).

L'idée de base est que la valeur d'un pixel est combinée avec au moins trois des valeurs des pixels voisins (A, B, C) pour former une valeur de prédiction. Cette valeur est ensuite soustraite à la valeur du pixel original (x). Une fois que toute l'image ait subit ce codage, la différence entre la valeur du pixel(x) et sa prédiction (erreur de prédiction) va être codée en utilisant un codage entropique. Le codage d'Huffman est le plus utilisé.

Aujourd'hui, ce mode est remplacé par le JPEG-LS (lossless and near-lossless) basée sur l'algorithme LOCO-I (*LOw COmplexity LOssless COmpression for Images*), la compression est réalisée par la combinaison d'un codage adaptatif (extension des codes de Golomb) avec un codeur entropique proche du codeur de Huffman pour les zones à faible entropie.

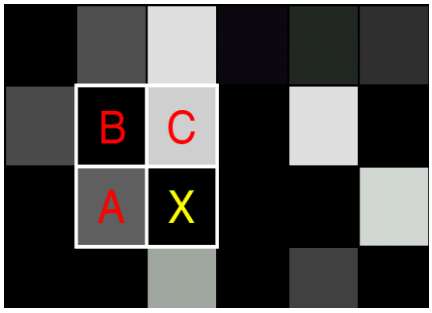


Figure 1.11 : principe du codage prédictif se basant sur les valeurs des pixels voisins

1.4.3.3 Mode hiérarchique

Le mode hiérarchique répond aux besoins de « scalabilité[5] » de certains décodeurs (dans un même flot binaire : plusieurs résolutions, plusieurs modes, …) par l'imbrication d'opérations d'échantillonnage, de codage, de décodage et d'interpolation.

[5] Pour autoriser un mode de codage compatible entre différents niveaux de qualité.

1.4.4 Les extensions de JPEG

- ✓ **Le standard JBIG**

Le standard nommé JBIG (*Joint Bi-level Image Experts Group*) a été développé pour la compression sans perte d'une image à deux niveaux. Il peut également être utilisé pour le codage des images en niveaux de gris ou de couleur n'excédent pas 6 bits par pixel. Il est destiné en particulier aux télécopieurs.

- ✓ **JPEG++**

Une extension appelée JPEG++ (Déposée par la société Storm Technology) s'occupe des éventuelles dégradations de textes présents sur une image : un opérateur offre la possibilité de sélectionner une région rectangulaire pour la compresser avec un algorithme ne supprimant aucune information.

- ✓ **JFIF**

Quand on parle de JPEG, on sous-entend un algorithme de compression ou une organisation de standardisation. Les fichiers communément appelé JPEG sont en réalité des JFIF (*JPEG File Interchange Format*) qui lui, est un véritable format de fichier développé par CCube Microsystems dans le but de stocker des images codées sous JPEG et de pouvoir les échanger entre différents systèmes.

- ✓ **MPEG**

MPEG l'acronyme de Motion Picture Expert Groups est défini pour compresser et synchroniser des signaux audio et vidéo avec un flux de données. Il est dérivé de JPEG car il utilise le même algorithme de compression spatiale. Il y a quatre types principaux : MPEG-1, MPEG-2 et MPEG-3 et MPEG-7.

L'application visée par la norme MPEG-1 est l'enregistrement. Elle a trouvé sa mise en œuvre dans plusieurs produits : le CDI, le VCD. La norme MPEG-2 est définie également pour les applications de stockage et de transmission vidéo. Pour le MPEG-4, il offre des fonctionnalités très diverses, tournant principalement autour de : la compression, l'interactivité, permettant de définir des scènes complexes objet par objet, et d'en manipuler la composition et les objets directement dans le flux (copier-coller…) sans avoir à les décoder ; la transmission, offrant des outils permettant d'adapter les flux à tous types de réseaux, dès le

codage (scalabilité, outils pour la robustesse aux erreurs…) ou au niveau de la couche systèmes.

On entend parler parfois de MJPEG qui est lui est destiné spécifiquement à stocker des films animés. Il va capturer chaque image séparément et la compresser en utilisant JPEG. Le temps de compression est amélioré, mais on perd en qualité.

- ✓ **JPEG 2000**

JPEG 2000 est donc un nouveau système de codage d'images qui utilise les connaissances actuelles dans le domaine de la technologie des ondelettes.
Précisons, au cœur de JPEG il y a la transformée de Fourrier discrète. Au cœur de JPEG 2000, il y a une décomposition en ondelettes. Le principe même du codage est différent. JPEG 2000 n'est pas une amélioration de JPEG, il constitue une autre manière d'analyser, de décomposer l'image pour la compresser avec ou sans pertes en apportant des fonctionnalités complètement nouvelles, en particulier pour les transmissions à faible bande passante.

La différence avec le JPEG est l'utilisation des ondelettes qui divise l'image d'abord en «tuiles » de taille fixe. Chaque tuile est rééchantillonnée de manière à ce que longueur et largeur soient divisées par 2 (voir figure1.12). Les informations perdues dans l'opération sont enregistrées sous forme de coefficients d'ondelettes. On recommence ensuite l'opération avec la nouvelle image et ainsi de suite tant qu'il reste des pixels.

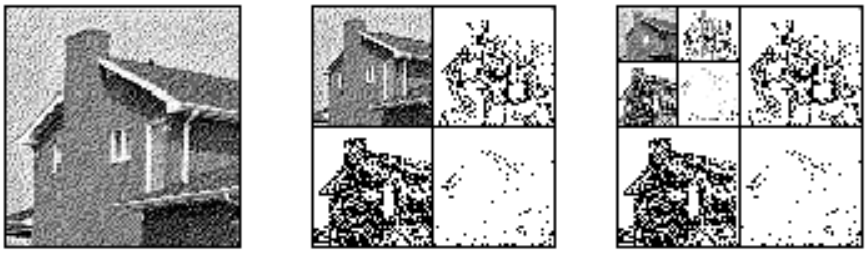


Figure 1.12 : illustration de la décomposition en ondelettes

Les principaux avantages que présente JPEG 2000 par rapport à JPEG c'est que la compression DCT du format JPEG analyse l'image par bloc de 8 * 8 pixels ce qui produit un effet de mosaïque (les limites des blocs sont visibles à fort taux de compression). La compression par ondelettes ne présente pas cet effet de mosaïque indésirable.

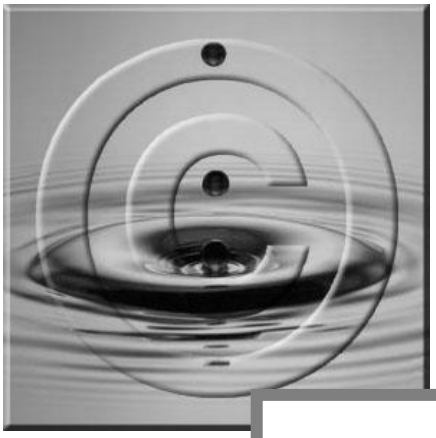
Il est donc possible de compresser des images par ondelettes avec un taux de compression élevé tout en conservant une bonne qualité picturale.
Les blocs JPEG 8 x 8 sont quantifiés indépendamment les uns des autres ce qui ne permet pas de réduire les redondances au delà d'un bloc. Au contraire, la compression par ondelettes est une méthode globale sur toute l'image.

1.4.5 Les limites du JPEG

Visuellement, la quantification utilisée dans l'algorithme JPEG tend à lisser l'image. Les changements graduels des nuances sont plus réguliers que dans l'image d'origine, sans que l'œil en soit pour autant choqué mais cet adoucissement de l'image fait perdre de la netteté aux contours et aux détails précis. Des anneaux apparaissent parfois près des contours restés nets, surtout lorsque le taux de compression est favorisé au détriment de la qualité d'image.
Lorsque le taux de compression est élevé, les blocs de 8*8 deviennent discernables à l'œil nu, nommé effet de bloc ou pixellisation de l'image.
En conséquence, pour des taux de compression plus élevés, on préférera éventuellement la compression par ondelettes ou fractale.

1.5 Conclusion

La compression des données est appelée à prendre un rôle encore plus important en raison du développement des réseaux et du multimédia. Son importance est surtout due au décalage qui existe entre les possibilités matérielles des dispositifs que nous utilisons (débits sur Internet, sur Numéris et sur les divers câbles, capacité des mémoires de masse,...) et les besoins qu'expriment les utilisateurs (visiophonie, vidéo plein écran, transfert de quantités d'informations toujours plus importantes dans des délais toujours plus brefs). Les méthodes déjà utilisées couramment sont efficaces et sophistiquées (Huffman, LZW, JPEG) et utilisent des théories assez complexes, les méthodes émergentes sont prometteuses (fractales, ondelettes) mais nous sommes loin d'avoir épuisé toutes les pistes de recherche. Les méthodes du futur sauront sans doute s'adapter à la nature des données à compresser et s'associeront à d'autres techniques telles que le tatouage et la cryptographie afin d'authentifier les données et de protéger les droits d'auteur. Dans le prochain chapitre les techniques de tatouage d'image sont introduites.



Chapitre 2

Les techniques de tatouage

2.1 Introduction

L'information étant synonyme de pouvoir, sa protection et sa dissimulation ont étés les préoccupations de l'homme depuis la nuit des temps, il a donc fait preuve d'imagination et de génie pour y parvenir, cryptographie et stéganographie en sont les preuves. Des mémoires d'Herodotus (486-425 av.JC) relatant le fait que Polybius rasa le crane de son messager et y tatoua un message (dans le but de soulever une révolte contre les Perse) et qui disparu à la repousse des cheveux, aux travaux de Shannon, en passant par les courriers codés que Richelieu adressait à sa police secrète [7], mais face à l'explosion des réseaux de communication (internet, réseaux sans fil…) et à l'engouement du grand publique pour les nouvelles technologies de l'information, la donnée a été prise comme cible par les pirates informatiques et les utilisations frauduleuses, par conséquent, de nouvelles craintes sont nées quant à la protection des droits d'auteurs et de l'authenticité des documents.

En effet, de par la nature volatile des documents numériques qui peuvent être dupliqués, modifiés, transformés et diffusés très facilement et par le développement des bases de données multimédias, transactions bancaires par internet, documents confidentiels (tel que le document médical), un besoin de sécurité se fut ressentir. Le tatouage numérique est l'une des solutions répondant à ce besoin en renforçant les systèmes déjà existants, en introduisant d'une manière invisible et indélébile une information dans le document à protéger.
Ce chapitre présente les origines du tatouage, les différentes méthodes utilisées ainsi que ses principales applications.

2.3 La triade du secret

Il y a une variété importante de domaines d'applications des méthodes de dissimulation d'information. Ces méthodes disposent de différentes caractéristiques et peuvent être classifiées selon leurs objectifs et leurs contraintes. D'une façon générale, les méthodes de dissimulation d'information peuvent être groupées en deux grandes familles, la première, utilise des techniques pour rendre incompréhensible le message : la cryptographie. La deuxième famille utilise une porteuse comme enveloppe pour cacher le message, nous distinguons la stéganographie qui cherche une communication invisible et qui a donné naissance au tatouage (watermarking) qui concerne l'insertion d'une marque.

De nos jours, cryptographie, stéganographie et tatouage sont des sciences à part entière qui étudient les techniques de la transmission d'information à caractère confidentiel. Ces trois disciplines sont très proches l'une de l'autre, cette partie dresse les différences et similitudes entre elles.

2.2.1 La cryptographie

La cryptographie, ou l'art de chiffrer consiste à transformer un message pour qu'il devienne illisible. On a recours à une opération mathématique, un algorithme de chiffrement, contrôlé par un code ou une clé. Seuls, la connaissance de la clé et du moyen de cryptage permettent de décoder le message afin de le rendre lisible [8]. Plus le code (la clé de chiffrement) est long, plus le système est sûr. Cette technique a pour but de protéger le document pendant sa transmission, autrement dit une fois que le document est en clair, il n'est plus protégé. La figure 2.1 nous illustre le principe de cryptologie.

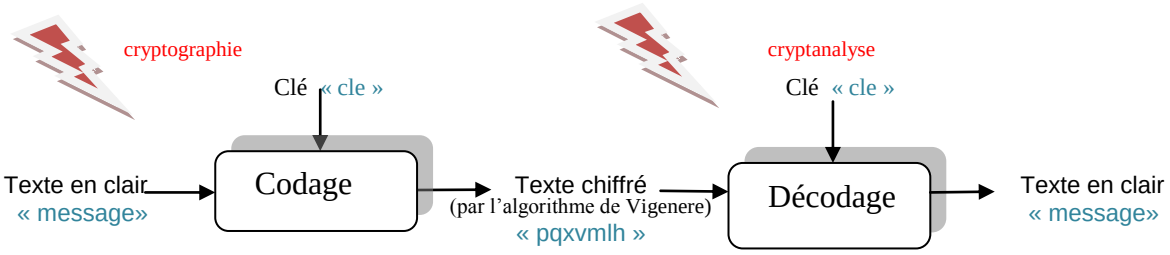


Figure 3.1: Illustration du principe de cryptologie

Utilisée depuis l'antiquité, l'une des utilisations les plus célèbres pour cette époque est le chiffre de César, nommé en référence à Jules César qui l'utilisait pour ses communications secrètes. Mais la cryptographie est bien antérieure à cela : le plus ancien document chiffré est une recette secrète de poterie qui date du XVI^{e} siècle av. J.-C., qui a été découverte dans l'actuelle Irak. Bien qu'éminemment stratégique (à usage militaire et diplomatique) la cryptographie est restée pendant très longtemps un art, pour ne devenir une science qu'au XXI^{e} siècle, avec l'apparition de l'ordinateur, et s'étend aujourd'hui au domaine civil pour la protection des données circulants sur les réseaux informatiques. Ainsi, la cryptographie moderne est maintenant une discipline de recherche utilisant des outils mathématiques sophistiqués.

On distingue traditionnellement les systèmes symétriques et asymétriques. En cryptographie symétrique (ou à clé secrète), les correspondants partagent la même clé pour chiffrer et déchiffrer. Les connaissances académiques dans ce domaine sont assez récentes et remontent à l'invention du système de chiffrement par bloc appelé Data Encryption Standard (DES) au début des années 1970. En 1976, Diffie et Hellman ont révolutionné la cryptographie en inventant des systèmes asymétriques dans lesquels émetteur et récepteur ne partagent plus une clé commune mais une clé, rendue publique, permet de chiffrer un message, la seconde est gardée secrète et permet au destinataire de déchiffrer [9], c'est ce qui est utilisé actuellement lors d'échange d'un code de carte bleue avec un site marchand, sans avoir besoin de rencontrer auparavant le responsable du site.

2.2 La stéganographie

La stéganographie du grec *Stéganô*, signifiant *Je couvre* et *Graphô*, signifiant *J'écris*. Elle consiste à cacher, de manière subliminale (invisible), un message secondaire dans un message primaire. Le message primaire reste lisible de tous, tandis que le message secondaire n'est lisible que par une ou plusieurs personnes propriétaires d'une information secrète (la clé) [10]. Contrairement à la cryptographie qui est immédiatement perçue comme incompréhensible, le message stéganographié n'est pas immédiatement perçu comme existant, leur différence essentielle réside dans le fait que, pour la cryptographie, la clef empêchera celui qui n'en a pas la connaissance de déchiffrer le message, alors que la stéganographie empêchera de suspecter son existence même.

Pour la petite histoire, une forme de stéganographie très connue est le principe de l'encre invisible. Cette technique était très utilisée au moyen âge pour envoyer des messages secrets. A l'époque, l'encre était fabriquée simplement à base de jus d'oignons et de chlorure d'ammoniac. L'écriture était alors rendue visible en approchant le papier d'une flamme de bougie.

Elle est également d'un usage stratégique, en effet, il conviendra aisément que l'important pour un assiégé est bien qu'on ne puisse pas *soupçonner* ses communications plutôt qu'on ne puisse les déchiffrer, c'est précisément à ce problème que les États-Unis et l'Union soviétique ont été confrontés lors d'un traité sur la prolifération des armes nucléaires (SALT 2) [11]. Les protagonistes étudiaient un dispositif devant permettre de détecter la présence de missiles

dans les silos, sans révéler les emplacements des silos. Parmi les contraintes imposées au système, il devait empêcher une manipulation de l'information à transmettre , et également ne pas pouvoir transmettre plus d'information que nécessaire, en utilisant une faille du système pour transmettre une dizaine de bits de façon indétectable. Mais la voie la plus intéressante pour la stéganographie moderne est la dissimulation d'information dans les fichiers multimédias, particulièrement les images. Si l'on introduit une modification dans les deux bits les moins significatifs (LSB) de la composante chrominance, cela est imperceptible à l'œil humain. La figure 2.2 nous illustre ce principe.

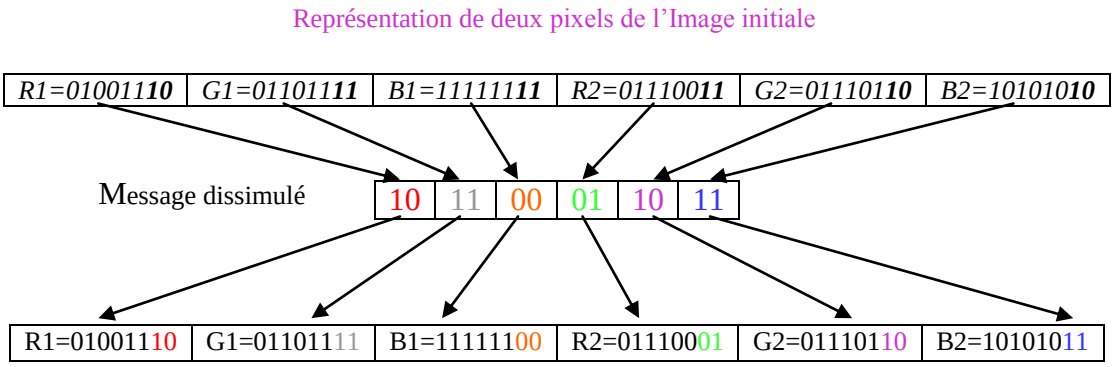


Figure 2.2 : Exemple de la stéganographie

Si la stéganographie offre de nombreux avantages, tels une grande capacité d'insertion, elle offre également une grande discrétion, par contre la robustesse et la sécurité sont ses points faibles, un changement de format du document ou une compression JPEG font perdre systématiquement le message caché.

2.2.3 Le tatouage numérique

Le tatouage numérique (*digital watermarking)* est une technique qui consiste à dissimuler une information (une marque) dans un signal hôte (image), permettant de répondre aux différents problèmes que rencontres un document numérique. La marque doit être suffisamment imperceptible pour ne pas surcharger l'image, c'est-à-dire que la déformation doit être faible pour que l'utilisateur ne puisse pas différencier le document tatoué de

l'original. Elle doit être également indélébile, une fois la marque insérée elle doit être impossible à enlever par des personnes non autorisées.
Les premiers exemples rapportés datent du treizième siècle [12], à la grande époque de l'imprimerie en Italie, les fabriquants de papiers en produisaient diverses sortes de plus ou moins bonnes qualités à des prix plus ou moins élevés. Pour contrer la fraude et les escroqueries, ils apposèrent un tatouage visible dans le papier qui permettait de connaître le fabriquant. Le tatouage est utilisé également sur les billets de banque, en effet, le filigrane électronique (*digital watermark*[6]) est d'abord invisible et n'est révélé que par une transformation spécifique. L'intérêt d'une telle opération est que le tatouage est indépendant du format de stockage des données, puisqu'il est intrinsèque au document.

Le tatouage de donnée numérique quant à lui, est considéré comme une science nouvelle, qui a été essentiellement motivée par la protection des droits d'auteur. Il débuta en 1988, par un groupe de chercheur qui a proposé une méthode pour insérer un code d'identification dans un signal vidéo. En 1990, le terme tatouage ou digital watermarking a été utilisé pour la première fois et ce n'est quand 1995 que la discipline pris de l'ampleur, ce qui s'est concrétisé par la création de l'atelier IHW (*Information Hiding Workshop*) en 1996, d'une conférence spécifique au sein de SPIE en 1999 et de l'atelier IWDW (*InternationalWorkshop on Digital Watermarking*) en 2002.

Quatre journaux dédiés aux problématiques de sécurité de l'information ont été crées : *IEEE Trans « On Information Forensics and Security »* et *IEE Proc « Information Security »* en 2005, *LNCS « Transactions on Data Hiding and Multimedia Security »* et *EURASIP « Journal on Information Security »* en 2006, ce qui souligne le dynamisme du domaine [13].

Bon nombre de grandes compagnies du numérique ont ouvert grande leur porte à cette nouvelle technologie qui s'offrit à eux ; citons comme exemples : Digimarc, firme pionnière, qui rassemble des brevets de base sur le tatouage notamment celui de l'estampillage[7] dont elle vend la licence. Elle est également auteur du module de tatouage du logiciel de traitement d'image Photoshop de la compagnie Adobe, et la création du concept smart image (voir 2.6.7). Son concurrent Verance fournit les outils de contrôle de flux audiovisuel Broadcast

[6] Sur un billet de banque, les fibres sont marquées au moment de la sortie du bain d'eau, ce qui est à l'origine du terme anglais *water mark.*

[7] Opération qui consiste à apposer le cachet du service de documentation sur le document (Larousse).

Verification et ConfirmMedia. Le « Copy Protection Technical Working Group » a testé les techniques de tatouage pour protéger le format DVD.

Plusieurs associations sont également actives dans ce domaine, notamment, les associations japonaises, JASRAC et RIAS. Nextamp et MediaSec, filiales de Thomson, s'intéressent au suivi et à la sécurité vidéo, et ont proposé un système de tatouage vidéo pour une application de suivi des transactions, où le document téléchargé contient le nom de l'acheteur.

Egalement, une production scientifique particulièrement abondante est constatée comme en témoigne la figure 2.3.

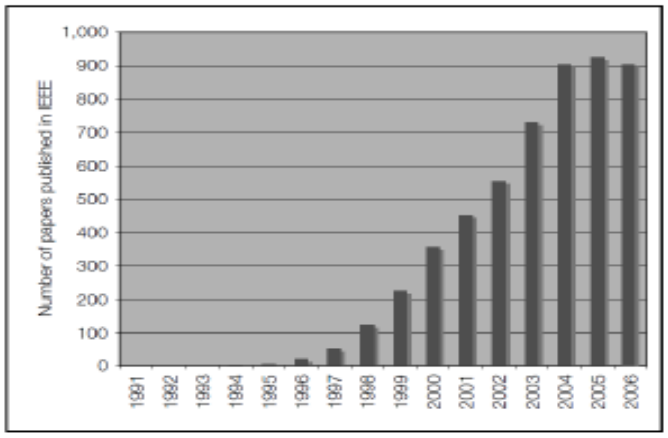


Figure 2.3 : nombres de publications sur le watermarking par IEEE [9]

2.4 Processus de tatouage numérique d'image

Le schéma classique de tatouage numérique d'image peut se décomposer en deux opérations distinctes. Une opération d'insertion et une opération de détection/extraction, tel qu'illustré sur la figure 2.4. Ce paragraphe résumera ces opérations ainsi que les contraintes liées au tatouage d'image [14].

