وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR – ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR – ANNABA

جامعة باجي مختار ـ عنابة

Faculté:Sciences de l'Ingénieur
Département: Informatique

Année : 2008

MEMOIRE

Présenté en vue de l'obtention du diplôme de MAGISTER

Thème

Tatouage robuste des images basé sur la transformée en ondelettes discrète

Option

Intelligence artificielle (Texte image parole)

Par

Bakhouche Amara

DIRECTEUR DE MEMOIRE: Professeur N. DOGHMANE

DEVANT Le JURY

PRESIDENTE :	**Mme.**	**B. TIGHIOUART**	**M.C.**	**Univ. ANNABA**
EXAMINATEURS:	**M.**	**H. TEBBIKH**	**Prof.**	**Univ. GUELMA**
	Mme.	**H. MEROUANI**	**M.C.**	**Univ. ANNABA**
	Mme.	**K. BOUKARI**	**M.C.**	**Univ. ANNABA**

ملخص

نقترح في هذه المذكرة ، طريقة جديدة لوشم الصور ، حيث أن نوع الوشم المختار في العمل المقترح هو الوشم الاضافي و غير الاعمى . وهي تعمل في المجال المتحول بالاعتماد على التحويلة الي الموجات لمنفصلة (رانسفرمى أون أندولات دسكرات)، نطبق فى هذه المذكرة الطريقة المقترحة سواء على صور رمادية أو ملونة ذات حجم 512 x 512 .

فى مجال البحث هذا وهو وشم مختلف المعطيات الرقمية ، الأهداف المرجوة كثيرة ولكن الأكثر أهمية هى حقوق المؤلف خاصة مع وجود وتطور الشبكات ، مثل الأنترنت وقلة مراقبة توزيع المعلومات فى هذه الشبكات .

طرق الوشم المقترحة فى هذه المذكرة ترتكز على تغير معاملات الأندولات عن طريق اضافة قيم الوشم عدة مرات ، وبطريقة متوازية مع استخدام طريقة الانتشار الطيفى .

تظهر النتائج التجريبية أن المخططات المقترحة فعالة فى مواجهة عدة أنواع من الهجمات سواء كانت مقصودة (التزوير على سبيل المثال) أو غير مقصودة (الضغط ، بروى ،الترشيح ، التغيرات فى السطوع والضوء ، التحولات الهندسية مثل الدوران وحذف بعض الأجزاء وتغير الحجم ...الخ) ومع ذلك تظل الطرق المقترحة غبر فعالة فى حالة الهجوم المتكرر مثل الضغط وتغير السطوع.

Abstract

In this thesis, a new method of robust watermarking is proposed. It is based on an adaptive and not blind watermarking approach. It operates in the transform domain from the *DWT* (Discrete Wavelet Transform). The used images in our watermarking method are still images in gray scale or in color of size 512x512.

In this research, namely the tattoo images and data, the objectives are many. Nevertheless, the most sought is the protection of copyright following a less controllable distribution on networks communication such as the Internet.

in this thesis, the proposed approach's, make changes on the wavelet coefficients by multiple and parallel embedding of a watermark signal using the adaptive techniques .

The experimental results show that the proposed schemes are robust face several attacks, is voluntary (falsification for example) or non-voluntary (compression, Gaussian noise, filtering, changes of the luminance and contrast, geometric transformations such as rotation , cropping and the change of scale… etc.). However, these approaches remain weatherable in the case of repeated attacks such as compression and changes of the luminance.

Résumé

Dans ce mémoire, une nouvelle méthode de tatouage robuste est proposée. Elle est basée sur une approche de tatouage additive et non aveugle. Elle opère dans le domaine transformé à partir de la *DWT* (transformée en ondelettes discrète). Il s'agit de tatouer des images fixes en niveau de gris ou en couleur de tailles 512x512.

Dans cet axe de recherche, en l'occurrence le tatouage des images et des données numériques, les objectifs recherchés sont multiples. Néanmoins, le plus sollicité est la protection du droit d'auteur suite à une distribution toujours moins contrôlable sur des réseaux de communication tels que l'Internet.

Les schémas de tatouage proposés, dans ce mémoire, effectuent des modifications sur les coefficients d'ondelettes par l'insertion d'un signal de tatouage de façon multiple et parallèle selon la technique d'étalement de spectre.

Les résultats expérimentaux montrent que les schémas proposés sont robustes face à plusieurs attaques, soit volontaires (la falsification à titre d'exemple) ou non volontaires (compression, Bruit Gaussien, filtrage, modifications de luminance et de contraste, transformations géométriques tel que la rotation, le cropping et le changement d'échelle…etc). Cependant, ces approches restent altérables dans le cas d'attaques successives comme la compression et modifications de luminance.

Remerciements

Cette année, de magister a été riche en évènements de toutes sortes. Nous remercions tout d'abord notre Dieu tout puissant qui nous a permis d'atteindre notre objectif quant à la finalisation de ce travail.

En premier lieu, je tiens à remercier monsieur Doghmane Noureddine, mon encadreur. Il m'a constamment soutenu, encouragé et stimulé pendant ce travail de magister. Ses nombreuses remarques ont montré une très vaste connaissance des sujets abordés et ma donné les conduits et les améliorations de mon travail.

Ensuite Je tiens à exprimer mes remerciements aux membres du jury de m'avoir fait l'honneur de rapporter ce mémoire de magister. Je les remercie d'avoir contribué, par leurs remarques pertinentes, à enrichir et à corriger ce mémoire.

Je ne peux terminer ces remerciements sans mentionner mes proches et mes amis : khedairia sofiane et zarzour hafed, ghraibia abdelghani, fraga nasro, khélil habita, bachir, chaouki , ahmed ,mahdi, Merci pour tout.

Bien évidemment je remercie mes parents et ma famille pour leur confiance et leur soutien sans faille au cours de cette année, et pour m'avoir supporté pendant ces longues années d'études.

J'ai sans doute oublié plein de monde, toutes mes excuses, je sais que vous ne m'en tiendrez pas rigueur.

Liste des Tableaux

Liste des Figures

Liste des acronymes

JPEG	Joint Photographic Experts Group.
DVD	Digital Video Disc ou Digital Versatile Disc.
CPTWG	Copy Protection Technical Working Group.
SVH	Système Visuel Humain.
PSNR	Peak Signal to noise Ratio.
GIF	Graphics Interchange Format.
EQM	Erreur Quadratique Moyenne.
TFD	Transformée de Fourier discrète.
TCD	Transformée en cosinus discrète.
DCT	Discrete Consinus Transform.
MPEG	Moving Pictures Experts Group.
DWT	Discrete Wavelet Transform.
IDWT	Inverse Discrete Wavelet Transform.
LL	Low-Low frequency band.
LH	Low-High frequency band.
HL	High-Low frequency band.
HH	High-High frequency band.
LSB	Less Significant Bits.
MSB	Most Significant Bits.
VW2D	Variable-Watermark Two-Dimensional.
CMY	Cyan, Magenta Jaune.
STFT	Short Term Fourier Transform.
XOR	Opération logique OU exclusif.
LFSR	Linear Feedback Shift Register.
EZW	Embedded Zero-tree Wavelet.
YCbCr	(ou YUV) Codage d'image couleur suivant un plan de luminance (Y) et deux plans de chrominance et Sauration (Cb-Cr).
SRC	Système de Représentation Colorimétrique.

Table des Matières

2- Deuxième Chapitre
Etat de l'art des méthodes de tatouage.

3- Troisième Chapitre
Outils mathématiques.

4- Quatrième Chapitre
Algorithmes proposés.

Introduction générale

L'information a toujours eu un rôle primordial au cours de l'histoire. La transmission de cette entité était par manuscrit ou par la voix, elle peut maintenant parcourir les milliers de kilomètres en quelques dixièmes de seconde grâce aux réseaux de télécommunication. Un contenu (information) est une représentation physique d'une oeuvre créée par un artiste. Il s'agit d'un morceau de musique, d'une image, d'un film. Codé dans un format numérique, il est représenté par une séquence de mots binaires. Avec l'avènement et le développement des réseaux de télécommunication ainsi que la numérisation des documents, la distribution de l'information est devenue très facile, Ce qui pose de nombreux problèmes en terme de sécurité des contenues numériques. Une image numérique diffusée par exemple sur Internet peut aisément être récupérée par quiconque puis rediffusée sans subir de détérioration, soit sur un réseau, soit sur un CD-ROM. il est dans ce contexte très facile de s'approprier ces informations par une autre personne sans prise en compte des droits d'auteurs.

Les documents numériques quels qu'ils soient sont donc soumis au problème du piratage (copie des documents sans acquittement de droits d'auteur). Le piratage peut avoir une répercussion économique non négligeable. Selon une étude publiée par l'organisation professionnelle de lutte contre la piraterie *IIPA (International Intellectual Property Association)*.[1] , le piratage a coûté seulement pour 18 Etats européens considérés comme posant problème (2003) par *l'IIPA* :

- Au minimum 608 millions de dollars de pertes pour l'industrie cinématographique, soit 40 % des pertes dans les pays du monde.
- Au minimum 784 millions de dollars de pertes pour l'industrie phonographique, soit 35 % des pertes dans les pays du monde.
- Au minimum 169 millions de dollars de pertes pour l'industrie du logiciel de divertissement, soit 11 % des pertes dans les pays du monde.

Il s'est donc avéré nécessaire pour les propriétaires de contenus numériques de rechercher des solutions afin d'empêcher la copie de documents.

Le tableau de la situation de la piraterie dans 18 pays ci-dessous, indique les priorités proposées par *l'IIPA* en matière de politique commerciale.

	Motion pictures		**Records & Music**		**Business Software**		**Entertainment Software**		**Books**
	Loss	**Piracy level**	**Loss**	**Piracy level**	**Loss**	**Piracy level**	**Loss**	**Piracy level**	**Loss**
Priority Foreign Country									
Ukraine	45	90%	125	75%	n.a.	n.a.	n.a.	85%	n.a.
Priority Watch List									
Bulgaria	4	25%	7	80%	n.a.	n.a.	n.a.	n.a.	n.a.
Poland	30	30%	34	45%	n.a.	n.a.	n.a.	n.a.	5
Russian Federation	275	75%	405	64%	n.a.	n.a.	n.a.	80%	40
Watch List									
Azerbaijan	n.a.	n.a.	12,2	83%	n.a.	n.a.	n.a.	n.a.	n.a.
Estonia	2	35%	6,5	60%	n.a.	n.a.	n.a.	n.a.	n.a.
Hungary	20	30%	8	30%	n.a.	n.a.	n.a.	n.a.	n.a.
Italy	140	20%	42	22%	n.a.	n.a.	168,5	47%	23
Latvia	n.a.	85%	10	80%	n.a.	n.a.	n.a.	95%	n.a.
Lithuania	n.a.	n.a.	13,5	85%	n.a.	n.a.	n.a.	90%	n.a.
Romania	8	35%	18	80%	n.a.	n.a.	n.a.	2%	n.a.
Spain	30	10%	60	25%	n.a.	n.a.	n.a.	n.a.	n.a.
Turkey	50	45%	15	75%	n.a.	n.a.	n.a.	25%	n.a.
Special Mention									
Armenia	n.a.	n.a.	4,1	86%	n.a.	n.a.	n.a.	n.a.	n.a.
Bosnia and Herzegovina	4	90%	3	99%	n.a.	n.a.	n.a.	n.a.	n.a.
Georgia	n.a.	n.a.	8	80%	n.a.	n.a.	n.a.	n.a.	n.a.
Moldova	n.a.	n.a.	4	69%	n.a.	n.a.	n.a.	n.a.	n.a.
Serbia and Montenegro	n.a.	90%	9	75%	n.a.	n.a.	n.a.	n.a.	n.a.
Total 18 EUR countries	608		784		n.a.		169	n.a.	68
Total IIPA World list	1528		2260				1549		499,8
% Europe	40%		35%				11%		14%

Tableau 1 : *Situation de la piraterie dans 18 états européens considérés comme posant problème par l'IIPA.*

Les techniques cryptographiques classiques telle que le chiffrement peuvent s'appliquer à la protection des droits d'auteurs. Cette technique permet de protéger le document pendant sa transmission. Mais, une fois le document décrypté, il ne présente alors plus aucune protection.

La stéganographie, « l'art de cacher un message dans un autre », est une autre solution de protection. Contrairement à la cryptographie, cette technique est invisible et permet de protéger le document même lorsque celui-ci est diffusé. Sa faiblesse réside dans le manque de robustesse. En effet, il est facile d'effacer le message inséré par changement systématique du document.

De ce fait, la nécessité de recourir à des procédés plus performants de protection du copyright devient un besoin primordial. D'où l'apparition récente de la notion de tatouage numérique. En quoi consiste donc ce nouveau concept ?

Face à toutes ces interrogations, le tatouage numérique (ou « watermarking » est très naturellement apparu comme une solution alternative ou complémentaire pour renforcer la sécurité des documents numériques.

En effet, le principe du tatouage ou « watermarking » consiste à insérer dans un document numérique (image, son, vidéo. . .) une marque invisible, contenant un code, robuste face à toute attaque susceptible de modifier la donnée tatouée. Plusieurs algorithmes de tatouage ont vu le jour cherchant à optimiser un compromis robustesse-invisibilité, cependant, aucun d'eux ne satisfait un cahier de charge idéal. En outre, chacune de ces méthodes s'inscrit dans un certain contexte d'utilisation et est destinée à des types de documents bien précis. On ne connaît en effet aucune méthode de marquage s'adaptant à tout type de document, aucun modèle fonctionnel universel. Ceci contribue à l'expansion de ce domaine de recherche visant la découverte d'une meilleure solution.

Dans ce mémoire, nous nous focaliserons principalement sur le tatouage des images numériques. Le premier chapitre de ce mémoire vise à présenter le contexte général du tatouage numérique. Après une présentation du principe du tatouage et de ses applications, en particulier pour la gestion des droits d'auteur, nous analysons les principes de conception d'une technique de tatouage qui s'appui généralement sur deux étapes essentielles,

incrustation de la marque et détection de la marque. Nous présentons également dans ce chapitre les principales attaques auxquelles le document tatoué peut être soumis. Enfin, nous présentons les outils d'évaluations des systèmes de tatouage.

Dans le second chapitre, nous distinguons deux classes importantes de schémas de tatouage. Les schémas additifs (le plus souvent par étalement de spectre) représentent une catégorie de schémas où la marque est ajoutée à l'une des composantes de l'image. Dans la deuxième classe de schéma, les schémas substitutifs, certaines composantes de l'image sont remplacées par la marque. Ces deux classes de schémas peuvent être appliquées dans le domaine spatial de l'image ou bien dans un domaine transformé comme la transformée de fourier discrète ou encore la transformation multirésolution. Nous présentons également dans ce chapitre, les techniques du tatouage pour les images en couleurs.

Le troisième chapitre de ce mémoire présente les outils que nous utilisons : la transformée en ondelettes discrète, puis sa généralisation sur les images. Cette transformation redondante du signal permet une décomposition sur plusieurs bandes fréquentielles suivant différents niveaux de résolutions. La redondance de l'information contenue dans la décomposition en ondelettes permet de choisir différentes bases de représentation du signal.

Enfin, dans le quatrième chapitre, nous présentons nos algorithmes additifs basons sur la transformée en ondelettes discrète. Ce chapitre se décompose essentiellement en deux sections, dans la première nous détaillons les deux algorithmes proposés pour le tatouage des images en niveau de gris ainsi que les résultats obtenus suite à des attaques effectuées sur les différentes images de teste. La seconde section consiste à détailler de l'évaluation de l'imperceptibilité de nos méthodes de tatouage pour les images en couleur ainsi que leur résistance aux différents traitements visant à supprimer la marque.

Premier chapitre

Principes du tatouage d'images numériques

1.1 Introduction

Le tatouage des données numériques est un domaine scientifique récent qui trouve son origine dans la carence de techniques fiables de protections du contenu numérique. Nous présentons dans ce chapitre les différents enjeux offerts par le tatouage ainsi que le contexte technique du tatouage d'images numériques. La première section présente le principe général du tatouage d'images.

Nous détaillons ensuite les différents outils permettant de faire appliquer les droits de propriété. La cryptographie peut être utilisée pour sécuriser les transactions électroniques tendis que le tatouage est un domaine fortement lié à la stéganographie. Il permet l'insertion d'une information liée à l'exercice des droits d'auteurs.
La troisième section décrit les différentes applications qui découlent des techniques de tatouage. Outre la possibilité de répondre aux problèmes des droits d'auteurs, le tatouage peut aussi permettre l'authentification ou l'indexation des documents, nous définirons ensuite le processus général du tatouage qui se découpe en deux étapes fondamentales: L'insertion et la détection de la marque. Les attaques auxquelles une image tatouée est potentiellement soumise sont ensuite classées, Nous décrivons notamment dans cette section des techniques permettant d'évaluer une méthode de tatouage, puis nous donnerons les différentes applications de ces méthodes.

1.2 Principe général du tatouage d'images

Le tatouage numérique, pour la protection des droits d'auteurs, consiste à introduire une marque invisible, appelée W*atermarque*, dans un document numérique (une image par exemple). Le document ainsi tatoué ou marqué peut alors être distribué, il est donc susceptible de subir diverses déformations. Celles-ci peuvent être involontaires (par exemple : compression d'une image au format JPEG) ou volontaires (traitements visant la falsification de l'image tatouée). La robustesse face aux différentes attaques est l'une des propriétés importantes d'une méthode de tatouage. Les attaques les plus simples (rotation ou translation d'une image, rognage de quelques lignes ou colonnes) obtiennent déjà des résultats dévastateurs sur les méthodes initialement imaginées [2], et les chercheurs ont mis en évidence des attaques beaucoup plus perfectionnées [3]. Le tatouage est même modélisé comme un jeu entre le tatoueur et l'attaquant [4].

Une autre contrainte importante du tatouage est la quantité d'information que l'on espère insérer, ou capacité : Il paraît évident que plus on accroît la capacité, plus la déformation sera perceptible, et plus la robustesse s'amoindrira. Un compromis doit donc être trouvé entre ces trois paramètres: imperceptibilité, robustesse et capacité.

Une quatrième contrainte très importante et indépendante des trois premières, est la sécurité des algorithmes de tatouage. Cette contrainte repose essentiellement sur la sécurité de la clef qui diffère selon chaque utilisateur. Les systèmes de tatouage doit aussi respecter le principe énoncé par *Kerckhoffs* [5] : l'algorithme lui-même doit pouvoir être rendu public, la sécurité ne dépendant pas de son caractère secret.

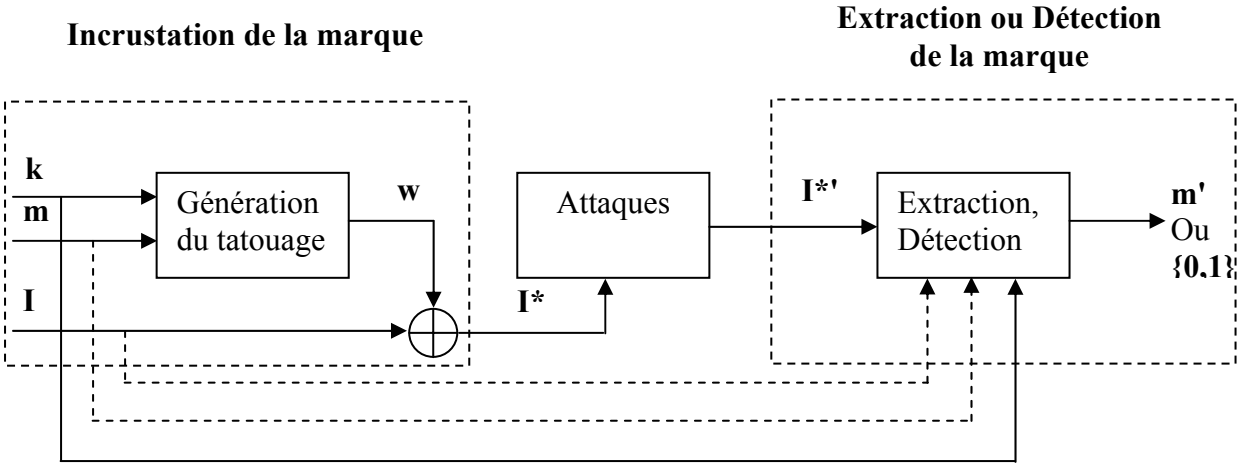


Figure 1.1 : *Schéma général d'un processus de tatouage numérique.*

Le schéma général d'un processus de tatouage numérique est résumé sur la *figure. 1.1* : Une image I (appelée également "hôte") est tatouée par une marque w (un message m contenant L bits est transformé par l'intervention d'une clef k en une marque w) pour donner une image tatouée I^*. C'est la phase d'implémentation. La marque w est représentée sous la forme d'un bruit qui est incrusté à l'image I, où la déformation dépendant de la puissance du bruit. k est secrète et spécifique au tatoueur. L'image résultante I^* est ensuite soumise à des attaques volontaires ou involontaires de nature inconnue, l'image reçue est appelée $I^{*'}$. Cette dernière constitue l'entrée de la deuxième phase qui peut être interprétée de deux façons : soit par une variable booléenne qui indique la présence ou l'absence de la marque dans l'image testée, soit par l'extraction de la marque elle-même. Dans les deux cas l'intervention de la clef k est nécessaire. Si l'image originale est nécessaire dans la détection, on parle alors d'extraction ou détection "non-aveugle" ou informée (l'image originale est utilisée dans la construction de w), dans le cas contraire, l'extraction est dite "aveugle". Une estimation m' de

m peut être calculée dans la phase de l'extraction. Si la taille du message inséré L est suffisamment grande et contient une information intelligible (par exemple, des caractères ASCII), certains auteurs considèrent que la détection devient inutile puisqu'on peut appliquer un simple décodage. Si la chaîne décodée est inintelligible (par exemple, non ASCII), on considère qu'il n'y a pas de tatouage [6][7].

Dans le cas où plusieurs marques sont insérées à la fois, quant il s'agit par exemple de plusieurs utilisateurs avec des marques différentes, on parle alors de tatouage multiple.

Nous allons présenter plus en détail les schémas d'implémentation et de détection de la marque dans la section 1.5. Nous accompagnerons ces schémas du formalisme donné par *Petitcolas et al*. dans [8] , généralement utilisé par la communauté des ‘’tatoueurs’’.

1.3 Techniques numériques pour la protection des données

Trois techniques interviennent dans la transmission des informations de manière secrète: La cryptographie, la stéganographie et le tatouage. Dans les trois cas, il s'agit de transmettre une information afin qu'elle soit inintelligible par une personne non autorisée;
La cryptographie et la stéganographie ont été utilisées avant le commencement de notre ère à des fins militaires. Elles font partie des sciences du secret. Le tatouage de document est un domaine beaucoup plus récent qui s'apparent à la stéganographie.
Cette section a pour but de détailler ces différents domaines en précisant les similitudes et les complémentarités.

1.3.1 La cryptographie

La cryptographie ou le chiffrement vise à transformer un message de manière à le rendre illisible. Seule la connaissance d'une clef et l'algorithme de cryptage peuvent conduire à décoder le message en le rendant lisible [9]. La cryptologie permet de protéger le contenu d'un message susceptible d'être intercepté lors de sa transmission. Elle permet aussi de:

- Assurer un service d'intégrité de données : elle assure que les données sont inchangées à l'aide d'une fonction de hachage.
- Service de confidentialité de données : seules les personnes autorisées peuvent accéder aux données.
- Service d'authentification : Seule la connaissance d'une clef peut permettre de changer les données.

Lorsque l'on parle de cryptographie, on peut distinguer deux grandes familles :

- Le cryptage symétrique (ou cryptage à clefs secrètes) : utilisation de la même clef lors des deux phases (cryptage et décryptage).
- Le cryptage asymétrique (ou cryptage à clefs publiques) : chaque utilisateur possède deux clefs une privée (secrète) et une publique (non secrète) calculées à partir de la première.

Jules César fut l'un des premiers personnages connus pour s'être servi de codes mathématiques, la formule de codage utilisée est la suivante : X la lettre du message initial, n la valeur du décalage et Y la lettre à écrire dans le message secret

$$Y=(X+n) \bmod 26 \qquad \textbf{1.1}$$

Où X la lettre du message initial, n la valeur du décalage et Y la lettre à écrire dans le message secret. La formule de décodage est la suivante:

$$X=(Y-n) \bmod 26 \qquad \textbf{1.2}$$

Néanmoins, l'inconvénient des méthodes cryptographiques est que le message crypté n'est sécurisé que lors de sa transmission.

1.3.2 La stéganographie

La différence majeure entre la cryptographie et la stéganographie, est que la cryptographie rend le document hôte (texte, image, son …) incompréhensibles ou illisible à toute personne qui ne possède pas la clef adéquate, alors que la stéganographie repose sur l'incrustation d'une marque utilisateur ou un message dans le document hôte d'une manière invisible à l'aide d'une clef secrète.

Parmi les applications permettant la stéganographie on trouve la communication sécrète de l'information par l'utilisation des réceptacles numérique comme l'image, texte, son, l'augmentation de contenus ou même pour assurer un service d'intégrité des documents que ce soit image, texte, son ou même des vidéos.

La stéganographie existe depuis longtemps, bien avant notre ère informatique. Elle a était généralement représentée par l'utilisation d'encres invisibles [8] majoritairement lors de la seconde guerre mondiale.

1.3.3 Le tatouage

Le tatouage d'images est une technique récente apparue au milieu des années 90. Cette technique de protection de documents peut être vue comme l'ajout ou l'incrustation d'une marque (message binaire, image, …) dans le document hôte, comme dans la stéganographie le tatouage doit être invisible. Alors, le tatouage de documents peut être perçu comme une branche de la stéganographie, mais avec une contrainte très importante qui est la robustesse. Ainsi la marque insérée appelée tatouage et doit respecter deux contraintes :

1. Elle doit être invisible,
2. Elle doit être robuste

La robustesse signifie qu'il est possible de détecter le tatouage même si le contenu a subi des transformations (la marque doit résister à l'effacement) que ce soit volontaire (falsification à titre d'exemple) ou non volontaire (compression JPEG, ajout de bruit, déformation géométrique, …) à condition que ces transformations appliquées sur le document tatoué, ne soient pas très prononcées, ainsi le document tatoué reste exploitable ou commercialisable après transformations ou attaques.

Nous détaillerons dans le chapitre suivant les différentes contraintes propres au domaine du tatouage d'images numériques.

1.4 Cadres applicatifs du tatouage d'images

Nous montrerons dans cette section quelques applications liées au tatouage. L'incrustation d'une marque (une image binaire par exemple) a pour objectif d'accroître la fonctionnalité du document hôte (image numérique dans notre cas). Le tatouage inséré peut permettre des fonctions de protection de droits d'auteurs, d'authentification du document ou encore de vérification de l'intégrité du contenu d'une image. Le niveau de robustesse exigé pour ces différentes applications est variable.

1.4.1 Protection de droits d'auteurs

La première application envisagée pour le tatouage d'image était la protection des droits d'auteurs. En effet, ce service reste toujours d'actualité et fait l'objet de la plupart des publications. L'objectif est d'offrir, en cas de litige, la possibilité à l'auteur ou au propriétaire

d'une image d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce même si l'image concernée a subi des distorsions par rapport à l'original. La mise en place d'un tel service doit respecter les trois contraintes suivantes :

Qualité de l'image : après l'insertion de la marque dans l'image originale la qualité visuelle de l'image tatouée doit être la même ou similaire que celle de l'image originale (avec une dégradation de l'image tatouée la plus faible possible). La notion d'invisibilité du tatouage est malheureusement très difficile à modéliser. Plusieurs facteurs influent en effet directement sur la notion d'invisibilité, tels que : la nature de l'image à marquer (photo satellite, texture, penture, image médicale, etc.), la qualité de l'image originale (plus une image est de bonne qualité, plus il est difficile de garantir l'invisibilité de la marque).

La non-ambiguïté de la preuve : la marque extraite devrait constituer une preuve irréfutable. Pour cela la conception du tatouage et des protocoles rattachés doivent exclure l'apparition de toute ambiguïté tel que le cas où l'image aurait été tatouée plusieurs fois avec des marques différentes.

La robustesse du tatouage : l'algorithme utilisé doit être capable d'extraire une marque de bonne qualité, même si l'image serait manipulée ou attaquée. Dans la section 1.6 de ce chapitre, nous détaillons plus précisément cet aspect du tatouage d'image, ainsi que les différentes familles d'attaque.

1.4.2 L'authentification des documents

La marque incrustée dans l'image à tatouer peut permettre d'affirmer qu'une image n'a pas été modifiée [10]. On parle alors d'un service ou d'une problématique de contrôle d'intégrité des documents. C'est le cas de la marque incrustée est dite fragile (ou "fragile watermarking" en anglais). Cette marque doit être détectée tant que l'image tatouée n'a pas été traitée [11]. Si le tatouage inséré résiste face aux quelques attaques tels que la compression, les transformations géométriques ou bien encore le filtrage de l'image, alors le tatouage est mentionné semi-fragile.

La figure 1.2 montre un exemple du tatouage pour l'authentification du papier d'identité. Le principe de ce système a été évoqué par *Kutter et al*. [12]. L'idée de ce système repose sur le tatouage automatique de la photo d'identité lors de prise de photo de la personne.

La marque incrustée résulte directement du numéro d'identité de la carte. Dans le cas de modification de la photo d'identité (falsification basique), la détection de la marque à partir du numéro d'identité permet d'affirmer que la marque n'est pas présente dans l'image substituée et donc que l'image a été falsifiée.