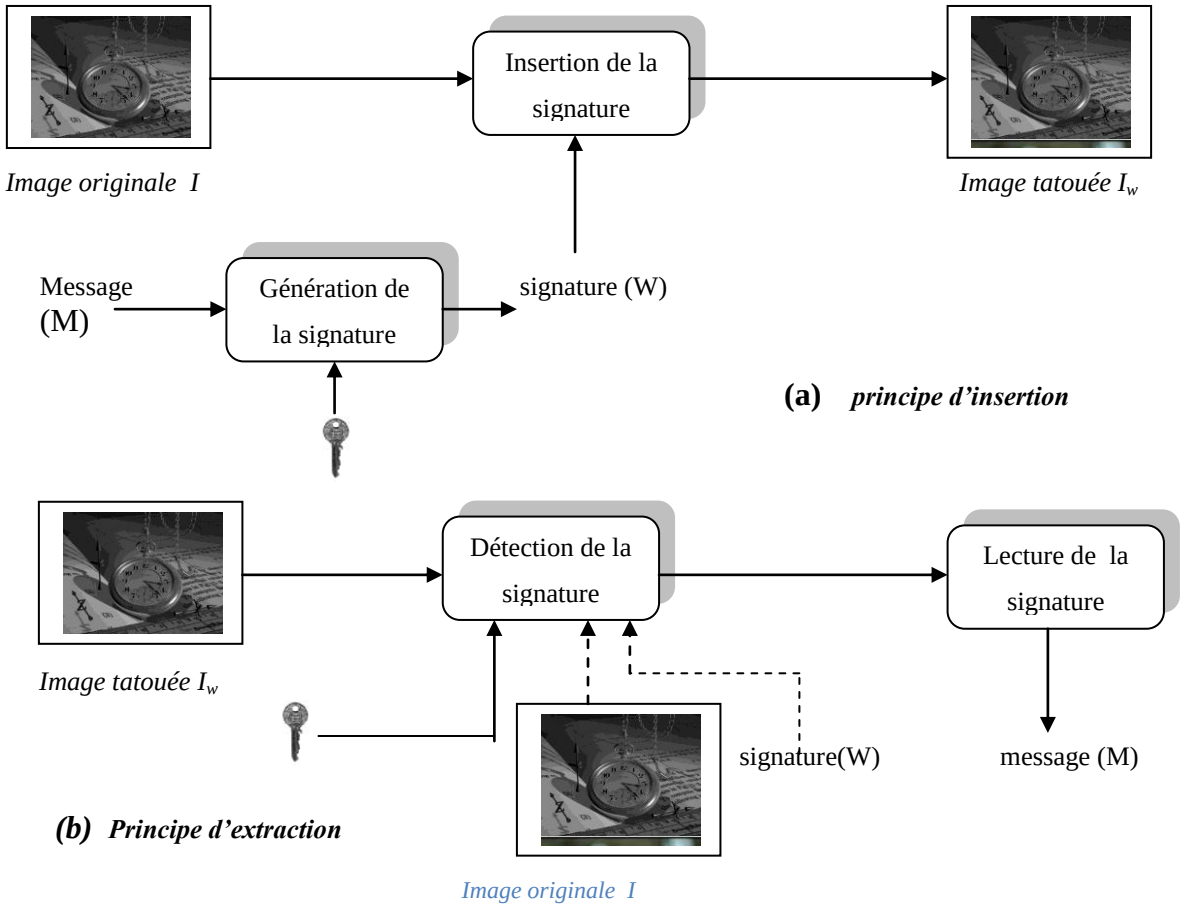


Figure 2.4 : Schéma général de tatouage d'image : (a)principe d'insertion, (b) principe d'extraction

2.3.1 Processus d'insertion

Le processus d'insertion consiste à introduire la marque dans le document. Pour une image numérique, il est possible d'insérer la signature dans le domaine spatial que dans le domaine des transformées (DCT, ondelette, etc).

2.3.1.1 Schéma général

L'image tatouée I^*, est issue du processus ε qui insère la marque *W* dans l'image hôte *I*, en s'aidant de la clé K que possède le propriétaire seulement. L'image I^* obtenue est perceptuellement similaire à *I* et contient la signature. La figure 2.5.illustre ce processus.

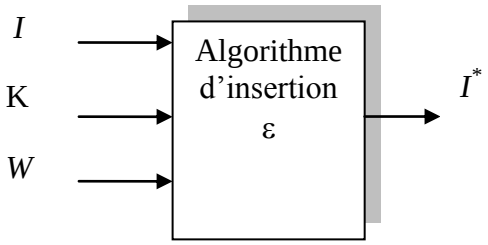


Figure 2.5 : Schéma général du processus d'insertion d'une marque

Nous pouvons modéliser ce processus par un formalisme mathématique tel que : ε est l'application des espaces des marques, des images et des clés (*I, W, K*), dans l'espace des images *I*. Elle fait correspondre à : une clé K, une marque *W* et une image hôte *I*, une image tatouée I^*.

$$\varepsilon : \begin{array}{l} (I, W, k) \longrightarrow I \\ (I, W, k) \longrightarrow I^* \end{array}$$

Ce formalisme, très général, représente le processus d'implémentation de la marque pour tous les processus de tatouage. Nous allons maintenant préciser les propriétés des espaces de départ et d'arrivée W, K et I.

2.3.1.2. Propriétés de la marque

L'ensemble W est l'ensemble de toutes les marques possibles. Bien qu'il faut qu'elle soit indélébile, les principaux défis sont posés en termes de capacité d'insertion, d'imperceptibilité mais également de robustesse face à des traitements, qu'ils soient bienveillants ou malveillants (attaques), au sein desquels la compression figure en bonne place. Les performances d'un système de tatouage diffèrent d'une application à l'autre, selon les contraintes de celle-ci. La figure 2.6 résume ces propriétés [14]

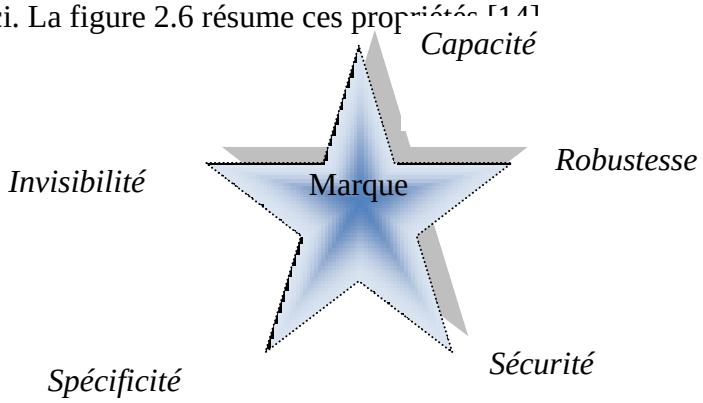


Figure 2.6: Spécificité de la marque

- ***L'invisibilité***

La notion d'imperceptibilité, consiste à cacher le message dans des régions aptes à le couvrir, sans gêner le confort visuel ni l'interprétation du contenu sémantique. Le but de cette propriété est de garder la valeur artistique et commerciale du document marqué en le rendant en même temps plus résistant aux attaques.

Elle pose ainsi la question de la représentation la plus efficace de l'information, en d'autres termes, vaut-il mieux tatouer dans le domaine initial ou dans un domaine transformé.

- ***La capacité***

Elle représente la quantité d'informations que l'on peut insérer à l'aide de ce schéma. Elle dépend de l'application ciblée ainsi que des contraintes pratiques imposées, comme la taille de l'image hôte, en effet, on ne peut inscrire trop d'informations dans un petit support.

De plus, la contrainte d'invisibilité impose une marque de petite taille. Il est évident que plus la marque est petite, plus il est facile de la cacher. Dans toutes premières approches, seul un bit d'information était inséré, le message correspondait donc à un message binaire signifiant, données marquées ou pas, mais aujourd'hui elle varie de quelques dizaines de bits dans le cadre d'une protection de la propriété intellectuelle à plusieurs kilobits lorsqu'il s'agit d'enrichir des documents.

- ***La robustesse***

Une procédure de tatouage est dite robuste, si l'information cachée est retrouvée avec succès dans toutes données marquées après avoir subit une attaque, voir section (2.5.1).

Dans certains cas, il est préférable de favoriser la fragilité de la marque plutôt que sa robustesse, comme dans le contrôle d'intégrité afin de s'assurer que le document n'a pas été manipulé, par contre le tatouage devra être robuste lorsqu'il s'agit d'application de type copyright.

Ces trois objectifs étant antagonistes, nous devons donc trouver le meilleur compromis possible selon l'application visée. Deux autres propriétés sont liées à la marque :

- ***La sécurité***

La marque doit être indétectable sans la connaissance de la clé K, autrement elle peut être retirée.

- ***La spécificité***

La marque doit constituer une preuve irréfutable. Pour cela il convient d'assurer l'unicité (éviter les problèmes de collision) et de l'authenticité de l'identifiant.

La clé et l'image hôte possèdent également des propriétés, dont la taille. En effet, pour la clé on doit choisir une combinaison assez longue (excédent 20bits) pour que le pirate n'utilise toutes les clefs possibles. Pour l'image hôte, quelques pixels sont insuffisants pour contenir la marque. Il est clair aussi que le support doit respecter d'autres contraintes, si par exemple l'image est trop monotone le tatouage sera trop visible, c'est pour cela que le tatouage s'intéressent essentiellement à des images de type photographie.

2.3.2 Processus de détection / extraction de la marque

Ce processus permet de retrouver la signature ou juste de détecter son existence. Dans le premier cas il sera possible d'extraire la marque « processus d'extraction ». Dans le second un booléen retournera 1 pour l'existence de la marque et 0 dans le cas contraire. Les processus de détection et d'extraction seront classés suivant l'utilisation ou non de l'image original, en trois catégories : schémas aveugle, semi privé et privé.

2.3.2.1. Schéma général

Le processus de détection doit avoir comme entrée une image I' (image test) sur laquelle est recherchée l'existence de la marque, et obligatoirement avoir la clé K (voir figure2.7). Dans certains schémas de détection on aura besoin de l'image originale, ce processus sera qualifié de privée. Dans le cas contraire, le schéma sera qualifié d'aveugle.

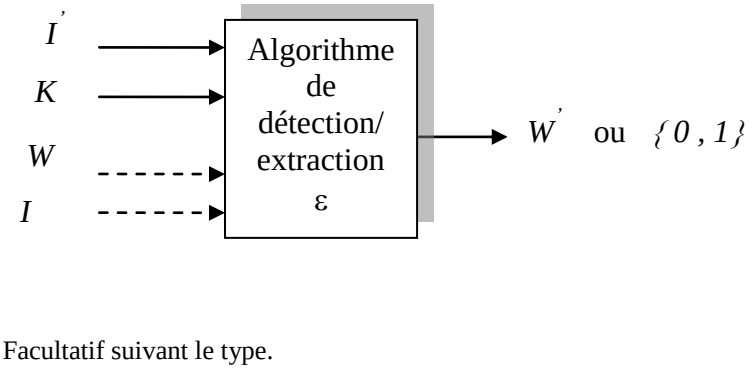


Figure 2.7 : Schéma général du processus de détection/extraction d'une marque

2.3.2.2. Processus de détection privé

Le caractère privé constitue un enjeu majeur dans les applications réelles, puisque cela permet de ne pas diffuser les données originales non marquées, y compris à une autorité de confiance. On distingue deux types :

- Type I : le processus est en mesure d'extraire la marque ;
- Type II : la marque ne sera pas extraite mais juste son existence sera révélée par un booléen (1 : marque présente et 0 : marque absente) ;

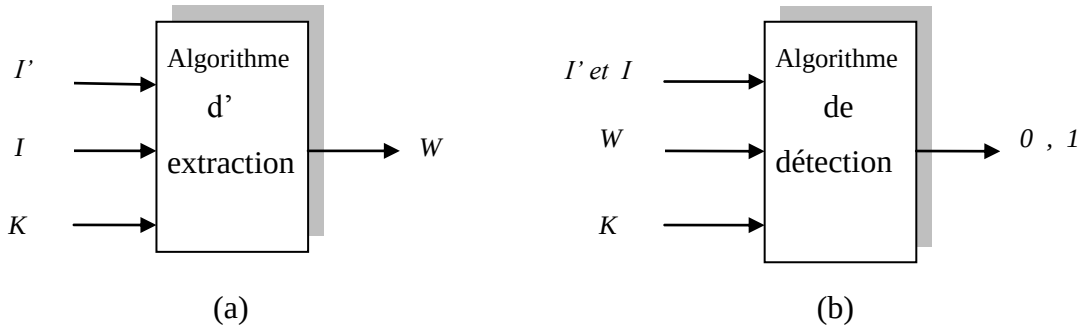


Figure 2.8: schémas privés : (a) schéma privé de type I ; (b) schéma privé de type II

2.3.2.3 Processus de détection aveugle

Si le paramètre « marque » est obligatoire le schéma est dit: semi -privé dans le cas contraire le schéma de détection est publique.

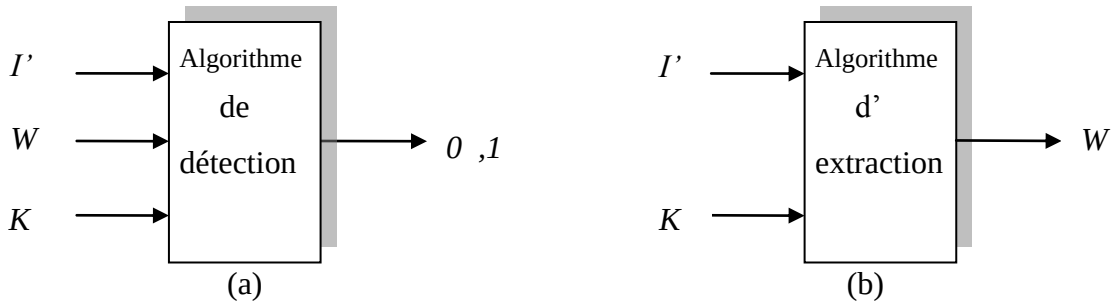


Figure 2.9 : Schémas aveugles : (a) schéma aveugle semi-privé (b) schéma aveugle publique

2.3.3. Propriétés du processus de détection

Le processus de détection, doit être : robuste, c'est-à-dire capable de détecter la marque malgré l'altération subie par l'image et sûre, répondant au principe de Kerckhoffs[8] [8].

Il existe une probabilité dite de fausse alarme, elle correspond à la probabilité de détecter la marque dans des données non marquées. Les études théoriques publiées recommandent que cette probabilité soit inférieure à 10^{-10} .Pour chaque application réelle, elle doit être estimée [1].

2.3.4 Les types de tatouage existants

Il est possible de regrouper les techniques de marquage selon différentes classifications : conformément au type de clef appliquée (asymétrique et symétrique) ; selon l'information nécessaire à l'extraction (aveugle, semi-aveugle et non-aveugle) ; conformément à la robustesse (fragile, semi-fragile et robuste) ; quant à la perception du SVH (visible et invisible) ; selon la préservation de l'image originale (inversible et non-inversible) et conformément à la technique d'insertion (additive et substitutive).

- ✓ Schémas symétriques et asymétriques

Le marquage asymétrique est une technique qui utilise des paramètres différents pour l'insertion et l'extraction de la marque, et qui permet donc de la relire à l'aide d'une seule clef publique [15]. Dans le marquage symétrique les paramètres utilisés pour insérer la marque sont les mêmes que pour l'extraire. Le rôle de clef-privée et clef-publique n'existe pas, l'insertion et l'extraction sont faites à l'aide de la même clé et la même procédure.

- ➢ Aveugle, Semi-privé et privé

Comme il a été présenté précédemment dans la section (2.3.2), les processus de détection et d'extraction seront classés suivant l'utilisation ou non de l'image original, en trois catégories : schémas aveugle, semi privé et privé.

- ➢ Fragile, Semi-fragile et Robuste

Les tatouages robustes doivent résister au maximum d'attaques et permettre la compression des images tout en préservant la signature. Les tatouages fragiles quant à eux sont conçus pour détecter les changements survenus sur une image. Ils ne doivent pas résister à une

[8] Il stipule que l'inventeur d'une technique de chiffrement doit supposer que l'attaquant connaît tout de l'algorithme excepté la clé. Ainsi, la sécurité du crypto-système doit reposer uniquement sur la mise au secret de cette clé, l'algorithme étant public.

modification du contenu de l'image. Les tatouages semi-fragiles combinent entre les deux propriétés précédentes, ils doivent résister à une compression *JPEG* avec un haut niveau de qualité et à quelques attaques.

- Visible et Invisible [14]

Pour certaines applications, l'implémentation d'un watermark visible (un logo par exemple) peut être envisagée. Cette marque sert d'information aux consommateurs mais aussi d'argument dissuasif. Craver et al. [16] ont utilisé cette méthode pour la protection d'images digitales en introduisant un logo translucide qui recouvre toute l'image, sans pour autant gêner sa compréhension. Les avantages de cette méthode sont, la facilité d'implémentation et de détection de la marque, les inconvénients sont évidemment une plus grande fragilité du marquage aux attaques. Il est en effet très facile de couper la partie marquée de l'image où de supprimer la marque en reconstruisant l'image par interpolation. De plus, cette solution ne convient pas par exemple pour la vente d'images haute qualité.

Image originale (a) (b)

Figure 2.10 : Illustration d'un tatouage : (a) Visible, (b) Invisible

Le tatouage invisible quant à lui préserve la qualité commerciale et visuelle de l'image, il est destiné à des algorithmes robustes.

- Réversible et Non-réversible

L'image originale peut être parfaitement restaurée ou non, selon la technique utilisée par l'algorithme de tatouage. On perçoit donc les techniques réversibles et non-réversibles, comme le montre la figure 2.11. Une application est proposée dans le quatrième chapitre.

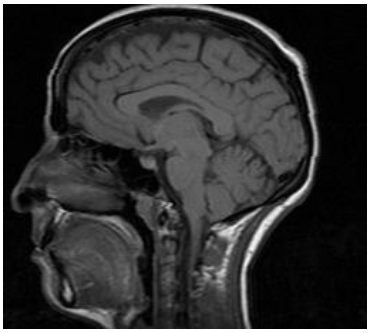
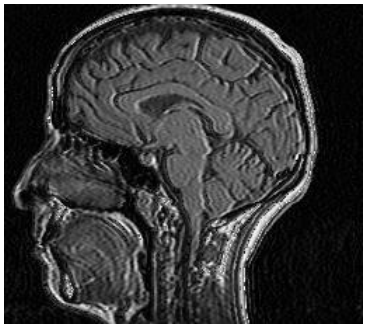


Image initiale



tatouée de manière réversible
(la dégradation est visible)

Figure 2.11: tatouage réversible

- Domaine d'insertion

On distingue trois domaines d'insertion, chaque domaine apporte diverses possibilités en termes de performance et de robustesse [17].

- ***Domaine spatial***

Le tatouage dans le domaine spatial modifie la luminance des pixels, il présente l'avantage de l'utilisation en temps réel mais également il supporte très bien les transformations géométriques puisque la marque ne disparait pas mais subit un décalage, dans ce cas il faut la synchroniser.

- ***Domaine fréquentiel***

Les schémas qui utilisent le domaine fréquentiel (DCT, TFD,…) comme domaine d'insertion, seront robustes aux opérations de compression. Par contre ils seront vulnérables aux transformations géométriques. La propriété d'invariance de la transformée TFD sera exploitée dans le cas des transformations géométriques.

- ***Domaine multirésolution***

Cela consiste à décomposer l'image en sous bandes, permettant d'isoler les composantes basses fréquences, celles-ci constituent un espace d'insertion moins sensible que l'image elle même.

- Schémas Additifs et Substitutifs

La différence entre les deux schémas (additifs et substitutifs) réside dans la façon dont la marque est inscrite dans l'image.

2.5 Etat de l'art sur les techniques de tatouage :

La classification en schémas additifs et substitutifs est la plus courante dans la littérature [14], [17], nous opterons pour cette classification, afin de dresser un état de l'art.

2.4.1 Tatouage additif

Les méthodes additives sont les plus nombreuses, elles consistent en l'ajout de la signature (équivalent à un ajout de bruit) à des composantes de l'image. Dans la majorité des cas les composantes sont choisies grâce à la clé. Nous citerons dans ce qui suit quelques méthodes additives.

- ***L'algorithme patchwork***

Cette méthode est introduite par Bender et al [18]. Elle est classée dans les méthodes à schéma semi-privé, avec insertion dans le domaine spatial, dont le principe est le suivant :
Deux ensembles de pixels *A* et *B* de même taille *N* (suffisamment grand), sont choisis pseudo aléatoirement à l'aide de la clé K. On pose a_i et b_i les valeurs de luminance d'une paire de pixels des deux ensembles A et B respectivement, et on leur fait subir les transformations suivantes :

$$\begin{cases} a_i^{'} = a_i + 1 \\ b_i^{'} = b_i - 1 \end{cases} \quad \text{..... (2.1)}$$

Avec : $S = \sum_{i=0}^{N-1} (a_i - b_i)$ .La somme S doit être nulle.

A la détection la somme s'exprime suivant la formule (2.2) :

$$S^{'} = \sum_{i=0}^{N-1} (a_i^{'} - b_i^{'}) = \sum_{i=0}^{N-1} (a_i - b_i) + 2N = S + 2N \text{.....(2.2)}$$

Si à la détection, on est en possession de la clé K, la somme $S^{'}$ devrait être égale à 2N. Si on n'est pas en possession de la clé K, les ensembles A et B seront générés par une autre clé K', si S est proche de 2*N*, on peut affirmer que la marque est détectée et que la clé $K^{'}$ est juste, sinon l'image est marquée par une autre clé.

On peut remarquer que l'implantation de la marque peut se résumer à l'addition de l'image avec une matrice W, de même taille que l'image et contenant la valeur 1 pour les pixels de l'ensemble A, -1 pour les pixels de l'ensemble B, 0 sinon. Si *I* est l'image originale, I^{*} l'image tatouée, on obtient [14] : $I^{*} = I + W$

L'avantage de cette technique est qu'elle est robuste aux changements d'intensité, les inconvénients sont : un très mauvais ratio, une vulnérabilité aux transformations géométriques, en plus elle ne résiste pas à la compression *JPEG*.

- ***Méthode d'étalement du spectre***

Cette technique qui date des années 40 a d'abord été utilisée pour des applications militaires et est très utilisée aujourd'hui en télécommunication. Elle peut s'utiliser sur notre système, on le modélisant comme un système de communication de telle sorte que l'image hôte soit le canal de transmission, la marque est le message à transmettre et les attaques comme du bruit. Son principe est d'étaler le spectre du message afin de se servir de toute la bande passante du canal. Le message ainsi étalé sera donc présent sur toutes les fréquences et sera plus résistant aux altérations de cette bande et c'est là où réside toute la difficulté pour un utilisateur non-autorisé à détecter la signature.

Cette méthode a été développée par Hartung et Girot [19], elle consiste à découper l'image en blocs de taille égale, le nombre de blocs correspondant au nombre de bits que l'on veut insérer dans l'image. Ensuite une Séquence Binaire Pseudo Aléatoire de la taille des blocs est générée à l'aide d'une clé secrète seulement connue du propriétaire. Cette séquence (S), est composée de (+1) et de (–1) et a une moyenne nulle. La marque à insérer est alors constituée par une succession de blocs égaux à +S ou – S suivant les bits du message. La marque ainsi formée est ajoutée à l'image. Un exemple d'insertion du message 11010010 est illustré par le schéma de la figure 2. 12.

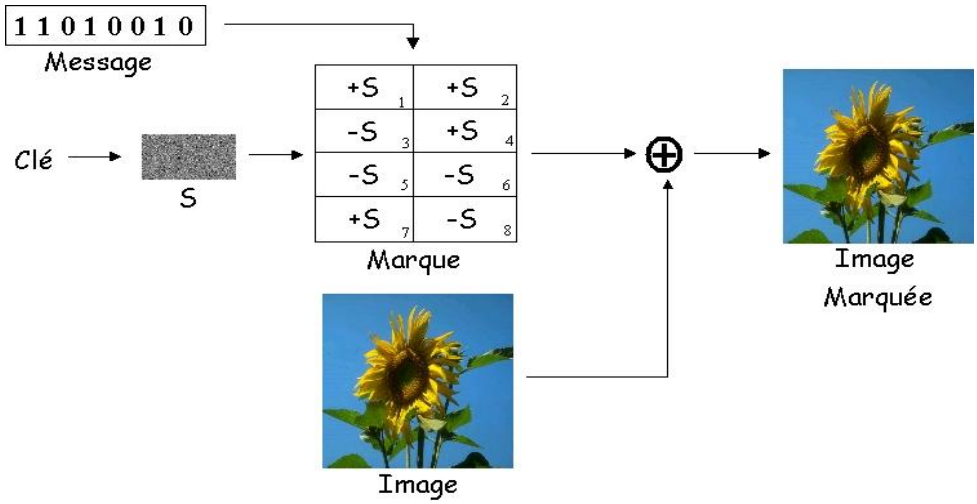


Figure 2.12: Schéma de tatouage par blocs

Pour détecter le message sur l'image marquée, on effectue la corrélation de S avec chaque bloc de l'image marquée. Si le résultat est positif on considérera que le bit associé à ce bloc est 1, dans le cas contraire on choisira 0.

Cette méthode peut être également utilisée dans le domaine fréquentiel, en effet, Cox et al. [20] présentent une méthode de tatouage à étalement de spectre dans les coefficients DCT de l'image. Leur principale motivation est de tatouer les composantes perceptuellement significatives de l'image c'est-à-dire les basses fréquences. Ils modifient les N coefficients de plus grandes amplitudes de la transformée mis à part la composante continue (DC).

- ***Méthodes basées sur la transformée de Fourier-Mellin***

Pour répondre aux problèmes qu'engendrent les transformations géométriques sur l'image tatouée, à savoir l'impossibilité d'extraire le tatouage, une solution a été envisagée et qui conduit à l'implantation du tatouage dans un espace transformé présentant une invariance aux transformations géométrique. En effet, la transformée de Fourier assure l'invariance par translation. Une autre version, qui est Fourier-Mellin, est invariante par translation, rotation et changement d'échelle. Une combinaison de ces deux transformées a été proposée dans l'algorithme de Ruanaidh *et al.* [21]. Cette technique a le grand inconvénient d'être très coûteuse en temps de calcul [12].

2.4.2 Tatouage substitutif

Le marquage substitutif modifie les bits de la couverture, afin de les faire correspondre à la marque. Ce type de marquage est connu comme marquage par contrainte, parce qu'il force l'image couverture à respecter certaines propriétés qui déterminent la marque, la figure 2.13 résume ce principe. [2] Nous citerons dans ce qui suit quelques méthodes substitutives.

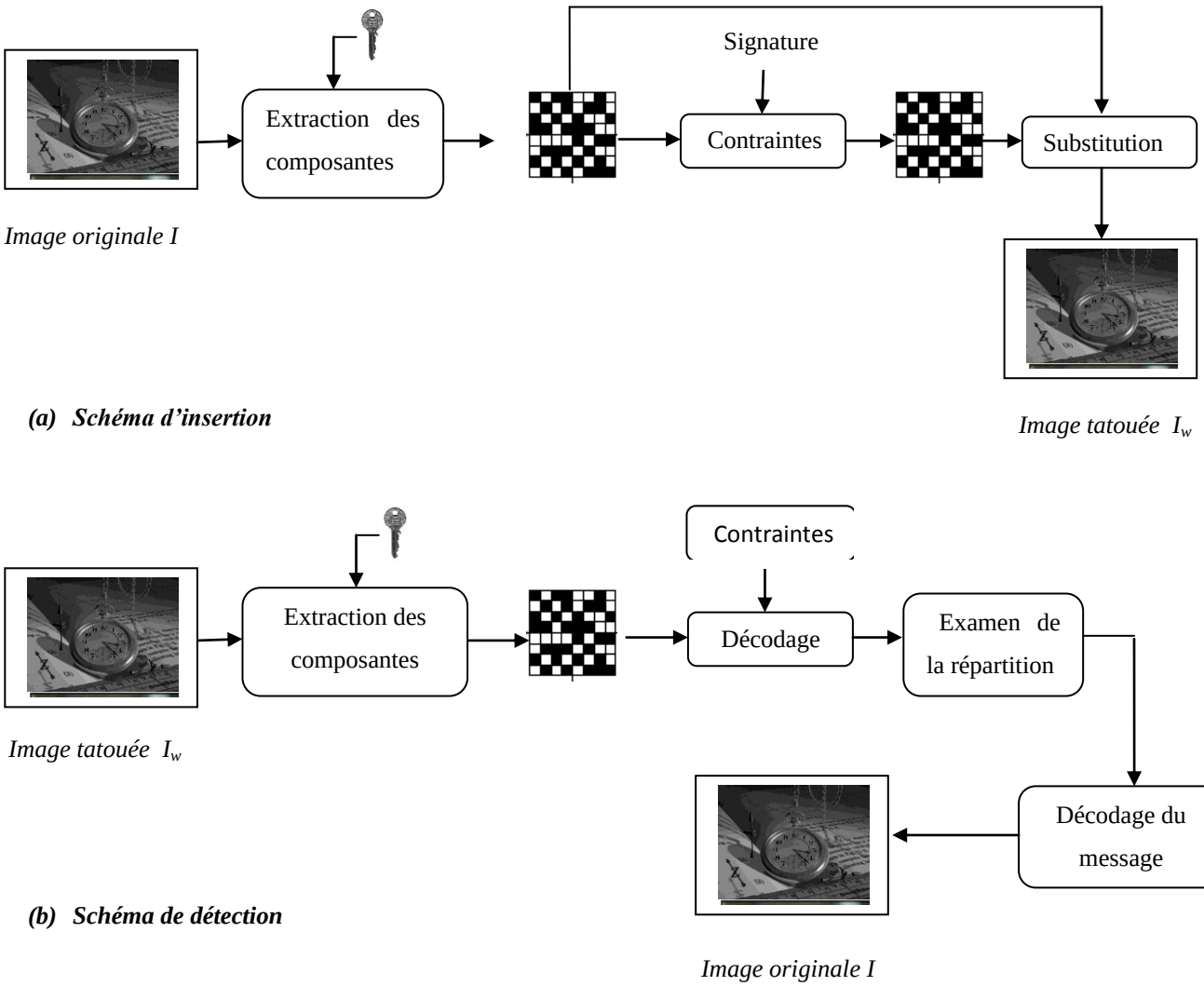


Figure 2.13: Schéma général d'un algorithme de tatouage substitutif

- ***Modification des bits de poids faibles***

Pour s'assurer de l'invisibilité de la marque, on se base sur le fait que l'œil humain ne fait pas la différence entre deux niveaux de gris consécutifs. Les premiers algorithmes de tatouage

insèrent la marque dans les bits de poids faible du niveau de gris (pour les images à niveau de gris), et les bits de poids faible de la luminance pour les images couleur.

Les algorithmes basés sur ce principe ont l'avantage d'insérer une quantité énorme d'information, sans dégrader l'image; le nombre de bits à insérer peut atteindre la taille de l'image mais la marque insérée est très facile à modifier ou à enlever; il suffit, par exemple, de mettre tous les bits de poids faible à '0', de plus, elle est sensible aux différentes modifications comme l'ajout de bruit, la rotation ou la compression avec perte telle *JPEG*.

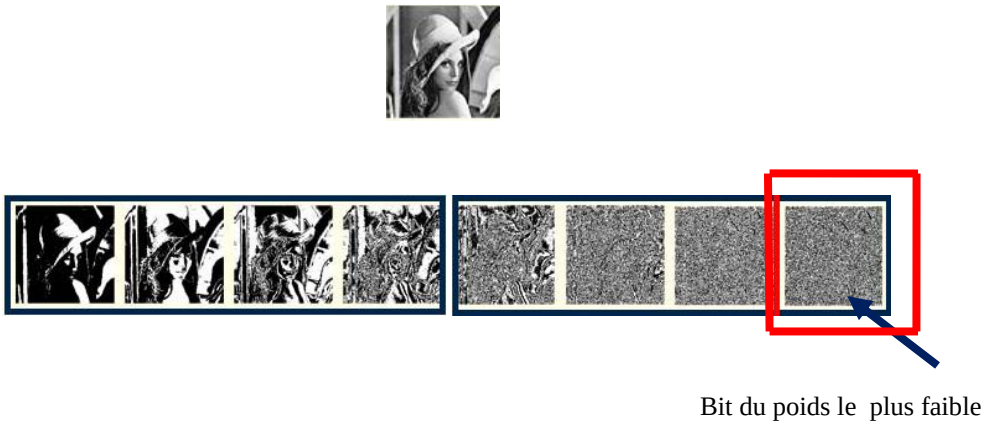


Figure 2.14 : modification du bit de poids faible d'un pixel.

- ***Méthode utilisant la DCT***

Le premier processus de tatouage par modification des coefficients DCT d'une image est présenté par Zhao and Koch. L'idée de base est de décomposer l'image en blocs de 8*8 pixels, dont certains sont choisis par une clé K pour porter le message. Les blocs sont ensuite transformés par DCT (voir section 1.4.2.2), puis les modifications se font sur un triplé (déterminé lui aussi par la clé) des coefficients de basse fréquences (C_1,C_2,C_3), le triplé doit appartenir à la zone gris de la figure (2 .15) .

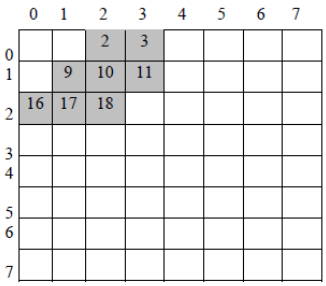


Figure 2.15: Les 8 coefficients sur lesquels on peut insérer un bit.

Le triplé modifié doit respecter les contraintes suivantes :

- Si w_i = 1 mettre : $C_1 > C_3 + Cte$ et $C_2 > C_3 + Cte$;
- Si w_i = 0 mettre : $C_1 + Cte < C_3$ et $C_2 + Cte < C_3$.

L'insertion n'est possible que si la différence entre les composantes pointées n'est pas trop importante, ce qui est généralement le cas pour des images réelles.

- ***Méthode utilisant la DWT***

Kundur *et al.* ont proposé dans [22] un algorithme qui permet d'insérer plusieurs bits en sélectionnant autant de triplé dans les trois sous-bandes de décomposition en ondelettes. Les coefficients de ces triplés seront modifiés afin de pouvoir identifier le bit inséré lors de la détection. Chaque triplé est ordonné de telle manière que $C_1 <= C_2 <= C_3$, on définit alors un pas de quantification μ. Tel que : $\mu = \frac{C_3 - C_1}{2Q - 1}$.

Q est une constante permettant de régler la force de tatouage et le degré de visibilité de celui-ci dans l'image. Ensuite, une échelle de quantification est construite, comme illustrée par la figure 2.16.

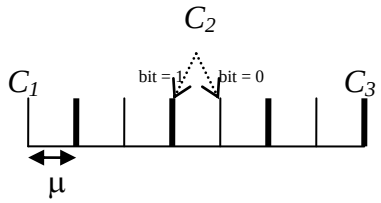


Figure 2.16: Quantification selon le bit à insérer.

Le coefficient C_2 est ensuite identifié sur cette échelle. Pour insérer un bit 1, C_2 est modifié de telle manière que le coefficient soit égal à la valeur correspondant au trait gras le plus proche. Pour insérer un bit 0, on affecte au coefficient la valeur correspondant au trait fin le plus proche. Lors de la détection, il suffira de déterminer à quel type de trait correspond la valeur de C_2 pour reconnaître le bit marqué.

- ***Codage fractal***

Le codage fractal est basé sur la définition d'une association entre différentes régions de l'image. Cette association est réalisée selon un critère d'auto-similitude fondé sur la minimisation de l'erreur quadratique entre les blocs cibles et les blocs sources transformés.

Pour un bloc cible donné, la recherche du bloc source associé s'effectue dans deux fenêtres de recherche centrées sur le bloc cible. La méthode de tatouage proposée modifie cette recherche en définissant deux sous fenêtres comme indiqué sur la figure 2.17, [6].

L'insertion du message consiste à tirer aléatoirement *N* blocs cibles dans l'image. Pour chacun des *N* blocs cibles, effectuer la recherche du bloc source associé dans la fenêtre de recherche de type 0 (respectivement de type 1) si le bit associé au message à pour valeur 0 (respectivement 1). Pour chacun des blocs cibles non précédemment traités, la recherche du bloc source s'effectue sans contrainte sur la fenêtre de recherche. En d'autres termes, la recherche est réalisée dans la fenêtre constituée de l'union des fenêtres de type 0 et 1.

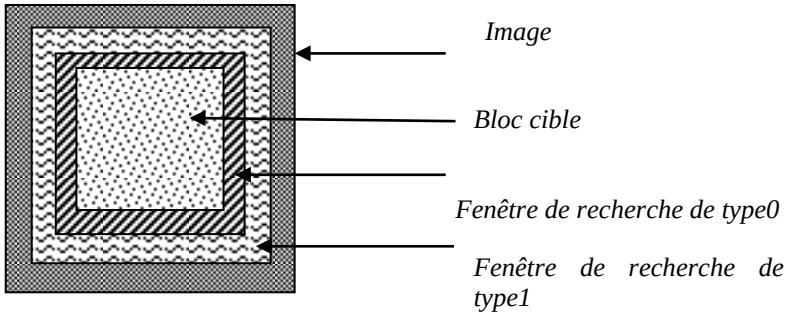


Figure 2.17: Décomposition en régions de recherche.

A partir du code IFS obtenu lors des deux précédentes étapes, effectuer le processus de décodage standard aux techniques de codage fractal afin d'obtenir l'attracteur qui constitue l'image tatouée.

L'extraction du message est réalisée de manière duale à l'insertion.

2.5 Evaluation des algorithmes de tatouage

2.5.1. Les attaques

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors de son extraction [23]. Dans la littérature, la classification des attaques se fait sur différents critères, dans [14] l'idée est d'étudier les attaques selon l'étape du tatouage qu'elles mettent en défaut c'est-à-dire lors du processus d'insertion ou d'extraction. Hurtung propose de classer les attaques en quatre catégories : suppression ou détérioration de la marque, attaques de synchronisation, attaques cryptographique et attaques

de confusion. La classification la plus répandue est celle exposée dans la thèse [12], qui divise les attaques en deux catégories : non intentionnelles et intentionnelles. Elles sont expliquées plus en détail dans l'annexe A.

2.5.2 Mesure de la qualité de l'image

La plupart des images qui peuvent être soumises à ces traitements sont destinées à notre sens (la vision). Or ce dernier n'est pas très commode pour mesurer objectivement. Et pourtant, le seul instrument vraiment capable d'apprécier la qualité d'une image est bien l'œil. Des stratégies mettant directement en œuvre des observateurs humains ont été élaborées pour effectuer des mesures dites subjectives.

Elles consistent à présenter à un groupe d'observateurs, les images modifiées et les images originales, les appréciations possibles de la qualité de l'image sont présentées dans le tableau 2.1 [14]. Selon la recommandation 500 du CCIR[9].

Tableau 2.1 Appréciations possibles de la qualité de l'image.

Note	Qualité
5	Excellente
4	Bonne
3	Assez bonne
2	Médiocre
1	Mauvaise

Ces mesures présentent les désavantages d'être lourdes et coûteuses, elles sont donc exceptionnellement utilisées. On leur préfère des mesures dites «objectives », parfois appelés critères de qualité, parce qu'elles résultent de calculs exécutables sur n'importe quel calculateur. Leur inconvénient majeur est d'être discutables dans la mesure où aucun de ces critères ne correspond exactement à ce que ressent l'ensemble du système visuel.

La notion de qualité doit être conservative c'est-à-dire que la qualité entre l'image originale et l'image tatouée doit être gardée, d'autre part les attaques auxquelles doit être robuste le tatouage, doivent conserver la qualité de l'image aussi.

[9] Comité consultatif international des radiocommunications.

On pourrait définir la mesure de qualité comme étant une mesure de distance entre deux images (originale et tatouée), la démarche la plus employée est alors d'utiliser une métrique d'erreur quadratique moyenne (EQM) ou MSE (Mean Squared Error), ainsi que le rapport signal sur bruit (SNR Signal to Noise Ratio) et le PSNR (Peak Signal to Noise Ratio). Ces équations sont données respectivement par les formules (2.3), (2.4) et (2.5).

$$MSE = \frac{1}{MN}\sum_{m,n}(I_{m,n} - I_{w_{m,n}})^2 \qquad \text{..... (2.3)}$$

$$(SNR)_{dB} = 10\log_{10}\left(\frac{\sum_{m,n} I_{m,n}^2}{\sum_{m,n}(I_{m,n} - I'_{m,n})^2}\right) \qquad \text{..... (2.4)}$$

$$(PSNR)_{dB} = 10\log_{10}\left(\frac{MN \max_{m,n}(I_{m,n}^2)}{\sum_{m,n}(I_{m,n} - I'_{m,n})^2}\right) \qquad \text{..... (2.5)}$$

Où $I(i,j)$ est la valeur de la luminance du pixel (i,j) de référence et $I_w(i,j)$ celle de l'image à tester (image tatouée) , les deux images étant de taille MxN. Cette mesure nous donne une indication sur la dégradation introduite au niveau du pixel.

Lorsque la *EQM* est nulle, il y a identité entre les deux images (la distorsion est nulle). Plus l'*EQM* est importante et plus les différences (ou la dissemblance) entre les deux images sont elles-mêmes importantes. Cette grandeur est considérée comme une distance entre les images.

Le PSNR quant à lui, ne renseigne qu'approximativement sur la qualité réelle de l'image décodée par rapport à l'originale. Les chiffres correspondants doivent être prudemment interprétés. Cela dit, pour se donner une idée, seulement une idée, on estime que, sur des images de scènes naturelles en niveaux de gris, un *PSNR* inférieur à 30 dB conduit à une image décodée dont les différences avec l'originale sont visibles à l'œil nu [1].

Ces mesures mathématiques sont basées sur une comparaison pixel à pixel, ce qui n'est pas le cas du système visuel humain qui tient compte du voisinage, la figure 2.18 en témoigne de cela, elle représente deux images compressées par des techniques différentes. La différence de dégradation entre ces deux images est très visible, et pourtant elles ont le même PSNR.

Image compressée par Ondelettes
PSNR = 28,66

Image compressée par JPEG
PSNR = 28,65

Figure 2.18: Comparaison d'images avec le même PSNR [24]

Un autre exemple, celui de la figure 2.19, montre que, même si le PSNR de l'image (b) est inférieur à celui de l'image (c), l'image (b) possède une meilleure qualité visuelle.

(a) : Image originale

(b) : Image fortement contrastée
PSNR=24,63 dB

(c) Image fortement comprimée
PSNR=28,80 dB

Figure 2.19: Évaluation du PSNR comme mesure de qualité visuelle [2]

En effet, le PSNR quantifie l'intensité de la marque. Cependant il ne s'adapte pas aux caractéristiques de l'image : la marque est en effet plus visible dans les zones peu texturées (à variance faible) et moins visible dans les zones plus texturés (à variance plus forte). Pour

quantifier plus efficacement la visibilité de l'image, il faudrait donc un PSNR qui serait plus pénalisant dans les zones planes que dans les zones texturées, d'où l'existence du PSNR pondéré ou Wpsnr. Il prend en compte la variance de l'image. Il est exprimé par l'équation (2.6).

$$(wPSNR)_{dB} = 10 * \log_{10}\left(\frac{\max_{m,n}(I_{m,n}^2)}{sum'}\right) \quad \text{.....(2.6)}$$

Avec :

$$sum' = \frac{1}{M * N} * \sum_{i,j=1}^{m,n} \left(\frac{I(i,j) - I_w(i,j)}{1 + Var(i,j)}\right)^2$$

Il est fort quand la variance est grande et plus faible quand la variance est petite, la figure 2.20 nous illustre la différence perceptuelle entre trois images qui possèdent le même PSNR mais un *w*PSNR différent.

✓ (b) (c)

PSNR =24.6dB *PSNR* =24.6dB *PSNR* =24.6dB

wPSNR= 26.4dB *wPSNR* =27.9dB *wpsnr*=29.3dB

Figure 2.20: Évaluation du PSNR comme mesure de qualité visuelle

Si ces mesures quantifient bien les dégradations par ajout de bruit, elles ne sont pas très significatives dans d'autre cas, les plus évidents concernent par exemple les transformations affines : Si on fait subir une symétrie à une image, le PSNR et wPSNR entre l'image modifiée et son original pourra être très bas alors que l'image n'est pas modifiée pour autant. On ne peut donc pas utiliser ces mesures de manière systématique, on introduira dans ce cas les mesures subjectives.

2.5.3 Banc d'essai

Toutes les attaques citées ci-dessus nous amènent à nous poser une question : comment évaluer et comparer différentes méthodes de marquages. Un banc d'essai (des logiciels standard dans notre cas) est nécessaire pour mettre en évidence les caractéristiques des algorithmes.

De nombreuses publications [6] : [25], [26], [27], [28] abordent cependant le sujet. Des outils et des projets de recherche Octalis [29], Optimark, CheckMark et Certimark tentent d'y apporter des solutions. Un aperçu est donné dans l'annexe B.

2.6 Différentes applications du tatouage numérique

Les applications du tatouage sont diverses [30]. Initialement dédié à la protection de la propriété intellectuelle des documents numériques, le tatouage est utilisé aujourd'hui pour le contrôle d'intégrité, de l'authentification ou encore de la production de documents enrichis.

2.6.1 Protection des droits d'auteur

La protection des droits d'auteur (*le copyright*) a été la première application envisagée pour le tatouage de document, car il a été bafoué par la démocratisation des technologies numériques. La technique consiste ici en l'insertion d'une signature numérique qui atteste de l'identité du dépositaire du document. Cette signature ne doit être connue que de la personne ou de l'organisme qui a inséré le tatouage. Elle dépend donc d'une clé secrète qui permet son insertion et sa détection, ainsi toute personne qui réclamera propriété illégale du document, pourra être condamnée légalement ; la marque faisant office de preuve devant les tribunaux.

La mise en place d'un tel service doit respecter les trois contraintes suivantes :

- Préserver la qualité de l'image de manière à ce que la qualité visuelle de l'image tatouée soit quasi identique à l'originale. Mais cette notion d'invisibilité est très subjective, d'autant plus qu'elle dépend de nombreux facteurs dont la qualité du document original.

- Le tatouage doit constituer une preuve irréfutable. Pour cela il convient d'assurer l'unicité (éviter les problèmes de collision) et de l'authenticité de l'identifiant, mais

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

- L'algorithme utilisé être doit robuste c'est-à-dire être capable d'extraire correctement la marque cachée, même si l'image a été manipulée.

2.6.2 Traçabilité dans un système commercial

Le tatouage de document assure aussi la traçabilité du produit, en remontant jusqu'à la personne qui a permis le piratage, pour cela le distributeur doit tatouer chaque produit avec une signature différente contenant le numéro d'une pièce d'identité ou un numéro de série différent pour chaque acheteur [12].