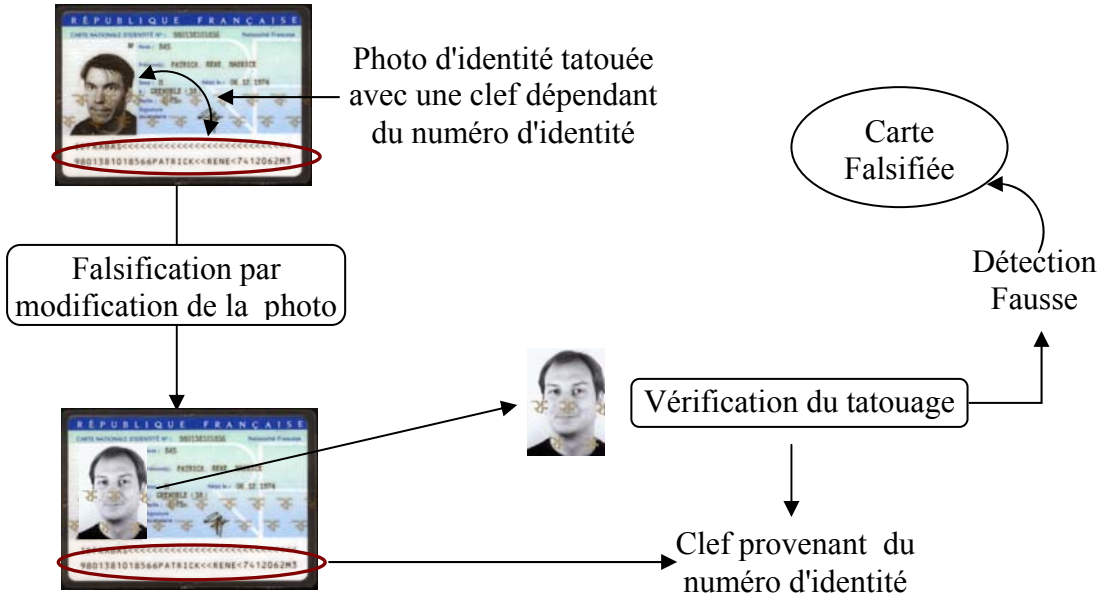


Figure 1.2 : *Application du tatouage d'images à l'authentification de documents.*

1.4.3 Gestion du nombre de copies d'une image

Il est évident que les données de nature analogique perdent progressivement la qualité par des reproductions successives des ces données, contrairement aux données numériques qui peuvent être stockées, copiées ou diffusées illégalement sans perdre de leur qualité. En effet, dès lors qu'une personne a accès aux données elle est potentiellement capable de les reproduire en préservant intégralement la qualité originale. Cette personne, peut ensuite redistribuer illégalement des copies avec une qualité égale au document d'origine sans tenir en compte des droits d'auteurs. De ce fait, certaines techniques de tatouage sont proposées afin de limiter l'ampleur de ce phénomène. Un exemple est constitué par les systèmes DVD, où un tatouage numérique indiquera si la vidéo pourrait être lue et/ou recopiée.

Cette méthode n'est bien entendu fiable que si tous les constructeurs de lecteurs et d'enregistreurs de DVD tiennent compte de l'indicateur de copie.

1.4.4 Autres application

Dans la littérature il existe plusieurs autres applications envisageables et qui sont différentes de celles décrites précédemment. Ces applications offrent plusieurs autres services en dehors des services de sécurités. On peut par exemple distinguer des applications de tatouage d'image pour la gestion des bases de données multimédia afin de faciliter la recherche des informations textuelles sur le contenu de ces bases. Le tatouage d'image trouverait aussi sa place dans un système de montage vidéo où il pourrait servir par exemple à étiqueter les différentes séquences dans le but de récupérer simplement la source d'un extrait à partir d'un enregistrement quelconque. D'autres techniques de marquage proposées par certains auteurs [13][14], sont utilisées pour corriger les erreurs détectées lors de la transmission de vidéos numériques.

1.5 Processus de tatouage

La majorité des schémas de tatouage d'image reposent sur le même prototype et diffèrent seulement par des techniques spécifiques à certains niveaux du processus d'insertion ou d'extraction. Il est donc possible de montrer d'une façon commune le tatouage d'images.

1.5.1 Incrustation de la marque

La *figure 1.*3 illustre le schéma général d'insertion de la marque. Une marque ***W*** est ajoutée à l'image originale ***I*** (appelée également "hôte") par l'intervention de la clef ***K.*** Les deux images, originale ***I*** et celle tatouée I^* sont perceptuellement identiques malgré que l'image tatouée contient le code de droit d'auteur ***W.***

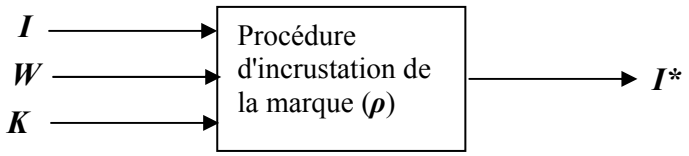


Figure 1.3 : *Schéma général du processus d'incrustation d'une marque.* ***I*** *est l'image hôte,* ***K*** *la clef privée,* ***W*** *la marque,* ***I**** *est l'image tatouée résultat de la procédure d'incrustation (****ρ****).*

On peut formaliser l'incrustation de la marque comme une application (***ρ***) qui correspond à une clef ***K*** *de* l'ensemble des clefs **ξ(K),** une marque ***W*** de l'ensemble des Watermarques **ξ(W)** et une image originale ***I*** de l'ensemble des images **ξ(I)**, une image tatouée ***I**** de l'ensemble des images **ξ(I).**

$$(W,K,I) \rightarrow I^* \qquad \textbf{1.3}$$

Le formalisme ci-dessus représente le processus général d'insertion de la marque pour tous les schémas de tatouage. Nous allons maintenant déterminer les contraintes que l'application (***ρ***) doive satisfaire et définir les ensembles d'entrées et de sorties **ξ(W)**, **ξ(K)** et **ξ(I).**

- **Contrainte d'imperceptibilité**

En effet, l'invisibilité de la marque est le fait que l'image tatouée est plus au moins similaire, au sens perceptuelle de l'image hôte, c'est-à-dire aucune dégradation visuelle ne doit être perçue sur l'image d'origine. L'importance de cette contrainte est due au fait d'une part que l'image tatouée reste toujours commercialisable c'est-à-dire elle doit garder toujours sa qualité commerciale, et d'autre part la marque visible peut être facilement piratée ou écrasée, donc plus le tatouage est imperceptible plus il est difficile à pirater ou à détruire.

Dans la majorité des schémas proposés, l'invisibilité du tatouage s'obtient en utilisant les zones d'intérêts les moins sensibles à l'oeil humain (contour, zone texturée,…) comme espace d'insertion de la marque, ou le masque Psychovisuel adaptant la marque à l'image à tatouer, ou par l'utilisation d'un seuil calculé à partir de l'image originale, les modifications de l'image ne peuvent se faire qu'à concurrence de ce seuil. L'outil le plus utilisé pour quantifier les dégradations causées par le tatouage est le *PSNR (Peak Signal to noise Ratio).*

- **Sécurité du tatouage**

La Sécurité du système est assurée seulement par la sécurité de la clef ***K*** qui diffère selon l'utilisateur comme dans tous les systèmes de sécurités de l'information numérique.

En effet, si la clef est confidentielle aucun pirate ne doit pouvoir récupérer l'image originale sans l'utilisation des moyens plus coûteux que l'achat des droits d'auteurs. Cette contrainte est similaire au deuxième principe de *Kerckhoffs* [5] : lorsque ***K*** est inconnu, aucun utilisateur ne doit pouvoir retrouver l'image originale. D'autres schémas n'exigent aucune sécurité pour la clef ***K*** c'est le cas des schémas à clef publique [15].

On peut aussi distinguer d'autres contraintes qui ne sont pas obligatoires comme, l'inversibilité de la procédure d'incrustation qui permet d'enlever la marque par le

propriétaire de l'image pour en ajouter une autre, cette contrainte d'inversibilité est conditionnée par la connaissance de la clef.

Nous allons maintenant définir plus clairement ce que représentent les ensembles d'entrées et de sorties du processus, c'est à dire l'ensemble des marques, celui des clefs, puis nous parlerons des images.

- **ensemble des marques**

L'espace $\xi(W)$ représente l'ensemble de toutes les Watermarques envisageables. Cependant, la marque W joue un rôle primordial dans le système de tatouage d'image où la longueur de la marque W doit être la plus grande possible est doit satisfaire en même temps la contrainte d'invisibilité qu'oblige une Watermarque de taille réduite. Une autre contrainte très importante influe directement sur la langueur de la Watermarque W est la taille de l'image originale parce qu'on ne peut pas incruster une grande quantité d'information dans une petite image. Il y a aussi un compromis entre l'ensemble des marques $\xi(W)$ et la robustesse du système de tatouage, plus la marque est redondante plus elle est robuste face aux différentes attaques, Cette redondance s'exprime de plusieurs manières, soit la même marque est ajoutée plusieurs fois dans l'image hôte ou plusieurs marques différentes sont ajoutées en même temps.

Dans la plupart des schémas de tatouage d'image proposés, la langueur de la marque est fixée à une centaine de bits pour une image 512 x 512 codée en niveau de gris.

- **Ensemble des clefs**

L'ensemble des clefs $\xi(K)$ est l'axe de sécurité du tatouage. Dans les système de tatouage à clef privée, si la clef K est divulguée, quiconque peut détecter facilement la marque est par conséquence retrouver l'image originale est invalider la détection ou l'extraction de la marque et par la suite la rediffusion de l'image par une autre marque propre au pirate. Ainsi, toute tentative de recherche de la clef doit être trop coûteuse à achever même plus que l'achat des droits d'auteurs. Pour cela, la taille de la clef doit être grande et de structure compliquée, ce qu'impose la complexité de la structure de la clef et cela ne peut se faire qu'avec une taille importante de la clef. Dans la plupart des schémas de tatouage la clef K est issue d'un processus cryptographique ou à partir des endroits de la marque dans l'image.

- **L'ensemble des images hôtes**

Il est clair qu'on ne peut pas tatouer les images de tailles très réduites parce que de telles images ne peuvent pas contenir une marque protégeant le propriétaire de l'image (la marque est trop petite). La majorité des schémas de tatouage fixent la taille minimale des images originales à 512x512 pixels. Ce choix est justifié par le fait que les images de taille inférieure à 512x512 pixels ne présentent pas généralement de valeur commerciale importante. Alors la majorité de ces schémas de marquage éliminent de l'ensemble des images originales les images de tailles réduites.

L'image hôte doit donc respecter d'autres contraintes très importantes comme par exemple la qualité de l'image, si par exemple l'image à tatouer est de qualité médiocre qui peut contenir par exemple de grandes zones uniformes, c'est le cas des images synthétiques comme les dessins.

1.5.2 Détection de la marque

L'entrée de la phase de détection est constituée de la clef sécrète d'extraction ***K*** et d'une image tatouée et éventuellement attaquée ***I*',** c'est le cas du tatouage aveugle. D'autres algorithmes nécessitent en plus la présence de la marque incrustée ***W*** (le cas du tatouage semi aveugle) et de l'image originale ***I*** (pour les schémas de tatouage non aveugle). La sortie de cette phase peut être la marque extraite ***W'*** (une extraction) ou un résultat de décision indiquant si la marque ***W*** a été retrouvée dans ***I*'** ou non (une détection).

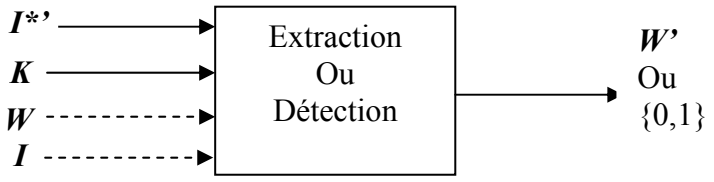


Figure 1.4 : *Schéma général du processus de détection d'une marque.* ***I*'** *est l'image test,* ***K*** *la clef privée,* ***W*** *la marque,* ***I*** *est l'image originale. Le résultat de la détection peut être une marque ou une décision.*

1.5.2.1 Les différents types de détection

Les entrées et les sorties de la phase d'extraction ou de détection peuvent varier selon

les schémas de tatouage ou plus précisément conformément au type de détection. Nous allons ici expliquer ces différents types.

- **Les schémas non aveugle (privés) :** l'extraction est dite non aveugle si l'image originale est nécessaire à la détection.
  - Deux cas sont possibles soit le résultat est une marque extraite ***W'***:

$$(K, I, I^{*'}) \rightarrow W' \qquad \textbf{1.4}$$

  - ou le résultat est une décision de présence de la marque (sa sortie sera 1 si la marque est détectée 0 sinon) :

$$(W, K, I, I^{*'}) \rightarrow \{0, 1\} \qquad \textbf{1.5}$$

- **Les schémas semi- aveugle (semi- privés) :** l'extraction est dite semi- aveugle si la présence de la marque est obligatoire (la présence de l'image originale n'est pas nécessaire dans ce type).

$$(W, K, I') \rightarrow \{0, 1\} \qquad \textbf{1.6}$$

- **Les schémas aveugles:** Dans ce type de détection la présence de l'image hôte et la marque ne sont pas nécessaires.

$$(K, I') \rightarrow W' \qquad \textbf{1.7}$$

- **Les schémas à clef publique (asymétriques) :** c'est le cas où la clef d'incrustation n'est pas la même que celle de l'extraction, dans ce cas la clef secrète de détection est connue par tout le monde. La contrainte la plus importante à satisfaire de ce type de tatouage est la robustesse contre les attaques et l'invalidation de la marque alors que tous les utilisateurs connaissent la clef.

Généralement le type de détection utilisé pour la protection des droits d'auteurs est le tatouage non aveugle qui nécessite une extraction de la marque, cette extraction doit être suivie d'une étape de comparaison entre la marque extraite et la marque originale afin de décider si l'image I*' est tatouée ou non.

La figure 1.5 explique le principe de détection par extraction. La marque extraite W' est comparée à la marque originale W par mesure de corrélation ou de distance de Hamming.

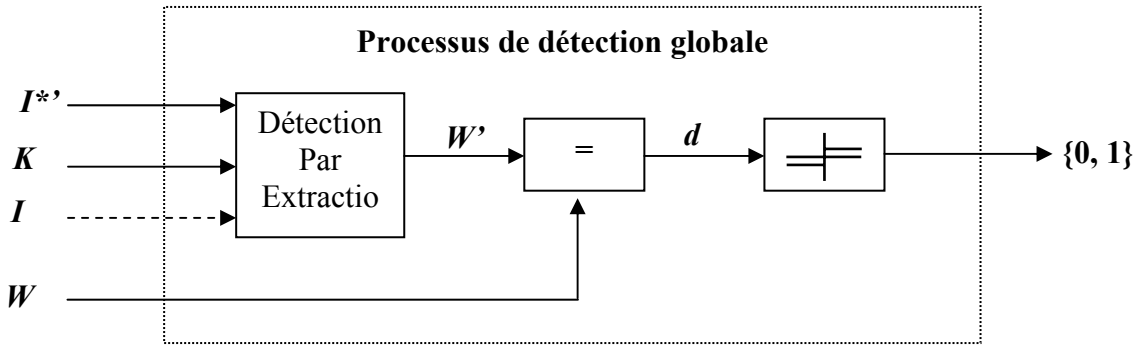


Figure 1.5 : *Schéma général du processus de détection par extraction.*

Dans la suite de ce mémoire, nous nous appuierons sur le formalisme des schémas non aveugle (privés) (voir la *relation 1.4*).

1.5.2.2 Évaluations du processus de détection

- **Robustesse aux attaques**

Les images diffusées après tatouage peuvent être soumises à des transformations quelconques. Ces transformations, qu'elles soient licites ou illicites, constituent des attaques sur le processus de tatouage. La sixième section dans ce chapitre donne des exemples d'attaques possibles. Si ces attaques ne gênent pas la détection de la marque, à condition que l'image tatouée et attaquée reste toujours commercialisable, alors le détecteur est dit robuste à ces attaques.

Soit ***t*** une transformation quelconque de l'image, soit ***I**** une image tatouée de la marque ***W*** avec la clef ***K***, on peut formaliser la contrainte de détection par la définition suivante :

$$t(I^*) = I^{*\prime} \qquad \textbf{1.8}$$

$$\text{Si} \quad I^{*\prime} \sim I^* \qquad \textbf{1.9}$$

$$\text{Alors} \quad D(K, I, I^{*\prime}) \rightarrow W \qquad \textbf{1.10}$$

Où ~ signifie similarité perceptuelle : $A \sim B$ signifie que les images ***A*** et ***B*** se ressemblent et qu'aucune ne paraît dériver de l'autre.

Cette définition pose deux problèmes techniques, le premier est qu'on n'a aucune connaissance a priori sur l'attaque ***t***, la seconde est la difficulté d'évaluation de la similarité perceptuelle.

- **Sécurité de la détection**

La sécurité de la détection repose essentiellement sur la sécurité de la clef d'après le principe de *Kerckhoffs* [5], la connaissance de l'algorithme de détection utilisé ne doit pas permettre de retrouver la clef ***K.***

1.6 Robustesse et évaluation des systèmes de tatouage

Cependant, il n'existe pas jusqu'à présent, une méthode immédiate pour l'évaluation du processus de tatouage, ni un cahier des charges qui fixe la longueur de la marque, ou la qualité de tatouage en terme d'imperceptibilité ou même l'ensemble des transformations auxquelles le tatouage doit être robuste.

1.6.1 Manipulation volontaires et non volontaires

Comme nous l'avons vu dans les sections précédentes, le tatouage doit être robuste aux maximums face aux différentes attaques que peut subir l'image après tatouage. Dans cette section, nous allons montrer une liste non exhaustive des transformations les plus courantes que peut subir une image. On distingue deux grandes catégories d'attaques:

- Les attaques volontaires.
- Les attaques non volontaires.

En effet il existe d'autres classifications des différentes attaques que peut subir une image. *Hartung et al* [16] proposent d'ordonner les attaques en cinq catégories:

-A- Les attaques simples : Ces manipulation visent la falsification du tatouage sans prise en compte de sa structure ou sa signification.

-B- Les attaques de désynchronisation : Ces manipulations visent la rupture de la synchronisation du processus de détection afin d'invalider la détection. Généralement cette désynchronisation est effectuée par les transformations géométriques, comme la rotation, le changement d'échelle et la suppression de lignes ou de colonnes de l'image.

-C- Les attaques confusion : le but des ces attaques est d'introduire un doute dans la pertinence de la marque par l'ajout de plusieurs autres marques.

-D- Les attaques de suppression : L'objectif de cette catégorie est de supprimer totalement la marque de l'image. Cette dernière contient aussi les attaques de type Collusion [17], Filtrage non linéaire [18] ou encore les attaques de Débruitage.

Pereira et al [19] a ajouté de nouvelles attaques afin d'améliorer la classification précédente. Il regroupe les attaques en quatre classes détaillées dans le *tableau 1.1*.

Plusieurs autres classifications sont proposées dans la littérature qui visent à améliorer le regroupement des attaques selon différents critères comme celle proposée par *Vassaux et al* [20].

Avec ce classement, les auteurs proposent une classification plus simple des attaques permettant de regrouper les attaques volontaire et non- volontaire.

- **Les attaques volontaires**

Les manipulations volontaires sont celles qui ont pour seul objectif d'invalider la marque en conservant au maximum la qualité de l'image originale. En effet la majorité des attaques regroupées par *Hartung et al*. [16] dans son article, sont des manipulations volontaires visant à pirater les droites d'auteurs, cette classification est améliorée par *Pereira et al* [19] dans son article, comme le montre le *tableau 1.1*.

Type d'attaque	**Exemples**
Suppression ou détérioration de la marque	Estimation et débruitage Compression Quantification Remodulation Collusion Moyennage
Attaques de désynchronisation	Transformations géométriques Distorsions Jitter attack
Attaques cryptographiques	Recherche de clefs Attaque Oracle
Attaques de confusion	Remarquage Attaque copie

Tableau 1.1 : *Classification des attaques sur les schémas de tatouage d'après Pereira et al [19].*

- **Les attaques non intentionnelles**

Cette catégorie regroupe les manipulations résultantes d'une utilisation de l'image dans un cadre usuel. Dans cette classe les attaques que l'on faits subir à l'image n'ont pas pour objectif d'invalider la détection ou de falsifier la marque, mais seulement de pouvoir exploiter l'image afin d'optimiser la qualité par exemple en utilisant le filtrage, ou pour des raisons d'enregistrement et de diffusion ce qui impose la compression au format JPEG, ou souvent le changement d'échelle de l'image pour l'adapter à l'utilisation qui en sera faite. La marque doit donc pouvoir résister à ces attaques.

La figure 1.6 montre quelques attaques non volontaires sur l'image ''Peppers-color'' de taille 512x512 (24 bits/pixel).

Plusieurs bancs de test sont mis à la disposition de la communauté pour évaluer la robustesse des algorithmes de tatouage. Les systèmes existants sont au nombre de quatre:

- StirMark
- Optimark
- Checkmark
- Certimark

Le premier banc de test utilisé pour l'évaluation de la robustesse des schémas de tatouage est le StirMark. Le logiciel StirMark proposé par *Petitcolas et al* [21][22] est le plus utilisé parmi ceux cités ci-dessus. Ce logiciel fournit un grand nombre de tests que l'on peut appliquer à l'image. Parmi les fonctionnalités que propose le logiciel on distingue :

- Le calcul du PSNR de l'image après incrustation de la marque afin d'évaluer la qualité de l'image tatouée.
- Estimation du temps nécessaire à l'incrustation de la marque.
- Plusieurs types d'attaques comme la compression JPEG, le filtrage et les transformations géométriques.

a : Image Originale. **b:** Ajout de Bruit Gaussien. **c:** Gamma Correction.

a : Intensity Adjustment. **b:** Compression JPEG 25%. **c:** Compression JPEG 5%.

a : Rotation sans Cropping. **b:** Rotation avec cropping. **c:** Cropping

Figure 1.6 : *Exemples d'attaques non volontaire sur l'image ''Peppers-color'' de taille 512x512 (24 bits/pixel).*

1.6.2 Transparence du tatouage

Dans le cadre d'augmenter les performances d'un processus de tatouage, la contrainte de transparence, qui s'exprime généralement en terme de qualité, doit être respectée deux fois dans les systèmes de tatouage d'image. D'une part, il faut que l'image tatouée soit similaire perceptuellement à l'image originale, c'est le critère d'imperceptibilité du tatouage présenté au *paragraphe 1.5.1*. D'autre part, les transformations auxquelles le tatouage doit être robuste doivent conserver la qualité de l'image, comme le précise *l'équation 1.9*.

- **Mesure de la qualité d'une image**

Dans les systèmes de tatouage, lors de l'incrustation de la marque, la mesure de la dégradation apportée sur l'image est très importante. La démarche la plus employée est alors d'utiliser une métrique d'erreur quadratique moyenne (EQM) pour calculer le PSNR - (Peak Signal to Noise Ratio).

Le PSNR est la mesure de la dégradation entre l'image tatouée et l'image originale. Il est défini par :

$$EQM = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I_o(i,j) - I_t(i,j)\right\|^2 \qquad \textbf{1.11}$$

$$(PSNR)_{db} = 10\log_{10}\left(\frac{\max^2}{EQM}\right) \qquad \textbf{1.12}$$

Où I_o est l'image originale ou de référence , I_t est l'image tatouée ou celle à tester, m est le nombre de lignes, n le nombre de colonnes et max est la valeur maximale du pixel codé sur un octet est max = 255. L'unité du PSNR est le décibel dB, plus il est élevé et moins la distorsion est importante (il est évident qu'une image de *PSNR* inférieure à 35 dB sera probablement de mauvaise qualité).

Malgré l'utilisation courante du PSNR pour mesurer la qualité des images, celui-ci n'est pas bien ajusté au Système Visuel Humain - SVH. Le SVH ne perçoit pas tous les signaux de la même façon, comme la sensibilité au contraste par exemple. L'utilisation seule du PSNR ne peut donc pas être considérée comme une mesure objective de la qualité visuelle d'une image [23].

- **Compromis invisibilité-robustesse**

Un des grands soucis dans le tatouage d'image est la détermination de la *force* du tatouage. Cependant, cette force permet l'amplification de la puissance moyenne du signal à incruster, qui est la marque, afin d'augmenter la robustesse du système, *l'équation 1.13* montre la méthode générale utilisée pour cette amplification.

$$I^* = I + \alpha W \qquad \textbf{1.13}$$

Où I^* représente l'image tatouée, I l'image originale, $\boldsymbol{\alpha}$ est la force du tatouage et W représente la marque à incruster.

En effet cette force $\boldsymbol{\alpha}$ intervient directement dans la contrainte d'invisibilité du tatouage ainsi que dans les performances de robustesse du schéma. Plus la force $\boldsymbol{\alpha}$ est élevée, plus le tatouage est visible et plus il est robuste face à certaines attaques.

1.7 Conclusion

Ce chapitre a introduit les principes du tatouage des données multimédia. Cette nouvelle discipline, au champ d'application très large, consiste à créer et à étudier des processus de *Stéganographie* permettant d'introduire dans un support numérique une marque puis de la détecter. Parmi les applications possibles, nous avons détaillé celle concernant la protection du copyright. Les contraintes imposées au schéma de tatouage découlent directement du caractère applicatif de la discipline. Pour la protection copyright, ces contraintes peuvent se résumer en termes d'imperceptibilité du marquage et de robustesse aux attaques.
En ce qui concerne la conception d'un schéma de tatouage nous avons insisté sur l'importance de l'étape de détection qui s'avère la plus fragile aux attaques.

Dans le chapitre suivant, nous étudierons ce que les chercheurs ont proposé dans ce domaine. Nous allons présenter brièvement les méthodes les plus importantes dans le domaine du tatouage en général, et le tatouage des images en particulier. Nous verrons que ce domaine de recherche est bouillonnant et propose des méthodes très diverses pour la création d'algorithmes de tatouage.

Deuxième chapitre

Etat de l'art des méthodes de tatouage

2.1 Introduction

Les schémas de tatouage que l'on peut rencontrer dans la littérature scientifique sont très variés et peuvent sembler à première vue très différents les uns des autres. Le domaine d'insertion de la marque (spatial ou fréquentiel), les méthodes utilisées pour détecter le message ou encore la catégorie d'attaques visées (compression JPEG, transformations géométriques, etc…) sont autant de paramètres qui permettent de distinguer les différents schémas.
Nous présentons dans ce chapitre une classification des techniques utilisées pour le tatouage des documents numériques.

Après avoir souligné l'importance du choix du domaine d'insertion, nous présentons deux grandes classes de schémas de tatouage. Nous définirons premièrement la classe des schémas additifs où la marque est ajoutée à une composante de l'image pour être ensuite détectée par corrélation ou à l'aide de la distance de Hamming. Nous distinguerons ensuite la classe des schémas substitutifs pour lesquels la marque prend la place d'une composante de l'image.

Nous présenterons ensuite les différents types de tatouage d'images en fonction de leurs résistances aux attaques. Il existe trois types de schéma de tatouage en fonction de leur résistance : Tatouage fragile, tatouage semi-fragile et tatouage robuste.

Enfin, la dernière partie de ce chapitre décrit les méthodes de tatouage propres aux images en couleurs.

2.2 Domaine utilisé pour le tatouage

La variété des algorithmes de tatouage est liée aux différents espaces de représentations appelés domaines d'insertion. La fiabilité du système en termes de robustesse, invisibilité et sécurité est variée entre ces domaines d'insertion. Nous présenterons dans cette section les différents rôles des différents espaces d'insertion de la marque.

2.2.1 Incrustation dans le domaine spatiale

Dans ce domaine de tatouage, les algorithmes modifient directement la luminance des pixels de l'image, c'est-à-dire que ce domaine ne nécessite aucune transformation préalable

sur l'image ce qui permet d'optimiser le temps de calcul lors d'incrustation et de détection de la marque et de travailler en temps réel.

Le domaine spatial offre dans l'ensemble, de très bonnes performances, en termes de robustesse, face aux transformations géométriques comme la rotation avec ou sans cropping. Si par exemple une subit une rotation, dans ce cas la marque ne sera pas détruite mais seulement déplacée.

Une des méthodes de base qui se situe dans ce domaine est le schéma du « patchwork », cette technique additive a été proposée par *Bender et al.* [24]. L'idée de base de cette technique, est de décomposer l'image originale en deux ensemble de même taille. Les pixels de chaque ensemble seront modifiés différemment. Pour la détection de la marque, une différence entre les moyennes des pixels des deux ensembles est effectuée. Si la valeur calculée est supérieure à un certain seuil, alors on peut affirmer la présence de la marque (voir la section 2.3).

En effet, cette méthode n'offre qu'une robustesse minimale face à la compression. Une compression JPEG de faible taux permet de supprimer la marque complètement. Cependant, de nombreux autres algorithmes [25] sont proposés afin d'augmenter la robustesse de cette méthode. Ils proposent d'utiliser des couples de blocs de pixels plutôt que des couples de pixels.

Parmi les méthodes de tatouage d'image utilisant le domaine spatial est celle proposée par *Kutter et al* [26]. Le type d'image utilisée dans cette dernière est l'image en couleur avec une marque binaire (0,1), l'incrustation des bits de la marque dans les pixels colorés de l'image originale se base sur l'augmentation ou la diminution de la composante bleue selon un facteur qui dépend de la valeur du pixel à marquer, si le bit à insérer = 1, alors on augmente cette composante, sinon (le bit à insérer = 0) on diminue la même composante. La détection de la marque est réalisée par l'estimation des valeurs de la composante bleue avant et après tatouage. Dans le but d'améliorer la robustesse de l'algorithme, chaque pixel de la marque (0,1) est ajouté plusieurs fois.

Pitas, dans [27], utilise une méthode similaire à celle proposée par *Kutter et al* [26], mais il a remplacé l'utilisation des pixels par deux ensembles aléatoires de pixels. Une autre méthode importante de tatouage d'image dans le domaine spatial est le tatouage des images

contenant du texte [28], par la modification de l'espacement vertical et horizontale entre phrases et mots.

Dans l'ensemble, le tatouage dans le domaine spatial n'offre pas de bonne robustesse face à la compression et aux attaques de type traitement de signal, une légère modification de l'image tatouée suffit pour supprimer la marque, d'où l'idée des algorithmes agissant dans le domaine fréquentiel.

2.2.2 Incrustation dans le domaine fréquentiel

Le tatouage dans le domaine fréquentiel est effectué par l'utilisation d'une TFD (transformée de Fourier discrète) ou d'une TCD (transformée en cosinus discrète). L'utilisation de la TCD ou DCT en anglais est justifiée par le fait que cette transformée est utilisée par les algorithmes de compression d'image JPEG. Ce qui rend la marque plus robuste à la compression. L'un des premiers algorithmes proposé et robuste face à la compression JPEG, en utilisant la transformée en cosinus discrète DCT, est l'algorithme de *Barni et al* [29]. Après la sélection des coefficients DCT à tatouer, une séquence pseudo – aléatoire est adaptée à l'image à l'aide des caractéristique de masquage du système visuel humain afin d'assurer la contrainte d'invisibilité de la marque. En effet, plusieurs tests effectués sur cette méthode ont montré le manque de robustesse de cette méthode face aux transformations géométriques. Dans le but d'améliorer la robustesse de l'algorithme face à ces attaques, *Barni et al* proposent d'utiliser la TFD qui est une technique possédant des propriétés d'invariance lui permettant d'être robuste face aux attaques géométrique.

Mais le développement de nouveaux standards comme JPEG2000 a dirigé les regards vers la recherche d'autres domaines d'insertion ; soit le domaine multirésolution.

2.2.3 Incrustation dans le domaine multi résolution

Un autre domaine du tatouage amplement utilisé est celui généré par une transformée en ondelettes discrète (DWT). Cependant, ce domaine est devenu populaire après la création de la norme JPEG 2000, qui utilise la DWT. L'analyse multirésolution permet la décomposition de l'image en sous-bandes par les sous-échantillonnages successifs de l'image, celle-ci permet un isolement affiné des composantes basse-fréquences [30] afin de former un espace d'insertion moins sensible.

Un algorithme de tatouage d'image non-aveugle opérant dans le domaine multirésolution par utilisation de la DWT (discrete wavelet transform ou transformée d'ondelette discrète) est proposé par *Xia et al.* dans [31]. Ce schéma repose sur l'ajout d'un code pseudo-aléatoire sur les coefficients des bandes à haute fréquence de la DWT. La détection de la marque est réalisée par une inter-corrélation entre les bandes de l'image initiale et ceux de l'image tatouée.

2.3 Les schémas additifs

Les méthodes de tatouage les plus sollicitées sont les méthodes additives. Le principe de base de ces méthodes est d'ajouter la marque à des coefficients ou des pixels de l'image originale.

2.3.1 Incrustation de la marque

L'incrustation de la marque pour les schémas additifs peut se décomposer en plusieurs étapes. La *figure 2.1* illustre le schéma général de l'incrustation de la marque.

Dans la première étape la marque W_0 est générée par la modulation d'un bruit blanc par un message M. La deuxième étape est la pondération de W_0 par la force de tatouage α, issue du calcul d'un masque psychovisuel de l'image. La dernière étape est l'incrustation de la marque amplifiée par α dans l'image, soit dans le domaine spatial ou via un domaine transformé.

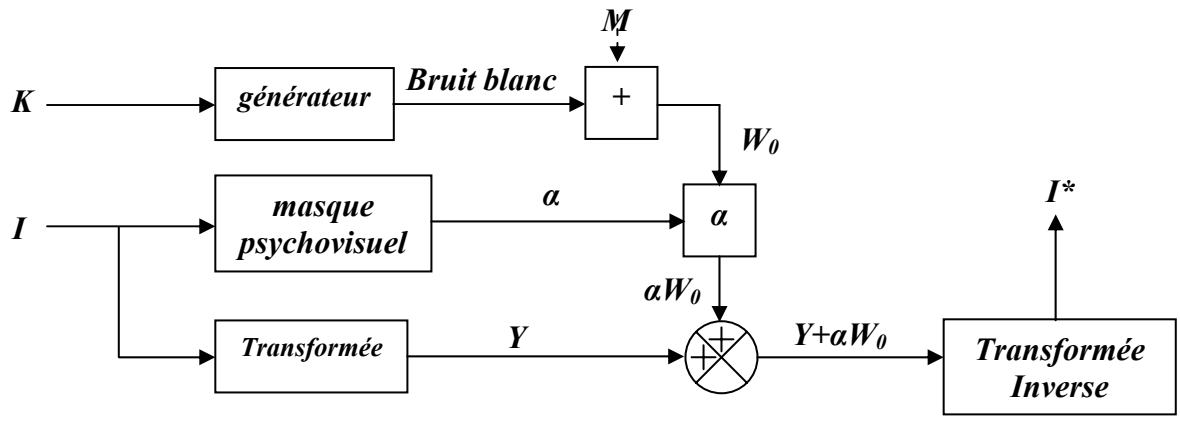


Figure 2.1 : *Schéma général d'une méthode de tatouage additive.*

En fait, les deux méthodes les plus utilisées en tatouage d'images additif, sont celles qui sont fondées sur l'insertion des *patchs* à des endroits secrets de l'image à travers un

domaine spatiale. La deuxième méthode opérant soit dans le domaine spatial ou via un domaine transformé, basée sur les méthodes dites par étalement de spectre. Dans les deux méthodes le principe de base est d'ajouter un bruit à l'image hôte. Après une présentation de ces deux méthodes (Section 2.3.3), nous montrerons qu'on peut les considérer comme une unique méthode.

2.3.2 Détection de la marque

La détection de la marque est effectuée par deux hypothèses H1 et H0.

- H_1 représente la présence de la marque :

$$H_1 : I^* = I + W \quad \textbf{2.1}$$

- H_0 représente l'absence de la marque :

$$H_0 : I^* = I \quad \textbf{2.2}$$

Cependant plusieurs types de détection de la marque sont envisagés, parmi ces types on peut trouver :

- **Détection par corrélation**

Cette technique de détection de la marque est largement utilisée dans le tatouage aveugle et semi-aveugle, elle donne dans la majorité des cas une information révélatrice de la présence de la marque. La corrélation entre l'image tatouée I^* et la marque W est effectuée par un vecteur d'observation *r*, cette corrélation peut s'exprimer sous la forme :

$$r = \langle W ; I^* \rangle = \sum w_{i,j,} i^*_{i,j} \quad \textbf{2.3}$$

Si la marque est présente (H_1) :

$$r(H_1) = \langle W ; I + W \rangle = \langle W ; I \rangle + \langle W ; W \rangle \# \langle W ; W \rangle \quad \textbf{2.4}$$

Si le marque n'est pas présente (H_0) :

$$r(H_0) = \langle W ; I \rangle << r(H_1) \quad \textbf{2.5}$$

La *figure 2.2* montre les étapes permettant la détection de la marque, la première étape de la procédure de détection, consiste à extraire les composantes tatouées, dans la seconde

étape la marque de base est générée à partir de la clef secrète. Ensuite, une corrélation entre la marque de base et les composantes tatouées est effectuée. La marque peut enfin être décodée.

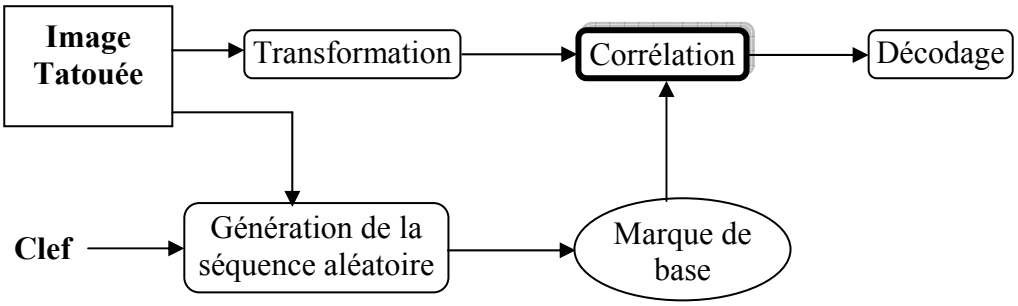


Figure 2.2 : *Détection de la marque par corrélation*.

- **Estimation par filtrage Passe-Haut**

Cette méthode de détection de la marque, repose sur le même principe que la détection par corrélation mais avec le calcul d'une estimation E_w du vecteur W, à partir des composantes tatouées extraite. Cette estimation permet d'augmenter les performances de la corrélation en calculant :

$$r' = <W; E_w> = \sum w_{i,j,}\, e_{w,i,j} \qquad \textbf{2.6}$$

Cette estimation E_w est calculée par un filtrage passe-haut afin d'éliminer une partie des composantes propre à l'image et ainsi l'augmentation de la corrélation.

Kutter [32] utilise notamment un filtrage par un masque h de taille 7x7 afin de prédire la marque. La forme de h est donné par :

$$h = \begin{matrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 12 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{matrix}$$

- **Estimation par filtrage de Wiener**

hernandez et al [33][34] proposent d'utiliser la minimisation par les moindres carrés, obtenue à partir de l'erreur de prédiction afin d'améliorer la détection de la marque.

En supposant que l'image tatouée I^* est obtenue après l'insertion de la marque W sur l'image originale I, on obtient alors la formule :

$$I^* = I + W \qquad \textbf{2.7}$$

Ensuite une combinaison linéaire en fonction du vecteur d'observation I^* est effectuée, cette combinaison exprime l'estimation E_w :

$$E_w = \alpha I^* + \beta I_d \qquad \textbf{2.8}$$

Où I_d représente la matrice identité et α et β sont deux inconnues à trouver à partir de deux conditions. La première s'écrit en calculant l'espérance de E_w qui par définition doit être nulle :

$$\alpha E[I^*] + \beta = 0 \qquad \textbf{2.9}$$

La deuxième condition s'exprime par l'estimation qui doit être orthogonale au vecteur d'observation :

$$E[(E_w - W)\, I^*] = 0 \qquad \textbf{2.10}$$

Si en supposant que I et W sont indépendant (E[IW] = 0), la résolution de ce système donne l'expression de E_w :

$$E_W = \frac{E[W^2]}{E[W^2] + E[I^2]}(I^* - E[I]) \qquad \textbf{2.11}$$

Le calcul de E_w est obtenu pratiquement, par l'évaluation des moyennes et de variances de façon locale, c'est-à-dire dans un voisinage autour de chaque composante de l'image tatouée.

Parmi les types de détection les plus utilisés : la détection par décision optimale. Ce type de détection est utilisé lorsque la marque est générée par un bruit blanc gaussien et additif. L'idée de base de cette méthode est d'utiliser un maximum de vraisemblance pour retrouver la marque. Dans le cas par exemple d'une incrustation par étalement de spectre (Section 2.3.3), la décision est réalisée par un seuil sur la valeur de corrélation selon la loi suivante :

Si $< E_w; W >$ est positif; *alors* le bit détecté est égal à 1. **2.12**

Si $< E_w;W >$ est négatif, *alors* le bit détecté est égal à 0. **2.13**

2.3.3 Tatouage additif dans les différents domaines

- **Domaine spatial**

Nous présentons dans cette section un éventail de différentes méthodes de tatouages additifs dans le domaine spatial. Les sections suivantes sont consacrées aux domaines transformés.

- **"patchwork"**

L'algorithme « Patchwork » a été proposé par *Bender et al.* [24]. Cet algorithme opère directement dans le domaine spatial, c'est-à-dire au niveau les valeurs des luminances des pixels. Cette méthode consiste à sélectionner *N* paire de pixels de l'image originale notés $(a_i, b_i)_i = [1...N]$ à partir de deux ensembles disjoints *A1* et *B* de pixels qui dépendent d'une clef secrète *K*. Ensuite ces pixels, sont modifiés différemment selon l'ensemble *A1* et *B* auxquels ils appartiennent, selon les formules suivantes :

$$a^*_i = a_i + 1 \quad \textbf{2.14}$$

$$b^*_i = b_i - 1 \quad \textbf{2.15}$$

A la détection, une différence *S* de luminance des couples de pixels sélectionnés, est calculée :

$$S^* = \sum_{i=1}^{N} (a_i^* - b_i^*) \quad \textbf{2.16}$$

Cependant, Une personne ne disposant pas de la clef *K* ne peut que générer deux ensembles différents de *A, B* et obtiendra $S^* = 0$ (l'espérance de la somme est alors nulle). Seule la personne disposant de la clef sera en mesure d'obtenir la bonne valeur de S^*, c'est-à-dire *2N*.

Alors, si l'on choisit pseudo-aléatoirement deux ensembles de pixels de même cardinal que *A* et *B*, l'espérance mathématique *E* de la somme de leur différence est nulle :

$$E(S) = \sum_{i=1} [E(a_i) - E(b_i)] = 0 \quad \textbf{2.17}$$

Cette méthode peut se résumer par l'addition de l'image et une matrice *W* pseudo-aléatoire obtenue à partir de la clef *K,* ne contenant que des 1,-1 et 0 et étant de la même taille que l'image à tatouer. Où 1 représente les pixels de l'ensemble *A*, -1 pour les pixels de *B* et le 0 sinon. Si *I* est l'image originale, *I** l'image tatouée, on obtient :

$$I^* = I + W \qquad \textbf{2.18}$$

Cette technique, détaillée par *Pitas et al*. [35] fait partie des techniques dites à 1 bit d'insertion. C'est la connaissance de la clef qui identifie le propriétaire. *Langelaar* et *al*. [36] appliquent successivement la méthode de *patchwork* sur plusieurs blocs de l'image dans le but d'augmenter la robustesse du schéma.

- **Utilisation de l'etalement de spectre**

Le principe de cette méthode est d'étaler le spectre du signal de tatouage (la marque à incruster) sur un canal de transmission bruité (l'image hôte) en utilisant une large bande passante. Autrement dit, c'est une incrustation d'information extrêmement redondante. La marque ainsi étalée sera donc présentée sur toutes les fréquences et sera plus robuste aux attaques.

Tirkel et al. [37][38] On été les premiers auteurs à utiliser la technique de l'étalement de spectre pour insérer un signal dans une image. Cette technique se base sur le marquage des bits de poids faible de l'image d'une façon redondante en utilisant la même marque. La détection s'effectue par l'inter–corrélation entre les séquences ajoutées. Cette technique a été améliorée par *Hartung et al* [39] par l'utilisation d'un masque représentant l'activité de l'image comme espace d'insertion. La marque étalée a alors la même taille que l'image, avec des 1 et -1 dans les même coordonnés que les pixels du masque présélectionné, 0 sinon. Avant la pondération de la marque par le masque sélectionné, cette marque doit être modulée par une séquence aléatoire (*figure 2.3*). La séquence obtenue est ensuite ajoutée à l'image.

La détection s'effectue par corrélation entre la séquence aléatoire et l'image marquée sur le masque d'étalement. Le signe de la corrélation donne la valeur du bit inséré. Les auteurs précisent que les performances de la corrélation peuvent être améliorées en estimant la marque à l'aide d'un filtre passe-haut.

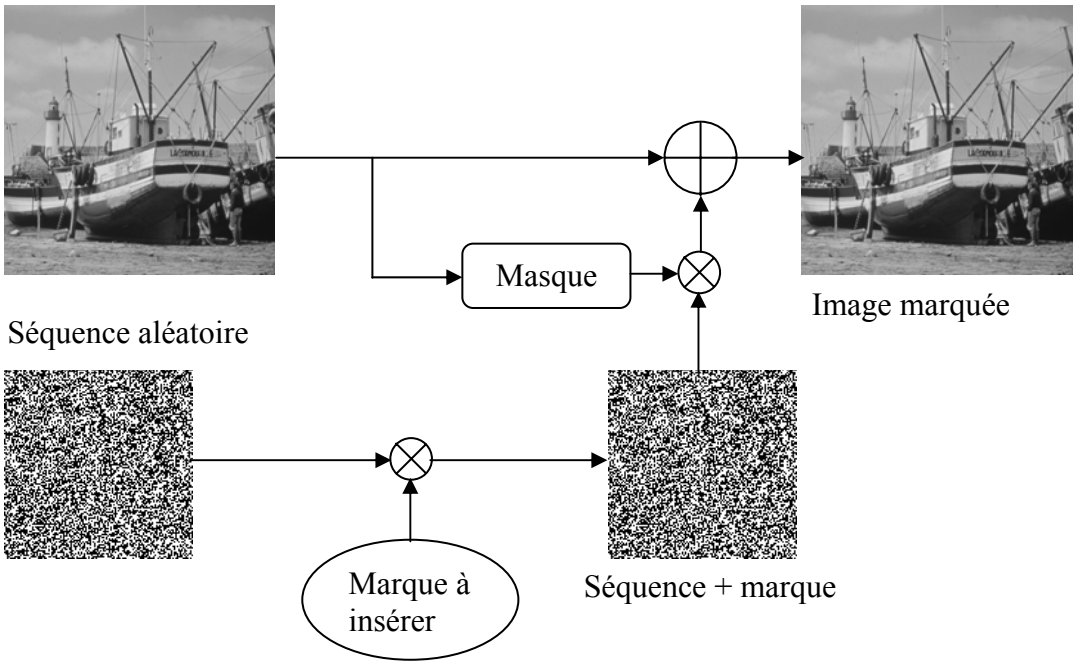


Figure 2.3 : *Principe d'incrustation du schéma de Hartung et al [39].*

Remarque:

Le tatouage par ''patchwork'' et par étalement de spectre sont donc très similaires. L'incrémentation d'un ensemble de pixels et la décrémentation d'un autre ensemble, pour le ''patchwork'' est équivalent à ajouter un signale aléatoire W (la marque à ajouter après modulation par une séquence aléatoire) sur l'image I pour le tatouage par étalement de spectre.

- **Domaine fréquentiel**

Cox et al. [40][41] proposent de n'incruster la marque que dans les basses fréquences de la DCT (Discrete Consinus Transform) appliquée à l'image originale.
Dans cette méthode un seuil est utilisé afin de ne modifier que les coefficients de plus grande amplitude (supérieur au seuil sélectionné) suivant l'une des formules suivantes:

$$y_i = x_i + \alpha w_i \quad \textbf{2.19}$$

$$y_i = x_i(1 + \alpha w_i) \quad \textbf{2.20}$$

$$y_i = x_i e^{\alpha wi} \quad \textbf{2.21}$$

Où :

y_i : Coefficient DCT de l'image tatouée.

x_i : Coefficient DCT de l'image à tatouer.

α : force du tatouage.

w_i : Coefficient de la marque.

En effet, la modification des basses fréquences qui constituent les composantes les plus significatives de l'image, par un facteur de robustesse élevé, dégrade fortement la qualité de l'image. La différence entre l'image originale et l'image tatouée (tatouage non aveugle) nous permet d'extraire la marque incrustée. La marque extraite w'_i est comparée à la suite par un calcul de corrélation s :

$$s = \frac{W'W}{\sqrt{W'W'}} \qquad \textbf{2.22}$$

La même méthode a été proposée par *Piva et al.* [42] mais avec une détection aveugle (sans l'intervention de l'image originale).

La modification des coefficients de la DCT s'effectue suivant la formule :

$$y_i = x_i + \alpha|x_i|w_i \qquad \textbf{2.23}$$

La détection s'effectue en évaluant la corrélation:

$$z = \frac{I^* W}{M} \qquad \textbf{2.24}$$

Où M représente le nombre de coefficients marqués.

- **Domaine multirésolution**

Barni et al. [43] proposent un schéma d'incrustation additif dans l'espace obtenu à partir de la transformée par ondelettes, avec une détection non aveugle.

Plusieurs autres schémas ont utilisés ce domaine [31][44][45], la différence entre ces schémas est celui proposé par *Barni et al* [43] se situe au niveau de la phase de détection.

L'espace utilisé pour l'incrustation de la marque est les trois sous-bandes de détails de la décomposition *(LH_1, HL_1, HH_1)* afin d'obtenir un meilleur compromis entre robustesse d'algorithme et invisibilité de marque. Le marquage des coefficients des ces trois bandes X_1^{LH}, X_1^{HL} *et* X_1^{HH}, s'effectue par une pondération d'une séquence pseudo-aléatoire W de même taille que la somme des trois bandes (3MN) (*figure 2.4*).

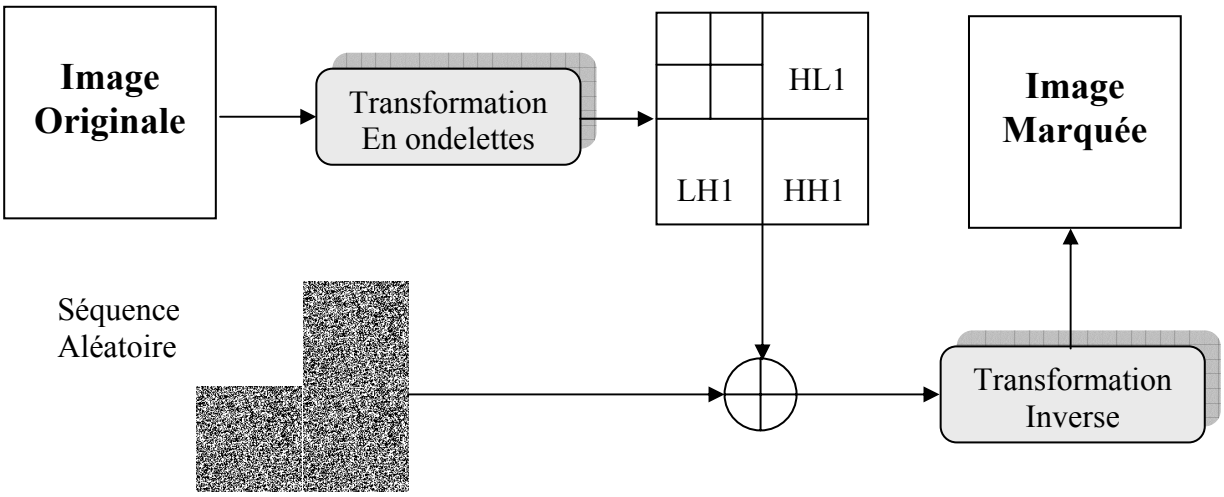


Figure 2.4 : *Incrustation de la marque après une décomposition multirésolution selon le schéma de Barni et al [43].*

Le marquage des trois sous-bandes s'effectue par addition:

$$Y_1^{LH}(i,j) = X_1^{LH}(i,j) + \alpha \, .p^{LH}(i,j)w_{iN+j} \quad \textbf{2.25}$$

$$Y_1^{HL}(i,j) = X_1^{HL}(i,j) + \alpha \, .p^{HL}(i,j)w_{MN+iN+j} \quad \textbf{2.26}$$

$$Y_1^{HH}(i,j) = X_1^{HH}(i,j) + \alpha \, .p^{HH}(i,j)w_{2MN+iN+j} \quad \textbf{2.27}$$

Où :

α désigne la force du tatouage.

p est la fonction de pondération qui dépend de l'algorithme d'incrustation de la marque proposé. La détection de la marque est obtenue par corrélation :

$$\rho = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [Y_1^{LH}(i,j)w_{iN+j} + Y_1^{HL}(i,j)w_{MN+iN+j} + Y_1^{HH}(i,j)w_{2MN+iN+j}] \quad \textbf{2.28}$$

p est ensuite comparé à un seuil qui dépend de la probabilité de fausse alarme qui est exigée.

2.4 Les schémas substitutifs

Contrairement à la classe des schémas additifs, la marque dans cette classe est substituée à des composantes de l'image. Nous détaillons dans cette section les différentes particularités de cette classe.

2.4.1 Incrustation de la marque

Les schémas substitutifs peuvent se décomposer en quatre étapes (*figure 2.5*).

1. Les composantes $C_K(I)$ *à* utiliser comme espace de marquage sont sélectionnées à partir de la clef secrète *K*. L'espace de marquage sélectionné peut par exemple désigner des coefficients de la DWT ou de la DCT de l'image, des pixels de l'image, ou encore des propriétés géométriques de l'image.
2. La marque à incruster est obtenue en appliquant une contrainte *F* sur $C_K(I)$ en fonction de la marque modulée par la clef *K (W(K))*. Cette contrainte s'exprime généralement par une relation d'ordre, un critère de corrélation, ou une propriété géométrique de l'image.
3. On procède ensuite à l'étape de substitution:

$$C_k(I_w) = F(C_k(I), W(K)) \qquad \textbf{2.29}$$

4. La dernière étape est la reconstruction de l'image tatouée à partir des composantes propres à la marque.

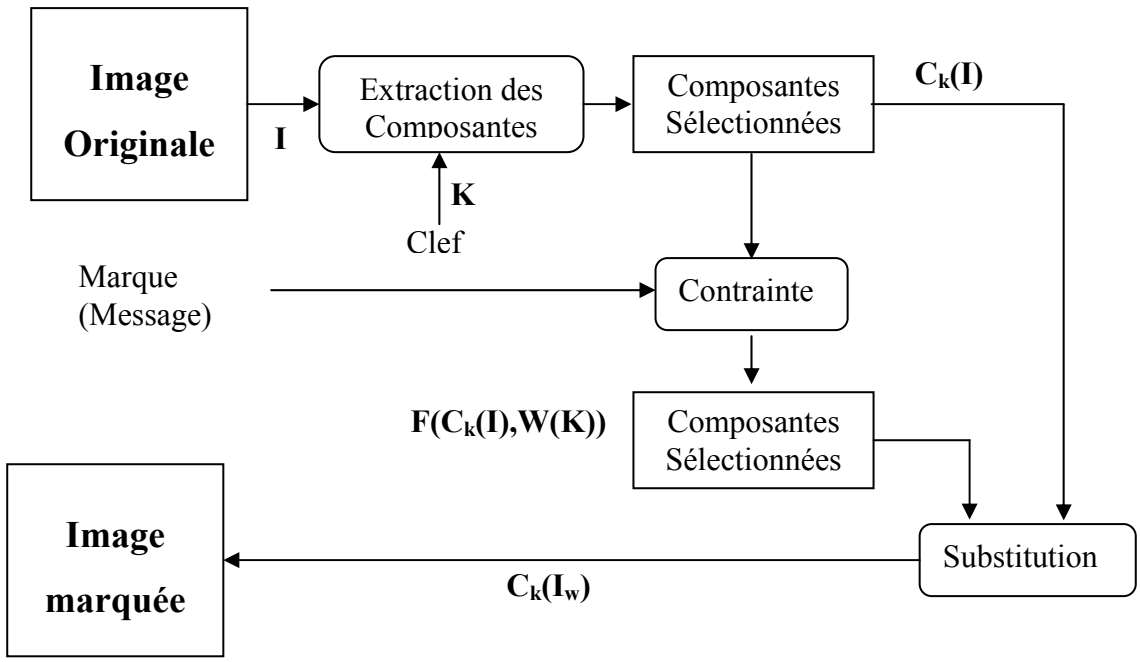


Figure 2.5 : *Principe de l'insertion par substitution.*

2.4.2 Détection de la marque

Les étapes permettant la détection de la marque sont au nombre de quatre (*figure 2.6*), la première étape est l'extraction des composantes de l'image tatouée I_t , ($C_K(I_t)$) en utilisant la clef secrète k. On procède dans la seconde étape à l'extraction de $W(K)$ par l'utilisation de la contrainte F utilisée lors de la phase d'incrustation. On compare dans la troisième étape le degré de similitude entre la séquence retrouvée et la séquence utilisée lors de l'incrustation pour détecter la marque. La marque peut ensuite être décodée.

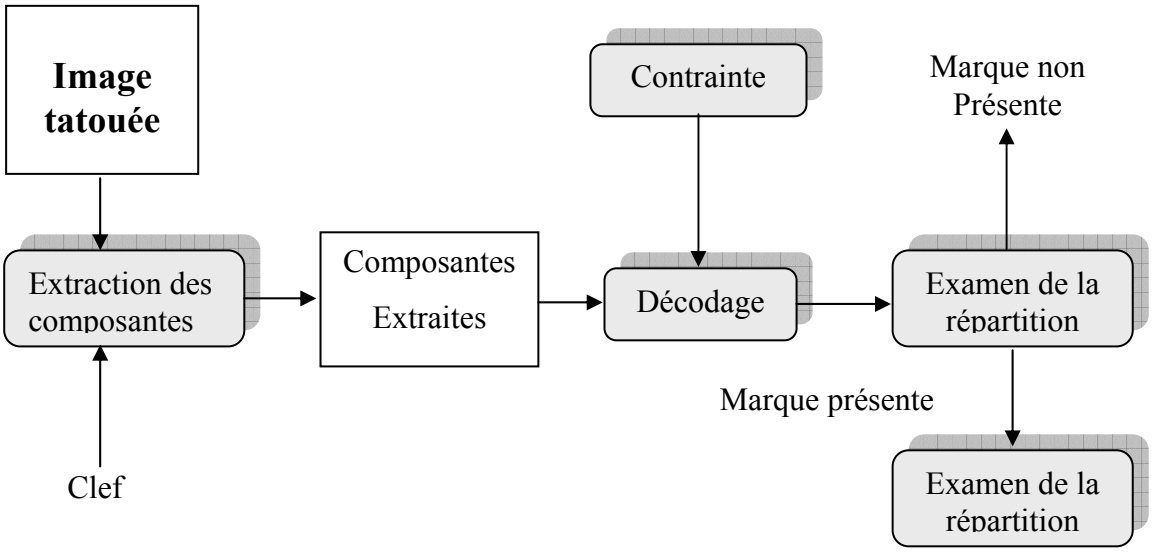


Figure 2.6 : *Détection de la marque par substitution.*

2.4.3 Tatouage substitutif dans les différents domaines

Nous montrons dans cette section plusieurs schémas de tatouage qui opèrent par substitution de la marque.