2.6.3 Authentification du document

L'authentification consiste à certifier le contenu du document et son origine. Dans le premier cas il s'agit de contrôle d'intégrité, l'information insérée au sein de l'image permet de prouver qu'elle n'a pas subie d'altération, l'idée de base consiste à utiliser les techniques de tatouage d'image afin de cacher dans certaines zones de l'image des informations sur d'autres zones, pour cela la marque doit être fragile, conçue d'une manière à se détériorer lors d'un ajout ou d'effacement d'une partie et non pas face à une compression ou une transformation géométrique [17]. Le but de l'insertion dans le deuxième cas d'authentification, est de certifier l'identité de la source originale du document tatoué, dans ce cas la marque doit résister à toutes les attaques, la marque devra être robuste.

2.6.4 Contrôle d'accès

Le but dans ce cas est d'ôter tout intérêt commercial à l'image en insérant une marque visible (nom de la société, logo…). La figure 2.21 nous illustre cette application.

Figure 2.21: Contrôle d'accès par masquage visible d'une image [10]

Seules les personnes ayant les droits d'accès sont en mesure d'inverser le processus de marquage de manière à reconstituer l'image originale.

2.6.5 Gestion du nombre de copies

Contrairement aux données de nature analogique, pour lesquelles une reproduction entraîne une perte significative de la qualité (exemples : les bandes magnétique vhs, K7,…), les données numériques peuvent être dupliquées quasiment à l'infini, une personne malintentionnée, peut en faire des copies et les redistribuer illégalement avec une qualité égale au document original. C'est la raison de l'introduction tardive du DVD sur le marché.

2.6.6 Contrôle de diffusion audiovisuelle

La marque insérée peut contenir des informations sur les permissions attachées au document. En prenant l'exemple d'un film vidéo : il pourrait être marqué en copie illimitée, copie interdite (commercialisation du film) ou copie une fois seulement (une diffusion gratuite à la télévision) dans ce cas c'est le "magnétoscope" qui transforme cette marque en une marque de copie interdite. Dans ce type de marquage, c'est au matériel de copie que revient la charge de détecter la marque.

Cette application concerne essentiellement la diffusion des contenus à travers les réseaux télévisés, radiophoniques ou à travers Internet.
Les principales entités concernées par la surveillance audiovisuelle sont les agences de publicité, les musiciens, la SACEM[10], ainsi que toute personne qui cherchera à s'assurer de la diffusion effective de l'œuvre dont elle a la charge.

En 1997, un scandale a éclaté à la télévision japonaise quand, par manque de temps pour les annonces publicitaires, deux chaînes n'avaient pu passer une publicité mais avaient pourtant perçu la rétribution financière de la part de l'agence de publicité. Le tatouage des documents peut s'avérer très utile dans le cas de ce scénario puisqu'il suffit de tatouer les clips, vidéos ou images qui vont être diffusés. Ensuite muni d'un appareil de surveillance automatique, il sera possible d'identifier si l'œuvre a été diffusée ou non [12].

[10] SACEM (Société des Auteurs, Compositeurs et Editeurs de Musique) société de protection des droits d'auteur des produits musicales, ″http://www.sacem.fr (décembre 2005).

2.6.7 Indexation des documents

L'indexation des images consiste à classer de manière automatique des images selon leur contenu, en facilitant ainsi la recherche dans une base de données. La marque insérée décrit brièvement l'image, comme elle peut être un pointeur vers lequel il y a une description plus détaillée, cette technique commence à être appliquée dans les services hospitaliers, où les clichés sont classés dans des bases de données suivant l'âge, le nom ou la pathologie du patient.

Dans cette application, la marque n'a pas besoin d'être robuste aux attaques, puisqu'il ne s'agit plus de protection mais juste d'identification.

Un nouveau concept d'image intelligente (smart image) a été introduit par la société « Digimarc[11]». A des fins publicitaires, le tatouage est utilisé pour insérer un pointeur vers un lien internet qui pourra donner toute la description du produit, en le présentant juste à un dispositif d'acquisition, en le décodant, tous les détails concernant le produit seront affichés sur un navigateur Web [17] comme l'illustre la figure 2.22.

Figure 2.22: Application du tatouage pour l'indexation d'image (smart image)

2.6.8 Autres applications

Sont également apparus plus récemment de nouveaux champs d'application, comme par exemple celui de l'autocorrection d'erreurs, lorsque des paquets de données d'une image ont été perdus pendant leur transport. Il s'agit dans ce cas de tatouer au préalable une version

[11] Concepteur de solution de sécurité des médias, société pionnière en tatouage d'image numérique, http://www.digimarc.com/

simplifiée de l'image dans elle-même afin d'en bénéficier lors de la reconstruction en cas d'informations manquantes. Un autre exemple d'application est celui développé par Campisi et al [31] qui proposent de tatouer les chrominances d'une image couleur à l'intérieur de la luminance afin d'employer un algorithme de compression d'images à niveaux de gris pour compresser une image couleur. Le tatouage d'image trouverait également sa place dans un système de montage vidéo où il pourrait servir par exemple à étiqueter les différentes séquences. Un des avantages de cette technique par rapport à des méthodes traditionnelles, est qu'elle offre la possibilité de retrouver facilement l'origine d'un extrait à partir d'un enregistrement quelconque.

2.7 Conclusion

Ce chapitre aborde dans un premier lieu les sciences qui ont été à l'origine du tatouage d'image qui sont la stéganographie et la cryptographie, il expose également les raisons qui ont fait l'engouement de la communauté scientifique vers ce domaine qui s'avère prometteur, mais les attentes suscitées par le tatouage jusqu'à une date récente ont été très élevées et pour l'instant pas tout à fait satisfaites, du fait que le tatouage est une science relativement récente et n'étant arrivé à maturité il présente quelques failles.

Une controverse a été lancée sur son utilité, notamment par C. Herley [32] où il y affirmait que la variété des attaques envisageables sur un document tatoué est bien plus grande que les cas de figure traités jusqu'ici. Les applications les moins orientées sur la sécurité sont les plus exploitables à l'heure actuelle : contrôle de diffusion, tatouage fragile, amélioration de contenu. Cependant, le tatouage numérique est un domaine jeune qui progresse rapidement. Si la robustesse aux attaques géométriques reste le point faible des techniques de tatouage, de nouvelles solutions continuent d'être proposées, l'une des pistes de recherche qui commence à donner ses fruits et l'association de la cryptographie au tatouage et la compression jointe au tatouage.

La suite du mémoire est consacrée à ces nouvelles techniques. Le chapitre 3 dresse un état de l'art des techniques déjà existantes dans le domaine du tatouage d'images compressées et expose la méthode que nous avons proposée à savoir, la combinaison du tatouage et du cryptage sur des images compressées *JPEG*, le dernier chapitre sera consacré aux tests et résultats obtenus et donne les différentes utilités qu'offre cette méthode, en particulier pour le WEB.

Chapitre 3

Tatouage des images JPEG

3.1 Introduction

Dans ce chapitre nous présentons un aperçu sur les méthodes de tatouage appliquées aux images JPEG, nous proposerons ensuite deux schémas de marquage de l'image JPEG qui permettront de l'authentifier: un premier schéma non réversible qui sera basé sur l'insertion de la marque dans les coefficients DCT quantifiés. L'objectif est d'étudier l'impact de l'insertion dans différents coefficients sur la qualité de l'image, et sur le taux de compression. Dans ce schéma la sécurité de la marque est basée sur des outils de cryptographie. Dans un deuxième schéma une méthode réversible sera présentée. Elle a pour objectif de garder une qualité médiocre de l'image dans une base de données, sauf pour les personnes autorisées à exploiter ces images, ils auront la possibilité de restaurer l'image originale. Les résultats de l'implémentation seront présentés dans le chapitre suivant.

3.2 Etat de l'art sur les techniques de tatouage appliquées aux images JPEG

On rencontre dans la littérature plusieurs travaux d'insertion d'un tatouage dans une image brute, en prenant en considération la robustesse aux attaques *JPEG* ou *JPEG 2000*. Toutefois, on retrouve beaucoup moins de travaux concernant le tatouage d'images compressées. Ces méthodes sont souvent basées sur l'insertion de la marque dans le domaine fréquentiel DCT ou DWT [33] [34]. Toutefois, il existe moins de travaux qui proposent l'insertion de la marque directement dans le format *JPEG*, malgré qu'il soit le format le plus utilisé, notamment pour le Web.

Nous présentons dans ce qui suit quelques méthodes de tatouage appliquées au format *JPEG* :
La figure 3.1 (a), présente un modèle générique pour l'insertion de la marque durant la compression *JPEG*. Le message secret est inséré après l'étape de quantification. Quant à la figure 3.2 (b), elle illustre la possibilité d'insérer la marque dans une image déjà compressé et ce en effectuant d'abord un décodage entropique [35]. L'étape de détection ou d'extraction de la marque se fait sur le fichier *JPEG*, au niveau des coefficients quantifiés, après l'étape de décodage entropique.

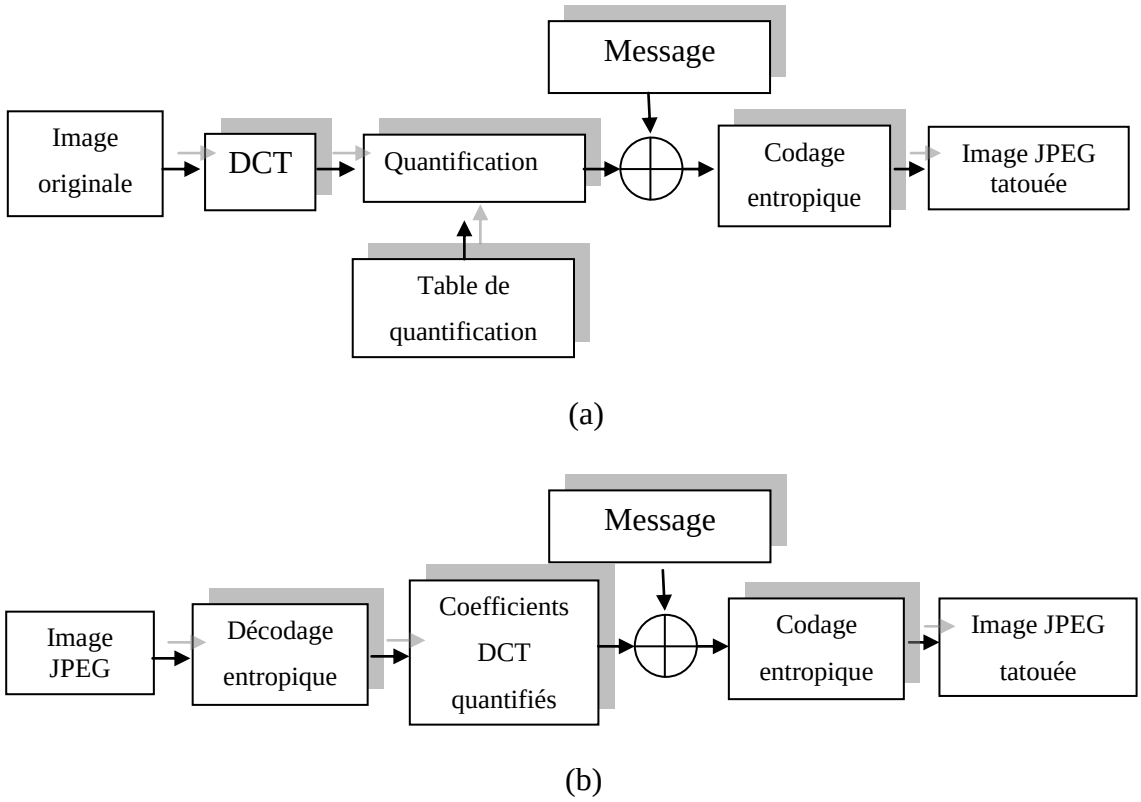


Figure 3.1 : Schémas génériques pour l'insertion de la marque dans un fichier JPEG

- Mateev *et al.* [36] Ont proposé une méthode de tatouage de l'image JPEG basée sur la modification des coefficients DCT 8x8 quantifiés. Les auteurs se basent sur l'idée que lorsque nous modifions ces coefficients de « +1 » seulement, ceci n'est souvent pas perceptible. Prenant comme exemple : soit un coefficient DCT, c=22, si le paramètre de quantification lui correspondant est 4, le coefficient deviendra égal à 5.5, après l'opération du *round* il deviendra 5. Si ce coefficient est incrémenté de 1 pour insérer un bit, il deviendra égal à 6, une valeur qui est aussi proche de 5.5 que 5. Les auteurs proposent de ne pas utiliser la valeur DC pour éviter des éventuels changements sur la luminosité de l'image. Dans ce schéma l'insertion de la marque se fait avec un code correcteur d'erreur. Les attaques géométriques sont prises en considération, les auteurs proposent d'utiliser les transformations affines qui permettraient d'ajuster l'image JPEG attaquée à partir de l'image originale.

- Kobayashi *et al.* [35] ont proposé d'insérer la marque au niveau des hautes fréquences (voir figure 3.2) et de modifier la table de quantification pour ce coefficient. Ce schéma, bien qu'il offre une imperceptibilité parfaite de la marque, il a l'inconvénient majeur d'augmenter la taille du fichier compressé. Dans d'autres travaux [35] deux bits sont insérés dans les moyennes fréquences pour augmenter la capacité d'insertion, toutefois pour préserver la qualité de l'image on ne peut pas changer librement le facteur de quantification, le taux de compression reste donc restreint.

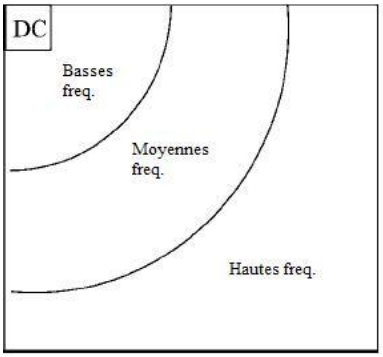


Figure 3.2 : Distribution des fréquences dans un bloc DCT

- Le schéma de tatouage fragile désigné par CWA (Compressed Watermarking Algorithm) a été proposé par Wang *et al.* [37]. Selon les auteurs, cette méthode assure un contrôle de l'authentification de l'image et diminue même la taille de l'image compressée d'environ 6.3% tout en préservant l'imperceptibilité de la marque.

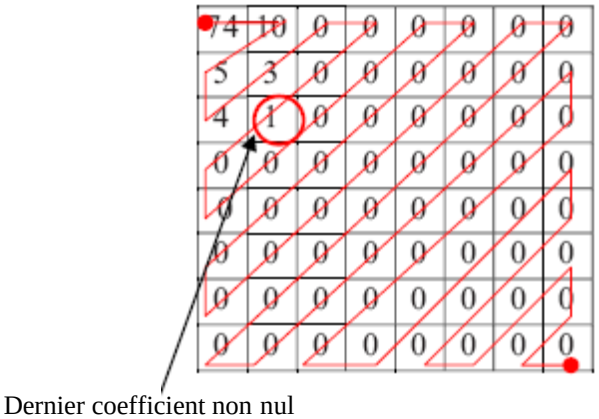


Figure 3.3 : Bloc DCT 8x8 quantifié

L'algorithme CWA consiste à insérer la marque dans une image JPEG en modifiant le dernier coefficient significatif de chaque block DCT, qui est identifié en effectuant un balayage en zigzag tel qu'illustré sur la figure 3.3. La marque à cacher est constituée d'une combinaison du message secret avec une empreinte[12] calculée avec la fonction de hachage MD5 pour chaque groupe de quatre blocs.

- Stankovic *et al.* [38] ont effectué une étude dont l'objectif est de voir l'effet de la quantification sur les coefficients DCT 8x8 tatoués et sur la signature même. Les auteurs ont proposé un critère pour la sélection des coefficients adéquats offrant une détection fiable et fournissant la robustesse pour des degrés de quantification arbitraires. Dans le même contexte, TSENG *et al.* [33] ont proposé un schéma de marquage à grande capacité pour les images *JPEG*. La méthode proposée utilise une table de la capacité pour estimer le nombre de bits qui peuvent être cachés dans chaque composant DCT de sorte que les distorsions de l'image peuvent être évitées. Ce tableau des capacités est dérivé de la table de quantification *JPEG* par défaut et des propriétés du système visuel humain (HVS). Ensuite, la méthode de marquage basée sur les LSB est utilisée pour insérer la marque au niveau des coefficients DCT quantifiés.

- Wong *et al.* [39] ont aussi voulu exploiter les propriétés du système visuel humain pour la sélection des blocs DCT à tatouer. Ils ont présenté une méthode appelée "J-Mark" basée sur une sélection des blocs DCT selon les zones texturées ayant des propriétés de masquage importantes basée sur un calcul d'énergie des blocs. Dans ce cas le taux d'insertion va être différent d'une image à l'autre.

- Parmi les méthodes réversibles qui ont été proposées pour les images JPEG, Xuan *et al.* [40] ont proposé une méthode basée sur le décalage de l'histogramme. Le schéma général d'insertion et d'extraction de la marque est illustré sur la figure 3.4.
  La technique du décalage de l'histogramme a été initialement effectuée sur l'image brute, le principe de cette technique consiste à générer l'histogramme des coefficients DCT quantifiés, et de trouver la valeur qui a la plus grande fréquence et celle qui a la

[12] L'empreinte est obtenue par une fonction de hachage. Cette fonction convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe.

plus petite fréquence. Entre ces deux limites, un décalage de valeurs sera appliqué vers les fréquences minimales afin de créer un vide dans l'histogramme (dans N1) qui va contenir le bit « 1 » de la marque, les bits « 0 » seront insérés dans la valeur voisine (N1+1) tel que présenté sur la figure 3.4. Pour restaurer l'image il suffit d'effectuer le décalage vers la fréquence maximale après extraction de la marque. Les valeurs des niveaux correspondant aux fréquences minimales et maximales doivent être enregistrées pour la restauration.

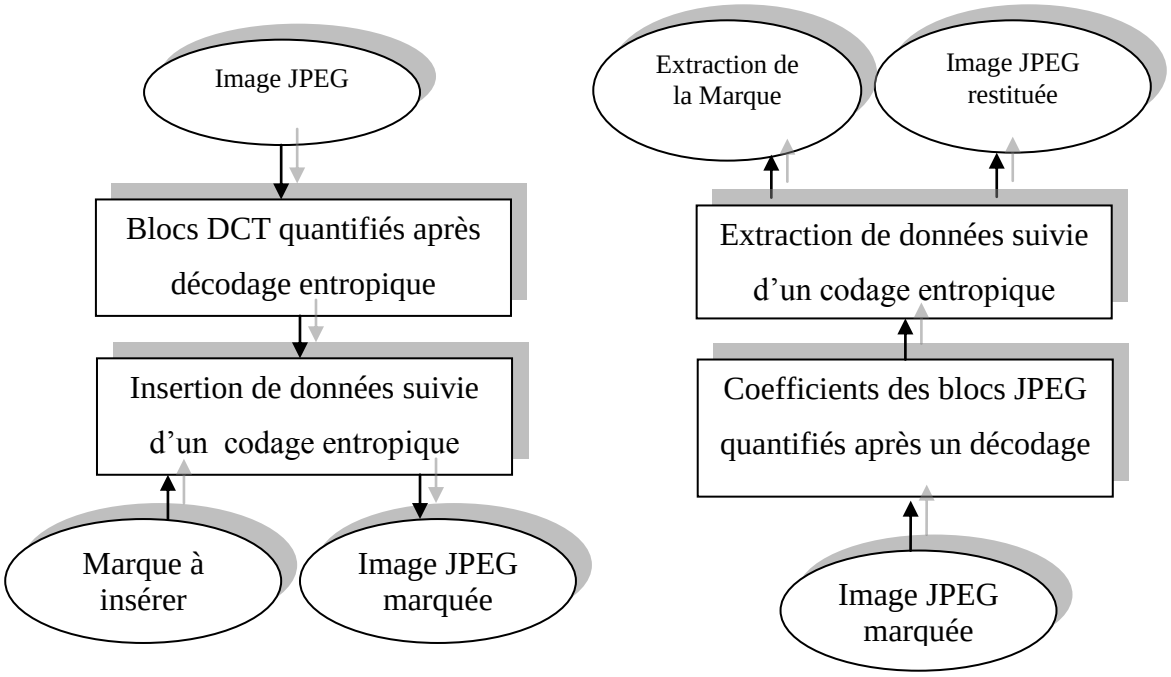


Figure 3.4 : Schéma général d'insertion et d'extraction de la marque de la méthode de Xuan *et al.*

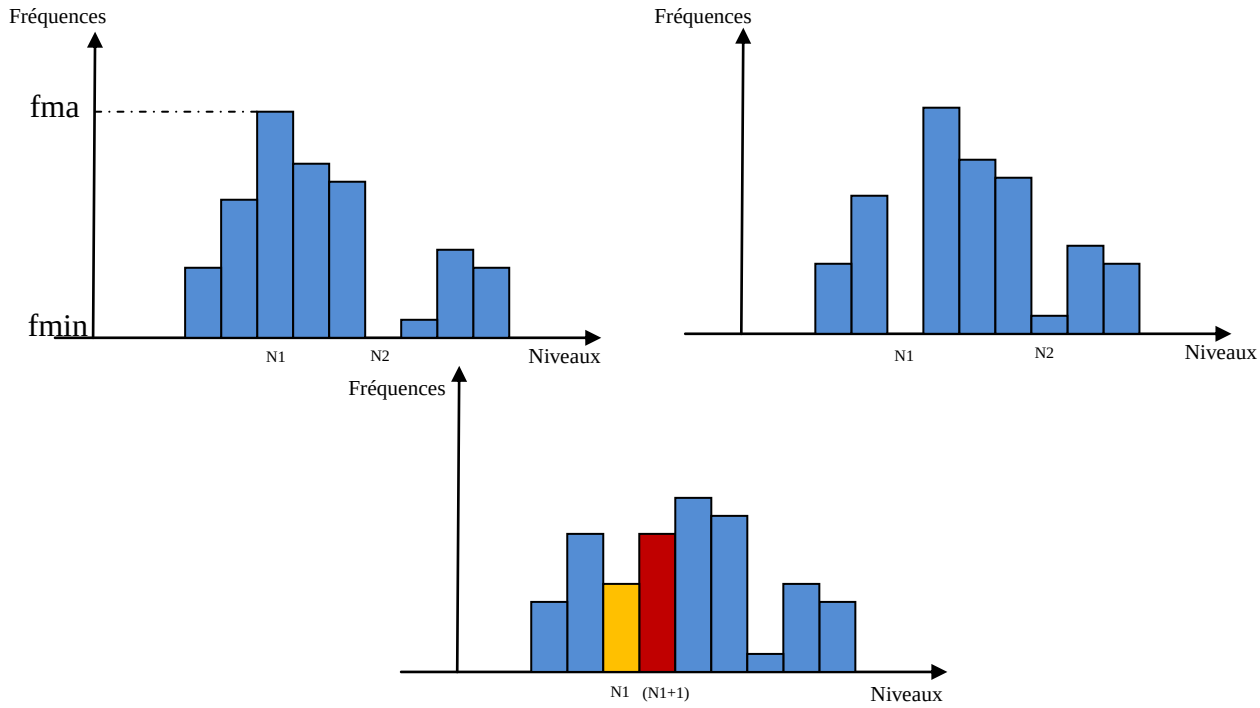


Figure 3.5 : Illustration de la technique du décalage de l'histogramme : (a) Histogramme des valeurs, (b) Décalage de l'histogramme à droite entre les niveaux correspondants aux fréquences fmax et fmin (c) Insertion de la marque

3 3.3 Application

Dans cette partie nous présentons deux schémas de tatouage que nous avons proposé pour l'image JPEG.