- **Domaine spatial**

Plusieurs approches sont développées, dans l'objectif d'améliorer la robuste des schémas de tatouage, par l'utilisation du domaine spatial. Parmi ces techniques nous pouvons citer:

- **Quantification Vectorielle Spatiale**

Le principe de base de la quantification vectorielle est de remplacer l'espace d'insertion (généralement, des blocs de pixels de l'image) par des blocs appartenant à un dictionnaire

constitué préalablement à partir de la marque à insérer. Une distance minimale entre les blocs du dictionnaire et les blocs de l'image est exigée afin d'assurer une robustesse maximale de l'algorithme.

Ce principe a été utilisé par *Chen et al* [15] pour incruster la marque au sein de l'image originale.

La détection de la marque est définie en vérifiant que les blocs de l'image appartiennent bien au dictionnaire utilisé lors de l'incrustation. L'inconvénient de la quantification vectorielle par rapport aux autres techniques, l'étalement de spectre à titre d'exemple, est sa dégradation prononcée après les différentes attaques.

- **Substitution d'histogramme**

Cette méthode de tatouage repose généralement sur la modification de la forme initiale de l'histogramme de l'image originale par l'utilisation des caractéristiques de ce dernier.

Coltuc et al. [46] proposent d'incruster la marque directement sur l'histogramme de l'image originale afin d'assurer une bonne invisibilité de la marque.

Les auteurs utilisent comme espace d'insertion les pixels de même valeur, ces pixels peuvent être différenciés selon la moyenne des valeurs associées à différents voisinages (plus de quatre voisinages). L'histogramme de l'image hôte est alors substitué par un histogramme modifié. La détection de la marque est effectuée par le calcul de l'histogramme.

Le principal défaut de cet algorithme est le manque de robustesse. En effet rien n'empêche de modifier à nouveau l'histogramme de l'image marquée pour enlever la marque.

- **Tatouage par incrustation de similarités**

Les schémas de marquage basés sur l'incrustation de similarités substituent des blocs de l'image par des blocs qui sont similaires. La détection de la marque s'effectue le plus souvent par recherche de ces similarités.

Plusieurs autres auteurs ont proposé d'incruster la marque par les techniques de substitution via un domaine spatial en utilisant d'autres techniques que la similarité et l'histogramme. *Maes et al.* [47] proposent d'utiliser la substitution des caractéristiques géométriques de l'image originale pour tatouage.

- **Domaine fréquentiel**

o **Modification des coefficients TCD**

Cette transformation est utilisée dans les normes de compression JPEG et MPEG par blocs de taille 8x8. Cette caractéristique est très souvent reprise dans les techniques de tatouage utilisant la DCT.

Zhao et al [48] ont choisi de découper l'image en bloc de 8x8 afin d'être d'avantage robuste à la compression JPEG. On fait ensuite la transformée DCT de chacun des blocs.

L'incrustation de la marque est effectuée à partir les 8 coefficients choisis parmi les fréquences moyennes de chaque bloc (*figure 2.7*). Seulement trois de ces coefficients $\{C_1,C_2,C_3\}$ sont choisis avant tatouage.
Un bit égal à 1 est incrusté en rajoutant une certaine valeur aux trois coefficients C_1, C_2, C_3 :

$$C1 > C3 + Cte \quad \textbf{2.30}$$

$$C_2 > C_3 + Cte \quad \textbf{2.31}$$

On leur enlève cette même valeur pour coder un 0 :

$$C_1 + Cte < C_3 \quad \textbf{2.32}$$

$$C_2 + Cte < C_3 \quad \textbf{2.33}$$

La détection de la marque s'obtient par la lecture des coefficients tatoués dans les blocs sélectionnés. L'algorithme proposé est bien adapté à la compression JPEG, mais avec une faible robustesse face à plusieurs autres attaques comme les transformations géométriques et les attaques de type collusion.

Bors et al [49] procèdent de manière similaire, mais utilisent soit une quantification scalaire dont la pas de quantification est en fonction de la marque:

$$FxW = Cte \quad \textbf{2.34}$$

Où W est un vecteur qui dépend de la marque et F est le vecteur des coefficients DCT tatoués. Le calcul de F s'effectue par minimisation des moindres carrés. La seconde méthode correspond à une quantification vectorielle réalisée sur certains coefficients DCT des blocs de

8x8. Cela revient à choisir le vecteur F tel que:

$$\left\| F - W_k \right\|^2 = \min_{i=1}^{H} \left\| F - W_i \right\|^2 \qquad \textbf{2.35}$$

Où W; étant un ensemble de vecteur provenant de la marque.

Dans le schéma proposé la détection de la marque s'effectue par une comparaison de la répartition des blocs marqués.

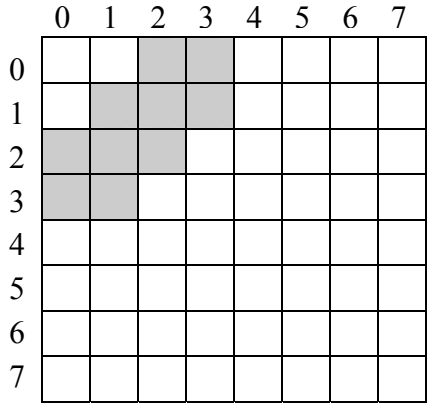


Figure 2.7: *Incrustation de la marque dans les coefficients moyenne fréquence du bloc TCD (représentés en grisé sur la figure) selon les schémas de Zhao et al [48][49].*

Langelaar et al. [50] proposent également une méthode de tatouage substitutive utilisant les coefficients DCT de blocs 8 x 8 de l'image.

Les blocs de l'image sont tout d'abord mélangés à l'aide d'une fonction aléatoire qui dépend d'une clef. Chaque bit du message à insérer est associé à une région de l'image après le mélange. Chaque région est divisée en deux régions de même taille et contenant le même nombre de bloc. Un bit est inséré en introduisant une différence d'énergie entre les blocs de la première région et les blocs de la seconde région. La différence d'énergie est créée en annulant les coefficients TCD se trouvant au-delà d'une fréquence de coupure f_c et la valeur du bit est encodée par la sélection d'une des régions.

Les auteurs proposent une approche statistique permettant de définir leurs paramètres d'insertion de manière optimale (nombre de blocs à l'intérieur d'une région, fréquence de coupure, pas de quantification maximale). Le message peut être codé en utilisant des codes correcteurs d'erreur (BCR) afin d'augmenter le nombre de bits insérés pour une probabilité de fausse alarme donnée.

- **Domaine multirésolution**

Un autre domaine d'incrustation couramment utilisé est celui engendré par une transformée en Ondelettes discrète (DWT). L'intérêt de ce domaine, outre son utilisation par JPEG2000, est l'aspect multi-échelle permettant une répartition plus robuste du tatouage.

Kundur et al [51] incrustent plusieurs bits dans l'image sur les triplets de coefficients de la DWT $\{C_k^{\ H}, C_k^{\ V}, C_k^{\ D}\}$où k représente le niveau de décomposition appliqué sur l'image originale et *H, V* et *D* représentent respectivement les sous-bandes Horizontales, Verticales et Diagonales. Une séquence aléatoire permet de sélectionner les différents triplets dans lesquels la marque sera incrustée. Ces triplets sont ordonnés en fonction de la valeur du bit à insérer.

La détection de la marque s'effectue en localisant les coefficients tatoués grâce à la séquence aléatoire utilisée lors de l'insertion. Les auteurs proposent d'utiliser la marque originale pour estimer la fiabilité de système de tatouage à partir de la mesure de la corrélation:

$$cor(w,w') = \frac{\sum w(n)w'(n)}{\sqrt{\sum w^2(n)}\ \sqrt{\sum w'^2(n)}} \qquad \textbf{2.36}$$

Où *W* est la marque originale et *W'* la marque extraite après tatouage.

Manoury et al. [52] utilisent également la transformée en ondelettes comme espace d'insertion de la marque.

L'algorithme proposé par les auteurs, utilise la décomposition en paquets d'ondelettes qui est une extension de la DWT. Dans cette décomposition chaque sous-bande peut être décomposée ou non en quatre autre sous-bande (*LL, LH, HL, HH*). L'algorithme proposé se décompose en deux étapes principales.

La première étape consiste à rechercher les vecteurs de la base optimale à l'incrustation de la marque. Les auteurs utilisent dans la seconde étape une clef secrète pour sélectionner les nœuds de la décomposition. Ces nœuds porteront la marque. L'incrustation de la marque s'effectue en modifiant la parité de la somme des nœuds sélectionnés pour chaque résolution. Un noeud sélectionné est égal à 1 s'il est contenu dans la base, sinon il est égal à 0. La

détection de la marque s'effectue en vérifiant la parité des vecteurs appartenant à la base optimale.

2.5 Types de tatouage D'images

2.5.1 Tatouage fragile

- **Principe**

Si l'on désire contrôler l'intégrité d'un document, alors il faut que le tatouage disparaisse dès que le document subit des modifications : on parle alors de tatouage fragile, et c'est la présence de la marque qui garantit l'intégrité.

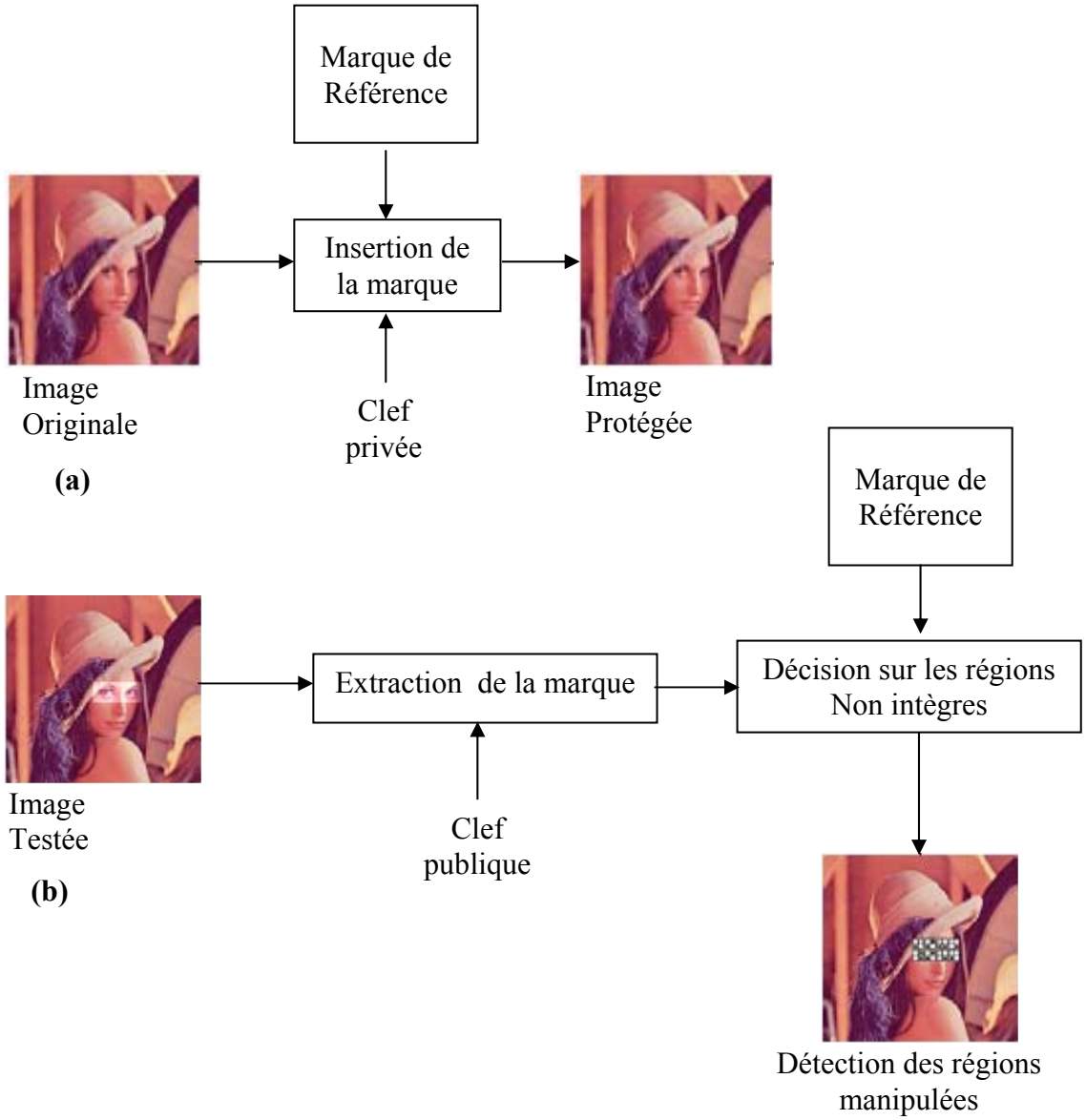


Figure 2.8 : *Schéma général d'un système d'intégrité basé sur un tatouage fragile.*

Le principe de tatouage fragile est d'incruster une marque binaire (généralement prédéfinie et indépendante des données à protéger [53]) dans l'image hôte de telle sorte que le tatouage disparaît à la moindre manipulation apportées à l'image tatouée (figure 2.8 (a)). La vérification locale de la présence de la marque peut permettre la vérification de l'intégrité d'une image (figure 2.8 (b)).

- **Utilisation des LSB**

Walton [54] est parmi les précurseurs des schémas de tatouage fragile par les LSB. L'auteur a choisi d'incruster des valeurs de contrôles « checksums » dans les LSB des pixels de l'image afin d'assurer une bonne invisibilité de la marque. Le schéma proposé par l'auteur consiste à sélectionner, par l'intervention d'une clef, des blocs de pixels et de mesurer, pour chacun d'eux, une valeur de checksum. Voici l'algorithme tel qu'il était proposé à l'origine :

Algorithme 1 - Etape d'incrustation

1. Soit une valeur de N suffisamment grande ;
2. Diviser l'image en blocs de taille 8×8 pixels ;
3. Pour chaque bloc Bi :
   - Définir un ordre de parcours pseudo-aléatoire (selon par exemple une clef secrète et l'indice du bloc Bi) des 64 pixels ($p1$, $p2$, ..., $p64$) ;
   - Générer une séquence pseudo-aléatoire de 64 entiers ($a1$, $a2$, ..., $a64$) du même ordre de grandeur que N ;
   - La valeur de checksum S est alors calculée de la manière suivante :

$$S = \sum_{j=1}^{64} (a_j . g(p_j)) \bmod N \qquad \textbf{2.37}$$

Avec $g(p_j)$ le niveau de gris du pixel p_j en ne tenant compte que des 7 MSB (Most Significant Bits).

- coder S en binaire ;
- insérer la séquence binaire obtenue au niveau des LSB des pixels du bloc

A la phase de détection, l'algorithme nécessite la présence de l'image originale ainsi que l'image tatouée (tatouage non aveugle). Elle consiste à calculer la valeur de checksum à partir des MSB des pixels de l'image tatouée et éventuellement manipulée.

L'algorithme proposé, présente plusieurs avantages en termes d'invisibilité de la marque et de qualité de tatouage vis-à-vis de la quantité d'information incrustée. Et le plus important, est la sensibilité de l'algorithme à la moindre modification de l'image. Si on permute, par exemple, les MSB de deux pixels quelconques d'un même bloc, la valeur de S s'en trouvera automatiquement modifiée car chaque pixel p_j est multiplié par un coefficient a_j différent.

L'inconvénient de l'algorithme proposé, est qu'il est possible d'échanger deux blocs de même position à partir de deux images tatouées avec la même clef, sans que le système ne découvre une perte d'intégrité. Plusieurs algorithmes ont été proposés [55] pour remédier à ce problème.

Le deuxième inconvénient est que, si l'image est attaquée par une légère compression par exemple, l'algorithme décèle une perte d'intégrité alors que le contenu sémantique de l'image reste le même.

- **Utilisation de la méthode Self-embedding**

Dans le but de reconstruire partiellement les régions détériorées après attaques, *Fridrich et al* [56] ont proposés d'insérer une grande quantité d'information à l'aide des LSB. Le schéma proposé opère dans le domaine transformé en utilisant la DCT. Cette transformée est appliquée sur des blocs de 8x8 pixels de l'image. La seconde étape consiste à quantifier les coefficients DCT de chaque bloc, à l'aide de la table de quantification correspondant à une compression JPEG d'une qualité de l'ordre de 50%. Après l'étape de quantification de bloc, les coefficients résultats, sont encodés sur 64 bits est incrustés dans les LSB des pixels d'un bloc suffisamment distant du bloc quantifié afin d'assurer que les distorsions locale que peut subir l'image ne détériore à la fois l'image et les informations de reconstruction.

Afin d'améliorer la qualité de la reconstruction, les auteurs ont proposés d'agrandir la matrice de quantification, par l'utilisation des deux bits de poids faible. Cette modification donne des bons résultas pour la reconstruction avec une qualité moyenne en termes d'imperceptibilité.

L'inconvénient majeur de cette méthode est dès lors que l'image subit une légère distorsion globale comme un filtrage passe-bas, la reconstruction correcte des blocs sera très difficile. Ce problème a dirigé les regards vers la recherche d'autres types de tatouage ; soit le tatouage semi-fragile.

2.5.2 Tatouage semi-fragile

Ce type de tatouage doit résister à certaines classes de distorsion légères de l'image, tant que le contenu sémantique de l'image n'est pas manipulé, comme la compression JPEG par exemple. On distingue donc pour le tatouage semi-fragile, deux classes d'attaques : les attaques auxquelles l'algorithme est robuste, et les attaques auxquelles il est fragile.

Lin et al [57] proposent un algorithme de tatouage robuste à la compression avec perte ainsi qu'au ajustement de la luminance des pixels, afin d'assurer une bonne reconstruction des zones altérées, même après un taux de compression important. Le schéma proposé repose sur deux propriétés invariantes des coefficients de la DCT avant et après compression JPEG.

La première propriété montre bien que si nous modifions les coefficients TCD originaux à un pas de quantification multiple, qui est plus grande que celles utilisées dans une compression JPEG acceptable, alors ces coefficients peuvent être reconstruits exactement après un taux de compression JPEG acceptable.

La deuxième propriété définit une règle d'invariance de la relation d'ordre entre les coefficients homologues de deux blocs DCT vis-à-vis de la compression JPEG. En effet, lors de la compression, les différents blocs DCT d'une image sont tous divisés par la même table de quantification. De ce fait la relation qui lie les coefficients de mêmes coordonnées de deux blocs reste inchangée après le processus de quantification. La seule exception est que dans certains cas, des inégalités strictes peuvent devenir de simples égalités, par le biais de la quantification.

Wolfgang et al [58][59] proposent de découper l'image originale en blocs b relativement grandes et d'incruster, dans chacun d'eux, une marque différente $W(b)$ afin d'améliorer la vérification de l'intégrité de l'image. Les auteurs ont proposés de générer la marque binaire en utilisant les principes initiés dans [38][60], pour augmenter la robustesse du système vis-à-vis de l'ajout de bruit.

L'idée de base de l'algorithme proposé, est de transformer la marque binaire à incruster {0,1} en une marque de {-1, +1}, puis de moduler cette marque par les blocs de l'image que l'on souhaite tatouer. Cette modulation est effectuée en augmentant ou en diminuant un niveau de gris :

$$Y(b) = X(b) + W(b) \qquad \textbf{2.38}$$

Où : X est l'image originale, et Y l'image tatouée.

Une autre méthode très similaire, a été proposée par *Fridrich* [61][62], mais l'auteur préconise, de générer la marque de façon dépendante du bloc dans lequel elle est incrustée. Le schéma proposé repose sur l'utilisation d'une technique d'étalement de spectre, similaire à celle utilisée dans [63]. Ce choix est motivé par le fait qu'il a une bonne robustesse à une variété de manipulations classiques telles que la compression JPEG, l'ajout de bruit, l'ajustement de contraste ou de luminosité.

Plusieurs autres méthodes de tatouage semi-fragile ont été proposées, parmi celles-ci on peut citer celle de *Kundur et al* [64], et celle de *Lin et al* [65] qui utilisent les ondelettes comme espace d'insertion de la marque.

2.5.3 Tatouage robuste

Les schémas des méthodes que nous proposons pour protéger les droits d'auteurs sont basés sur un tatouage robuste et non aveugle. Cependant, l'algorithme de marquage doit néanmoins disposer d'une forte capacité d'incrustation et doit être capable d'extraire la marque après des éventuelles attaques de différents types.

- **Principe général**

Cependant, les schémas de tatouage robuste sont les plus nombreux. Ceci est dû au fait que le contexte de la protection des droits d'auteur (la classe qui constitue la majorité des publications) nécessite une grande robustesse de la marque aux différentes attaques, volontaire ou non volontaire afin de protéger le contenu des propriétaires. Généralement, dans le tatouage robuste, la marque qui est utilisée n'est pas fixe, mais dépend de l'image elle-même.

Zhao et al [48] appliquent la DCT à des blocs de 8x8 de l'image originale, afin de rendre le schéma proposé plus robuste à la compression JPEG.

Un autre schéma robuste, a été proposé par *rey* [66], dans le but de vérifier l'intégrité d'une image. L'auteur dans sa thèse, propose d'utiliser une marque qui dépend de l'image elle-même, construite à partir certaines caractéristiques de l'image hôte. Le principe de base de cette méthode est de comparer simplement la marque incrustée avec les caractéristiques préalablement utilisées (caractéristiques de l'image originale). Si les caractéristiques sont identiques, cela signifiera que l'image n'a pas été manipulée, sinon les différences indiqueront les régions qui ont été altérées.

2.6 Tatouage d'images couleurs

En effet, les pixels d'une image couleur peuvent être vus comme un vecteur à 3 dimensions [67], Où chaque valeur d'un pixel est contenue dans un triplet (R;G;B) où le R représente la quantité de rouge, G la quantité de vert et B celle de bleu, ou à partir de l'espace chromatique (Y; U; V) qui est obtenu par la combinaison des trois composantes (R;G;B), dont Y représente la luminance du pixel, U et V représentent la chrominance (*voir la section 3.2.4 chapitre 3*).

Contrairement au tatouage d'images en niveau de gris, le tatouage couleur nécessite d'autres traitements à l'incrustation de la marque comme à l'extraction. Après une transformation d'espace couleur, de RGB vers YUV ou YCrCb (*équations* 3.1,3.2,3.3), la marque étant incrustée dans la luminance de l'image. Les schémas développés en niveaux de gris peuvent alors s'appliquer sur la luminance des images couleurs. Ce choix est généralement motivé par des raisons de robustesse vis-à-vis de la compression JPEG. Néanmoins, il aurait été tout à fait envisageable d'incruster la marque dans un autre espace colorimétrique, comme par exemple dans la composante bleue afin de minimiser la distorsion visuelle. Bien évidemment dans ce cas, le compromis capacité/visibilité/robustesse s'en trouve changé.

Kutter et al. [68] proposent de n'utiliser que la composante bleue *B*, comme espace d'incrustation, le tatouage de cette composante s'effectue par la modification de certains pixels dont les positions sont définies à partir d'une clef secrète. Chaque bit *s* est incrusté par l'opération :

$$B'_{ij} = B_{ij} + (2s - 1)L_{ij}\alpha \qquad \textbf{2.39}$$

Où $L_{ij} = 0.299R_{ij} + 0.587G_{ij} + 0.114B_{ij}$ et α est une constante qui détermine la force de la marque.

La détection de la marque s'effectue en estimant le bit inséré. Cette opération s'effectue en calculant la différence entre le pixel considéré et la moyenne locale du voisinage du pixel:

$$\delta = B'_{i,j} - \frac{1}{4c}\left(\sum_{k=-c}^{k=c} B_{i+k,j} + \sum_{k=-c}^{k=c} B_{i,j+k} - 2B_{i,j}\right) \qquad \textbf{2.40}$$

Le signe de δ permet d'estimer la valeur du bit inséré. Pour réduire la probabilité de fausse alarme (détection erronée), chaque bit est inséré à plusieurs endroits de l'image.

Fleet et al [69] utilisent une décomposition en trois bandes de nature distincte, basée sur un modèle psychovisuel plus complexe. La première bande désigne la composante noir/blanc, la deuxième représente la composante rouge/vert et la troisième est la composante jaune/bleu.

L'incrustation de la marque s'obtient par l'ajout de composantes sinusoïdales dans la composante Jaune/Bleu. La détection de la marque s'effectue par la détection de sinusoïdes dans le spectre de l'image.

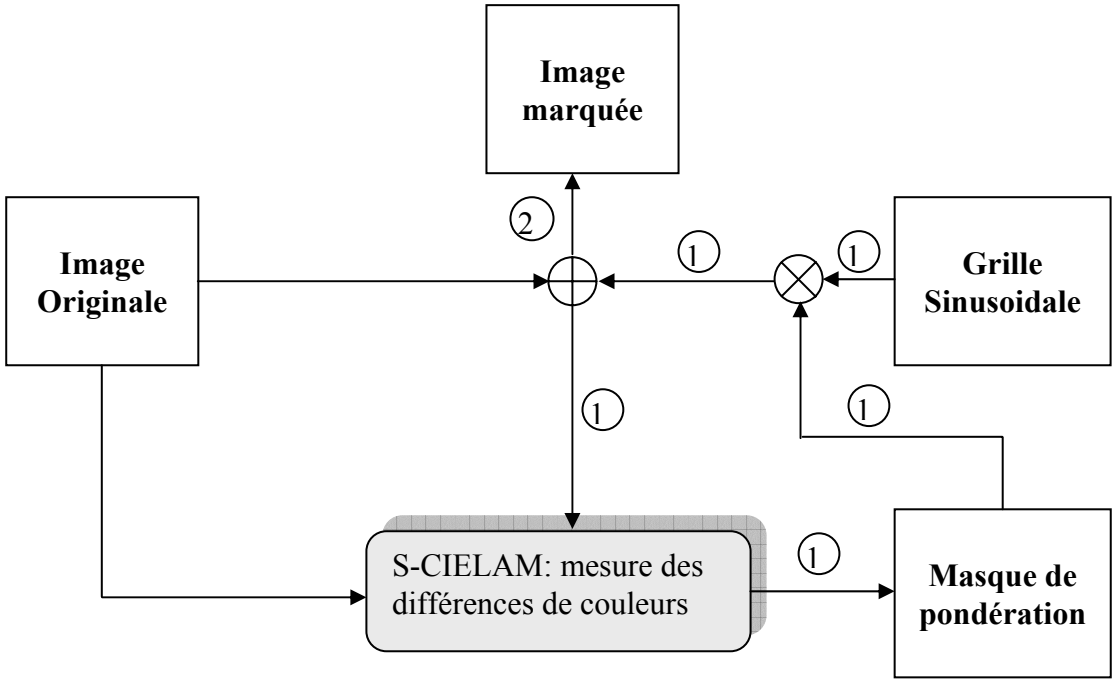


Figure 2.9 : *(1) La pondération de la grille s'effectue par itérations successives en mesurant*

la différence visible entre l'image originale et l'image tatouée. (2) Lorsque la différence n'est plus visible, l'image tatouée est créée.

Piva et al. [70] proposent d'incruster la marque de manière indépendante dans les trois canaux RGB, en utilisant la transformation en cosinus discrète.

Les auteurs ont proposé d'utiliser une force de marquage différente en fonction de la réponse de l'œil aux différentes longueurs d'ondes pour chaque canal (R, G et B).

La marque W est incrustée ainsi d'une façon indépendante dans les trois composantes R, G et B:

$$\begin{cases} y'_{R_i} = y_{R_i} + \alpha_R \left| y_{R_i} \right| & \textbf{2.41} \\ y'_{V_i} = y_{V_i} + \alpha_V \left| y_{V_i} \right| & \textbf{2.42} \\ y'_{B_i} = y_{B_i} + \alpha_B \left| y_{B_i} \right| & \textbf{2.43} \end{cases}$$

Les facteurs $(\alpha_R , \alpha_V , \alpha_B)$ déterminent la force de la marque . Ils dépendent de la réponse de l'oeil humain aux différentes longueurs d'onde. Les auteurs utilisent la courbe de sensibilité de l'oeil en fonction de la longueur d'onde $E(\lambda)$:

$$\begin{cases} \alpha_R + \alpha_V + \alpha_B = \alpha_{RVB} & \textbf{2.44} \\ \alpha_R / \alpha_G = E(\lambda_V / \lambda_R) = 1.89 & \textbf{2.45} \\ \alpha_B / \alpha_G = E(\lambda_B / \lambda_V) = 10.48 & \textbf{2.46} \end{cases}$$

La détection de la marque s'effectue par une corrélation entre les trois canaux, afin d'extraire une marque de bonne qualité.

2.7 Conclusion

Nous avons présenté dans ce chapitre les différentes classes de schémas qui ont marqué l'évolution du tatouage.

Si au départ les schémas de marquage étaient de type additif [38][40], ils ont ensuite évolué vers des schémas opérant par substitution [48] et sont devenus de plus en plus

performant. L'augmentation de la robustesse des différents schémas est liée à la prise en compte du contenu de l'image. Ceci a permis d'augmenter la puissance de la marque, au travers de méthodes basées sur le système visuel humain, ou encore de synchroniser la détection de la marque après une transformation géométrique (cas des schémas auto-synchronisants).

Dans la suite de ce mémoire, nous nous attachons à développer des schémas de tatouage additifs et non aveugles basés sur une marque ou une marque fixe. Le chapitre suivant présente l'outil de base qui nous a permis d'atteindre cet objectif : la transformée on ondelettes discrètes.

Troisième chapitre

Outils mathématiques

3.1 Introduction

La *transformée en ondelettes* d'un signal permet de représenter le signal sur un espace bidimensionnel appelé le plan *temps-échelle*, fournissant sur le signal des informations conjointes en temps et en fréquence. Le pavage du plan *temps-fréquence* induit par cette transformée a pour particularité de permettre une résolution temporelle fine aux hautes fréquences et une résolution fréquentielle fine aux basses fréquences. Cette propriété permet souvent une analyse intéressante du signal mais reste rigide.