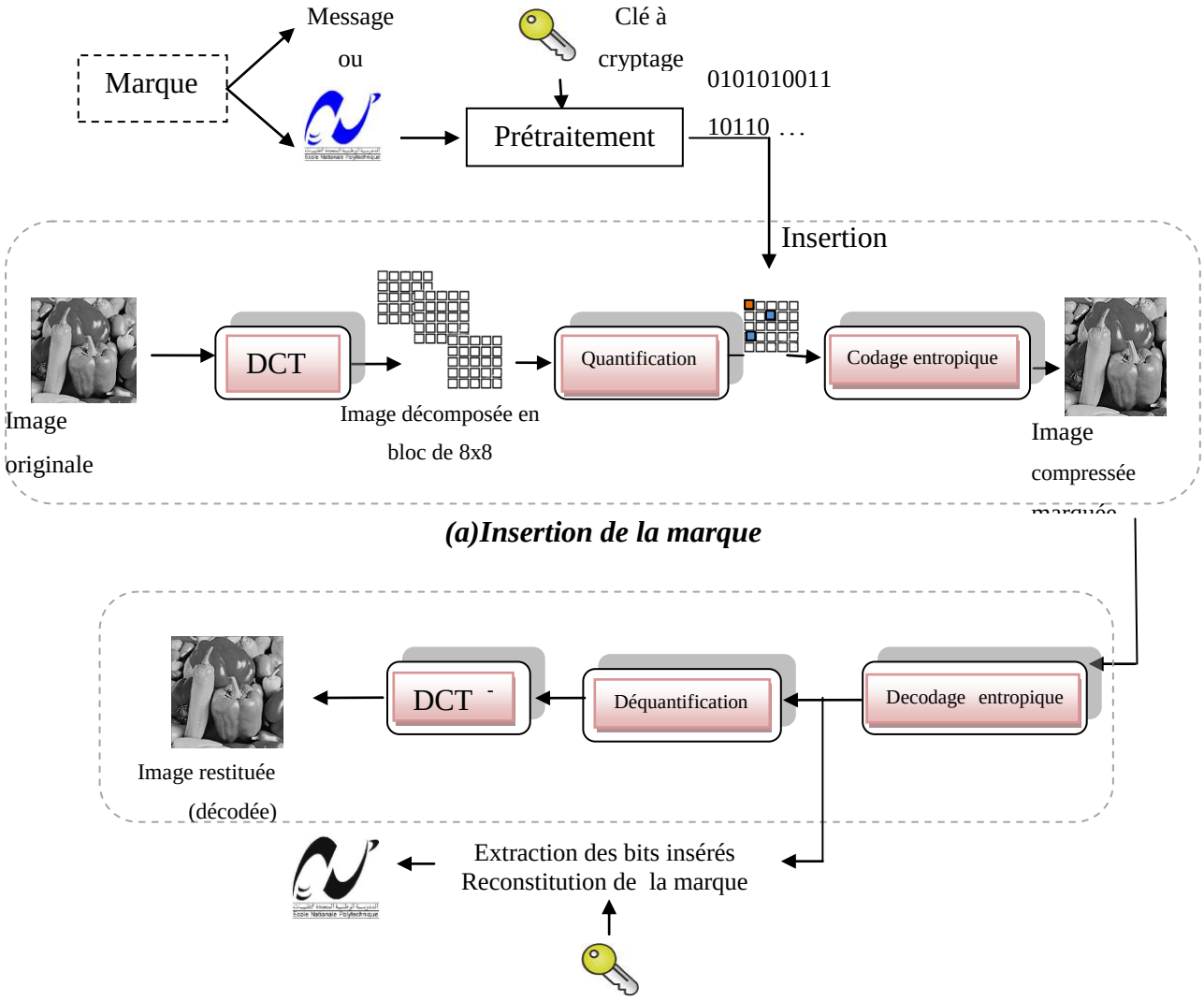
3.3.1 Méthode non-réversible

Dans cette méthode, le travail effectué consiste à étudier l'impact de la signature sur la qualité de l'image et sur le taux d'insertion, et ce en insérant d'abord un seul bit par bloc DCT 8x8 quantifié, dans des emplacements différents, ensuite en insérant deux ou trois bits par bloc pour élever le taux d'insertion.

Afin de maintenir le taux de compression, les coefficients choisis pour l'insertion appartiennent aux basses et moyennes fréquences.

La marque qu'on veut insérer subit d'abord un prétraitement. Ce point est expliqué dans la section 3.3.3.

La figure 3.6 représente le schéma d'insertion et d'extraction de la marque.



(a)Insertion de la marque

(b)Extraction de la marque

Figure 3.6 : Schéma proposé : insertion et extraction de la marque

Tout d'abord l'image est divisée en blocs de 8x8 pixel, à lesquels serait appliquée la transformation DCT (voir section 1.4.2.2).

Après l'étape de quantification, l'image subit des distorsions selon le niveau de compression désiré. Chaque coefficient DCT est divisé par la valeur correspondante dans Q(*u*,*v*) (matrice

ou table de quantification) et le résultat sera arrondi à l'entier le plus proche suivant la formule (3.1).

$$C'(u,v) = round\left[\frac{C(u,v)}{Q(u,v)}\right] \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (3.1)$$

Quelques tables standards *JPEG*, pour la quantification, ont été générées grâce à une série de caractéristiques du système visuel humain (SVH) qui est plus sensible aux basses fréquences qu'aux hautes fréquences. Les valeurs prennent donc en compte cette caractéristique et introduisent majoritairement de la distorsion dans les hautes fréquences, dans le but de créer un maximum de redondance, notamment un grand nombre de valeurs nulles. Cependant, il est tout à fait possible de personnaliser la table [24], c'est le cas de ce schéma de tatouage où la matrice a été construite suivant la formule (3.2).

$$Q(u,v) = (1 + u + v) \times Fq \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (3.2)$$

Le facteur Fq détermine la qualité relativement à l'image originale. Il amplifie ou réduit les valeurs des facteurs de quantification pour augmenter ou diminuer les dégradations.

L'étape suivante est l'étape d'insertion, le choix des coefficients qui porteront la marque est fait d'une manière à conserver le taux de compression obtenu avant tatouage et de garder la qualité visuelle de l'image tout en ayant une capacité d'insertion intéressante et une bonne robustesse.
L'insertion consiste à changer uniquement le bit poids faible (*LSB*) des coefficients concernés, moyennant les relations suivantes (3.3), (3.4):

$$si\ C'\ mod\ 2 = 0 \begin{cases} si\ Wi = 1\ \ alors\ Cw = C' \\ si\ Wi = 0\ \ alors\ Cw = C' + 1 \end{cases} \dots\dots\dots\dots\dots\dots\dots (3.3)$$

$$si\ C'\ mod\ 2 = 1 \begin{cases} si\ Wi = 1\ \ alors\ Cw = C' + 1 \\ si\ Wi = 0\ \ alors\ Cw = C' \end{cases} \dots\dots\dots\dots\dots\dots\dots (3.4)$$

Où W_i représente le mot binaire à insérer et C_w le coefficient quantifié après insertion.

Enfin, le codage entropique compresse l'image. En utilisant le code de Huffman et RLE, les coefficients DCT quantifiés sont transformés en une forme plus compacte. En particulier, les coefficients nuls créés par la quantification, améliorant grandement le taux de compression.
Pour retrouver la marque insérée, nous devons décoder partiellement l'image marquée transmise par le canal, en effectuant d'abord un décodage entropique qui nous permet d'obtenir les coefficients DCT quantifiés. L'extraction du mot binaire est aveugle et sera réalisée simplement par les relations suivantes (3.5), (3.6) :

$$si\ Qr\ mod\ 2 = 0 \quad alors : Wi = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.5)$$

$$si\ Qr\ mod\ 2 = 1 \quad alors:\ Wi = \ 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.6)$$

3.3.2 Méthode réversible

La méthode réversible a pour objectif d'offrir aux personnes autorisées la possibilité de restaurer l'image marquée. La qualité de l'image restera médiocre pour les personnes non autorisées à l'exploiter. Le contenu de la marque peut être utilisé pour la protection des droits d'auteurs où sa sécurité peut être renforcée avec un chiffrement.

La méthode présentée ci-dessous est la méthode initiale utilisée dans notre application pour l'authentification de l'image. C'est une méthode additive, où l'insertion se fait toujours au niveau des coefficients DCT 8x8 quantifiés. Les coefficients utilisés pour l'insertion sont choisis aléatoirement, à l'aide d'une clé numérique secrète K_1, entre les basses et moyennes fréquences. La formule utilisée pour l'insertion de la marque est [41] :

$$Cw = 2.C + Wi \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.7)$$

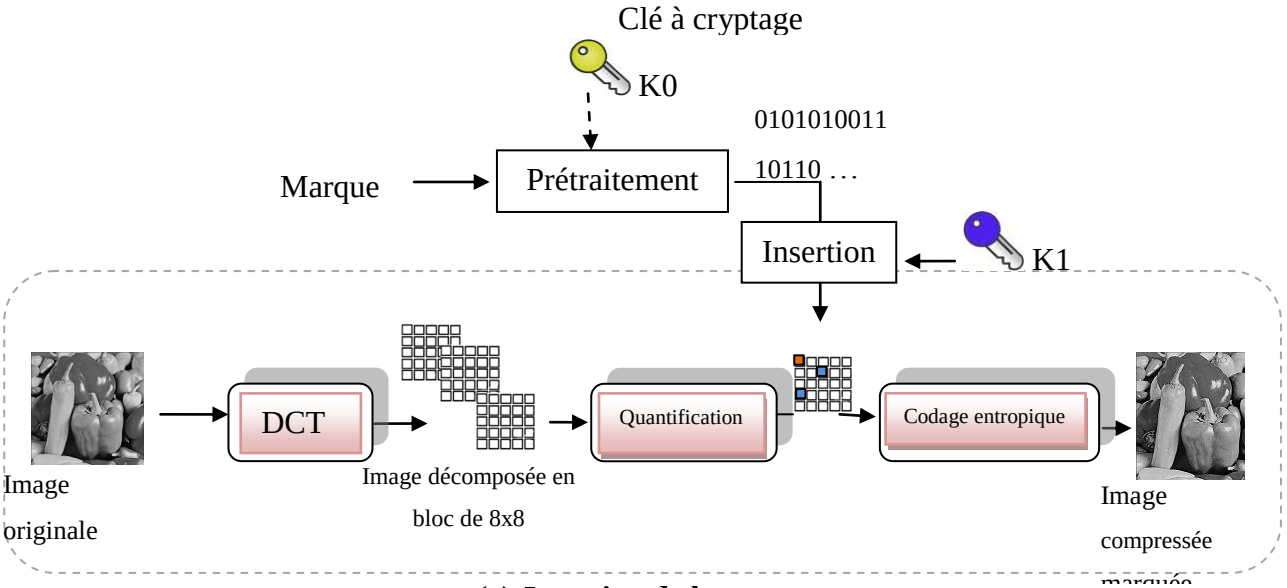
La marque est préalablement cryptée à l'aide de l'algorithme de Vigenére et dépend d'une seconde clé secréte K_0.
Avec Cw est le coefficient marqué, C est le coefficient avant marquage et Wi est le bit à insérer. L'extraction se fait en contrôlant la parité du coefficient utilisé pour l'insertion, sa position étant identifiée après insertion de la clé K.

Si Cw mod 2 =1 alors Wi = 1 sinon Wi = 0.

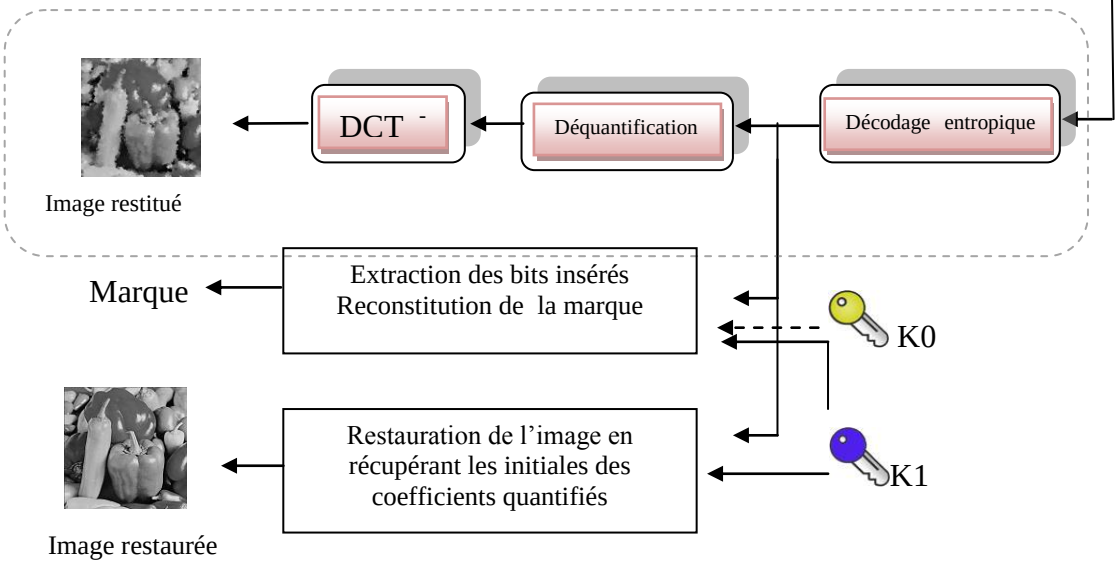
Pour la restauration de l'image, il suffit de retrouver la valeur de C avec la formule :

$$C=(Cw-Wi)/2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.8)$$

La figure 3.6 illustre les étapes d'insertion et d'extraction de la marque.



(a) Insertion de la marque



(b) Extraction de la marque et restauration de l'image

Figure 3.7 : Schémas de tatouage réversible

L'objectif de cette méthode est de pouvoir :

- Insérer une marque visible dans l'image, c'est-à-dire que la distorsion introduite est significative, seule la personne ayant droit sur cette image pourra restaurer la version originale. La distorsion introduite contient généralement les données relatives à l'œuvre ou la photographie, le nom de celui qu'il l'a conçue ou du nouvel acquéreur.
- Authentifier l'image sans ambiguïté.

Cette méthode combine un schéma de watermarking réversible appliquée à une image compressée *JPEG, avec* les outils de cryptographie détaillés dans ce qui suit.

3.3.3 Prétraitement de la marque

4 Le prétraitement de la marque permet d'adapter la marque avant l'opération d'insertion. Pour augmenter le taux d'insertion, il est possible d'appliquer une compression sans perte (voir chapitre 1). Une binarisation pourrait éventuellement être nécessaire.

Pour renforcer la sécurité de la marque, nous lui appliquons un algorithme de chiffrement ou une fonction de hachage.

3.3.3.1 Algorithme de chiffrement

Le chiffrement est l'application de transformations à un message pour le rendre incompréhensible. Le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Un exemple est présenté ci-dessous :

L'un des algorithmes utilisés est l'algorithme de Vigenère, dont le principe est de dissimuler un message en utilisant un tableau appelé « le carré de Vigenère ».

Le carré de Vigenère est composé de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder (voir figure 3.8).

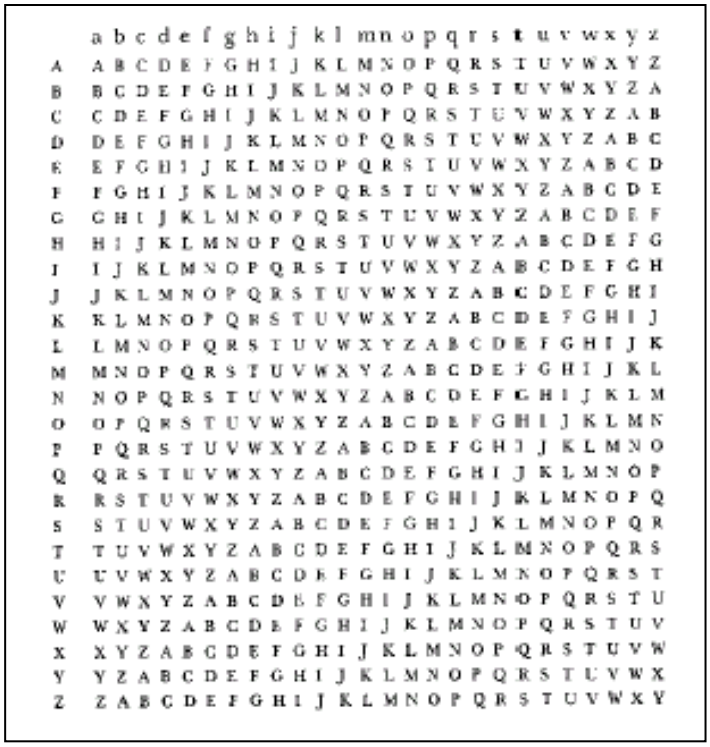


Figure 3.8 : Le carré de Vigenère

Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire. On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé. On regarde dans le tableau l'intersection de la ligne de la lettre à coder, avec la colonne de la lettre de la clé.

Exemple: chiffrons le texte "MARQUAGE DU JPEG" avec la clef "CHIFFRER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte en clair).
Pour coder la lettre M avec la lettre C, on regarde dans le tableau l'intersection de la ligne donnée par M, et de la colonne donnée C, on retrouve la lettre O.

Texte en clair	M	A	R	Q	U	A	G	E	D	U	J	P	E	G
Clef	C	H	I	F	F	R	E	R	C	H	I	F	F	R
Texte codé	O	H	Z	T	N	Z	K	V	E	B	R	U	J	X

3.3.3.2 Fonction de hachage

Une fonction de hachage, aussi appelée fonction de condensation, est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe ; la chaîne résultante est appelée *empreinte* (*digest* en anglais).

Tableau 3.1: Exemple d'un chiffrement de Vigenère

La fonction de hachage est dite sans collision, c'est à dire qu'il est impossible de trouver deux messages ayant la même empreinte [42].

Nous prenons l'exemple pour la fonction de hachage, la SHA-256, qui est devenue le nouveau standard recommandé en matière de hachage cryptographique après les attaques sur MD5 et SHA-1. Elle diffère des autres par la longueur du résultat obtenu mais aussi par certaines opérations.

L'empreinte obtenue pour l'image de Lena de taille 512x512 est la suivante :

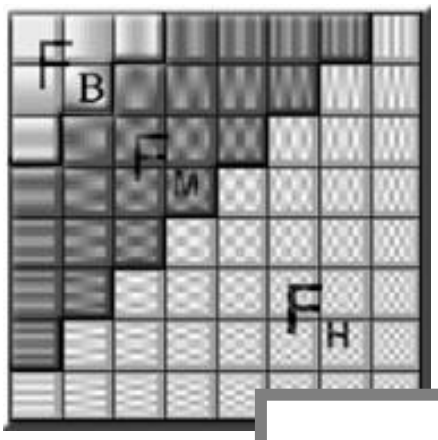
1e9c74bc87cc5c9bbca4753839f6f9ad0e62c35785136416867d79a2afa2c02b

3.4. Conclusions

Dans ce chapitre nous avons présenté un aperçu sur les méthodes de tatouage appliquées aux images JPEG.

Notre application consiste à étudier l'impact de l'insertion d'une marque dans les coefficients DCT 8x8 quantifiés, sur la qualité de l'image et le taux de compression à travers l'étude et l'implémentation d'une méthode non réversible. Une méthode réversible a été également proposée offrant la possibilité, aux personnes autorisées de restaurer l'image et récupérer ainsi la même qualité de l'image non marquée.

Les résultats obtenus seront présentés dans le chapitre suivant.



Chapitre 4

Applications

4.1Introduction

Les schémas que nous proposons insèrent la marque dans les sites favorables au tatouage pour l'invisibilité de l'information introduite, tout en gardant un bon niveau de robustesse. Les sites retenus du bloc proviennent d'une cartographie résultant de l'application de la matrice de quantification sur les coefficients DCT. Tel que cité dans le chapitre 3, nous retenons deux méthodes, une méthode non-réversible et une méthode réversible.

L'utilité première de la méthode non-réversible est l'authentification, en effet elle pourrait être utilisée dans des applications particulières, telles que les bases de données d'images ou de photographies, dans ce cas l'image marquée est envoyée par compression sur un canal de transmission à la banque d'images pour rechercher l'image originale, afin de tester l'authenticité ou la falsification éventuelle du message.

Quant à la méthode réversible, en plus du domaine militaire et médical, elle voit son utilisation grandir dans le domaine commercial. En effet, grâce à une clé numérique, que seul le propriétaire possède, il lui est possible de restaurer l'image afin de retrouver la même qualité que l'image non marquée. Afin de garantir un plus haut niveau de sécurité, la marque introduite est cryptée à l'aide de l'algorithme de Vigenère.

Dans ce chapitre nous présentons les résultats obtenus pour chaque méthode. Quelques perspectives ou améliorations sont abordées pour conclure le chapitre.

5 4.2 Méthode Non-réversible

La méthode proposée consiste à tatouer une image sous compression *JPEG*, elle s'inscrit dans les méthodes virtuelles où la marque n'est pas ajoutée ni substituée, mais elle impose des contraintes aux valeurs de l'image [14].

La procédure s'appuie sur la quantification de l'image préalablement décorrelée par la DCT. Lors de l'incrustation de la marque, les coefficients sont judicieusement choisis d'une manière à ce que la distorsion introduite soit la moins visible possible et que le taux de compression soit maintenu, tout en ayant une bonne robustesse et une bonne capacité d'insertion. Le schéma de tatouage est détaillé dans le chapitre précédent et illustré par la figure 3.6.

Pour retrouver la marque insérée, nous devons décoder l'image marquée transmise par canal par la suite calculer la transformée inverse des sous blocs 8x8. Pour être en phase avec le codeur l'ensemble des coefficients est déquantifié.

L'extraction de la marque est aveugle et sera réalisée simplement par les relations (3.3) et (3.4), en effet dans le cadre de l'authentification et le contrôle d'images photographiques, outre, les caractéristiques qui sont la robustesse et l'imperceptibilité, l'extraction de la marque devra être aveugle.

A partir de l'image décompressée, nous récupérons le message dissimulé qui sera utilisé pour authentifier le document présenté ou pour rechercher l'image correspondante dans la banque de données. Cependant, cette transmission de données à travers un système de communication peut faire apparaître des erreurs sur les suites de données initiales. Pour compenser ces imperfections, le message introduit est répété un certain nombre de fois.

Le travail effectué consiste en premier lieu à étudier l'impact de la signature sur la qualité de l'image, et sur le taux d'insertion, et ce en insérant d'abord un seul bit par bloc DCT 8x8 quantifié, dans des emplacements différents, basses fréquences, moyennes fréquences et hautes fréquences, ensuite en insérant deux ou trois bits par bloc pour évaluer le seuil maximal du taux d'insertion.

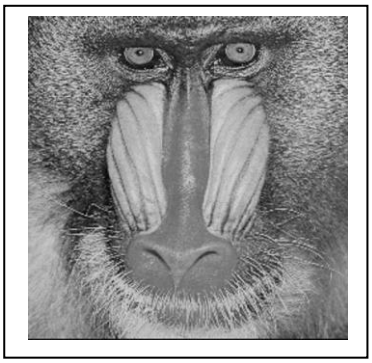
4.2.1 Résultats et interprétations

Afin d'évaluer les performances de l'algorithme proposé dans ce mémoire, nous nous sommes servis de douze images tests, de format BMP, de taille 256 x 256 et 512 x 512, codées en 256 niveaux de gris, illustrées par la figure 4.1. L'évaluation de ce schéma de tatouage se fait en trois étapes ; l'évaluation perceptuelle en terme de PSNR et wPSNR, l'évaluation du taux de compression et de la capacité d'insertion.