Nous allons présenter dans ce chapitre les différents outils cités ci-dessus. Nous commençons à introduire quelques définitions et propriétés des images numériques, ainsi que les espace de représentation de la couleur RGB et l'espace YCbCr de type luminance – chrominance, puis nous parlerons de la *transformée en ondelettes discrète* et de l'*analyse multirésolution* permettant de générer certaines de ces ondelettes.

3.2 L'image numérique

3.2.1 Signaux

Le principe de toute communication est l'échange de l'information entre un émetteur (source) et un récepteur (destination) par l'utilisation d'un support de communication (canal). L'information transmise entre l'émetteur est le récepteur est codée par un signal. Un signal est donc la représentation physique de l'information, qu'il convoie de sa source à son destinataire. En effet, depuis quelques années, la théorie du traitement du signal [71][72][73][74], a amplement évoluée afin de satisfaire des besoins de transmission et de compression des données numériques (audio et vidéo).

Dans la majorité des cas, les signaux réels sont des fonctions du temps et sont issus de capteurs physiques (capteur de température, de vitesse, de pression. . .). De nombreux signaux dépendent également de variables d'espace. Ainsi, les signaux peuvent être mono ou multidimensionnels en fonction de la grandeur qu'ils représentent.

En effet, on peut distinguer plusieurs types de classification pour les signaux suivant leurs propriétés, parmi ces types on peut distingue :

Les signaux déterministes : sont les signaux reproductibles lors d'expériences dont les propriétés sont parfaitement connues. On retrouve dans cette classe les signaux périodiques, les signaux transitoires, les signaux pseudo-aléatoires, etc…

Les signaux aléatoires : ces signaux ne sont pas reproductibles, on ne peut qu'obtenir des réalisations d'un processus lors d'expériences. Ces réalisations ne permettent pas de caractériser le signal, il faudrait procéder à une infinité de mesures pour définir parfaitement le signal. Le comportement du signal aléatoire est décrit par des données statistiques estimées à partir des réalisations.

Une autre classification très importante des signaux repose sur les représentations du temps et de l'amplitude. On peut distinguer alors quatre types de signaux selon le temps et l'amplitude :

- Signaux analogiques : dont le temps et l'amplitude sont continus.
- Signaux quantifiés : dont le temps est continu et l'amplitude discrète.
- Signaux échantillonnés : dont le temps est discret et l'amplitude continue ;
- Signaux numériques : dont le temps et l'amplitude sont discrets.

On peut dire ainsi que les signaux numériques sont des signaux échantillonnés et quantifiés. La *figure 3.1* montre un signal continu et le signal numérique correspondant.

Dans le cas des images qui sont représentés par des signaux numériques bi-dimensionnels, les niveaux de gris sont quantifiés et représentés sur une grille discrète. Les méthodes d'analyse des images sont des techniques numériques [73].

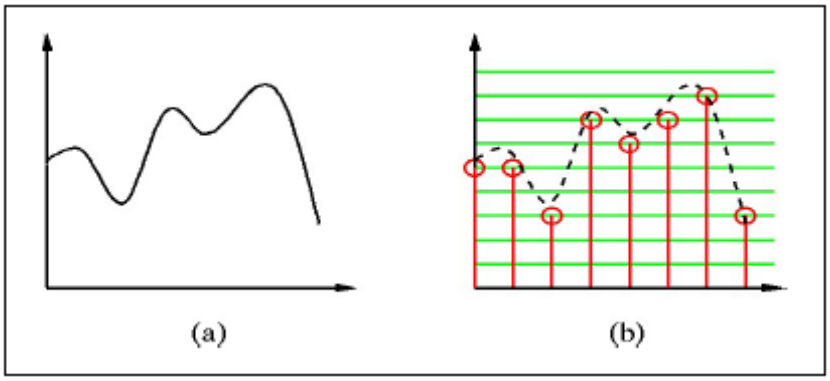


Figure 3.1: *(a) signal continu, (b) signal numérique.*

Les signaux qui apportent de l'information sont les signaux qui varient au cours du temps. En traitement du signal, on va donc chercher à détecter les transitions (singularités) qui vont apporter des informations sur le signal étudié.

En plus de la représentation spatiale ou temporelle du signal, il existe une représentation fréquentielle. Tout signal peut être décomposé à l'aide de la transformée de Fourier en composantes sinusoïdales caractérisées par leur fréquence et leur amplitude. Les basses fréquences correspondent à l'allure générale du signal (variations lentes), tandis que les hautes fréquences sont caractéristiques des détails du signal (variations rapides).

3.2.2 Définition d'une image

Avant d'entrer dans le sujet proprement dit, il est important de comprendre la notion des objets que nous allons manipuler. Intéressons-nous à la définition d'une image, qu'est-ce qu'une image ? La définition du dictionnaire le petit robert [75] donne : une image est la « reproduction exacte ou représentation analogique d'un être ou d'une chose ».

Alors, l'image codée sur un ordinateur (représentation discrète) est la représentation numérique d'un objet quelconque appartient au monde des réels (représentation continue).

Cette représentation numérique d'une image, peut être exprimée mathématiquement par une fonction à 2 dimension d'intensité *f(x,y)* avec :

- Une amplitude de l'intensité de cette image nommée *f,*
- *(x,y)* étant un point dans un espace *2D*.

L'image *f(x,y)* est représentée par une matrice de *M* x *N* éléments, Sachant que chaque élément *f(i,j)* de cette matrice représente un pixel(*pic*ture *el*ement) de l'image *f(x,y).*

$$f(x,y) \sim \begin{vmatrix} f(0,0) & f(0,1) & f(0,2) & \dots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & \dots & f(N-1,M-1) \end{vmatrix}$$

Les images numériques sont des images *bitmapped*, puisque les coordonnées x,y d'un pixel sont localisés (*mapped*) par les *bits*. C'est une image matricielle.

La numérisation (conversion du signal analogique en signal numérique) nécessite deux opérations :

- La discrétisation des coordonnées spatiales (ou échantillonnage spatial) : l'image analogique est découpée en petits pixels de coordonnés *x,y*.
- La discrétisation de l'amplitude *f* (ou quantification des niveaux de gris ou en couleurs).

Ces deux opérations déterminent respectivement la taille (par le nombre de pixels) et la dynamique (par l'étendue de la gamme des teintes de gris ou de couleurs liée au nombre d'octets) de l'image et influencent la quantité d'information contenue dans une image numérisée.

3.2.3 Codage des niveaux de gris

Une image en niveau de gris (généralement 256 niveaux) est une image composée de points gris plus ou moins foncés. Chaque pixel tient sur 8 bits (2^8 = 256 niveaux de gris), du noir pur niveau 0 (code : 00000000) au blanc maximal 255 (code : 11111111), alors pour chaque pixel l'ordinateur enregistre une valeur de gris entre le noir et le blanc.

Exemple : le niveau de gris 245 s'écrit 11110101. C'est un gris très clair, proche du blanc 255 comme le montre le *tableau 3.1.* .

000	008	016	024	032	040	048	056	064	072	080	088	096	104	112	120	128
	255	248	240	232	224	216	208	200	192	184	176	168	160	152	144	136

Tableau 3.1: *Codage des niveaux de gris.*

Ce codage de la simple intensité lumineuse est également utilisé pour le codage d'images couleurs : l'image est représentée par trois images d'intensité lumineuses (*figure 3.3.*), chacune se situant dans une composante distincte de l'espace colorimétrique (par exemple, intensité de rouge, de vert et de bleu).

3.2.4 Représentation de la couleur

La couleur peut être vue comme une information trichromatique des stimuli du spectre visuel. Sans entrer dans une analyse physiologique de la perception humaine, décrivons

brièvement les principaux espaces couleurs que nous avons étudiés et utilisés durant ce travail. Pour plus d'informations sur ces espaces, le lecteur pourra se référer à l'ouvrage [76].

Comme l'expliquent Colantoni et al. dans [77], la visualisation des images, dans différents espaces couleurs peut fournir des éléments fondamentaux quant à l'attente que nous pouvons avoir de certains algorithmes de traitement d'image. De plus, cette visualisation peut permettre de comprendre les raisons de l'échec d'une méthode dans un espace d'étude donné par rapport à un autre espace.

3.2.4.1 L'espace initial RVB

Dans la quasi totalité des applications actuelles, l'espace d'acquisition et de sauvegarde des images est basé sur l'espace couleur RVB. L'acquisition utilise cet espace pour des raisons techniques évidentes dues aux capteurs de type RVB. Il existe différents types d'espaces RVB, qui dépendent du matériel utilisé : choix des longueurs d'ondes et des primaires par exemple. En fait, dans très peu de cas, nous pouvons considérer que l'espace RVB correspond à l'espace additif défini dans [78], avec les primaires rouge (*700 nm*), vert (*546.1 nm*) et bleu (*435.8 nm*).

Un autre espace couleur dépendant du matériel, principalement pour l'impression des couleurs, est l'espace Cyan, Magenta, Jaune. Cet espace soustractif est défini comme le triplet $(C,M,Y) = (1 - R, 1 - V, 1 - B)$. La distance couleur associée à ces espaces est la distance euclidienne.

Le triangle de Maxwell représenté dans l'espace RVB (*figure 3.2*) est le triangle reliant les trois couleurs pures Rouge, Vert et Bleu. Il nous permettra suivre les différentes distorsions dues aux changements d'espaces couleur.

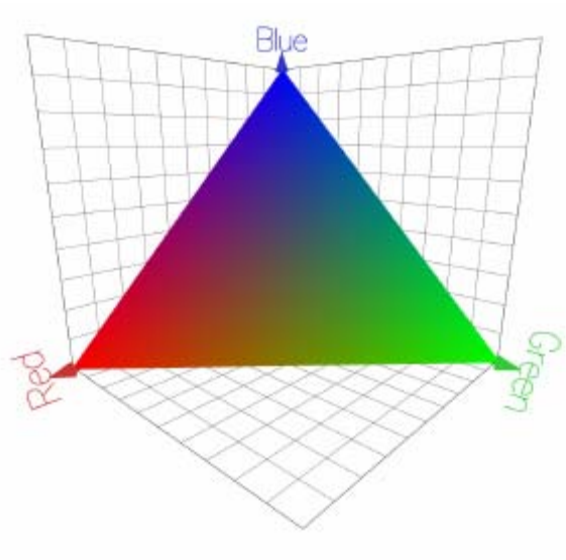


Figure 3.2 : *Triangle de Maxwell dans l'espace RVB.*

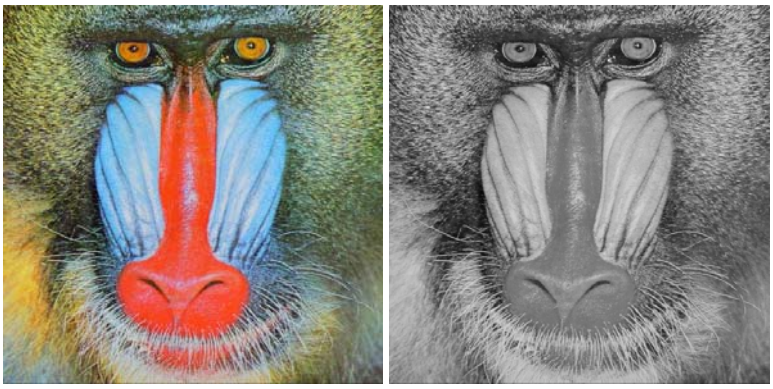
Dans le modèle RVB, les couleurs sont décrites par trois couleurs primaires : le Rouge, le Vert et le Bleu (*figure 3.3*). Sur un ordinateur, les coefficients de chacune des couleurs vont de 0 à 255 (*tableau 3.2*); ils sont donc chacun codés sur un octet. Ainsi, dans l'espace RVB, on a 256*256*256 couleurs différentes, soit plus de 16 millions.

Pour stocker une image dans un ordinateur, on affecte une couleur à chacun de ses pixels. Cette couleur est codée en RVB, c'est à dire qu'elle est décrite par la proportion de rouge, de vert et de bleu qu'elle contient. Comme chacune des couleurs est codée sur un octet, il faut 3 octets pour décrire une couleur (ou un pixel).

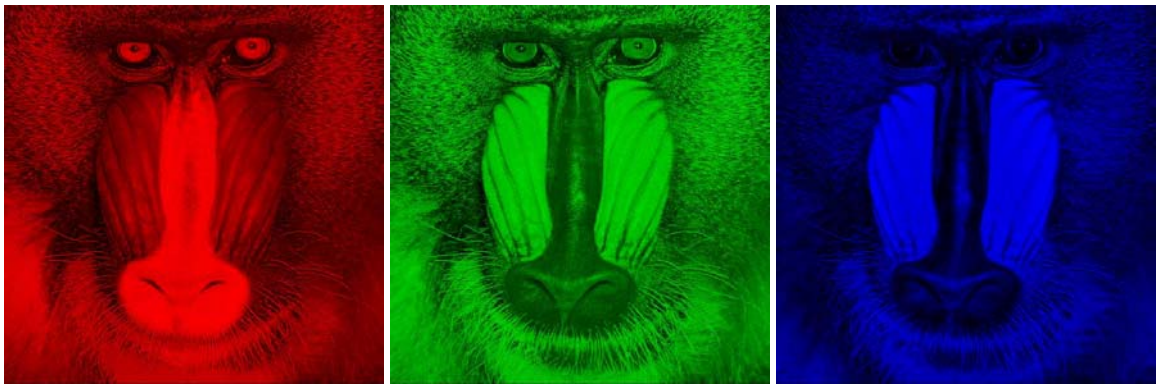
R	V	B	Couleur
0	0	0	noir
0	0	1	nuance de noir
255	0	0	rouge
0	255	0	vert
0	0	255	bleu
128	128	128	gris
255	255	255	blanc

Tableau 3.2: *Codages des couleurs.*

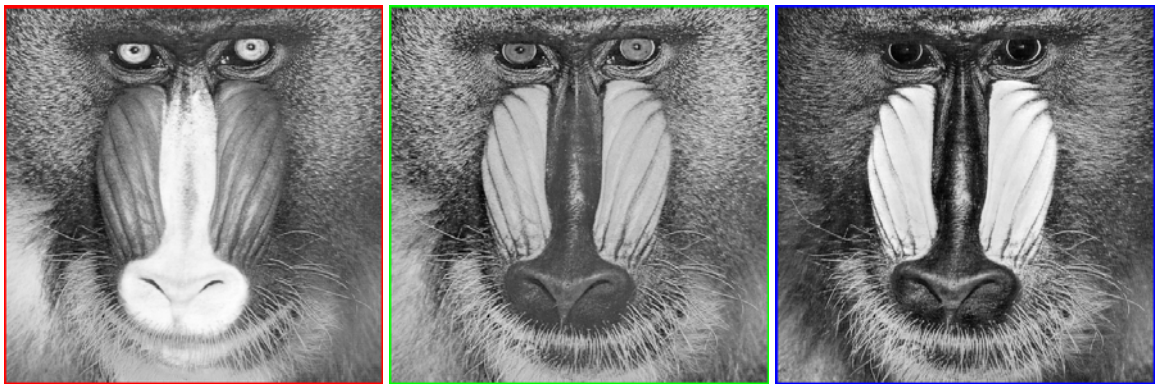
L'avantage du RVB est qu'il est parfaitement adapté à l'informatique. De plus, il contient un grand nombre de couleurs, 16 millions, et le gamut est équilibré dans toutes les couleurs.



a: *Image en RVB.* **b:** *Image en niveaux de gris.*



c: *La composantes R.* **d:** *La composantes G.* **e:** *La composantes B.*



f: *Niveaux de gris de R.* **g:** *Niveaux de gris de G.* **h:** *Niveaux de gris de B.*

Figure 3.3: *La représentation du modèle RVB***.**

3.2.4.2 Les espaces chrominance – luminance (YCbCr)

Une autre possibilité intéressante, dans l'optique d'un traitement de la couleur, est de décorréler la chrominance de la luminance. Ainsi, l'information chrominance est portée sur deux axes, et l'information luminance sur le troisième. Nous pouvons ici citer différents espaces de ce type, comme YCbCr, YIQ, YUV.

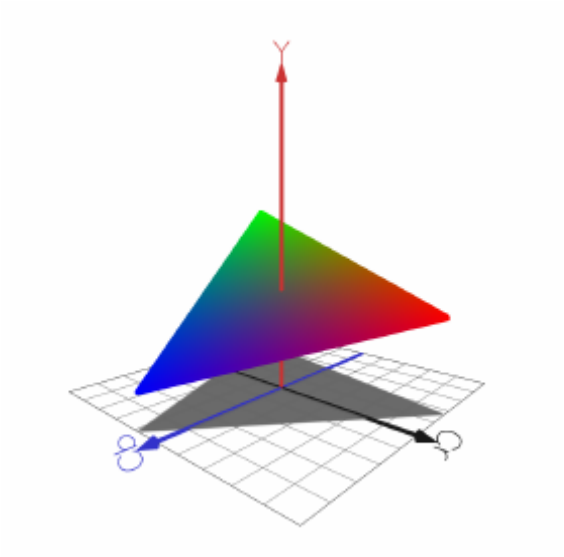


Figure 3.4: *Triangle de Maxwell dans l'espace YCbCr.*

Ce codage est utilisé par les professionnels de la vidéo numérique. Il ne code pas les trois couleurs rouge, vert et bleu mais le blanc, appelé luminance(Y), le bleu (Cb) et le rouge (Cr), appelés chrominances (*figure 3.5*). Ces trois signaux différents (notés aussi Y, U et V sont transmis et enregistrés sur des pistes différentes. Ce système de codage a été choisi car l'oeil humain est beaucoup moins sensible aux informations de couleurs qu'aux informations de luminosité.

3.2.4.3 RVB vers YCbCr

La transformation avec le RVB est simple puisque linéaire, et elle s'avère très utile. En effet, l'oeil est sensible à la luminance (écarts de lumière) et à la chrominance (écarts de couleur), mais pas à des écarts de rouge, vert ou bleu qu'il ne sait trop appréhender. Ainsi, il est plus facile d'agir sur ses composants de luminance et de chrominance pour pouvoir compresser et coder l'image et la vidéo de façon plus adaptée. En image, le passage de RGB à YCbCb est la base du codage JPEG. En vidéo, le MPEG et bien d'autres formats utilisent le YUV. Historiquement, ce format a été adopté pour que l'on puisse transmettre simplement aux télévisions noir et blanc (qui ne captaient alors que la composante de luminance). Les composantes Y,Cb et Cr sont obtenues à partir de l'espace RGB via la formule:

$$\begin{cases} Y &= 0.299\times R + 0.587\times V + 0.114\times B & \textbf{3.1} \\ Cb &= -0.169\times R - 0.331\times V + 0.500\times B & \textbf{3.2} \\ Cr &= 0.500\times R - 0.418\times V - 0.082\times B & \textbf{3.3} \end{cases}$$

Ces espaces sont donc également très importants dans le monde du multimédia. Les avantages de ces espaces est qu'ils sont parfaits pour être utilisé dans le codage de l'image et de la vidéo. Ils permettent de transmettre aisément de la vidéo sur les téléviseurs en noir et blanc.

a: *La composante Y.* **b:** *La composante Cb.* **c:** *La composante* Cr.

Figure 3.5: *Espace de représentation de la couleur YCbCr.*

3.2.5 Compression des images

- **Compression DCT (JPEG)**

La compression JPEG est basée sur le fait que l'œil est plus sensible aux changements de brillance (luminescence) de couleurs voisines : le but est donc de permettre un taux de compression important pour que les modifications apportées sur l'image ne soient pas visibles à l'œil (ceci est vrai pour les taux de compression les plus faibles mais n'est plus vrai pour les taux de compression les plus élevés).

Cette compression JPEG est une compression avec perte s'effectuant en plusieurs étapes :

- Conversion de l'image de son mode originale RVB dans un autre mode de couleur (YCbCr par exemple).
- Echantillonnage des composants de chrominance (information des couleurs auxquelles l'œil est moins sensible) : les pixels alloués à la chrominance forment des blocs de 2 x 1 ou 2 x 2 pixels alors que la luminescence est toujours codée sur 1 x 1 pixel.

- Application de l'algorithme DCT sur 8 x 8 blocs de pixels : chaque bloc est décrit par une fonction mathématique (la dérivée cosinus discrète).
- Quantification de la compression par l'utilisateur : il est possible de compresser plus ou moins les données en faisant varier le taux de compression de 1 à 99 %. Les coefficients de la fonction mathématique sont ainsi pondérés pour produire plus ou moins de détails.
- Codage des coefficients contenant des informations redondantes selon la méthode de *Huffman* : au lieu de prendre des suites de répétitions -exemple de suite de répétition : si un ciel uniformément bleu est décrit par 25 00 pixels et est codé 26, 54, 255 ; la suite est écrite sous la forme de (25, 54, 255) x 25 000- les codes sont indexés selon le nombre d'occurrence dans le fichier. La compression s'effectue en procédant d'abord à l'établissement d'une table statistique des différents codes, puis au tri des données, les occurrences les plus fréquentes étant placées en tête du fichier afin qu'à la décompression, chaque code retrouve son emplacement d'origine.

o Inconvénients de la compression JPEG :

- L'usage est limité à des données dont les changements sont imperceptibles pour un humain ; les artefacts introduits par la compression JPEG sont visibles sur des images contenant de grandes surfaces d'une seule couleur contrairement à des images chargées.
- Les phases successives de compression/décompression sont à éviter. Chaque fois qu'une image JEPG est enregistrée, il y a perte irréversible car il y a une compression. De plus, la perte n'est pas linéaire : comprimer 10 % ne signifie pas perdre 10 % des informations et l'échelle de compression varie selon les logiciels.
- Les phases de compression/décompression peuvent être lentes. La meilleure performance (compression/décompression rapide) correspond à un taux de compression 20:1.

Pour remédier à la faible qualité des images après modifications, ce format a subi une évolution, *JPEG 2000*, réunissant les avantages du *GIF* et du *JPEG*. Le *JPEG 2000* est basé sur une compression par ondelettes sans perte.

- **Compression par ondelettes (JPEG 2000)**

La compression par ondelettes est une technique de traitement du signal qui consiste à décomposer une image en une multitude de sous-bandes, c'est-à-dire des images de résolution inférieure.

Pour obtenir un niveau inférieur de sous-bande, il faut :

1. Moyenner les pixels de l'image originale deux à deux suivant l'axe horizontal :

$$H(X) = (X_n + X_{n+1})/2 \quad \textbf{3.4}$$

2. Calculer l'erreur entre l'image originale et l'image sous-échantillonnée dans le sens horizontal :

$$G(X) = (X_n - X_{n+1})/2 \quad \textbf{3.5}$$

3. Pour chacune des deux images intermédiaires, moyenner les pixels deux à deux suivant l'axe vertical :

$$H(Y) = (Y_n + Y_{n+1})/2 \quad \textbf{3.6}$$

4. Pour chacune des deux images intermédiaires, calculer l'erreur suivant l'axe vertical :

$$G(Y) = (Y_n - Y_{n+1})/2 \quad \textbf{3.7}$$

Le résultat est une image d'approximation qui a une résolution divisée par deux et trois images de détails qui donnent les erreurs entre l'image originale et l'image d'approximation. Cette transformation est répétée autant que nécessaire pour obtenir le nombre voulu de sous-bandes.

La transformation inverse par ondelettes reconstruit l'image originale à partir de ces 4 images sans perte.

Pour compresser une image, 3 étapes sont nécessaires :

1. Transformation par ondelettes ;

2. Quantification : les valeurs des images de détails inférieures à un certain niveau sont éliminées (pertes) ;
3. Codage des valeurs restantes.

La construction de l'image à partir des sous-bandes restitue l'image en mode progressif, l'affichage de l'image décompressée peut s'effectuer en 2 modes :

1. La taille de l'image augmente au fur et à mesure de la lecture du fichier décompressé
2. La résolution de l'image augmente au fur et à mesure de la lecture du fichier décompressé

- **Comparaison JPEG et JPEG 2000**

Compression DCT (JPEG)	**Compression par ondelettes (JPEG 2000)**
· La compression DCT analyse l'image par bloc de 8 x8 pixels ; ceci produit un effet mosaïque et les limites des blocs sont visibles à fort taux de compression	· Pas d'effet mosaïque indésirable ; il est possible de compresser des images par ondelettes avec un taux de compression élevé tout en conservant une bonne qualité picturale.
· De plus les blocs de 8 x8 pixels sont quantifiés indépendamment les uns des autres, ne permettant pas de réduire les redondance au delà d'un bloc.	· C'est une méthode globale sur toute l'image : on peut réduire fortement de grosses images de 50 Mo à 1 Mo.
	· Un ratio de compression est directement programmable et on peut prévoir la taille du fichier compressé quelle que soit l'image.
	· La compression est intrinsèquement progressive et permet de reconstruire facilement l'image à plusieurs résolutions.
· 3 s pour compresser et 1 s pour décompresser une image 640 x480 x24.	· 1 s pour compresser /décompresser.
· Ratio moyen de compression pour une image en couleur : 25 :1	· Ratio moyen de compression pour une image en couleur : 50 :1

Tableau 3.3: *Comparaison entre JPEG et JPEG 2000.*

3.3 Représentations temps-fréquence et temps-échelle

Un outil mathématique utilisé depuis très longtemps en traitement du signal est la transformée de Fourier que nous allons présenter en précisant quelques avantages et quelques inconvénients. Puis l'analyse en ondelettes que nous utilisons dans ce travail sera présentée en détails.

3.3.1 Transformée de Fourier à fenêtre glissante

La transformée de Fourier est un outil permettant de connaître le comportement fréquentiel d'un signal. En utilisant cette transformation, on perd toute information relative au temps. Pour remédier à cela, et dans le cadre des signaux à énergie finie ($x(t) \in L^2(R)$), on utilise un outil « temps fréquence » : on restreint l'existence du signal autour d'une date *t*, grâce à une fenêtre d'analyse g(u – t) centrée sur cette date, puis on en prend sa transformée de Fourier Gabor [79] :

$$\int x(u)g(u-t)e^{-i\,2\pi vu}du \qquad \textbf{3.8}$$

On fait alors glisser cette fenêtre le long du signal, ce qui permet d'en mesurer le contenu spectral au cours du temps. On appelle cette transformation la transformée de Fourier à fenêtre glissante (à Court Terme), on la note *STFT* (*Short Term Fourier Transform*).

$$T_x(v,t) = \int x(u)g(u-t)e^{-i2\pi vu}du = \int x(u)g^*_{v,t}(u)du = < x(u), g_{v,t}(u) > \qquad \textbf{3.9}$$

Cette transformation peut être vue comme la projection du signal sur des atomes temps fréquences, les $g_{v,t}$. Ces vecteurs sont obtenus par applications successives de deux opérateurs élémentaires à une fonction-mère de référence ***g***. L'opérateur de translation temporelle déplace celle-ci le long de l'axe des temps, tandis que l'opérateur de translation (ou de modulation) fréquentiel la fait glisser le long de l'axe des fréquences. On obtient alors la définition suivante des atomes :

$$g_{v,T}(t) = g(t-T)e^{i2\pi vt} \qquad \textbf{3.10}$$

- **La STFT et le plan temps fréquence**

La *STFT* ne contient pas plus d'information que la transformée de Fourier, elle fournit simplement une représentation du signal sur un espace bidimensionnel. $T_x(v,t)$ ne peut

cependant pas décrire le contenu du signal strictement à l'instant t et à la fréquence v car l'atome d'analyse $g_{v,T}$ est caractérisé par ses extensions conjointes temporelle Δt et fréquentielle Δv. Il y a donc mélange de l'information contenue dans le signal pour l'intervalle de temps $[t - \Delta t/2 , t + \Delta t/2]$ dans la bande de fréquence$[v - \Delta v/2 , v + \Delta v/2]$.

Une localisation temps-fréquence idéale, infiniment précise ($\Delta t = 0$ et $\Delta v = 0$) est interdite par le principe de *Gabor-Eisenberg* qui stipule que la résolution conjointe temps-fréquence est minorée :

$$\Delta t \Delta v \geq 1/4\pi \qquad \textbf{3.11}$$

Où :

$$\Delta t^2 = \frac{\int t^2 |g(t)|^2 dt}{\int |g(t)|^2 dt} \quad et \quad \Delta v^2 = \frac{\int v^2 |G(v)|^2 dv}{\int |G(v)|^2 dv} \qquad \textbf{3.12}$$

G étant la transformée de Fourier de la fenêtre d'analyse g.

Cette relation confère aux $g_{v,t}$ le statut d'atomes, portant une portion irréductible d'information temps-fréquence.