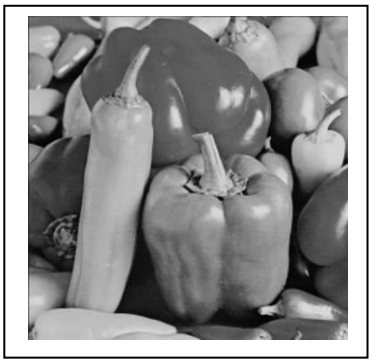
Lena

Eyes

Couple



Baboon



Pepper

Clown

Figure 4.1 : Images tests

4.2.1.1 Évaluation perceptuelle

Afin d'évaluer la meilleur qualité perceptuelle du tatouage, plusieurs essais ont été effectués sur différents coefficients pour déduire lequel porte le mieux la marque.
En premier lieu, les essais concernent l'insertion d'un bit, sur un coefficient de la zone, moyennes fréquences, deux autres insertions ont été faites dans la zone basses fréquences, dont le coefficient DC, la dernière insertion concerne un coefficient de la zone hautes fréquences. Les résultats sont exprimés dans les tableaux (4.1), (4.2), (4.3).

Dans le second cas on effectuera des insertions de deux, trois et quatre bits, dans différentes zones. Les résultats sont exprimés par les tableaux (4.4), (4.5), (4.6).

- Insertion d'un bit par bloc

Images	**Taille**	**Taux d'insertion**	**PSNR de l'image JPEG (dB)**	**Réduction du PSNR (dB)**	**wPSNR de l'image marquée (dB)**	**Variation du taux de compression (%)**
Lena	*512x512*	*4096*	40,629	0,4125	52,4504	-0,0131
Pepper	*512x512*	*4096*	40,280	0,4480	51,6243	-0,0056
Lena	*256x256*	*1024*	35,522	0,1400	54,6924	-0,0167
Pepper	*256x256*	*1024*	35,328	0,1490	53,8104	-0,0444

Tableau 4.1 : Insertion de la marque dans le coefficient DC.

Images	Taille	Taux d'insertion	PSNR de l'image JPEG (dB)	Réduction du PSNR (dB)	wPSNR de l'image Marquée (dB)	Variation du taux de compression (%)
Lena	*512x512*	*4096*	40,629	2,528	48,948	+ 7,2304
Pepper	*512x512*	*4096*	40,28	2,593	48,370	+ 7,5274
Lena	*256x256*	*1024*	35,522	0,955	52,649	+ 3,4641
Pepper	*256x256*	*1024*	35,328	0,761	52,013	+ 3,6844

Tableau 4.2 : Insertion de la marque dans la zone des moyennes fréquences.

Images	Taille	Taux d'insertion	PSNR de l'image JPEG (dB)	Réduction du PSNR (dB)	wPSNR de l'image Marquée (dB)	Variation du taux de compression (%)
Lena	*512x512*	*4096*	40,629	3,3	47,808	+ 7,7630
Pepper	*512x512*	*4096*	40,28	3,436	47,347	+ 7,7708
Lena	*256x256*	*1024*	35,522	1,357	51,819	+ 4,1575
Pepper	*256x256*	*1024*	35,328	1,407	51,285	+ 4,2454

Tableau 4.3 : Insertion de la marque dans la zone des hautes fréquences.

Tous les échantillons d'images marquées montrent une empreinte quasi identique à l'originale, une approche quantitative informe sur la qualité des images obtenues. Une note globale est traditionnellement donnée par le PSNR (Peak Signal to Noise Ratio) qui évalue les résiduels des pixels résultants de la mise en correspondance des images originales et marquées, dans notre cas les valeurs du PSNR sont nettement supérieures au seuil qui est de 30dB.

En ce qui concerne le wPSNR, rappelons qu'il permet de quantifier numériquement la visibilité de la marque en prenant en considération la variance de l'image. Plus le wPSNR est grand, moins la marque est visible dans les zones texturées (à variance élevée) de l'image, nous constatons également que les essais donnent de très bonnes valeurs le concernant. Néanmoins les meilleurs résultats perceptuels sont obtenus pour le marquage du coefficient DC.

Comme il a été cité précédemment (voir section 1.4.2.2), l'amplitude de la composante continue est positivement proportionnelle à la valeur moyenne des composantes du bloc d'origine, elle est également très proche d'un bloc au suivant de l'image, l'ampleur de celle-ci est beaucoup plus grande que celle de toutes les composantes AC.

Le tatouage des données peut être considéré comme comportant un ensemble de signaux sur un ensemble plus large de signaux de fond. Le signal intégré ne peut être détecté par le système visuel humain que quand il dépasse le seuil de détection de ce dernier. Pour être plus précis, la loi Fechner-Weber[13] stipule que le seuil de détection de la visibilité d'un signal intégré est proportionnel à l'ampleur du signal de fond. Ainsi, par rapport aux composantes AC, les composantes DC peuvent être modifiées par une plus grande quantité d'informations [35]. Cependant, les composants DC ne peuvent toujours pas être changées par un important pourcentage car des artefacts sont très susceptibles de se produire.

La figure 4.2, compare la qualité d'une image tatouée dans la composante DC et une autre image tatouée dans une composante AC, où l'image de couverture est de taille 512 × 512, à niveaux de gris. Selon les résultats, l'intégration des bits secrets dans les composants DC ne

[13] La **loi de Fechner-Weber** décrit la relation entretenue par la sensation avec la grandeur physique d'un stimulus « *la sensation varie comme le logarithme de l'excitation* ».

doit pas nécessairement entraîner une dégradation significative lorsque le taux de compression (facteur Q) est faible, mais elle conduit à une distorsion notable lorsque le taux de compression est élevé, ce qui diffère de ce qui se passe concernant les composantes AC.

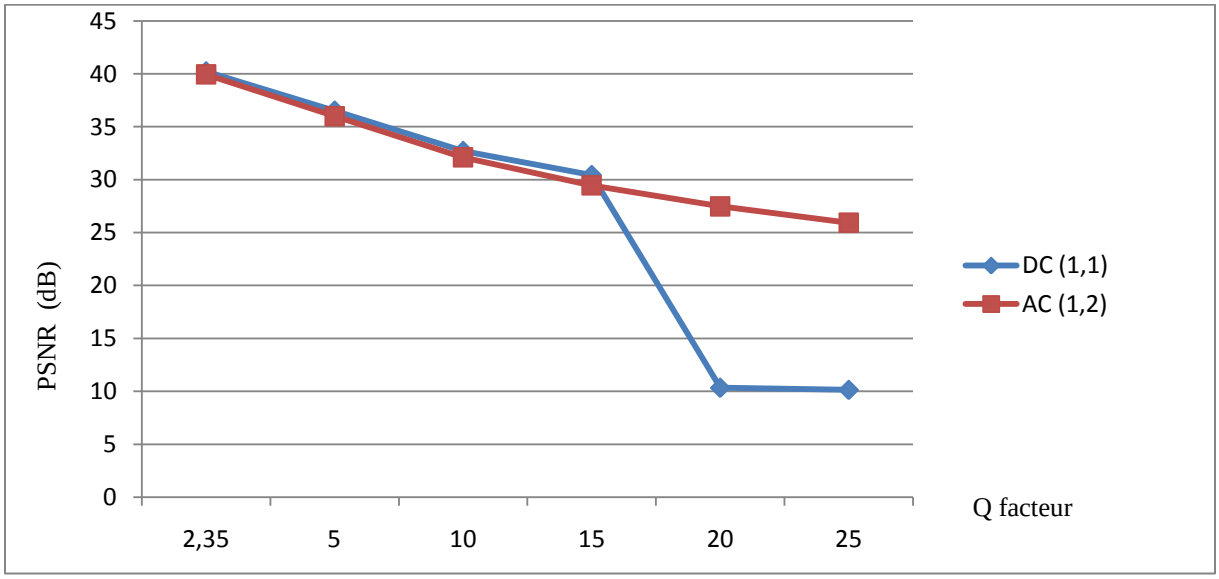
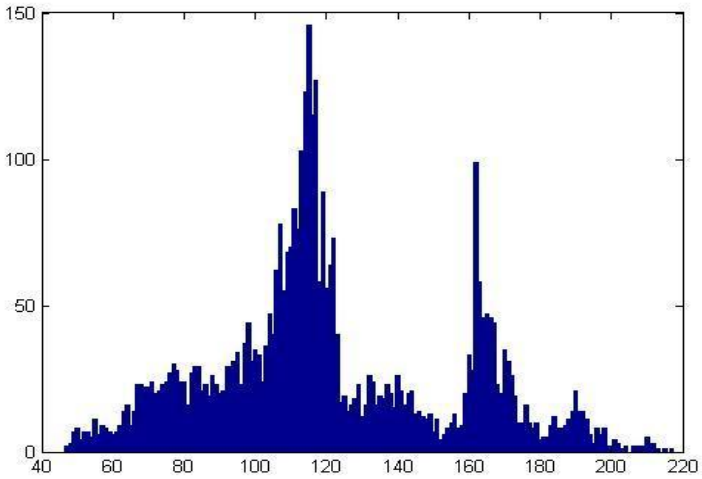


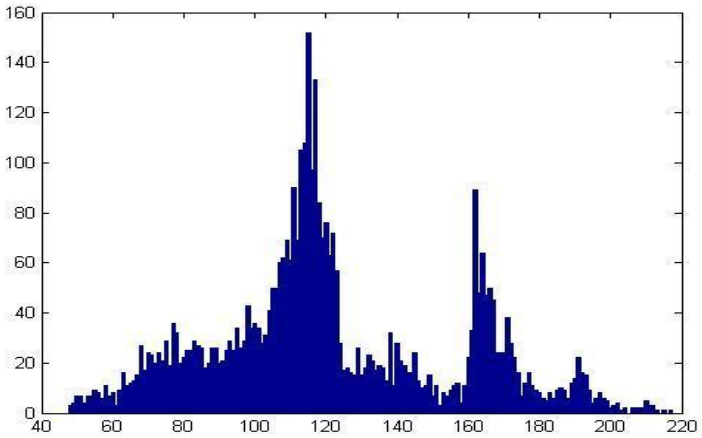
Figure 4.2 : Comportement du coefficient DC et AC sur l'image de Lena 512*512 en tatouant un seul bit par bloc.

Une autre approche est l'approche visuelle, elle fait appel à l'histogramme qui décrit la distribution des pixels des images.

Cette approche est basée sur une comparaison d'histogrammes des images avant et après insertion de la marque. Un exemple d'histogrammes de l'image Lena est représenté par la figure 4.3. Nous remarquons qu'il y a très peu de changements entre les deux histogrammes de l'image avant et après marquage, lorsqu'on introduit un seul bit par bloc.



Histogramme de l'image de Lena 256x256, compressée JPEG, avant marquage.



Histogramme de l'image de Lena 256x256, compressée JPEG, après marquage.

Figure 4.3 : Comparaison des histogrammes d'une image, avant , et après tatouage.

- Insertion de plus d'un bit par bloc

Images	Taille	Taux d'insertion	PSNR de l'image JPEG (dB)	Réduction du PSNR (dB)	wPSNR de l'image Marquée (dB)	Variation du taux de compression (%)
Lena	*512x512*	*8192*	40,629	1,059	51,279	+ 0,4174
Lena	*512x512*	*12288*	40,629	6,397	48,442	+ 1,7736
Lena	*512x512*	*16384*	40,629	6,164	47,718	+ 5,3623

Tableau 4.4: Insertion de la marque dans le coefficient DC et d'autres coefficients basses fréquences.

Images	Taille	Taux d'insertion	PSNR de l'image JPEG (dB)	Réduction du PSNR (dB)	wPSNR de l'image Marquée (dB)	Variation du taux de compression (%)
Lena	*512x512*	*8192*	40,629	2,611	48,868	+ 6,7770
Lena	*512x512*	*12288*	40,629	5,653	44,922	+ 19,7570
Lena	*512x512*	*16384*	40,629	9,982	45,57	+ 12,5965

Tableau 4.5: Insertion de la marque dans le coefficient DC et d'autres coefficients moyennes fréquences

Images	Taille	Taux d'insertion	PSNR de l'image JPEG (dB)	Réduction du PSNR (dB)	wPSRN de l'image Marquée (dB)	Variation du taux de compression (%)
Lena	*512x512*	*8192*	40,629	2,996	48,311	+ 7,3006
Lena	*512x512*	*12288*	40,629	4,781	45,970	+ 14,4060
Lena	*512x512*	*16384*	40,629	7,359	42,981	+ 20,0781

Tableau 4.6: Insertion de la marque dans le coefficient DC et d'autres coefficients hautes fréquences

Résultats :

- Le changement d'un seul ou deux bits LSB par bloc n'affecte pas grandement la qualité de l'image, ce qui s'explique par de très bonnes mesures concernant le PSNR et wPSNR, la distorsion introduite sur le DC sera répartie sur tout le bloc 8x8 lors de la reconstitution, la dégradation s'assimilera à un léger changement de luminosité de l'image. En effet les résultats montrent de petites variations de niveaux de gris sur l'image tatouée décompressée, (voir figure 4.4). Ces modifications de luminance semblent corrélées à la grande dispersion des coefficients TCD.

  Les lieux propices pour l'insertion de plus d'un bit par bloc restent la zone basses fréquences et en particulier le coefficient DC et les trois coefficients avoisinants, la raison et que généralement, c'est les seuls bits qui ne sont pas réduits à zéro lors de la quantification.

170	169	169	166	170	167	164	168
170	169	169	166	170	167	164	168
170	169	169	166	170	167	164	168
168	168	166	166	165	165	164	160
164	163	165	164	165	165	165	159
162	163	165	161	163	162	164	163
162	163	161	161	163	164	164	161
162	163	163	163	161	161	163	161

Bloc 8*8 de l'image originale

172	171	171	170	169	169	168	168
171	171	170	170	169	168	168	167
170	170	169	169	168	167	167	166
169	168	168	167	167	166	165	165
167	167	167	166	165	164	164	164
166	166	165	165	164	163	163	162
165	165	164	164	163	162	162	161
164	164	164	163	162	162	161	161

Le même bloc Après marquage

Figure 4 .4 : Distorsion introduite sur un bloc 8*8 de l'image de Lena 512*512.

- L'un des désavantages des méthodes où l'insertion se fait dans le domaine compressé, qu'elles soient substitutives ou additives, est l'accumulation de deux erreurs successives, qui sont la quantification et le tatouage.

  La méthode d'insertion proposée dans ce mémoire apporte une amélioration du fait qu'elle ne soit ni additive, ni substitutive (voir section 3.3.1), en effet en intégrant un tel schéma nous réduisons la dégradation finale. Pour cela l'approximation faite par la quantification et l'ajout de la marque sera minimisée. La qualité visuelle de l'image compressée marquée est ainsi améliorée.

- Une autre raison pour laquelle la dégradation est imperceptible, est que l'insertion est uniformisée c'est-à-dire qu'elle s'effectue pour les mêmes coefficients de chaque bloc. Dans le cas contraire chaque coefficient tatoué contribuera à une dégradation différente, ce qui donnera une image endommagée. La figure (4.5) nous illustre un tatouage effectué sur différents coefficients.

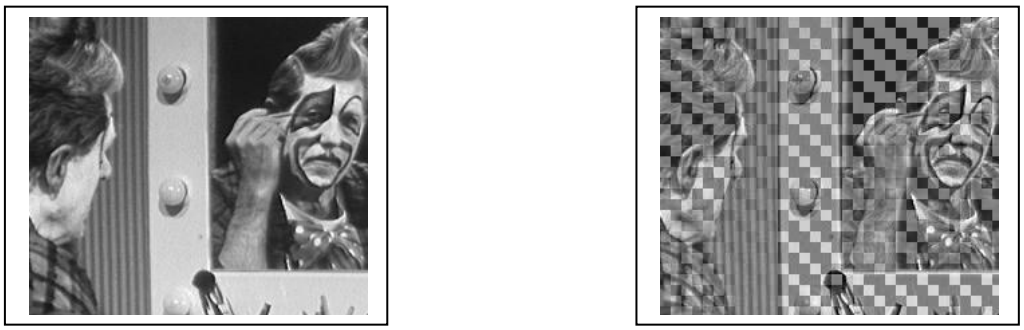


Figure 4.5 : Insertion d'un bit par bloc dans la zone basses fréquences, moyennes fréquences et hautes fréquences respectivement.

4.2.1.2 Évaluation de la capacité d'insertion

Le marquage d'un seul coefficient du bloc 8*8, nous confère une capacité d'insertion de ***4096*** bits pour une image ***512*512*** soit l'équivalent de ***586*** caractères en code ASCII. Afin d'améliorer cette capacité d'insertion d'autres tests ont été effectués en insérant deux coefficients et plus par bloc tout en gardant une très bonne qualité de l'image, les résultats sont résumés dans les tableaux (4.4), (4.5), (4.6), précédents.

Nous constatons qu'au-delà de l'insertion de deux bits par bloc, la distorsion introduite est visible, donc un seuil d'insertion sera donné de : **2048** bits pour les images ***256*256*** et de **8192** bits pour des images de ***512*512,*** dans le cas d'un codage ASCII sur 7 bits.

La figure (4.6) nous illustre la qualité d'image obtenue après insertion d'un, deux, trois et quatre bits pour des images différentes.

Résultats :

- Afin de maintenir le taux de compression, les coefficients choisis pour l'insertion appartiennent aux basses fréquences.

- La capacité d'insertion s'avère médiocre comparée à d'autres méthodes dont *JPEG/JSTEG*[14], en effet elle s'évalue entre ***0,19% et 0,78%*** de la taille de l'image, au-delà un effet de bloc apparait. Autrement dit le seuil maximal pour une image de 256x256 est de ***2048*** bits, soit ***410*** caractères et pour une image de 512x512 il est de ***8192*** bits, soit ***1638*** caractères, dans notre cas le codage se fait sur 5 bits.
  L'information à introduire pourrait subir certains prétraitements dont la compression.

[14] Elle consiste à tatouer les coefficients DCT de valeur absolue supérieure à 1.

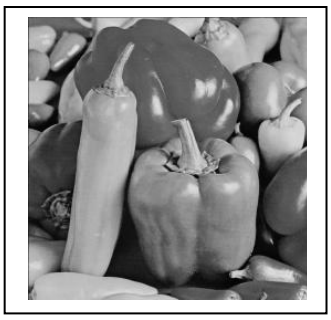
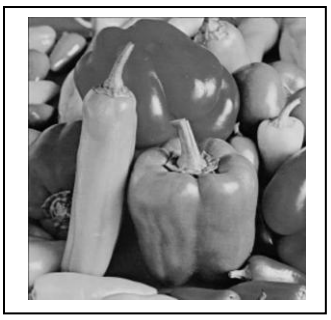
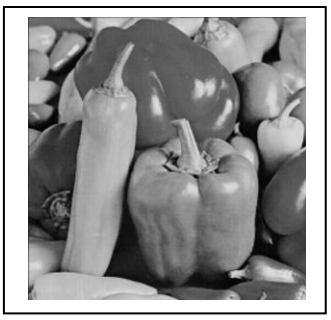


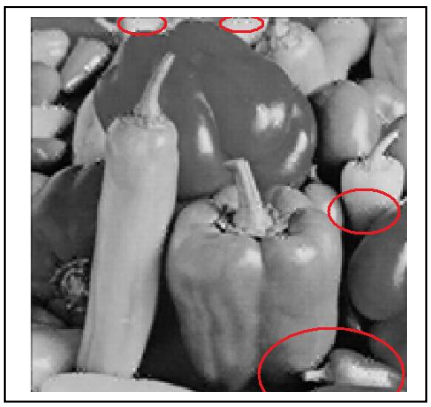
Image originale



coefficient DC tatoué



coefficient DC et AC tatoués



Trois bits tatoués

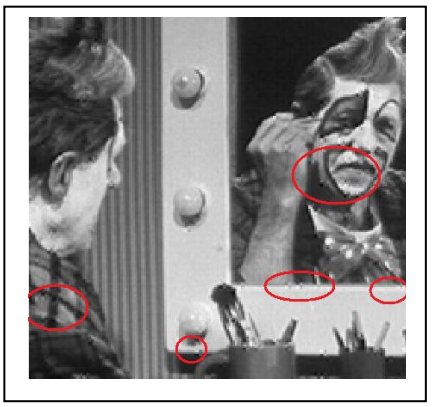
Quatre bits tatoués

Image originale

coefficient DC tatoué

coefficient DC et AC tatoués

Trois bits tatoués



Quatre bits tatoués

Figure 4.6: Evaluation de la capacité d'insertion

4.2.1.3 Evaluation du taux de compression

L'insertion d'un processus de tatouage dans un schéma de compression présente une autre contrainte, autres que la robustesse et la visibilité, qui est le taux de compression, en effet le but ne se limite pas à tatouer une image compressée mais également de maintenir son taux de compression avant marquage.

Une évaluation du taux de compression a été effectuée pour tous les schémas d'insertion précédents. Les figures (4.7), (4,8) nous illustrent ces résultats pour le cas d'un bit et de deux bits marqués.

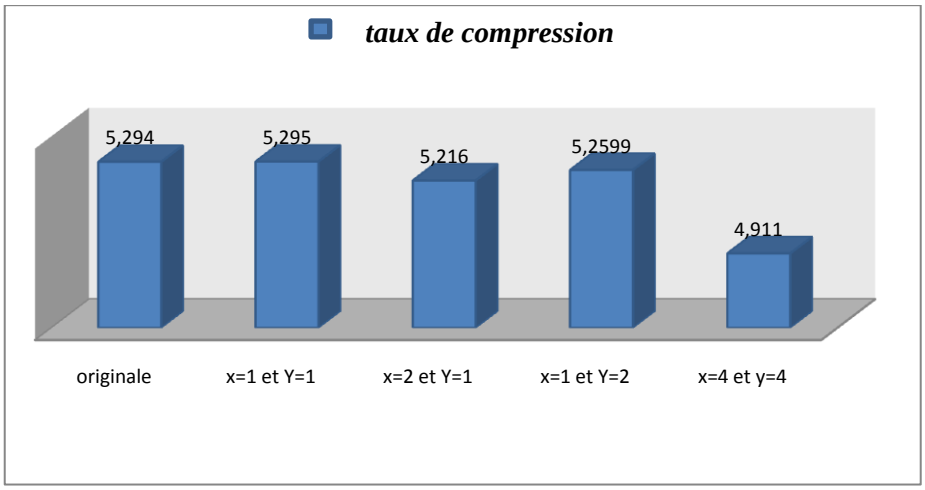


Figure 4. 7: Comparaison du taux de compression de différentes insertion d'un bit sur l'image de Lena 512*512

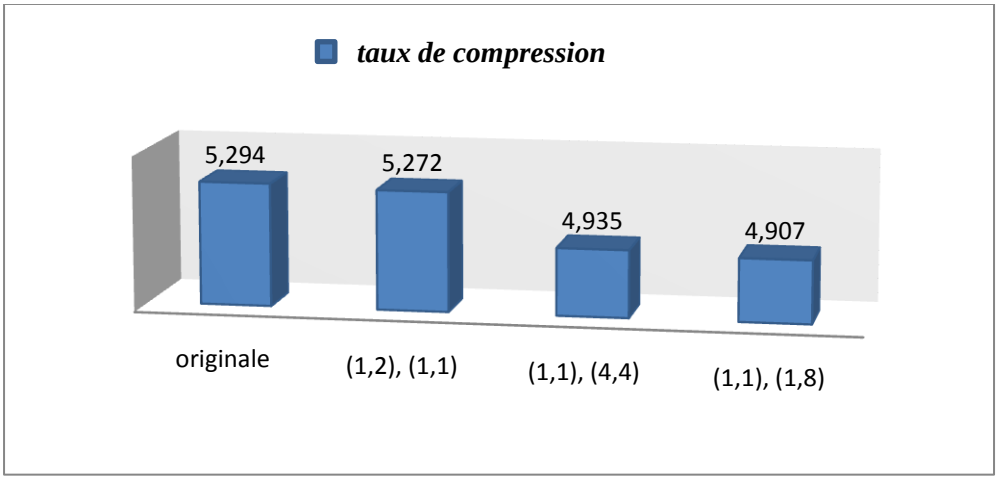


Figure 4.8: Comparaison du taux de compression de différentes insertion de deux bits sur l'image de Lena 512*512

Résultats :

- Grâce à la formule (3.2) on pourrait personnaliser la table de compression, ce qui nous permet de réduire ou d'augmenter le taux de compression au détriment de la qualité de l'image.