De plus, les résolutions temporelles et fréquentielles ne sont pas modifiées par les opérateurs de translation en temps et en fréquence et restent égales à celles de la fonction mère :

$$\begin{cases} \Delta t_{g_{v,t}} = \Delta t_g & \textbf{3.13} \\ \Delta t_{g_{v,t}} = \Delta t_g & \textbf{3.14} \end{cases}$$

Une représentation dans le plan temps-fréquence, conduit à un pavage en cellules élémentaires, dont la forme ne varie ni avec le temps, ni avec la fréquence, il est représenté par la *figure 3.6.*

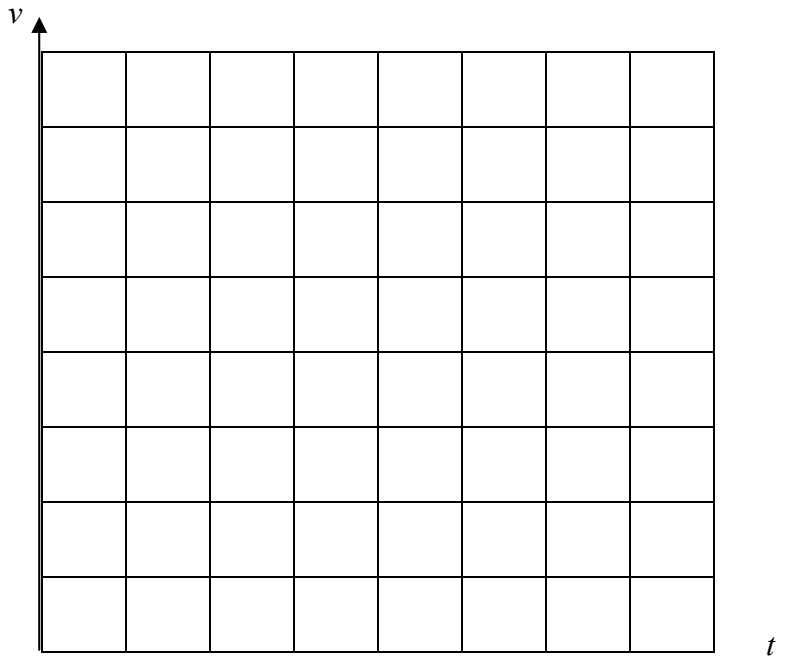


Figure 3.6: *Pavage du plan temps-fréquence.*

Remarque : *Le choix d'une fenêtre longue conduit à une bonne résolution en fréquence, mais à une résolution temporelle assez mauvaise. De même, une fenêtre courte privilégie la résolution temporelle au détriment de la résolution fréquentielle.*
Comme la transformée de Fourier, la STFT préserve l'énergie :

$$E_x = \int \int \left| T_x(v,t) \right|^2 dvdt \qquad \textbf{3.15}$$

De plus, on peut reconstruire le signal :

$$x(t) = \int \int T_x(v,t) g_{v,t} dtdv \qquad \textbf{3.16}$$

Si *g(t)* est d'énergie unité.

La STFT ne représente pas l'ensemble des représentations temps-fréquence mais elle permet d'en illustrer le principe et l'une des propriétés fondamentales : quelles que soient les dynamiques présentes dans le signal, elles sont analysées avec la même précision absolue.

En pratique, on a souvent des signaux composés de bouffées d'activité de courte durée, contenant des hautes fréquences, superposées à des composantes basses fréquences de longue durée. Il s'avère alors nécessaire de disposer d'une grande résolution temporelle dans les hautes fréquences afin de déterminer les instants d'occurrence de ces bouffées, tandis que dans

les basses fréquences, une bonne résolution fréquentielle aura l'avantage de mieux caractériser les composantes de longues durées.

Ce problème peut être résolu en utilisant des fenêtres telles que $\Delta v/v = Q = cste$. C'est ce que réalise la transformée en ondelettes.

3.3.2 Transformée en cosinus

Depuis quelques années, la transformée en cosinus discrète (DCT) est la représentation de choix pour la compression (MP3, JPEG et MPEG), grâce à son compromis intéressant entre pouvoir de décorrélation, proche de l'optimal, et complexité algorithmique.

Elle est utilisée dans les algorithmes de compression JPEG et MPEG par blocs de taille 8 × 8. Cette caractéristique est très souvent reprise dans les techniques de tatouage utilisant la DCT.

3.3.3 La transformée en ondelettes continue

Bien que délivrant une information temporelle, la transformée de Fourier à fenêtre glissante s'avère toutefois insuffisante pour certaines applications. Si l'on veut repérer, par exemple, l'apparition d'un choc, ou d'une singularité, dans un signal, on ne pourra être plus précis que la résolution de la fenêtre : celle-ci est à enveloppe rigide, ce qui limite l'adaptivité d'une analyse par transformée de Fourier à fenêtre glissante.

A l'inverse, la transformée en ondelettes est conçue pour être adaptative : elle consiste à analyser le signal f à l'aide d'une fonction bien localisée, ψ, de moyenne nulle, qu'on appelle ondelette, que l'on translate sur tout le signal et que l'on peut dilater.

Les ondelettes ont d'abord été introduites par Grossman et Morlet [80] comme un outil mathématique d'analyse de signaux sismiques. Ensuite la théorie s'est développée sous la conduite de nombreux contributeurs [81][82][83][84].

Une ondelette ψ est une fonction de moyenne nulle :

$$\int_{-\infty}^{+\infty} \psi(t)\, dt = 0 \qquad \textbf{3.17}$$

Que l'on dilate d'un paramètre d'échelle b et que l'on translate de a :

$$\psi_{a,b}(t) = \frac{1}{\sqrt{b}}\psi(\frac{t-a}{b}) \qquad \textbf{3.18}$$

La transformée en ondelettes de *f* à l'échelle *b* et à la position *a* se calcule en corrélant *f* avec l'ondelette correspondante :

$$W\ f(a,b) = \int_{-\infty}^{+\infty} f(t)\frac{1}{\sqrt{b}}\psi^{*}\frac{(t-a)}{b}dt \qquad \textbf{3.19}$$

La transformée en ondelettes W *f(a, b)* est la représentation bi-dimensionnelle d'un signal *f(t)* mono-dimensionnel. Ceci indique l'existence d'une redondance, qui peut être réduite et même supprimée, par sous-échantillonnage des paramètres de cette transformée, La figure 3.7 donne le pavage de l'espace temps-échelle pour la transformée ondelettes.

La transformée en ondelettes peut s'écrire comme un produit scalaire dans l'espace des signaux :

$$W\ f(a,b) = \int_{-\infty}^{+\infty} f(t)\ \psi_{a,b}^{*}(t)\,dt = \left\langle f,\psi_{a,b}\right\rangle \qquad \textbf{3.20}$$

Le sous-échantillonnage de la transformée définit une représentation complète du signal si tout signal peut se reconstruire par combinaison linéaire d'une famille d'atomes d'ondelettes $\left\{\psi_{a_n,b_j}\right\}_{(n,j)\in z^2}$

L'élimination complète de la redondance revient à construire une base de l'espace des signaux.

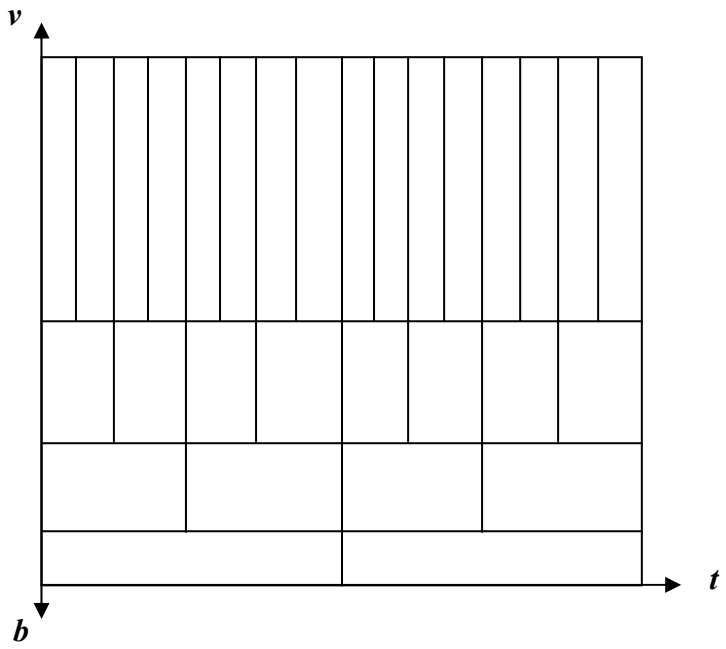


Figure 3.7: *Pavage du plan temps-échelle.*

Enfin, quand W *f(a, b)* n'est calculé que pour $b \leq b_0$ (ce qui est toujours le cas en pratique), pour reconstruire *f* on a besoin d'un complément d'information correspondant à W *f(a, b)* pour $b > b_0$. Ceci est obtenu en introduisant une *fonction d'échelle*, *Ø*, qui agrège les ondelettes d'échelles supérieures à 1. Le module de sa transformée de Fourier est défini à partir de la transformée de Fourier $\hat{\psi}$ de l'ondelette ψ :

$$\left|\hat{\phi}(w)\right|^2 = \int_1^{+\infty} \left|\hat{\psi}(bw)\right|^2 \frac{db}{b} = \int_w^{+\infty} \frac{\left|\hat{\psi}(\xi)\right|^2}{\xi} d\xi \qquad \textbf{3.21}$$

La phase de $\hat{\phi}(w)$ peut être choisie arbitrairement. On verra par la suite que la fonction d'échelle peut s'interpréter comme la réponse impulsionnelle d'un filtre passe-bas.

- **Discrétisation**

Les formules rappelées plus haut sont continues et ne peuvent pas être implémentées comme telles. Il faut les discrétiser. Le principe est de prendre un ensemble discret $\{b_n\}_{n=1\ldots n_{max}}$ d'échelles, et pour chaque échelle b_n, de prendre un ensemble discret de paramètres de translation $\left\{\left(x_n^i, y_n^j\right)\right\}_{i=1\ldots width\,,\, j=1\ldots height}$ couvrant tout le domaine de définition de l'image.

– La façon la plus immédiate mais la plus naïve pour discrétiser la transformée en ondelettes consisterait à échantillonner les échelles *b* et les paramètres de translation *a* de manière régulière:

$$b_n = b_0 n, \quad n = 1...b_{\max} \quad et \tag{3.22}$$

$$\vec{x}_k^{\,j} = \left(x_k^i, y_k^j\right) = (i, j) \tag{3.23}$$

À l'échelle k et pour i = 1 … width, j = 1 … height. les propriétés de la transformée en ondelettes continue sont alors conservées, en particulier l'invariance par translation, mais cette discrétisation n'est pas adaptée aux supports fréquentiels des ondelettes et le coût de calcul est prohibitif : une telle discrétisation n'est en pratique jamais utilisée.

– La discrétisation naturelle pour les échelles consiste à choisir $b = b^n{}_0$, avec $b_0 > 1$: on parcourt ainsi les fréquences du signal beaucoup plus rapidement, tout en restant précis sur les hautes fréquences (c'est à dire les petites échelles). Le choix le plus populaire est de prendre $b_0 = 2$: les échelles sont discrétisées sur des valeurs dyadiques. On obtient ainsi la transformée en ondelettes dyadique [85][86]).

– L'information donnée par un coefficient d'ondelettes correspond à un voisinage d'autant plus grand, dans le domaine spatial, que l'échelle est grande. Il n'est donc pas nécessaire d'utiliser, pour cette transformée, une discrétisation aussi précise aux échelles grossières qu'aux échelles fines.

3.3.4 La transformée en ondelettes discrète

La transformée en ondelettes continue est très redondante. Afin d'appliquer efficacement la transformée en ondelettes aux signaux discrets, il convient de discrétiser les coefficients de dilatation b et de translation a.

On impose donc une grille de valeurs discrètes pour a et b. On pose $b = b_0^m$ et $a = na_0b_0^m$ avec $b_0 \in Z$ *et* $b_0 \in Z$. La transformée en ondelettes discrète est donnée par :

$$\widetilde{f}(m,n) = b_0^{\frac{-m}{2}} \int_{-\infty}^{+\infty} f(t)\psi(b_0^{-m}t - na_0)dt \tag{3.24}$$

Si on choisit $b_0 = 2$ et $a_0 = 1$, on se place dans le cas dyadique. On a alors :

$$\widetilde{f}(m,n) = 2^{\frac{-m}{2}} \int_{-\infty}^{+\infty} f(t)\, \psi\left(2^{-m} t - n\right) dt \qquad \textbf{3.25}$$

3.3.5 Les familles d'ondelettes

Il existe une infinité de fonctions d'ondelettes parce que toute fonction oscillante localisée est une ondelette mère possible. Toutefois, elles ne possèdent pas toutes des propriétés intéressantes. Aussi, de nombreux spécialistes des ondelettes ont construit des familles d'ondelettes possédant certaines propriétés remarquables.

D'après le principe d'inégalité d'Heisenberg $\Delta_t \Delta_w \geq 1/2$, on ne peut pas à la fois localiser un signal en temps et en fréquence. Quand on améliore la localisation dans un des deux espaces, c'est au détriment de l'autre.

Parmi les familles d'ondelettes, les ondelettes de Haar sont les plus rapide et simples. Ingrid Daubechies a construit des ondelettes à support compact qui permettent d'utiliser des filtres de taille finie. Une autre famille d'ondelettes est la famille des ondelettes splines dont la réponse fréquentielle est bien localisée. Les différentes familles d'ondelettes sont utilisées selon leurs propriétés en fonction du problème à résoudre.

Dans notre travail, nous avons utilisé les ondelettes de Haar les plus rapide et simples.

- **Exemple d'ondelette (ondelette de haar)**

C'est la plus simple des ondelettes : définie sur l'intervalle [0, 1] (ou parfois sur [-1/2, 1/2] c'est la fonction H constante par morceaux qui vaut (*voir figure 3.8*) :

$$H(x) = \begin{cases} 1 \quad si \quad x \in \left[0, \frac{1}{2}\right[& \textbf{3.26} \\ -1 \quad si \quad x \in \left]\frac{1}{2}, 1\right] & \textbf{3.27} \end{cases}$$

Cette ondelette est très simple et est donc facile à mettre en oeuvre algorithmiquement. De plus, son support est compact : elle est bien localisée en espace. En contrepartie, elle n'a qu'un seul moment nul.

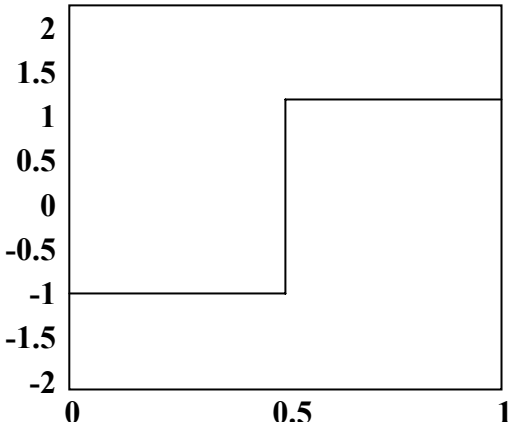


Figure 3.8 : *Ondelettes de Haar.*

3.3.6 L'analyse multirésolution

L'analyse multirésolution, introduite par *Mallat* [84], est un outil de traitement du signal qui permet de décomposer un signal à plusieurs échelles (résolutions) et de le reconstruire à partir des éléments de cette décomposition.

Une analyse multirésolution est un partitionnement de l'espace des fonctions d'énergie finie $L^2(R)$ par une famille de sous-espaces vectoriels V_j emboîtés les uns dans les autres tels que le passage de l'un à l'autre soit le résultat d'un changement d'échelle. Ces sous-espaces sont appelés des espaces d'approximation à l'échelle j ($j \in Z$) et vérifient les propriétés suivantes :

Soit un ensemble de sous-espaces de $L^2(R)$ (l'ensemble des signaux à énergie finie) tels que :

$$\begin{aligned} &\ldots \subset V_2 \subset V_1 \subset V_0 \subset V_{-1} \subset \ldots \subset V_{j+1} \subset V_j \subset \ldots \\ &\overline{\bigcup_{j \in Z} V_j} = L^2(R) \\ &\bigcap_{j \in Z} V_j = 0 \\ &\forall_j \in Z,\ f(x) \in V_j \quad \Leftrightarrow \quad f(2^{-1}x) \in V_{j+1} \\ &\forall_k \in Z,\ f(x) \in V_0 \quad \Leftrightarrow \quad f(x-k) \in V_0 \end{aligned} \qquad \textbf{3.28}$$

Ces propriétés définissent une analyse multirésolution dyadique sur $L^2(R)$.

L'analyse multirésolution a été définie par *Mallat* [84]. L'idée est de projeter un signal $f(t) \in L^2(R)$ appartenant à un espace V_j sur un sous-espace V_{j+1} et un sous-espace W_{j+1} dans le but de réduire la résolution de moitié. Le schéma est donné en figure 3.9. Il existe donc un

opérateur de projection A_j et un opérateur de projection D_j qui projettent respectivement le signal $f(t)$ sur V_{j+1} et W_{j+1}. V_{j+1} est le sous-espace d'approximation et W_{j+1} le sous-espace de détails.

On peut démontrer qu'il existe une fonction d'échelle $Ø(t) \in L^2(R)$ qui engendre par dilatation et translation une base orthonormée de V_{j+1} et une fonction d'ondelettes $\psi(t) \in L^2(R)$ qui engendre par dilatation et translation une base orthonormée de W_{j+1}. Les espaces obtenus ne sont pas quelconques, ils possèdent des propriétés intéressantes. Par construction, les espaces d'approximation V_{j+1} et de détails W_{j+1} sont complémentaires : $V_j = V_{j+1} \oplus W_{j+1}$. De plus, si les bases sont orthogonales, ils sont orthogonaux : $V_{j+1} \perp W_{j+1}$.

Les fonctions de bases dilatées sont données par les relations :

$$\phi_{j,n}(t) = 2^{-j/2}\phi(2^{-j}t - n) \text{ avec } n \in Z \text{ et } \psi_{j,n}(t) = 2^{-j/2}\psi(2^{-j}t - n) \text{ avec } n \in Z \qquad \textbf{3.29}$$

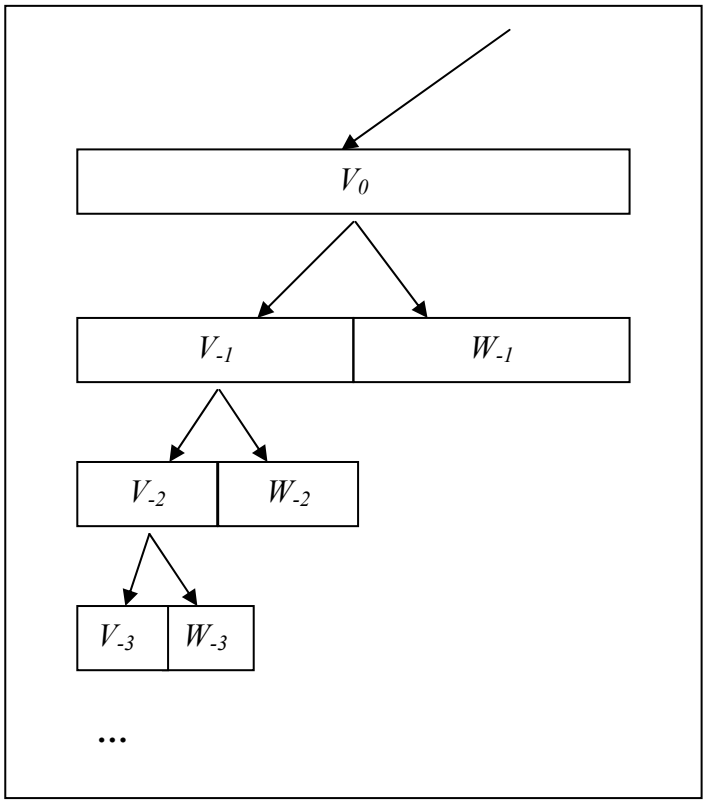


Figure 3.9 : *Principe de l'analyse multirésolution*.

On a donc

$$A_j f = \sum_n \langle f, \phi_{j,n} \rangle \phi_{j,n} \text{ et } D_j f = \sum_n \langle f, \psi_{j,n} \rangle \psi_{j,n} \qquad \textbf{3.30}$$

Où $\langle f(t), g(t) \rangle$ Désigne le produit scalaire de *f(t)* par *g(t)* :

$$\langle f(t), g(t) \rangle = \int_{-\infty}^{+\infty} f(t) g(t)^* \, dt \qquad \textbf{3.31}$$

Puisque les signaux analysés sont réels, on a $g(t)^* = g(t)$. On pose $a_{j,n} = < f, \emptyset_{j,n} >$ et $d_{j,n} = < f, \psi_{j,n} >$. $a_{j,n}$ et $d_{j,n}$ sont respectivement les coefficients d'approximation et de détails de la transformée en ondelettes de la fonction *f*.

Le résultat de l'analyse multirésolution d'une image est donné en figure 3.12. On voit la diminution de la résolution, l'image d'approximation et les images de détails horizontaux, verticaux et diagonaux.

3.3.7 Algorithmes récursif de Mallat

Stéphane Mallat a donné un algorithme d'analyse (ou décomposition) en ondelettes qui permet d'obtenir une analyse multirésolution du signal.

Cet algorithme travaille par filtrage de l'image suivant les lignes puis les colonnes par deux filtres, *g* passe-haut et *h* passe-bas. *h* va permettre de repérer les basses fréquences dans l'image (l'approximation) et *g* les hautes fréquences (les détails). *h* et *g* sont construits à partir des fonctions ψ et $\emptyset$. La figure 3.10 donne le schéma d'analyse (de décomposition) de Mallat.

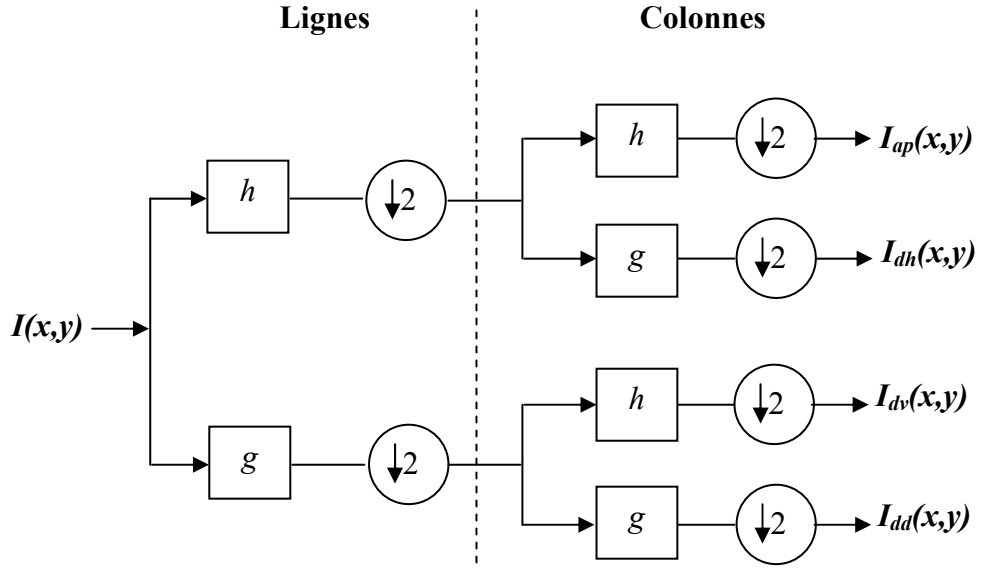


Figure 3.10 : *Algorithme récursif de Mallat.*

La figure 3.11 montre la disposition des coefficients de décomposition d'une image pour un seul niveau de décomposition.

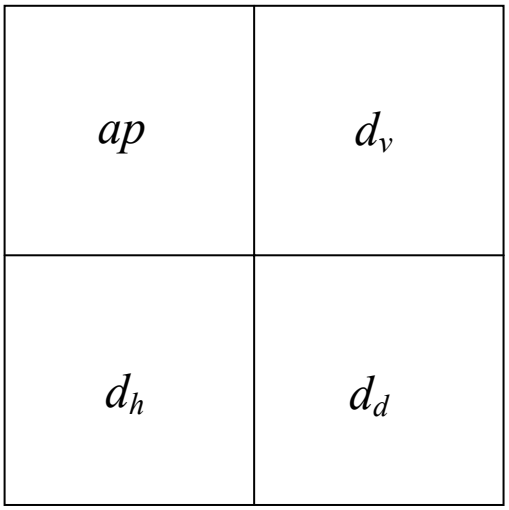


Figure 3.11 : *Disposition des coefficients de décomposition d'une image pour un niveau.*

La reconstruction des signaux analysés est effectuée à l'aide d'un banc de filtres h_c et g_c qui sont les filtres conjugués de h et g. En fonction de l'ondelette et du type de base (orthogonale ou bi-orthogonale) choisis pour l'analyse, les filtres d'analyse et de synthèse peuvent être de même taille, symétriques ou bien de taille différente, non symétriques. La figure 3.13 donne le schéma de synthèse (de reconstruction) de Mallat.

Figure 3.12: *Un exemple de décomposition en ondelettes de l'image ''Lena'' au premier niveau de résolution.*

Dans la reconstruction, on travaille alternativement sur les colonnes puis sur les lignes lorsque les ondelettes sont séparables.

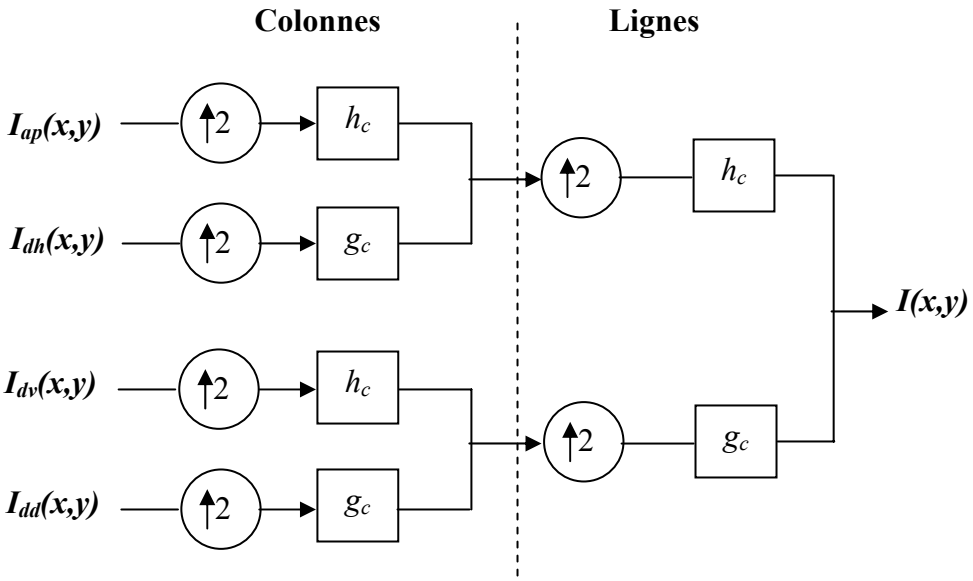


Figure 3.13 : *algorithme de reconstruction de Mallat.*

3.4 Conclusion

Dans ce chapitre nous avons présenté quelques définitions et propriétés des images numériques, puis nous avons introduit la transformée en ondelettes discrète d'un signal et d'une image. Si l'on adopte un point de vue fréquentiel, la transformée en ondelettes peut être assimilée à une segmentation fréquentielle de l'information contenue dans le signal à la manière d'un banc de filtres présentant une structure dyadique. La répartition de la résolution dans le plan temps-échelle est ainsi figée.

Quatrième chapitre

Algorithmes proposés

4.1 Introduction

Dans ce chapitre, nous allons présenter notre méthodologie de tatouage basée sur la modification des coefficients de la transformée en ondelettes discrète, à travers un ou deux niveaux de décomposition afin d'imposer un espace d'insertion fixé par la marque. Ce chapitre se décompose en deux parties :

Le tatouage des images en niveaux de gris, nous proposons dans cette partie deux algorithmes développés dans le cadre d'augmenter la robustesse du tatouage d'images en niveaux de gris face au différentes types d'attaques, soit volontaire (falsification à titre d'exemple) ou non volontaire (compression, filtrage, changement d'échelle, transformations géométriques …etc). Les résultats obtenus pour les deux algorithmes sont ensuite présentés.

La deuxième partie de ce chapitre illustre les travaux que nous avons effectués dans le cas des images en couleurs ainsi que les résultas obtenus. Dans cette partie, nous allons détailler les différentes étapes du processus de tatouage d'images couleurs. Deux algorithmes sont proposés, le premier algorithme consiste à utiliser l'espace initiale *RGB* puis nous améliorons l'approche proposée par l'intervention de l'espace YCbCr de type luminance-chrominance. Et en termine par une étude comparative entre les deux espaces couleurs.

Afin de tester nos schémas, nous avons décidé d'utiliser une base d'images de référence libre de droit. La *figure 4.1* regroupe quelques-unes des images que nous avons utilisées (Lena , Barbara, Baboon, Camera , Boat, Baboon-RGB , Peppers-color), Elles sont toutes de tailles 512 x 512 pixels.

a: Lena **b:** Barbara **c:** Baboon **d:** Camera

e: Boat **f:** Baboon-RGB **g:** Peppers-color

Figure 4.1: *Ensemble d'images tests.*

4.2 Tatouages d'images en niveaux de gris

4.2.1 Algorithme additif à base d'ondelettes

Dans l'étude présentée ici, notre méthode opère dans le domaine transformé, De nombreux algorithmes de tatouage ont été proposés cherchant à optimiser un compromis robustesse-invisibilité, certains entre eux proposent d'ajouter la marque dans deux bandes de décomposition da la transformée en ondelettes discrète qui sont LL et HH , [87][88][89][90]. Mais dans ce cas, la marque extraite ne sera pas robuste que face à certain nombre d'attaques (*tableau 4.1*). D'autres méthodes proposent d'insérer la marque que dans LH et HL, [91][92][93], qui soit aussi robuste que face à certain autre nombre d'attaques (*tableau 4.1*). Alors, que d'autres techniques proposent d'insérer la marque dans les quatre bandes [94]. Cette section a fait l'objet d'un article présenté lors de la conférence cisa'08 [95].

	Type d'attaques
La bande LL	JPEG compression, Blurring, ajout de Bruit Gaussien, Rotation, Cropping, Resize
La bande HH	Histogram equalization, Intensity Adjustment, and Gamma correction
Les bandes LH, HL	Histogram Equalization, Intensity Adjustment, Gamma Correction, Sharpening.
Les 4 bandes	Collusion

Tableau 4.1: *Robustesse des quatre bandes face à certain nombre d'attaques.*

4.2.1.1 Insertion de la marque

Le principe de la méthode de tatouage que nous présentons dans cette section consiste à généraliser l'idée présentée ci-dessus, où nous allons modifier les valeurs des pixels des quatre bandes de décomposition du deuxième niveaux de la transformée en ondelettes discrète afin d'imposer une structure fixée par la marque.

Le schéma de la *figure 4.2* montre le diagramme d'inclusion de la marque. Dans cette partie, nous allons détailler l'algorithme; l'image marquée ***X'*** résulte de l'inclusion dans l'image hôte ***X*** de la marque ***W***.

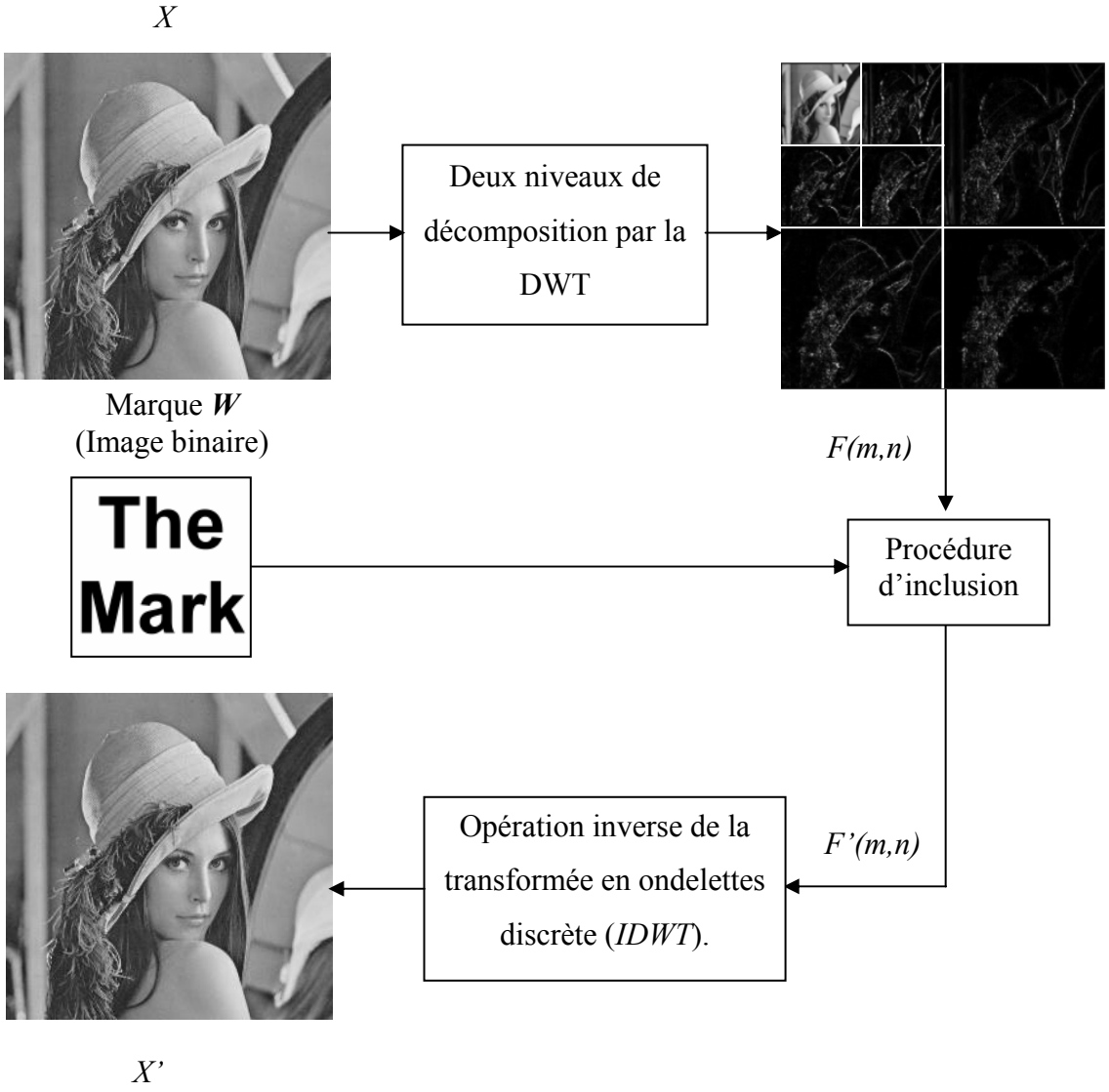


Figure 4.2: *Diagramme de la procédure d'inclusion de la marque.*

Où :

X : Image originale.

X' : Image marquée.

F(m,n) : dénote les coefficients de la DWT de l'image originale.

F'(m,n) : dénote les coefficients de la DWT après modification.

L'image originale est tout d'abord décomposée en utilisant la *transformée en ondelettes discrète* avec la structure pyramidale. Dans notre système d'inclusion de la marque, la décomposition est performée à travers deux niveaux de décomposition utilisant le « *Haar filter* ». La marque qui est de taille de 128 x 128 pixels, est additionnée dans les quatre bandes fréquentielles de l'image (LL_2, LH_2, HL_2 et HH_2),

La procédure d'inclusion est performée selon la formule suivante :

$$X^k_{w,ij} = X^k_{ij} + \alpha_k W_{ij}, \quad i, j = 1,...,n/2, \; et \; k = 1,2,3,4. \qquad \textbf{4.1}$$

Où $\boldsymbol{\alpha}$ est la force du tatouage. $w_{i,j} \in \{0,1\}$, $1 \leq i,j \leq n/2$.

L'image marquée est obtenue en appliquant l'inverse de la transformée en ondelettes discrète (*IDWT*).

4.2.1.2 Extraction de la marque

Dans la procédure d'extraction de la marque, l'image marquée et l'image originale toutes deux décomposées en deux niveaux par la *DWT*. Il est supposé que l'image originale est connue pour l'extraction (schéma d'extraction non aveugle).

La procédure d'extraction est décrite par la formule :

$$W^*_{ij} = (X^{*k}_{w,ij} - X^*_{ij}) / \alpha_k, \quad i, j = 1,...,n/2, \; et \; k = 1,2,3,4. \qquad \textbf{4.2}$$

$$Si \; W_{i,j} > 0.5, \; Alors \; W_{ij} = 1, \; Sinon \; W_{ij} = 0. \qquad \textbf{4.3}$$

Où $X^{*k}_{w,ij}$ sont les coefficients de la DWT de l'image marquée (et peut être attaquée).

X^*_{ij} sont les coefficients de la DWT de l'image originale

La *figure 4.3* montre le diagramme d'extraction de la marque ;

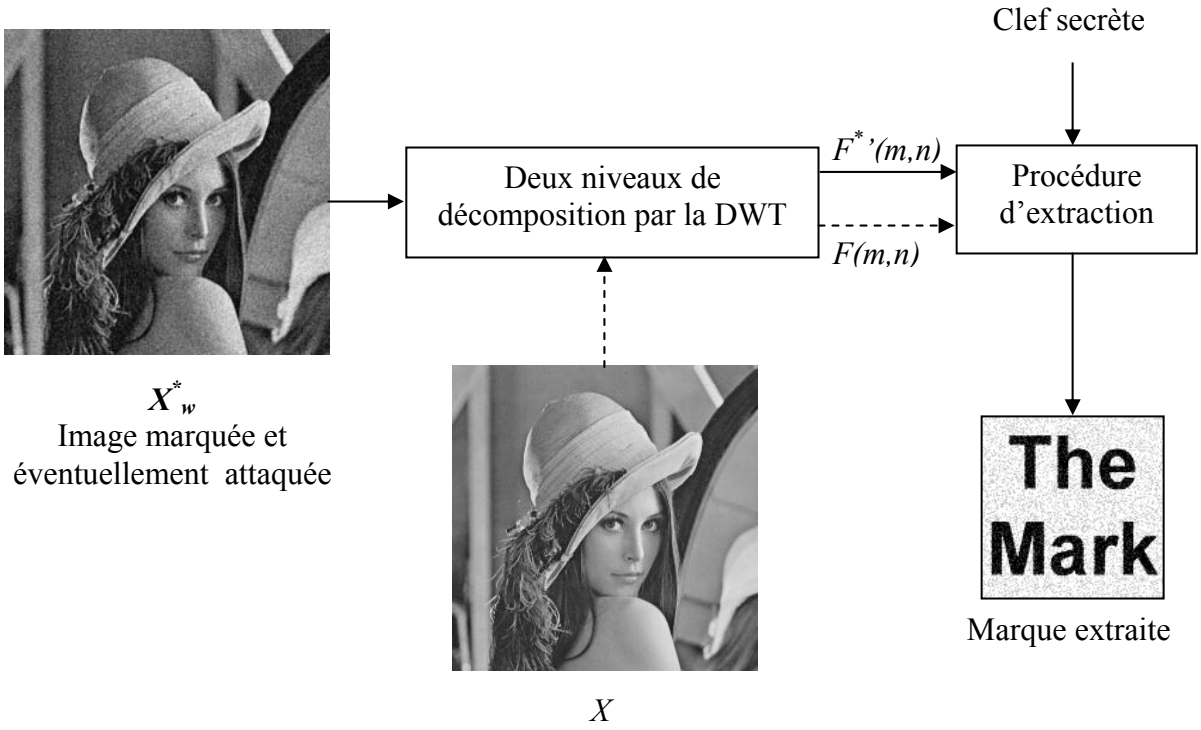


Figure 4.3: *Diagramme de la procédure d'extraction de la marque.*

X - Image originale.

X^*_w - Image marquée et éventuellement attaquée.

F(m,n) : dénote les coefficients de la DWT de l'image originale.

F'(m,n) :* dénote les coefficients de la DWT de l'image tatouée.

4.2.1.3. Robustesse vis-à-vis les différentes attaques

Les tests présentés ici sur l'image ''Lena'' ont été effectués avec une décomposition en ondelettes sur deux niveaux, et un facteurs de robustesse $\alpha = 20$ pour la bande fréquentielle LL_2 et 3 pour les trois autre bandes fréquentielles (LH_2, HL_2, HH_2).

Le message inséré est une image binaire de taille MxM, ou M = 128. Le *tableau 4.2* présente les PSNR obtenus pour les images tatouées (Lena , Barbara, Boat, Baboon).

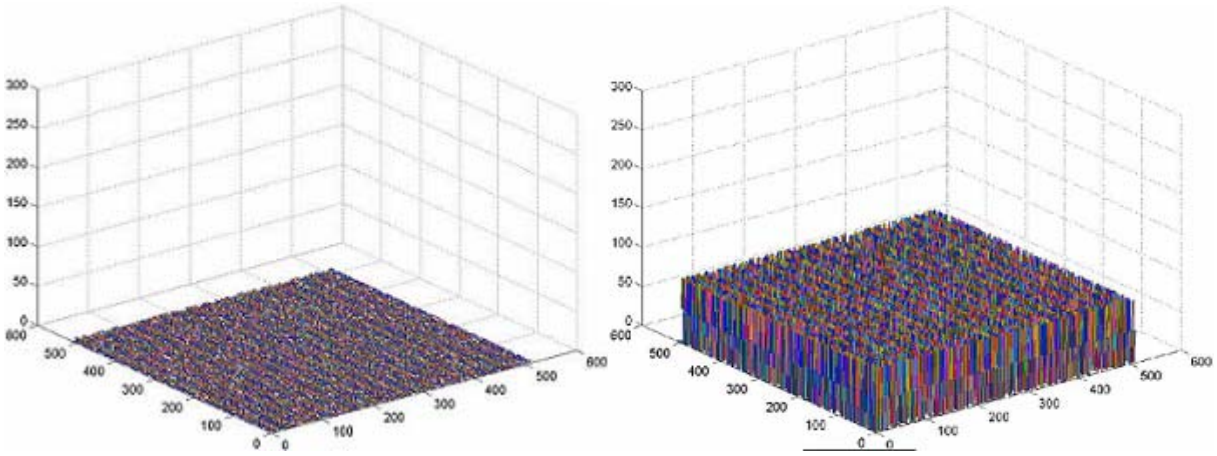
a: Image originale . **b :** Image marquée .

Figure 4.4 : *Application de la méthode proposée sur l'image ''Lena'' de taille 512x512 avec $\alpha = 20$ pour LL_2 et 3 pour LH_2,HL_2 et HH_2 .le PSNR entre les deux images est de 39.7 dB.*

	Lena	Barbara	Boat	Baboon
PSNR(dB)	39.7	39.87	39.69	39.71

Tableau 4.2: *PSNR obtenus pour les différentes images tests.*

La *figure 5 (a)* représente la différence absolue entre l'image originale et l'image tatouée (la marque est une image binaire de taille 128x128).



(a) **(b)**

Figure 4.5: *(a) Différence absolue entre l'image originale et l'image marquée, (b) Différence absolue amplifiée par un facteur de 20.*

Afin de montrer l'influence de différentes attaques sur la lecture de la marque, nous avons choisis d'illustrer nos résultats sur la seule image ''Lena'', sachant que des résultats

similaires ont été obtenus sur les autres images tests de même taille. Nous avons décidé de valider l'algorithme face à des attaques de type « traitement du signal » (Filtrage, ajout de Bruit Gaussien, modifications de l'histogramme, etc. *tableau 4.1*).

Nous nous intéressons ici plus particulièrement à la compression JPEG. *La figure 4.6* illustre quelques unes des attaques testées. Les résultats obtenus sont présentés dans le tableau ci-dessous.

Attacks	**PSNR**	**Distance de Hamming**			
		LL_2	**LH_2**	**HL_2**	**HH_2**
JPEG 75%	37.41	0.0	0.396	0.360	0.486
JPEG 50%	33.58	0.006	0.349	0.350	0.379
JPEG 25%	32.39	0.138	0.460	0.442	0.466
Filtering	33.84	0.055	0.197	0.415	0.355
Bruit Gaussien	29.32	0.118	0.423	0.453	0.422
Histogram-Equalization	36.90	0.444	0.138	0.187	0.373
Intensity Adjustment	25.44	0.494	0.077	0.122	0.056
gamma correction	24.27	0.505	0.100	0.130	0.081
rotate 20%	24.85	0.085	0.243	0.249	0.255
cropping 50%	25.28	0.373	0.371	0.373	0.104
cropping 25%	27.45	0.218	0.462	0.215	0.218
Resize 90%	36.31	0.139	0.447	0.438	0.435
Resize 75%	37.24	0.163	0.564	0.564	0.472
Resize 125%	24.71	0.069	0.462	0.453	0.435

Tableau 4.3 : *PSNR et réponse du détecteur pour l'image ''Lena'', face certaines attaques.*

L'algorithme de tatouage proposé offre dans l'ensemble de bonnes performances en termes de robustesse face à certains nombres d'attaques. On constate que le tatouage reste très résistant aux modifications de luminance et de contraste, ainsi qu'aux ajustements et compression JPEG.

L'algorithme permet d'insérer 128x128 bits dans chaque bandes de décomposition du deuxième niveau de la transformée en ondelettes discrète et satisfait les propriétés de transparence et de robustesse.

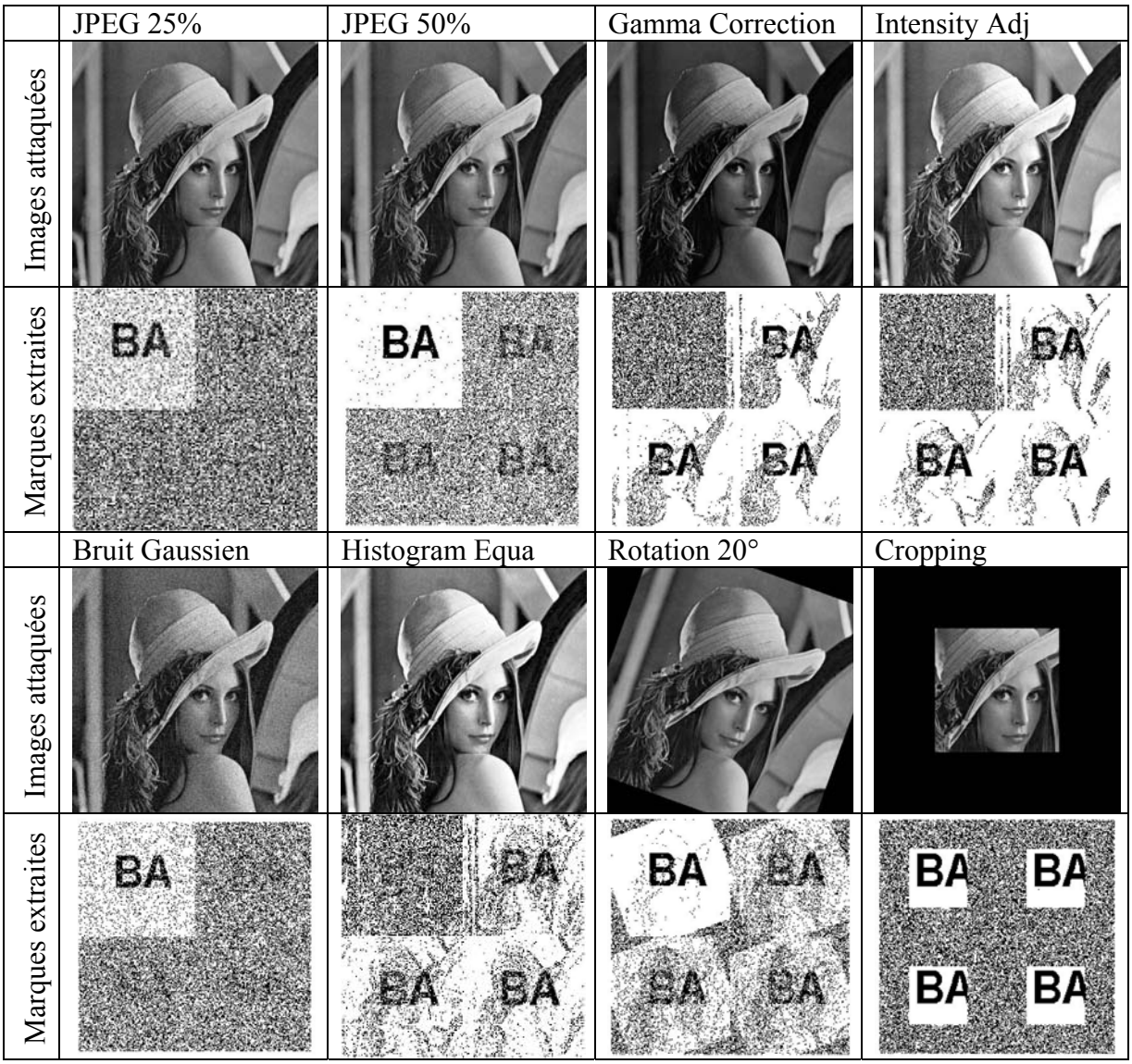


Figure 4.6*: L'image ''Lena'' marquée et attaquée.*

On peut représenter les performances de notre algorithme par un graphique, comparant la marque extraite avec la marque voulue. On utilise pour cela la distance de Hamming : on calcule la moyenne des valeurs absolues des différences bits à bits entre la marque extraite et la marque voulue, c'est à dire la moyenne des erreurs. Dans notre cas, cette distance est de 0 : la marque a bien été retrouvée.

La figure 4.7 présente les réponses du détecteur à 1000 marques générées aléatoirement. La marque w^* pour LL_2 band apparaît en position 200 et en positions 400,600,800 respectivement pour les trois autres bandes (LH_2, HL_2, HH_2),elle est parfaitement détectée, la distance de Hamming est nulle.

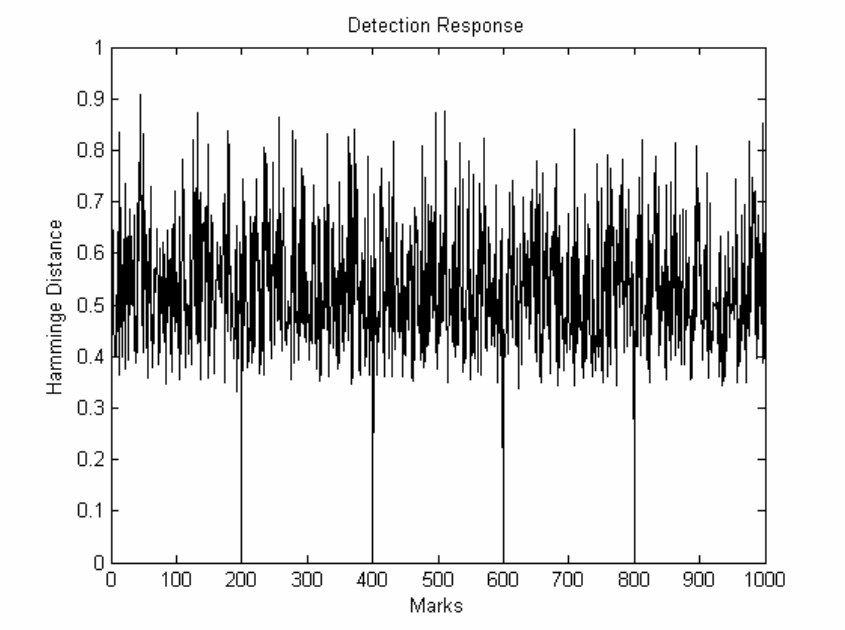
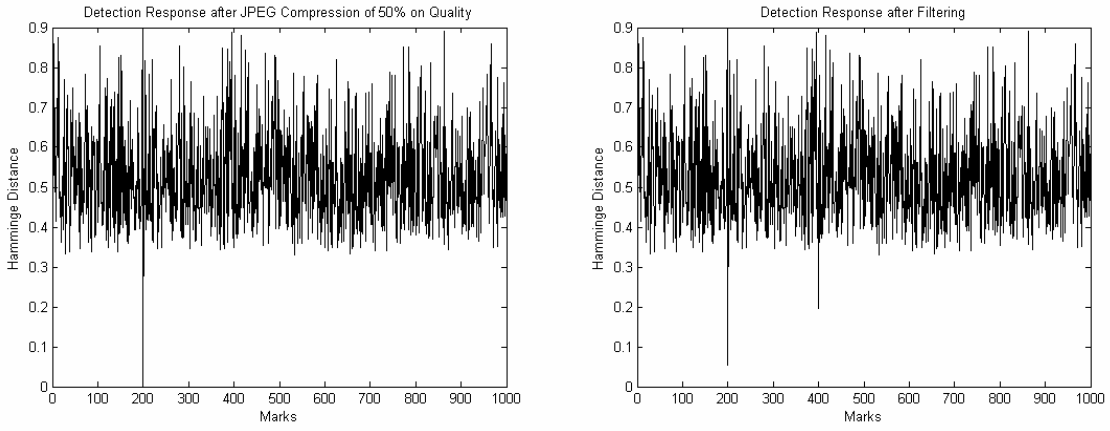
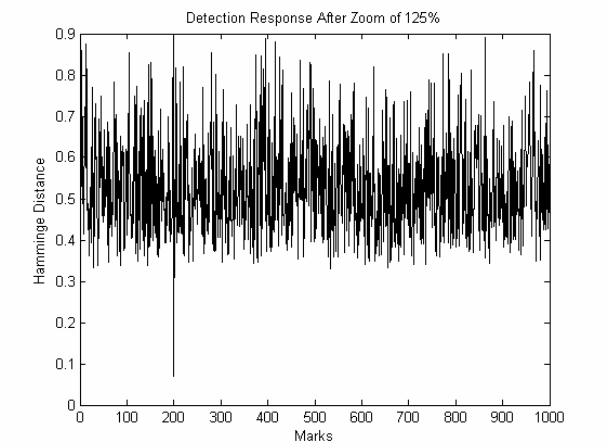


Figure 4.7: *Réponse du détecteur à 1000 marques générées aléatoirement, notre marque apparaît en position 200 pour LL_2 bande et en positions 400, 600, 800 respectivement pour les trois autres bande (LH_2, HL_2, HH_2).*

La figure 4.8 montre le comportement du détecteur après les trois types d'attaques compression JPEG de 50% de qualité, filtrage, et resize de 125%. La détection est excellente et la marque est reconnue que pour les bandes LL_2. Ce qui explique que les trois bandes fréquentielles LH_2, HL_2, HH_2, ne sont pas robuste face au ces trois types d'attaques.



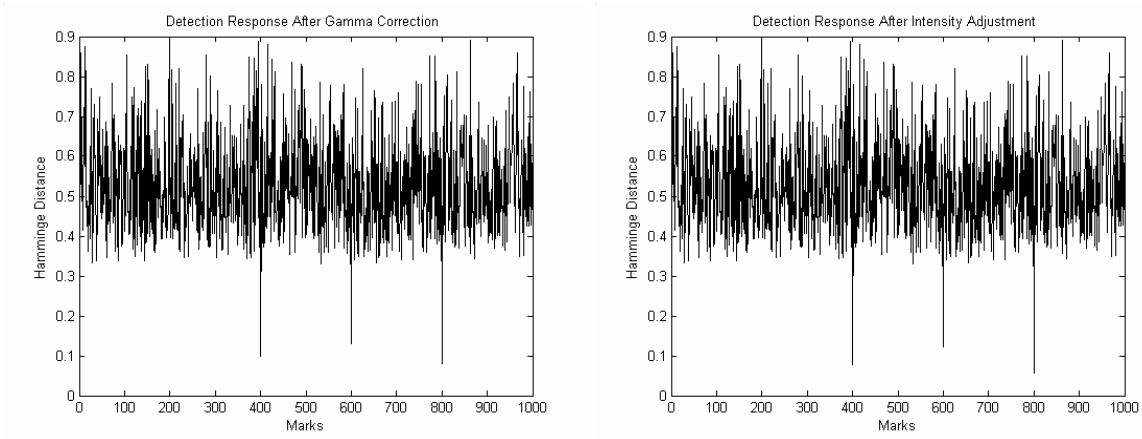
(a) **(b)**



(c)

Figure 4.8: *Réponse du détecteur après attaque. (a) compression JPEG 50% ,(b) filtrage,(c) resize 125%.*

De même il existe d'autres types d'attaques qui sont robuste que pour les trois bandes LH_2, HL_2, HH_2 (*figure 4 .9*).



(a) (b)

Figure 4.9: *Réponse du détecteur après attaque. (a) Gamma correction, (b) Intensity Adjustment.*

Les attaques présentées ci-dessus dégradent plus ou moins l'image. La *figure 4.10* présente la variation de la valeur de la réponse du détecteur en fonction du type d'attaque pour les quatre bandes fréquentielles.

Les abscisses représentent les différentes attaques selon l'ordre que nous avons donné ci-dessus (*tableau 4.3*).

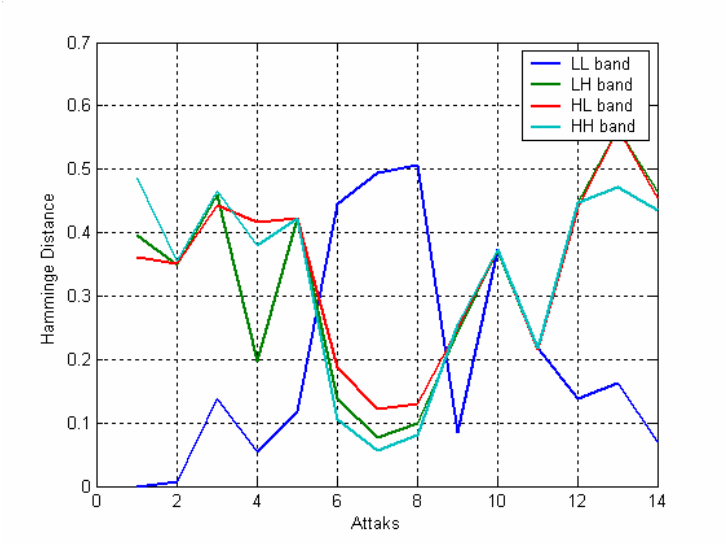
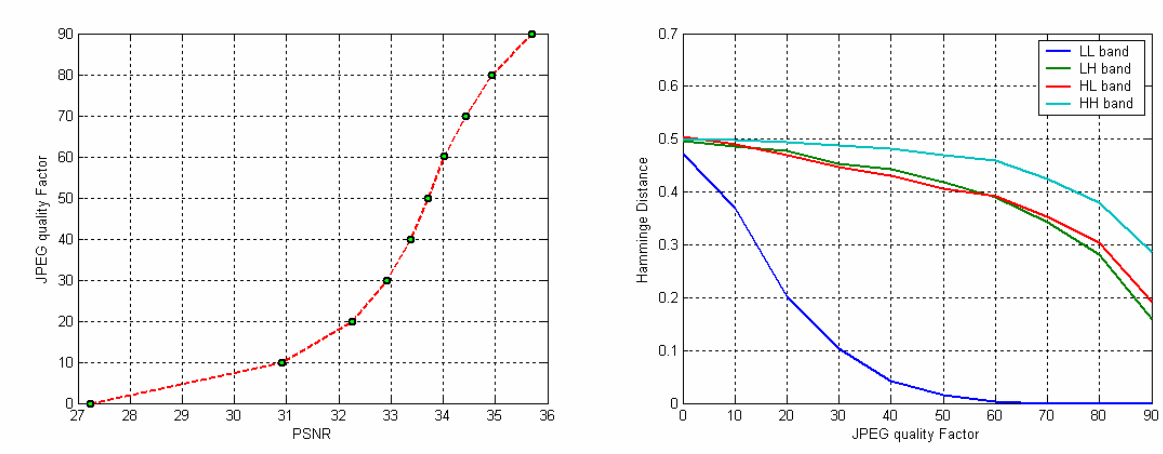


Figure 4.10: *La réponse du détecteur en fonction du type d'attaque pour les quatre bandes fréquentielles.*

Nous présentons dans la *figure 4.11* des résultats obtenus face à différents taux de compression JPEG. Le premier graphique de la *figure 4.11 (a)* représente la variation du PSNR calculé entre l'image hôte et celle marquée et attaquée en fonction du taux de compression, le second *(b)* représente la variation de la réponse du détecteur en fonction du taux de compression.