- Le fait de tatouer dans la zone basses fréquences (les coefficients qui ne sont pas réduits à zéro par la quantification) permet de maintenir le taux de compression.

4.2.4 Avantages et inconvénients

La méthode de tatouage d'image JPEG non réversible présente les avantages suivants :

- L'insertion de données dans le coefficient DC, révèle plusieurs avantages dont la robustesse [20], elle est assurée dans la mesure où toute attaque du coefficient DC entrainerait une perte significative de la qualité de l'image.

- Le tatouage doit constituer une preuve irréfutable. A cet effet, il convient d'assurer l'unicité et l'authenticité de l'identifiant, pour cela la marque subit un prétraitement, dans notre cas la marque est cryptée à l'aide de l'algorithme de Vigenère, sa sécurité repose sur une clé de cryptage (voir section 3.3.3), plus cette clé est longue plus le système est sûre, elle est donc robuste contre l'attaque de « copiage » qui consiste à prélever (recopier) une marque pour l'insérer dans une image non marquée. Cette dernière pourrait être considérée alors comme l'image authentique.

  Bien que la cryptographie suffit pour sécuriser la marque, on peut encore renforcer la sécurité en faisant un choix aléatoire des coefficients qui porteront la marque, à l'aide d'une clé qui est en possession uniquement des personnes ayant droits sur le document. Notre choix porte sur les coefficients de basses fréquences conformément aux résultats établis précédemment. Une autre sécurité est celle de répéter la marque un certain nombre de fois.

- C'est une méthode aveugle, elle consiste à extraire la marque de l'image à l'aide de la clef privée de détection, l'image originale n'est pas divulguée.

- C’est une méthode symétrique, en effet les algorithmes symétriques sont conçus pour chiffrer très rapidement d’importants volumes de données, également les clés des systèmes symétriques sont relativement courtes.

- L’insertion s’effectue en temps réel et ne ralentis pas le processus de compression.

- Elle possède une capacité d’insertion acceptable qui peut être de la taille de l’image voir même le double c'est-à-dire de 2048 bits pour une image 256x256 et de 4096 bits pour une image de 512x512.
- On peut gérer le taux de compression.

Une amélioration de la robustesse peut être apportée par la technique de l’étalement spectral où chaque bit de la marque sera représenté par plusieurs bits, c'est-à-dire par une séquence binaire pseudo aléatoire ce qui nous donne la possibilité de récupérer le bit du watermark même si on perd quelques bits de la séquence, ceci peut être fait en étalant le bit sur plusieurs blocs. L’inconvénient c’est qu’on perd de la capacité d’insertion.

Une autre amélioration peut être apportée vis-à-vis de la distorsion introduite après tatouage. Après l’étape de quantification au lieu de prendre l’arrondi le plus proche, on prend l’entier par défaut, par exemple le coefficient après quantification est de 9,6, et le bit à marquer et 0, la méthode utilisée retourna après arrondi la valeur 10, et après tatouage elle retourne la valeur 11, alors qu’en prenant l’entier, le coefficient quantifié tatoué serait égale à 10, ce qui est plus proche de 9,6.

Cette méthode présente un inconvénient concernant le taux de compression, en effet on n’est par libre d’avoir différent taux de compression, la raison est que le tatouage dans la zone basses fréquences est invisible seulement pour un taux de compression pas très élevé, les essais nous ont permis de donner une estimation concernant le facteur de qualité qui doit être compris entre 2,30 et 15, ce qui nécessite une étude plus approfondie de l'influence de la quantification sur les coefficients, permettant de faire un choix adéquat de l'insertion avec plus de liberté.

4.3 Méthodes réversibles

La plupart des méthodes de tatouage sont des méthodes non réversibles. Cela signifie qu'après insertion, l'image porteuse a été modifiée. Nous ne pouvons donc pas retrouver l'image originale et certaines informations importantes peuvent être perdues. Pour des applications particulières telles que l'imagerie médicale, le domaine militaire ou encore la conservation du patrimoine artistique ou à des fins commerciales, l'image originale doit absolument être conservée. Les méthodes de tatouage réversibles sont la réponse à cette question. Ces méthodes peuvent être utilisées pour associer à l'image des informations cruciales en offrant la possibilité de restaurer son contenu.

4.3.1 Résultats et interprétations

Dans notre application, cette méthode contrairement à la précédente ne ce soucis pas du PSNR de l'image marquée, puisque son but et d'introduire une distorsion visible, par contre le PSNR de l'image restituée doit être identique à l'image compressée sans marquage.

Concernant la capacité d'insertion, étant donné que la formule utilisée pour la réversibilité (voir la formule 3.7) introduit une grande distorsion, il est préférable de se limiter à une insertion d'un bit par bloc, d'une part pour que les détails de l'image restent visibles, et d'autre part pour que le taux de compression soit maintenu, en effet au delà de l'insertion d'un bit par bloc la réduction du taux de compression passe de 0,0509 % à 4 ,246 % pour l'insertion de trois bits par bloc. On évitera le coefficient DC où l'insertion peut conduire à un débordement qui causerait une erreur de détection.

Images	Taille	Taux d'insertion	PSNR de l'image JPEG	PSNR de l'image restituée	PSNR de l'image restaurée
Clown	*512x512*	4096	40,787	16,391	40,787
Baboon	*512x512*	4096	40,629	17,223	40,629
Clown	*512x512*	8192	40,787	16,437	40,629
Baboon	*512x512*	8192	40,629	16,965	40,629

Tableau 4.7: tableau récapitulatif de la méthode réversible

Image originale

Image JPEG

Image JPEG tatouée

Image restaurée

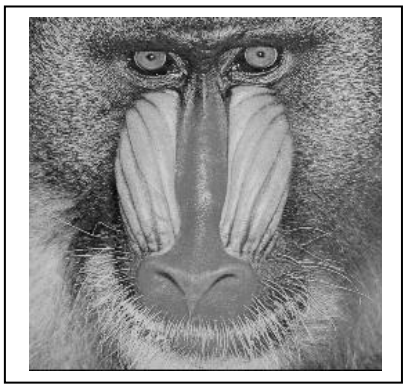


Image originale

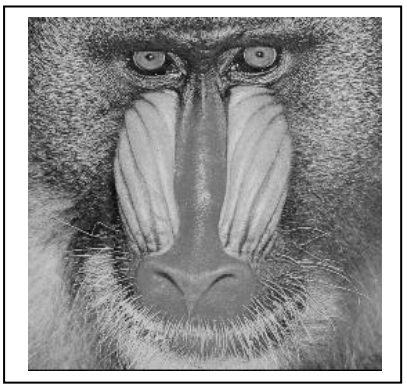


Image JPEG

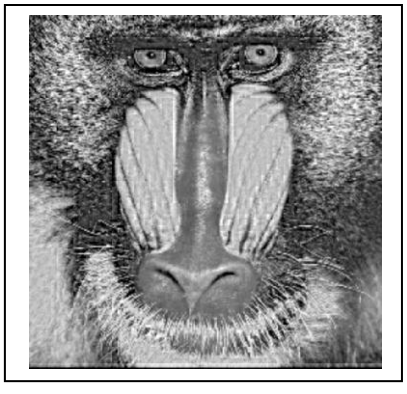


Image JPEG tatouée

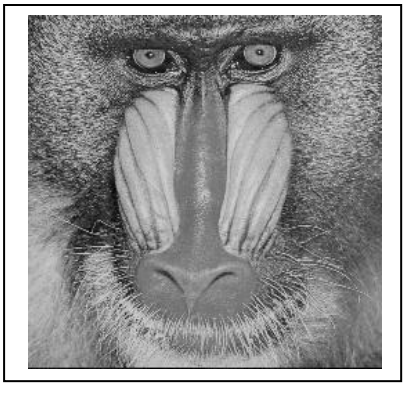


Image restaurée

Figure 4.9: Illustration du tatouage réversible.

4.3.2 Intérêts de la méthode réversible

Après extraction et vérification de la validité de la marque, les méthodes ***réversibles*** sont capables de restituer un duplicata exact de l'image compressée JPEG sans marquage. On pourrait imaginer leur application dans la protection du patrimoine artistique. Dans ce domaine le critère de réversibilité est primordial pour beaucoup de considérations d'ordre éthique.

En effet, afin de conserver et d'analyser le patrimoine muséologique, bon nombre de musée ont entrepris dès l'année 1992, la numérisation de leurs peintures ainsi que des images photographiques formant une base de données interne, juste les personne autorisées d'y accéder, possèdent la clé.

En effet, la marque insérée dans les images d'œuvres d'art peut contenir des informations sur la toile ou la photographie, son histoire, son état, etc.…, elle permettra alors d'accompagner chaque image d'un dossier entier la concernant. Afin de renseigner la personne intéressée (chercheur, enseignant, étudiant de l'histoire de l'art,…) sur l'œuvre, elle devra juste introduire la clé numérique pour extraire la marque et la clé de Vigenère pour la décrypter, l'image sera restituée à l'identique de l'image JPEG originale. La robustesse dans ce cas réside dans la connaissance des deux clés (cryptage et numérique).

Un tel outil permettrait dans le cadre du projet TSAR[15] de stocker toutes les images, accompagnées de leur dossier dans une base de données.

L'application peut être également d'ordre commercial. Ces dernières années les ventes des produits numériques à travers Internet ont proliféré, on pourrait actuellement télécharger des images photographiques à condition qu'on ait la clé numérique sur laquelle repose la sécurité de l'image, autrement elle n'a aucun intérêt commercial vu l'importance de la distorsion introduite.

4.4 Interface graphique

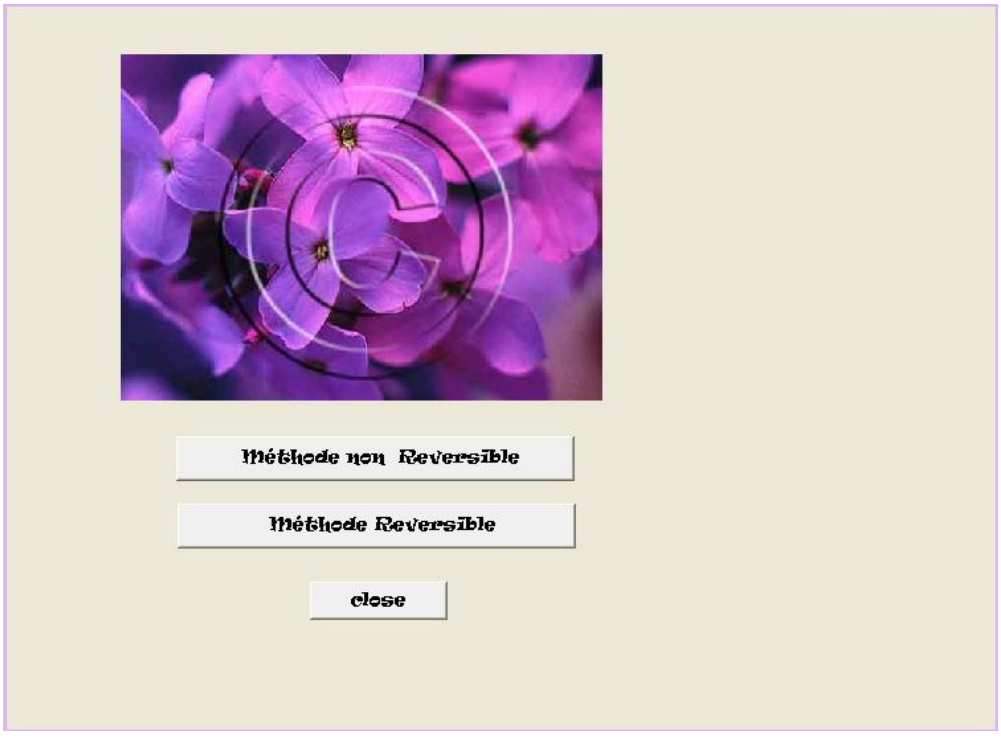
Afin de simplifier l'utilisation du schéma de tatouage et de le rendre convivial, une interface graphique a été conçue. Elle permet de personnaliser la table de quantification en introduisant le facteur de qualité, ainsi l'utilisateur pourra choisir la qualité de l'image obtenue et pourra

[15] ***T****ransfert* ***S****écurisé d'image d'****A****rt haute* ***R****ésolution.*

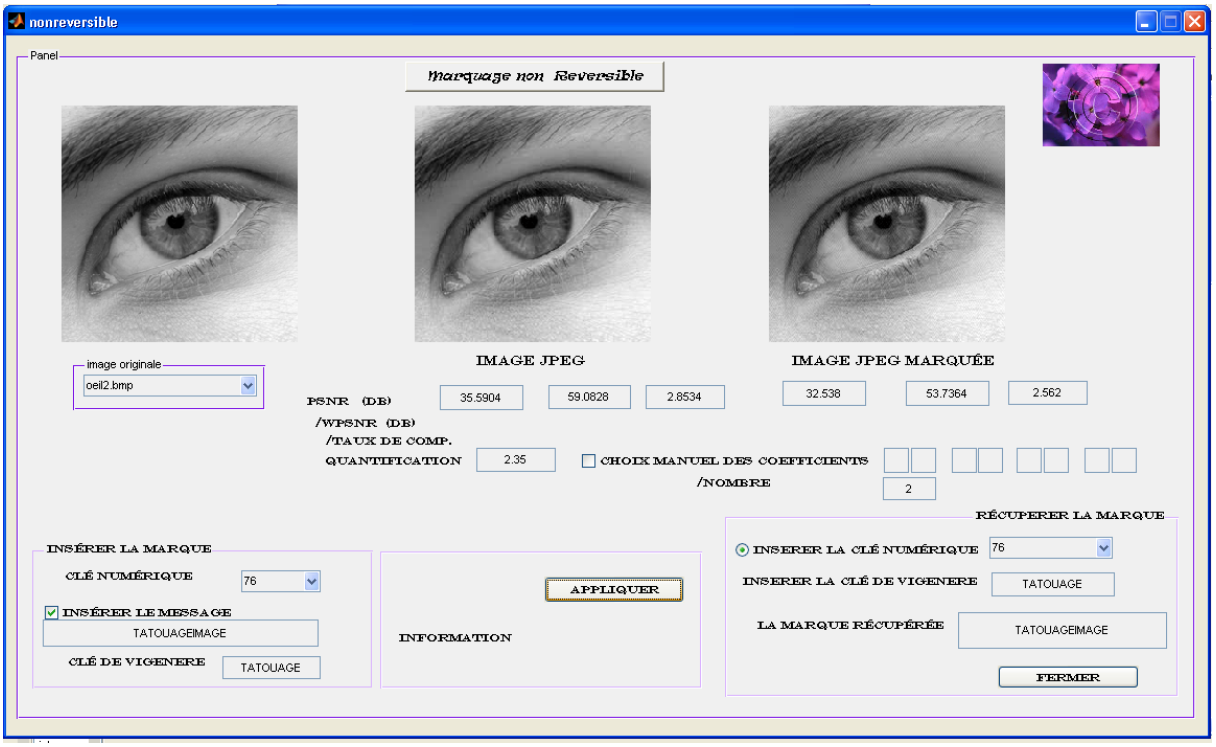
gérer l'espace mémoire qu'elle occupe. Il introduira également la marque dans les coefficients souhaités en choisissant un marquage non réversible, il pourra également générer aléatoirement les coefficients qui seront tatoués à l'aide d'une clé numérique.

Une fenêtre du tatouage réversible est disponible aussi, où les coefficients sont choisis aléatoirement dans la zone basses et moyennes fréquence à l'aide d'une clé numérique.
Pour les deux schémas de tatouage, il y a possibilité de crypter la marque introduite à l'aide de l'algorithme de Vigenère.

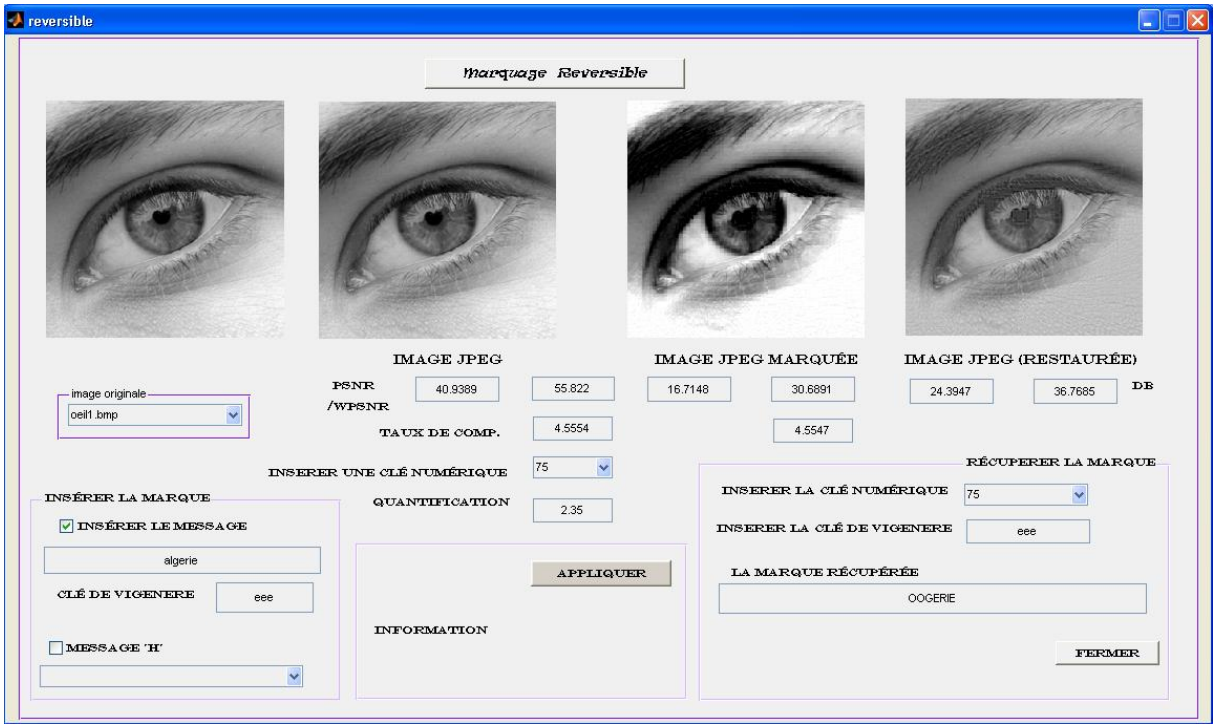
L'interface permettra de connaitre le *PSNR* et *wPSNR* ainsi que le taux de compression avant et après marquage, il aura également la possibilité de choisir les images tests. La figure (4.10) nous donne un aperçu de l'interface créée sous Matlab à l'aide de l'outil *GUI (graphic user interface).*



Page d'accueil de l'interface



Interface de la méthode non réversible



Interface de la méthode réversible

Figure 4.10 : Interface graphique

4.5 Conclusion

Ce chapitre résume les résultats obtenus en appliquant les deux méthodes réversible et non réversible.

Concernant la méthode non réversible les meilleurs résultats sont obtenus pour l'insertion dans le coefficient DC, jusqu'à un certain taux de compression, nous avons pu également insérer jusqu'à 2048 bits pour une image 256x256 et 4096 bits pour une image 512x512 sans qu'il y est une distorsion visible, et ce pour une réduction du taux de compression négligeable.

Cette méthode peut être utilisée pour le contrôle de l'authenticité du document, elle pourrait éventuellement être utilisée dans le contrôle de la traçabilité du document, en cas où il y aurait distribution de copies illégales, ce type de tatouage pourrait remonter jusqu'au premier propriétaire.

En ce qui concerne la méthode réversible, la qualité de l'image restera médiocre pour les personnes non autorisée à l'exploiter, par contre elle permet une récupération parfaite de l'image compressée *JPEG* pour les personnes possédants la clé.

Cette méthode pourrait être appliquée dans les banques de données des musées où chaque image pourra être accompagnée de son dossier, elle pourrait également être utilisée dans la vente de photographies sur internet, seule la personne possédant la clé, pourra restituer la qualité de l'image originale.

CONCLUSION GENERALE

La plupart des travaux étudiants les techniques de tatouage d'images, considèrent la compression comme une attaque, en ce qui nous concerne, la compression ne constitue pas une source d'interférence. Notre travail consiste à l'application d'une méthode dans laquelle l'information adjacente est non pas le signal original mais le signal comprimé, en ajoutant une étape d'insertion dans le schéma général de compression.

Nos motivations reposent sur plusieurs points, parmi lesquels l'intérêt et la diversité des applications du tatouage, la dualité entre tatouage et compression, et le fait que la compression représente un passage obligatoire du stockage ou du transfert d'images. Notre choix a été fait sur le format *JPEG*, puisqu'il est le plus populaire en ce qui concerne les images numériques.

Dans un premier temps une méthode de tatouage non réversible est proposée, elle consiste à rajouter une étape de tatouage après l'étape de quantification, du schéma de compression *JPEG*. Nous avons pour cela utilisé une méthode d'insertion adaptative, capable de conserver une bonne qualité visuelle de l'image, tout en ayant une bonne capacité d'insertion, et ce en maintenant le taux de compression, dans un mode d'extraction aveugle. Cette approche réalise ainsi une première solution de tatouage et compression combinés.

Afin d'améliorer les performances de cette méthode, en particulier en termes de sécurité, des outils de cryptographie ont été associés à la méthode de base. Des tests concernant la capacité d'insertion ont été également effectués, et qui ont abouti à l'établissement d'un seuil maximal d'insertion, pour des images de taille 256x256 et 512x512.

Cette méthode voit son utilité dans la vérification de l'authenticité de l'image et assure la confidentialité des données marquées. Elle pourrait éventuellement être utilisée dans le suivi des copies illégales, et ce en marquant l'image avec les données des acquéreurs.

Une seconde méthode est proposée, qui permet une récupération d'une image quasi identique à l'image non marquée, il s'agit d'une méthode de tatouage réversible. Elle est utilisée dans des applications particulières telles que l'imagerie médicale, le domaine militaire ou encore la conservation du patrimoine artistique ou à des fins commerciales, où l'image originale doit absolument être conservée. Ces méthodes peuvent être utilisées pour associer à l'image des informations cruciales, telles que le nom du destinataire, des informations sur l'œuvre, ou l'empreinte de l'image originale, sans changer le contenu de celle-ci. L'extraction de la marque est accessible uniquement aux personnes détentrices de la clé de sélection aléatoire des coefficients, et de la clé de cryptage.

Enfin, plusieurs perspectives peuvent être envisagées, comme l'insertion de données par modification de la matrice de quantification. Cette méthode d'insertion propose de choisir des coefficients qui ne seront pas quantifiés et pourront intégrer l'information sans dégrader l'image. La capacité est connue à l'avance et dépend simplement du nombre de coefficients non quantifiés.

Une autre méthode est envisagée, qui consiste à l'insertion de données adaptée au système visuelle humain. Une étude sur les caractéristiques des zones texturées de l'image originale pourrait conduire à une meilleure sélection des blocs porteurs de la marque et ce en masquant le tatouage dans les zones hétérogène de l'image.

Concernant la méthode de tatouage réversible, une nouvelle méthode basée sur la technique de l'étalement spectral peut être appliquée. En effet, même si cette technique pourrait réduire la capacité d'insertion, sa formule d'insertion (section 3.3.2) pourrait mieux maintenir le taux de compression et offrirait un meilleur contrôle de la distorsion de l'image.

Annexes

Annexe A : Les attaques

1. Introduction

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors de son extraction [23]. Dans la littérature, la classification des attaques se fait sur différents critères, dans [14] l'idée est d'étudier les attaques selon l'étape du tatouage qu'elles mettent en défaut c'est-à-dire lors du processus d'insertion ou d'extraction. Hurtung propose de classer les attaques en quatre catégories : suppression ou détérioration de la marque, attaques de synchronisation, attaques cryptographique et attaques de confusion. La classification que nous avons choisie est celle de la thèse [12], qui divise les attaques en deux catégories : non intentionnelles et intentionnelles.

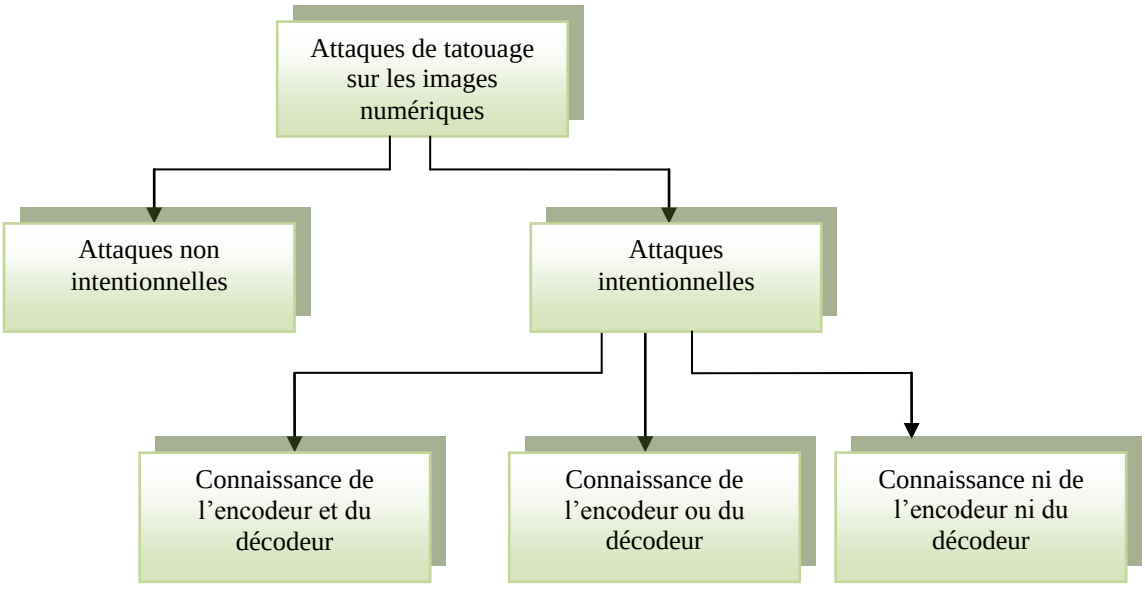


Figure A.1: Classifications des attaques sur les schémas de tatouage [12]

2. Attaques non intentionnelles ou innocentes

Ce sont des manipulations usuelles afin d'optimiser la qualité de l'image, ou pour son enregistrement comme l'utilisation de la compression. Ces manipulations peuvent apporter des distorsions importantes à la signature. Nous citerons ci-dessous les manipulations les plus courantes :

- ✓ ***La compression d'image***

La compression avec pertes est le mode de compression le plus utilisé, (pratiquement toutes les données audio, vidéo et images qui sont actuellement distribuées par l'intermédiaire de l'Internet ont été compressées). Elle a pour but de diminuer la taille du fichier image, comme détaillé dans le chapitre I. Les techniques de compression avec pertes suppriment les informations redondantes des images, comme la marque n'est pas généralement visible, elle peut donc être considérée comme non significative et être supprimée.

Si la marque doit résister à différents niveaux de compression, il est recommandé de l'insérer dans le même domaine où la compression a eu lieu. Par exemple, le watermarking d'image dans le domaine de DCT est plus robuste à la compression de JPEG.

(a)

(b)

Figure A.2 : Effet de la compression : (a) image originale (b) image compressée

- ***Rehaussement et lissage***

Le rehaussement correspond à l'augmentation des composantes hautes fréquences de l'image. Elle devient alors plus contrastée. Le lissage est l'opération contraire du rehaussement, il atténue les composantes hautes fréquences de l'image qui devient alors plus floue.

Ces opérations peuvent modifier également les composantes hautes fréquences du message et leur faire perdre leurs particularités.

- ***Transformations géométriques usuelles***

Parmi les transformations géométriques, les plus usuelles sont, la modification des dimensions de l'image et les transformations affines telles que la rotation, la translation, la symétrie, conversion analogique/numérique et le zoom. Ce genre de transformation provoque dans la plupart des cas une désynchronisation de la marque insérée lors de la détection et de l'extraction.

3. Attaques intentionnelles

Ces manipulations peuvent être vues comme des attaques malveillantes qui visent à la suppression, modification ou détérioration du message. Selon [12] elles se divisent en trois catégories selon la connaissance ou non du encodeur /décodeur.

- ***Connaissance de l'encodeur et du décodeur***

L'attaquant va chercher à introduire de l'ambigüité lors de la phase de détection en faisant un surmarquage par exemple [16], qui consiste à tatouer à nouveau une image déjà tatouée. La nouvelle signature w' est insérée de la même méthode que pour la signature authentique. Une nouvelle image tatouée est construite: $I_w^{'}=I_w+w'$ en disant que l'original est I_w alors que $I_w=I+w$.

- ***Connaissance de l'encodeur ou du décodeur***

L'attaque dite de collusion[16] a lieu lorsqu'il y a possession du même document portant plusieurs marques différentes.

[16] Entente secrète en vue de tromper quelqu'un (définition Larousse)

La mise en commun de ces documents permet de nombreuses opérations telles que :moyenne [43], en effet l'image résultante de la moyenne des images tatouées aura la même qualité que ces dernières. Elle contiendra toutes les marques, leurs amplitudes étant fortement diminuées. La détection sera alors perturbée à la fois par cette baisse d'amplitude et de possibles interférences entre les marques. Plus le nombre d'images utilisé est élevé plus il y a de chance que la marque disparaisse.

Kalker et al [44] ont proposé une méthode connaissant les failles du décodeur, qui consiste à compresser l'image tatouée suffisamment pour qu'aucun message ne soit détecté, par la suite des séquences binaire pseudo aléatoire sont ajoutées. Si lors de la détection cette séquence (Vi) est reconnue positive, on la considère comme hypothèse du signal ajouté dans le cas contraire ca sera (–Vi) qui sera prise comme hypothèse.
Ce processus est répété N fois, et une estimée de la marque insérée est la moyenne de ces N hypothèses, de préférence prendre N très grand.
Cette méthode est particulièrement efficace dans les schémas de détection et non d'extraction.

✓ *Attaques ne connaissant ni l'encodeur ni le décodeur*

Les données tatouées sont souvent distribuées sans aucune connaissance de la façon dont la marque a été créée ou comment elle sera détectée.
Les attaques les plus pénalisantes dans cette section sont celles qui visent à désynchroniser la marque avant l'étape de détection. Nous citerons :

- Attaque « Jitter» [28] : Le gigue (Jittering) est un phénomène connu en télécommunications. Lorsque le délai de transmission du signal varie, il en résulte une réplication ou une suppression d'un morceau du signal. Sur les images, il peut y avoir un ajout ou une suppression de lignes ou de colonnes.

- Attaque par mosaïques, permet d'invalider la détection sans pour autant supprimer la marque. Elle utilise le fait qu'on ne peut pas tatouer d'images de trop petite taille. Il s'agit de découper l'image marquée en plusieurs imagettes. L'objectif de cette attaque et non pas de détruire la marque, mais de tremper le détecteur.

Figure A.3: illustration de l'attaque mosaïque sur l'image de Barbara

Annexe B : Les bancs de tests

1 .Introduction

Toutes les attaques citées ci-dessus nous amènent à nous poser une question : comment évaluer et comparer différentes méthodes de marquages. Un banc d'essai (des logiciels standard dans notre cas) est nécessaire pour mettre en évidence les caractéristiques des algorithmes.

De nombreuses publications [6] : [25], [26], [27], [28] abordent cependant le sujet. Des outils et des projets de recherche Octalis [29], Optimark, CheckMark et Certimark tentent d'y apporter des solutions.

1.1 Stirmark

La première version de Stirmark[17] a été publiée comme un outil générique pour tester la robustesse de l'image, en introduisant des distorsions géométriques. Stirmark est actuellement en version 4.0, et continue d'évoluer.

Parmi les fonctionnalités que propose le logiciel sont : le calcul du PSNR de l'image après insertion de la signature avec différentes forces de marquage, le calcul du temps nécessaire à l'insertion de la signature et bien évidement les attaques géométriques citées dans la section (2.5.1.1).

Pour chaque image attaquée, le banc d'essai évalue l'algorithme en un score de 1 si la signature est toujours détectable et de zéro dans le cas contraire. Ce banc de mesure est très efficace, très peu d'algorithme de tatouage d'images y sont robustes.

[17] http://www.petitcolas.net/fabien/watermarking/stirmark/index.html

1.2 Checkmark[18]

Ce qui fait la différence avec Stirmark est qu'il prend en considération le contenu de l'image autrement dit le Système Visuel Humain (HVS) en utilisant le PSNR pondéré (wPSNR) et Watson métriques. Il a introduit également toute une batterie d'attaques en plus de celle connues de Stirmark dont : compression par ondelettes, attaque de copie. On peut noter que Checkmark n'a plus subi d'évolution depuis le 14 décembre 2001.

1.3 Optimark

Optimark fournit en plus des deux autres cités précédemment, la performance des algorithmes en termes de capacité d'insertion et du temps d'exécution. La dernière version du logiciel date du 29 janvier 2002.

1.4 Certimark

Avec le développement croissant de nombreux algorithmes de tatouage, la nécessité de définir des normes internationales est devenue une priorité pour la communauté du tatouage d'images. Le projet européen Certimark (**CERT**fication for water**MARK**ing techniques), débuté en 2000 et arrivé à terme fin 2002, a pour but d'obtenir une structure de banc qui est commune et flexible en développant un banc de test complet pour les schémas de tatouage et faire en sorte qu'il soit une référence aussi bien pour le fournisseur que pour les consommateurs sans oublier d'établir un processus de certification pour les algorithmes de tatouage.

[18] : http://watermarking.unige.ch/Checkmark/index.html

Annexe C : Les algorithmes

1 . variables initiales
// I : image originale, // q : facteur de qualité, // wi : Bit à insérer
// i , j :Le numéro de ligne et de colonne ; // s, g : numéro du bloc ;

2. ***Application de la DCT***
I_{DCT} = DCT (I) ;

3. Quantification
// introduire q
*// calcul de la matrice de quantification : Q_matrix(k,l) = 1 +(1 + k + l)*q*
// faire l'arrondi des coefficients quantifiés (dc_coeff_quant)

4. Introduction de la clé de sélection aléatoire

5. Introduction de la clé de chiffrement et la marque

```
for s=0:31
   for g=0:31
      dc_coeff_quant= dc_coeff_quant (8*s+1,8*g+1);
      a= mod ( dc_coeff_quant,2);  // vérification de la parité
if a==1
                 if wi==1
                 dc_coeff_quant=dc_coeff_quant+1;
               else
                 dc_coeff_quant=dc_coeff_quant ;
               end

else
     if wi==1
                 dc_coeff_quant=dc_coeff_quant;
      else
                  dc_coeff_quant=dc_coeff_quant+1;
      end
end
  end
     end
```

6. Codage
// lecture en Zigzag
// Codage Huffman
// codage RLE

7. obtention de l'image JPEG

Algorithme C1 : Insertion de la marque de la méthode non réversible

1. décodage
// lecture en Zigzag
// décodage Huffman
// décodage RLE
// obtention de la matrice « b_decode »

2. introduction de la clé de sélection aléatoire

3. extraction de la marque

```
for s=0:31
   for g=0:31
      dc_coeff_dequant= b_decode(8*s+1,8*g+1);
      d=mod (dc_coeff_dequant,2); // contrôle de parité
        if d==0
            wi=1;
        else
            wi=0;
        end
     end
end
```

4. Introduction de la clé de déchiffrement

5. Récupération de la marque

6. déQuantification

7. *Application de la DCT^{-1}* et *reconstitution de l'image marquée*

$I^*=DCT^{-1}(Id)$

// I*: image marquée
// Id: image déquantifiée

Algorithme C2 : extraction de la marque de la méthode non réversible

1 . variables initiales
// I : image originale, // q : facteur de qualité, // wi : Bit à insérer
// i , j :Le numéro de ligne et colonne ; // s, g : numéro du bloc ;
// dc_coeff_quant :coefficient DCT quantifié
//dc_coeff_quant_marqué : coefficient DCT quantifié marqué

2. *Application de la DCT*
I_{DCT} = DCT (I) ;

3. Quantification
// introduire q
// calcul de la matrice de quantification : *Q_matrix(k,l) = 1 +(1 + k + l)*q*
// dc_coeff_quant(l,k)= round [I_{DCT} */ Q_matrix(k,l)]*

4. Introduction de la clé de sélection aléatoire

5. Introduction de la clé de chiffrement et la marque

for s=0:31
  for g=0:31
    dc_coeff_quant = dc_coeff_quant (8*s+1,8*g+1);
    dc_coeff_quant_marqué = 2* dc_coeff_quant + w_i
  end
end

6. Codage
// lecture en Zigzag
// Codage Huffman
// codage RLE

7. obtention de l'image JPEG

Algorithme C 3: Insertion de la marque de la méthode réversible

1. décodage
// lecture en Zigzag
// décodage Huffman
// décodage RLE
// obtention de la matrice « b_decode »

2. introduction de la clé de sélection aléatoire

3. extraction de la marque

If dc_coeff_quant_marqué mod 2 =1
Wi = 1
else
Wi = 0
end

4. Introduction de la clé de déchiffrement

5. Récupération de la marque

6. déQuantification

7. *Application de la DCT^{-1}* et *reconstitution de l'image*

$I_{reconstituée} = DCT^{-1}(Id)$

// $I_{reconstituée}$: image reconstituée
// Id: image déquantifiée

8. Restaurer l'image JPEG originale

$I_{restaurée} = (I_{reconstituée} - Wi)/ 2$

Algorithme C 4: Extraction de la marque de la méthode réversible

BIBLIOGRAPHIE

[1] J.P. GUILLOIS, Techniques de compression des images, collection informatique, Hermes, pages 3-135, 1996.

[2] J. MARCONI, M. RODRIGUES, Transfert sécurisé d'images par combinaison de techniques de compression, cryptage et marquage, thèse de doctorat, université de Montpellier II, sciences et techniques du Languedoc, Octobre 2006.

[3] J.M MOUREAUX, Quantification vectorielle algébrique : un outil performant pour la compression et le tatouage d'images fixes, Thèse de doctorat, Université Henri Poincaré, Nancy 1, Décembre 2007.

[4] G. K. WALLACE, The JPEG Still Picture Compression Standard, publication in IEEE, Transactions on Consumer Electronics, December 1991.

[5] F. DOUAK, Reconstitution des Images Compressées en utilisant les Réseaux de Neurones artificiels et la DCT, thèse de magistère, université de Batna, faculté des sciences de l'ingénieur, 2008.

[6] G.CHAREYRON, Tatouage d'images : Une approche couleur, thèse de doctorat, université de Jean Monnet, Saint Etienne, Décembre 2005.

[7] F.A.P. PETICOLAS, La cryptographie militaire, journal des sciences militaires, Janvier 1883.

[8] A.KERCKHOFFS, La cryptographie militaire, journal des sciences militaires, Volume 6, pages 2969-2972,1998.

[9] W.DIFFIE, M.E. HELLMAN, New Directions in Cryptography, IEEE Transactions on Information Theory, n ^{o} 6, pages: 644-654, 1976.

[10] C. REY, Tatouage d'image : Gain en robustesse et intégrité des images, thèse de doctorat, université d'Avignon et des Pays de Vaucluse, Février 2003.

[11] G.J.SIMMONS, The History of Subliminal Channels, Lecture Notes in Computer Science, 1996.

[12] B.VASSAUX, Technique multicouches pour le tatouage d'images et adaptation aux flux vidéo MPEG-2 et MPEG-4, Thèse de Doctorat, Institut National Polytechnique de Grenoble, 2003.

[13] V. MARTIN, Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique, thèse de doctorat, institut national polytechnique de Toulouse, Novembre 2006.

[14] A. MANOURY, Tatouage d'images numériques par paquets d'ondelettes, thèse de doctorat, Ecole Centrale de Nantes et Université de Nantes, 2001.

[15] P. W. WONG, N MEMON, Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Transactions on Image Processing, October 2001.

[16] S. CRAVER, N. MEMON, B.L. YEO, and M.M. YEUNG. Can invisible watermarks resolve rightful ownerships, Technical report, 1996.

[17] P. BAS, Méthode de Tatouage d'image fondé sur le contenu, thèse de doctorat, Institut National Polytechnique de Grenoble, 2000.

[18] W. BENDER, D. GRUHL, N. MORIMOTO and A. LU, Techniques for data hiding, IBM Systems Journal, pages:313_336, 1996.

[19] B. GIROD, F. HARTUNG and J.K. SU, Spread Spectrum Watermarking: Malicious Attacks and Counterattacks, Telecommunications Laboratory, University of Erlangen-Nuremberg, Proc. SPIE, volume 3657, 1999.

[20] J.COX, MATT L. MILLER, A review of watermarking and the importance of perceptual modeling, Proc.of Electronic Imaging' 97, February 1997.

[21] T.PUN and J.J.K.O Ruanaidh, Rotation, Translation and Scale invariant digital image watermarking, in IEEE Signal Processing Society, International Conference on image processing(ICIP'97)Santa Barbara, California, Octobre 1997.

[22] D.HATZINAKOS, D. KUNDER, Digital Watermarking using multiresolustion wavelet decomposition, Proc.of IEEE Int. Conf. On Acoustics,Speech and Signal Processing, Volume.6, pages 2969-2972, 1998.

[23] F.A.P. PETICOLAS, M.G. KUHUN and R. J. ANDERSON, Attacks on copyright marking systems, Second workshop on Information Hiding, in Volume 1525 of Lecture Notes in Computer Science, Portland, Oregon, USA, pages 213-238, April 1998.

[24] J.L OLIVES, Optimisation globale d'un système imageur à l'aide de critère de qualité visuelle, thèse de doctorat, Ecole Nationale Supérieure de l'Aéronautique et de l'Espace, Toulouse, France, 1998.

[25] J. FRIDRICH and M. GOLJAN. Comparing robustness of watermarking techniques. In Proceedings of SPIE, Electronic Imaging'99, Security and Watermarking of Multimedia Contents, volume 3657, Janvier 1999.

[26] M. KUTTER and F.A. PETITCOLAS, Fair benchmark for image watermarking systems. In Proceedings of SPIE, Electronic Imaging'99, Security and Watermarking of Multimedia Contents, volume 3657, Janvier 1999.

[27] R.J.ANDERSO, F.A. PETITCOLAS, Weakness of Copyright Marking Systems. In Multimedia and Security – Workshop at ACM MM, volume. 41, pages. 55-61, Bristol, UK, September. 1998.

[28] R.J. ANDERSON, M.G. KUHN, F. PETITCOLAS , Attacks on copyright marking systems, in Proceedings Second International worshop on Information Hiding, Portland, in volume :1525 of lecture notes in computer science, pages 218-238, April 1998.

[29] J.M. BOUCQUEAU, M. KUTTER, L. PIRON, Octalis benchmarking: comparisons of three watermarking techniques. In Proceedings of SPIE, Electronic Imaging'99, Security and Watermarking of Multimedia Contents, volume: 3657, Janvier 1999.

[30] F. DAVOINE, S. PATEUX, Tatouage de documents audiovisuels numériques, Traité IC2, TSI, Hermès Lavoisier, 2004.

[31] P. CAMPISI, D. HATZINAKOS, D. KUNDUR and A. NERI, Compressive data hiding: an unconventional approach for improved color image coding, Eurasip Journal on Applied Signal Processing : Special issue on emerging applications of data hiding, volume: 2002, pages. 152-163, February 2002.

[32] C. HERLEY, Why watermarking is nonsense, Signal Processing Magazine, IEEE, pages: 10–11, 2002.

[33] S.K. AMIRGHOLIPOUR, A.R. NAGHSH-NILCHI, Robust Digital Image Watermarking Based on Joint DWT-DCT, International Journal of Digital Content Technology and its Applications volume. 3, Number 2, June 2009.

[34] G.A. BORS, I. PITAS, Image Watermarking using block site selection and DCT domain constriaints, Optics Express, Volume. 3, Issue 12, pages. 512-523, 1998.

[35] Chin-Chen CHANG, Hsien-Wen TSENG, High Capacity Data Hiding in JPEG-Compressed Images, INFORMATICA, Volume. 15, Number. 1, 127–142, 2004.

[36] N. MATEEV and L.ZHOU, Watermarking JPEG Images, Rapport technique, Department of Computer Science, Cornell University, Ithaca, NY , 1996. Sur le site http://www.cs.cornell.edu/home/mateev/Watermark/watermarkingJPEG.html, consulté en Mars 2010.

[37] Yu-Chang HSU, Chuen-Ching WANG, New watermarking algorithm with data authentication and reduction for JPEG image. J. Electron. Imaging, Volume 17, 2008.

[38] Irena OROVIC ,Srdjan STANKOVIC,Nikola ŽARIC, Robust watermarking procedure based on JPEG discrete cosine transform image compression, Journal of Electronic Imaging,Volume. 17(4), October–December 2008.

[39] Peter H. W. Wong, Oscar C. Au, Justy W. C. Wong, A Data Hiding Technique in JPEG Compressed Domain, IEEE International Conference on Image Processing, 2002 .

[40] Guorong Xuan, Yun Q. Shi, Zhicheng Ni, Peiqi Chai1 , Xia Cui, Xuefeng Tong, Reversible Data Hiding for JPEG Images Based on Histogram Pairs, *International Conference on Image Analysis and Recognition (ICIAR07)* , Montreal, Canada, 22-24 August 2007.

[41] Ming. CHEN, Zhenyong CHEN, Xiao.ZENG, Zhang XIONG, Reversible Data Hiding Using Additive Prediction-Error Expansion, Signal Processing, Volume 89, Issue 6, pages: 1129-1143, June 2009.

[42] S.BOUCHAMA, Le tatouage des images appliqué à l'imagerie médicale, mémoire de magistère, Ecole Nationale Polytechnique d'alger (ENP), 2007.

[43] H. STONE , Analysis of attacks on image watermarks with randomised coefficients, tech.rep, NEC Research Institute, 1996.

[44] M.V.DIJK, T. Kalker, J.P.LINNARTZ, Watermark estimation through detector analysis, in Proceedings Second International Workshop on Information Hiding, Portland, Avril 1998.