Nous avons constaté que même si l'image marquée subit une dégradation visible après une compression JPEG, il est toujours possible d'extraire une marque de bonne qualité.



(a) **(b)**

Figure 4.11: *Robustesse vis-à-vis de la compression JPEG.*

Finalement, les résultats expérimentaux présentés prouvent la robustesse et l'imperceptibilité de notre méthode de tatouage des images en niveaux de gris, dans la majorité des attaques que peut subir l'image marquée.

4.2.2 Nouvelle approche résistante aux distorsions géométriques

Plusieurs approches ont été développées dans l'objectif d'augmenter la robustesse des schémas de tatouage essentiellement face à une attaque involontaire de type compression. Ces méthodes de compression sont généralement de types EZW [96], JPEG [97] et/ou basées sur la quantification [98]. D'autres auteurs, par contre, cherchent à améliorer la robustesse des approches de tatouage face aux distorsions géométriques [99]. Certains d'entre eux ont proposé de dissimuler le filigrane en utilisant des régions d'intérêt [100] de l'image hôte, par exemple les contours. Soit dans le domaine spatial [101] ou via le domaine transformé [102][103].

Cette section a fait l'objet d'un article présenté lors de la conférence mcseai'08 [104]. Dans l'approche proposée dans cette section, seuls les coefficients de la bande de base LL de la DWT sont modifiés, dans le cadre d'augmenter la robustesse face aux distorsions géométriques. Ainsi, une bonne qualité de l'image tatouée est garantie, une grande robustesse, essentiellement faces aux distorsions géométriques, est obtenue.

Plusieurs types de filtres numériques RIF peuvent être utilisés pour calculer la DWT. Comme exemples le filtre de Haar et les filtres Daubechies. Nous avons opté pour le filtre de Haar compte tenu de certains de ses avantages [105] : Conceptuellement simple, Rapide, possède une mémoire efficace et il est exactement réversible sans effets de bord.

4.2.2.1 Insertion multiple et parallèle de la marque

L'inclusion de la marque passe par plusieurs étapes:

- L'image originale *I* est décomposée en utilisant la DWT.
- Après la génération d'une clef secrète K à l'aide d'un registre à décalage à rétroaction linéaire LFSR *(Linear Feedback Shift Register)*, nous appliquerons une opération de XOR (ou exclusif) entre la clef K et une marque W de taille NxN définie par l'utilisateur. Ou N = m/4 avec une image originale de taille mxm.

- Le message obtenue W(K), après l'opération XOR, est pondéré par une constante α, déterminant la force du tatouage. Le résultat est ajouté aux coefficients C_{ij} de la bande LL de l'image originale, pour obtenir les coefficients $C_{w,ij}$ de l'image marquée. Ce message est ajouté d'une façon redondante et parallèle. (*figure 4.12*).

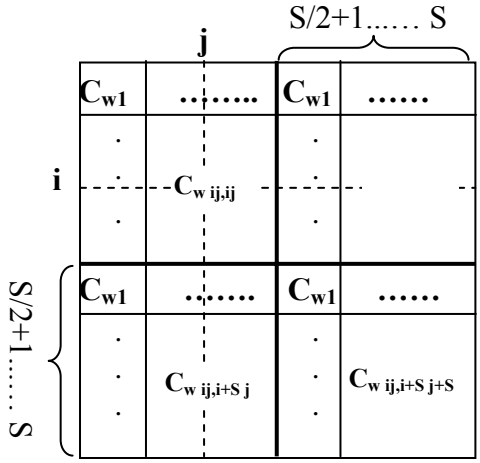


Figure 4.12: *L'opération d'ajout de la marque dans la bande fréquentielle LL de taille SxS.*

La même marque est donc dissimulée dans quatre parties de la bande LL en utilisant les expressions :

$$C_{w,\,ij} = C_{ij} + \alpha W_{ij} \quad \textbf{4.4}$$

$$C_{w,\,i+S\,j} = C_{i+S\,j} + \alpha W_{i+S\,j} \quad \textbf{4.5}$$

$$C_{w,\,i\,j+S} = C_{i\,j+S} + \alpha W_{i\,j+S} \quad \textbf{4.6}$$

$$C_{w,\,i+S\,j+\,S} = C_{i+S\,j+\,S} + \alpha W_{i+S\,j+\,S} \quad \textbf{4.7}$$

Où i,j = 1 … m/4 . S = m/2.

Où l'image originale est de taille mxm, et chaque sous bande fréquentielle et de taille SxS (S = m/2 pour un seul niveau de décomposition).

- Pour terminer l'image marquée I' est obtenue en appliquant l'inverse de la transformée en ondelettes discrète (IDWT).

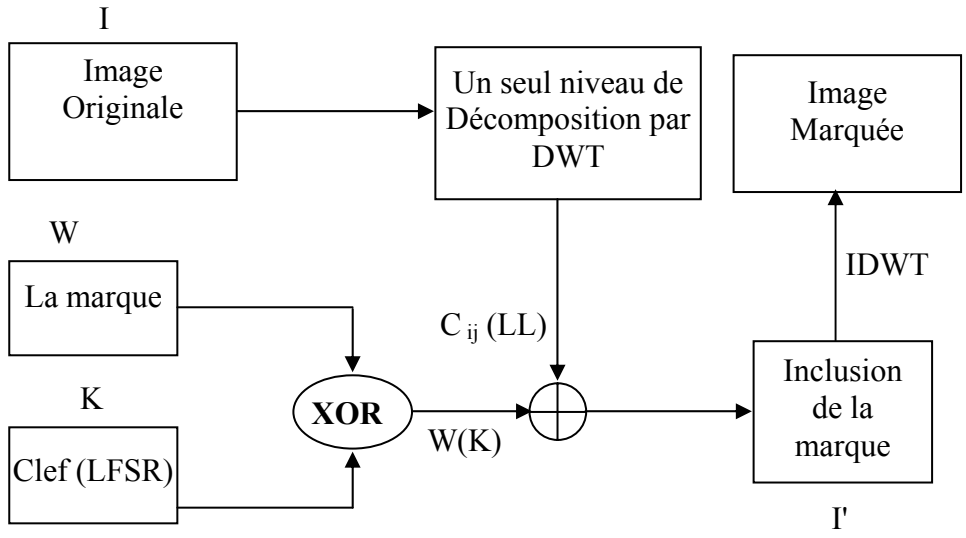


Figure 4.13: *Schéma proposé de l'inclusion de la marque.*

Où C_{ij} *(LL)* sont les coefficients de la bande LL de l'image originale.

4.2.2.2 Algorithme d'extraction

Le schéma d'extraction de la marque (*figure 4.14*) nécessite la présence de l'image originale *I* (schéma d'extraction non aveugle) ainsi que la clef *K* générée lors de la phase d'insertion par le LFSR. Après avoir décomposé les deux images, originale et marquée, sur un seul niveau par la DWT, la différence entre les deux bandes LL (de l'image originale et marquée) donne les quatre messages *W(K)* (même marque dissimulée d'une façon redondante). Une procédure similaire est utilisée pour l'extraction de ces marques à partir de la bande LL. La procédure d'extraction est décrite par:

$$W(k)_{1,ij} = (C^*_{w,ij} - C_{ij})/\alpha \quad \textbf{4.8}$$

$$W(k)_{2,\, i+S\, j} = (C^*_{w,\, i+S\, j} - C_{i+S\, j})/\alpha \quad \textbf{4.9}$$

$$W(k)_{3,\, i\, j+S} = (C^*_{w,\, i\, j+S} - C_{i\, j+S})/\alpha \quad \textbf{4.10}$$

$$W(k)_{4,\, i+S\, j+S} = (C^*_{w,\, i+S\, j+S} - C_{i+S\, j+S})/\alpha \quad \textbf{4.11}$$

Où i,j = 1 … m/4 , S = m/2.

$$Si\ \ W_{b,ij} > 0.5,\ Alors\ \ W_{b,ij} = 1,\ \ Sinon\ W_{b,ij} = 0. \quad \text{Avec } b = 1, 2, 3,4 \quad \textbf{4.12}$$

Où $C^*_{w,ij}$ sont les coefficients de la DWT de l'image marquée de la bande LL. C_{ij} sont les coefficients de la DWT de l'image originale.

Les marques sont obtenues par l'application de l'opération *XOR* entre la clef *K* et les quatre messages extraits *W(K)*. Ensuite, une comparaison est effectuée entre ces quatre marques pour qu'une seule représente la marque de sortie *W*. Cette comparaison est effectuée à partir de:

$$Si \quad (W_{1,ij} + W_{2,ij} + W_{3,ij} + W_{4,ij}) >= 1 \quad Alors \quad W_{i,j} = 1 \quad Sinon \quad W_{i,j} = 0 \qquad \textbf{4.13}$$

Où i,j = 1… 128.

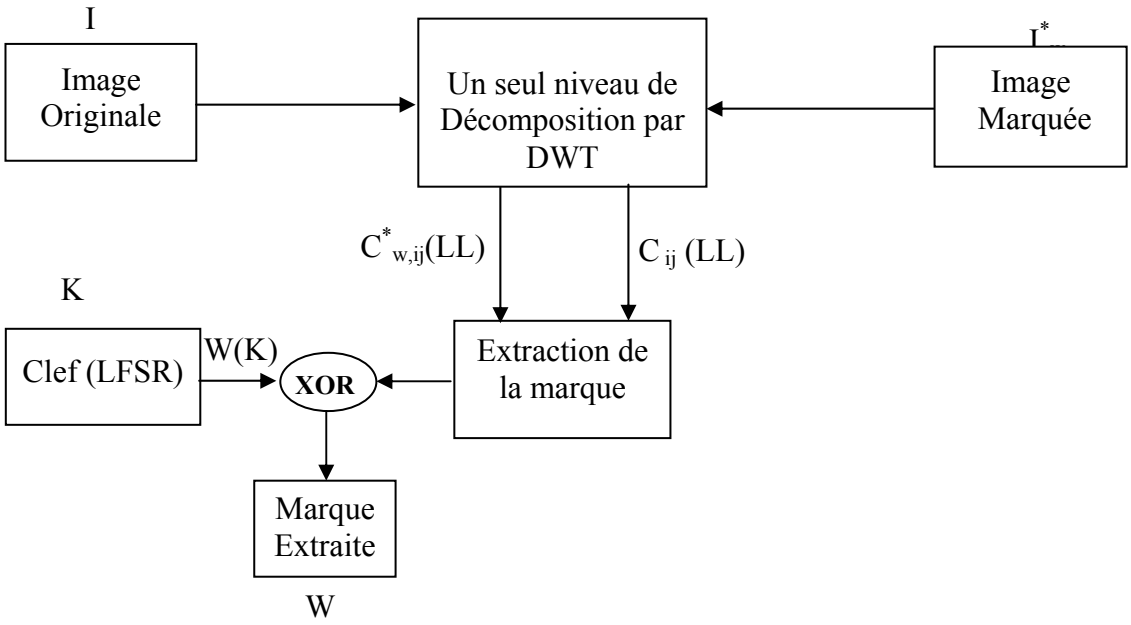


Figure 4.14: *Procédure d'extraction de la marque.*

Où I^*_w l'image marquée et éventuellement attaquée.

4.2.2.3 Robustesse face aux transformations géométriques

Afin d'évaluer la robustesse du schéma de tatouage proposé, nous avons appliqué plusieurs attaques de types transformations géométriques telle que la rotation le ''Cropping'' et le ''Resize'' ainsi que d'autres types de traitements (les falsifications à titre d'exemples). Nous nous sommes intéressés plus particulièrement au ''Cropping'' compte tenu de son effet dégradateur sur les marques utilisées dans le tatouage. Le facteur de robustesse (force du tatouage) utilisé dans notre algorithme est de 6.

La *figure 4.15* montre la contrainte d'invisibilité de l'approche proposée qui n'entraîne aucune dégradation perceptible sur l'image tatouée (Barbara) malgré que le message inséré est de taille relativement importante (128x128)x4 bits.

a: Image originale . **b :** Image marquée .

Figure 4.15: *Application de la méthode proposée sur l'image ''Barbara'' de taille 512x512 avec α (force du tatouage) = 6.*

La corrélation entre les marques extraites et les marques originales est donnée par :

$$\text{Corrélation} = (\sum\sum W(m,n)W'(m,n))/[W(m,n)]^2 \qquad \textbf{4.14}$$

Où W est la marque originale de taille mxn et W' la marque extraite de même taille. Le *tableau 4.4* présente le PSNR et la corrélation pour les quatre images tests. Pour ces valeurs, aucune dégradation visuelle après tatouage n'a été constatée.

	Barbara	Lena	Boat	Baboon
PSNR (dB)	41.63	41.62	41.60	41.60
Corrélation	1	1	1	1

Tableau 4.4: *PSNR et Corrélation pour les images tests.*

L'approche adoptée, offre dans l'ensemble, de très bonnes performances, en termes de robustesse, face aux transformations géométriques. Le tatouage réalisé résiste bien même si l'image tatouée perd plus de 50%, voire 75%, de son propre contenue. La *figure 4.16* illustre certaines distorsions géométriques subies par l'image ''Barbara'' et ''Lena'' ainsi que les marques extraites.

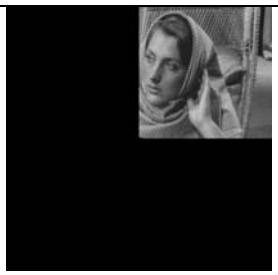
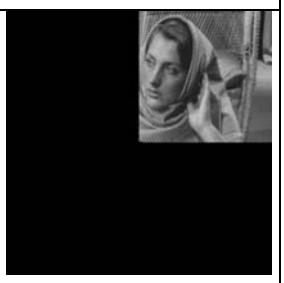
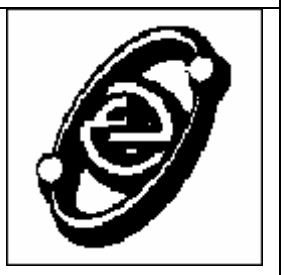
	PSNR=29.86	PSNR=25.30	PSNR= 27.00	PSNR = 28.56
Images attaquées				
	PSNR= 25.28	PSNR=24.57	PSNR= 27.58	
Images attaquées				
	Corrélation = 1.	Corrélation = 1.	Corrélation = 1.	Corrélation = 1.
Marque Extraite				

Figure 4.16: *Images, ''Lena'' et ''Barbara'', tatouées et attaquées par des transformations géométriques (cropping et rotation) et les marques extraites.*

Les marques extraites, après ces types d'attaques très pertinentes, sont donc identiques aux marques originales (corrélation = 1). 25% de l'image tatouée, par la méthode proposée, suffisent amplement pour extraire une marque de qualité excellente.

Nous avons également testé la robustesse de notre schéma face à d'autres types de traitements visant la falsification de l'image tatouée (attaques volontaires).

La *figure 4.17* présente certains exemples de traitements effectués sur les deux images ''Baboon'' et ''Boat'' ainsi que les marques extraites.

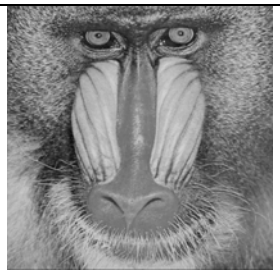
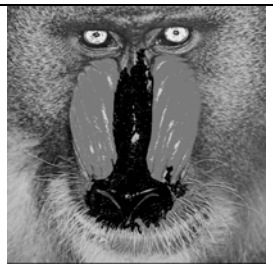
	Image Baboon marquée PSNR = 41.60 dB.	Image Boat marquée PSNR = 41.60 dB.	
Images tatouées			
	Baboon falsifiée PSNR = 29.93	Boat falsifiée PSNR = 28.51	Boat falsifiée PSNR = 27.11
Images falsifiées			
	Marque extraite Corrélation = 0.96	Marque extraite Corrélation = 0.99	Marque extraite Corrélation = 0.99
Marques extraites			

Figure 4.17: *''Baboon'' et ''Boat'' tatouées et attaquées (falsification) et les marques extraites après attaque.*

Pour bien étudier la robustesse de la méthode proposée, nous avons choisi une distorsion géométrique très prononcée celle appliquée sur l'image ''Lena'' (*figure 5 (e)*). La *figure 4.18* montre que l'extraction est toujours possible même pour ce cas extrême. Ceci est dû à la redondance de la marque (2 fois).

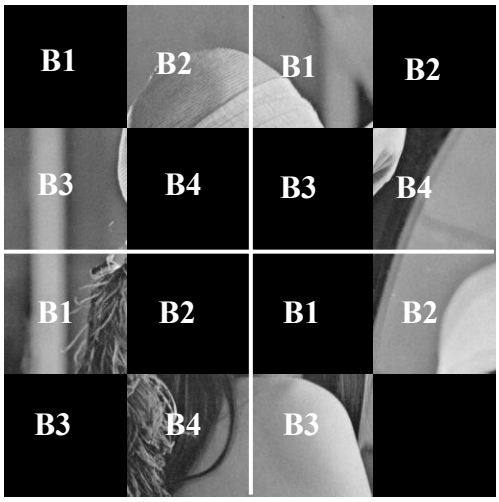
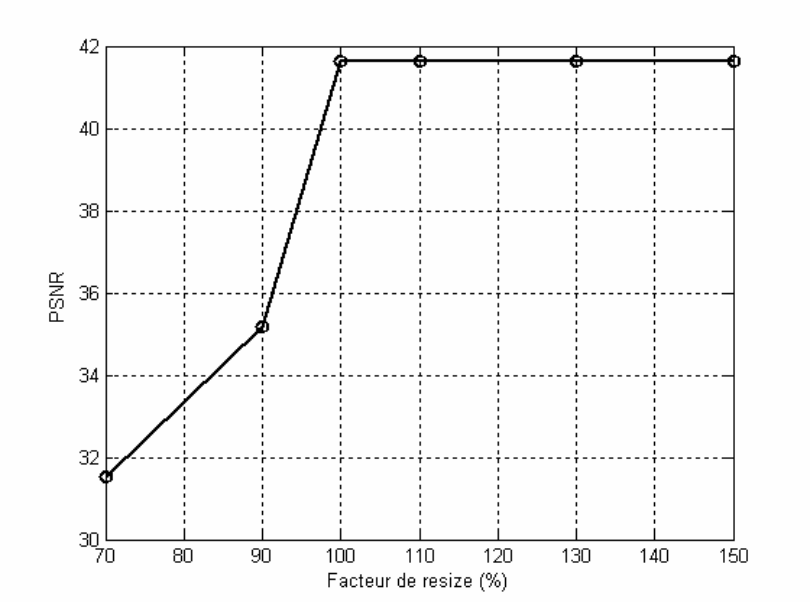
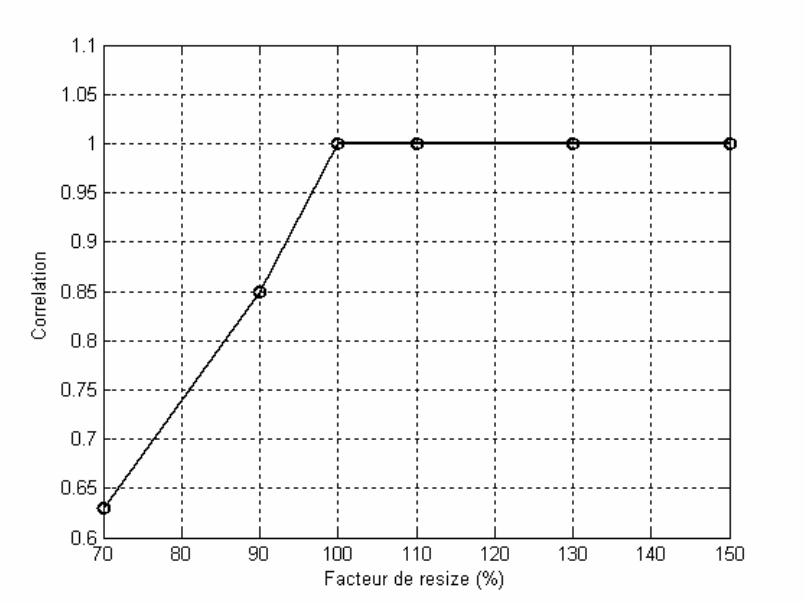


Figure 4.18: *Application de l'algorithme sur l'image ''Lena'' attaquée par le 'cropping'.*

Les deux courbes (a) et (b) de la *figure 4.19* permettent d'évaluer la robustesse de notre schéma face au changement d'échelle (Resize) pour différents facteurs de ''Resize'' dans le cas de l'image ''Barbara''.



(a) évolution du PSNR



(b) évolution du taux d'erreur (corrélation)

Figure 4.19: *La robustesse du système proposé face au changement d'échelle (Resize).*

4.2.2.4 Robustesse face à la compression

Nous avons aussi testé la robustesse de notre méthode face à la compression JPEG à 40%.

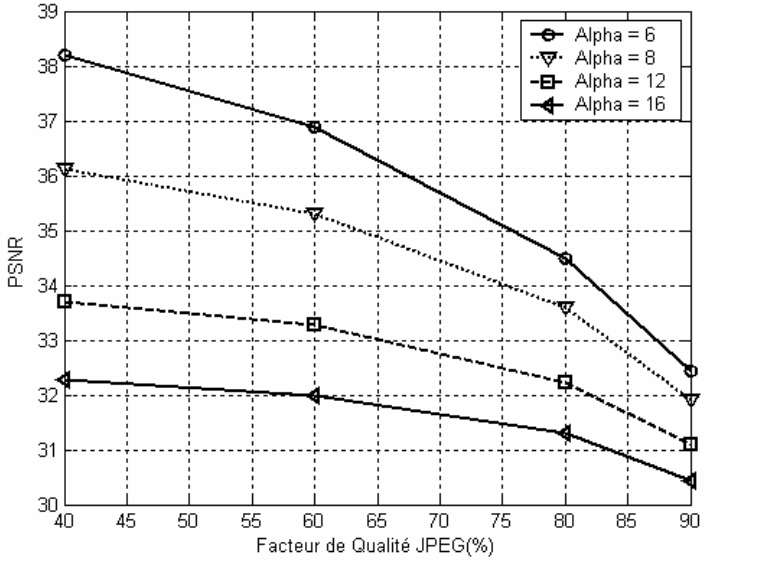
	Facteur de qualité JPEG (%)				α
	90	**80**	**60**	**40**	
PSNR	38.2	36.11	33.70	32.27	**α = 6.**
Corrélation	0.91	0.74	0.61	0.56	
PSNR	36.89	35.30	33.27	32.00	**α = 8.**
Corrélation	0.97	0.83	0.67	0.6	
PSNR	34.5	33.59	32.22	31.29	**α = 12.**
Corrélation	0.99	0.94	0.78	0.67	
PSNR	32.43	31.92	31.09	30.44	**α = 16.**
Corrélation	1	0.98	0.86	0.75	

Tableau 4.5: *PSNR et Corrélation en fonction du facteur de robustesse et du facteur de qualité JPEG.*

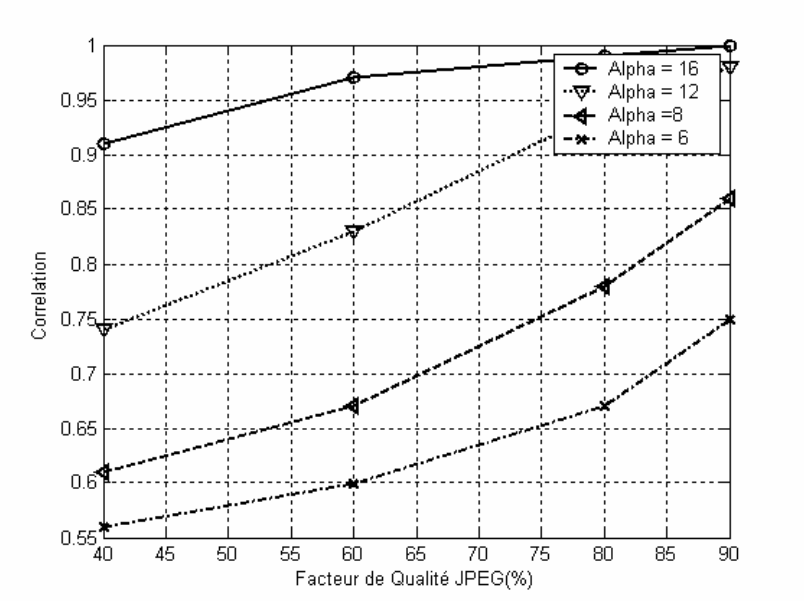
L'insertion de la marque dans les coefficients de la bande de base (bande LL) de la DWT, lui accorde une bonne robustesse face à la compression JPEG.

Il est important de noter que le facteur de robustesse (α) joue un rôle primordial dans le cas des attaques de type traitement de signal et compression. S'il est élevé, la corrélation est bonne avec une dégradation visible sur l'image tatouée (PSNR faible). Au contraire, s'il est faible, on obtient une marque de qualité médiocre avec une invisibilité importante (PSNR élevé). Les résultats obtenus pour l'image ''Barbara'' sont portés dans le *tableau 4.5*.

La *figure 4.20* présente les résultats obtenus dans le cas de la compression JPEG pour les différents facteurs de robustesse présenté dans le *tableau 4.5* (pour l'image ''Barbara''). La courbe (a) de cette figure montre la dégradation da la qualités du tatouage en terme d'invisibilité mesurée par le PSNR. L'évolution de la corrélation (mesurée entre la marque originale est celle extraite) en fonction du facteur de robustesse et facteur de qualité JPEG est présentée sur la *figure 4.20 (b)*.



(a) évolution du PSNR



(b) évolution de la corrélation

Figure 4.20: *Évaluation face à la compression JPEG.*

Dans le schéma proposé, la robustesse face à la compression JPEG dépend complètement du facteur de robustesse α. Mais, l'augmentation de ce facteur pose un problème de visibilité (dégradation de la qualité de l'image tatouée). Avec α = 6, des résultats similaires à ceux obtenu pour α = 12, peuvent être assurés avec la modification de l'expression (4.13):

$$Si \quad (W_{1,ij} + W_{2,ij} + W_{3,ij} + W_{4,ij}) >= \mathbf{3} \quad Alors \quad W_{i,j} = 1 \quad Sinon \quad W_{i,j} = 0 \qquad \mathbf{2.15}$$

Où i,j = 1… 128.

Mais cette modification diminue la robustesse de l'algorithme face aux transformations géométriques. Comme par exemples pour l'attaque de la *figure 4.18*, la marque extraite sera complètement détruite (Corrélation = 0).

4.2.2.5 Etude comparative

Afin d'évaluer les performances de l'approche proposée, nous avons comparé ses résultats avec ceux obtenus par d'autres méthodes (non-aveugles et additives) opérant soit dans le domaine spatial ou dans le domaine transformé [101][103][106]. Les tests de robustesse ont été effectuées essentiellement pour le ''cropping''.

Le *tableau 4.6* présente la quantité d'information ajoutée, en terme de bits, aux images tatouées pour chaque méthode. Pour ces valeurs, aucune dégradation visuelle après tatouage n'a été constatée. La qualité des méthodes est évaluée par la corrélation entre la marque originale et la marque extraite définie par (**4.14**).

	Verma's	Drira 's	Raval's	Méthode proposée
Quantité (bits)	50x50	119	32x32x2	128x128x4
Corrélation	0.86	0.92	0.68	1

Tableau 4.6: *Quantité d'information incrustée pour chaque méthode.*

La *figure 4.21* présente les variations du coefficient de corrélation entre la marque extraite et la marque originale pour les différentes méthodes testées.

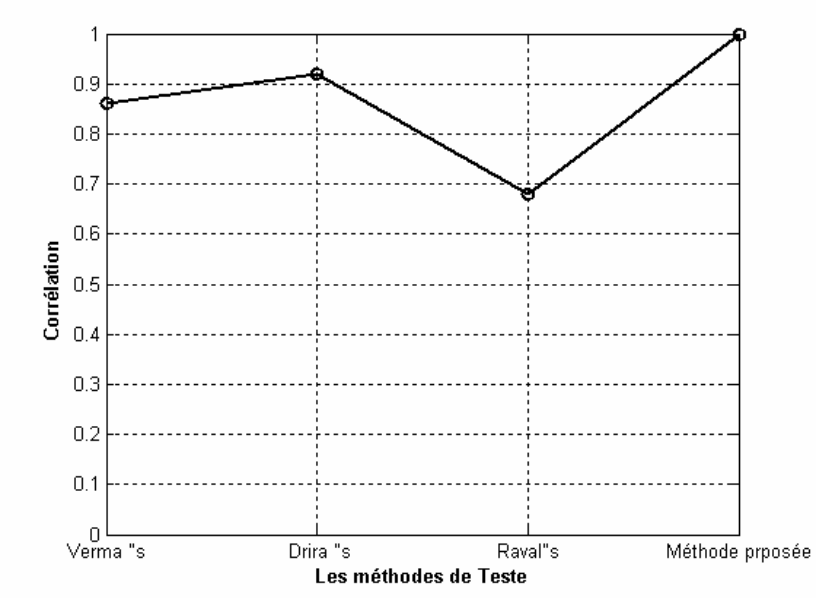


Figure 4.21: *Etude de la robustesse face au ''Cropping''.*

Nous avons proposé dans cette section, une méthode de tatouage additive, non aveugle basée sur la modification des coefficients de la bande LL du premier niveau de décomposition de la DWT.

La méthode permet d'insérer une information de taille relativement importante (128x128x4 bits) et peut satisfaire les propriétés de transparence et de robustesse. Nous avons inséré la marque d'une façon redondante et parallèle pour assurer la robustesse de l'algorithme face à plusieurs types d'attaques. Cet algorithme a prouvé sa robustesse face à des attaques

géométriques comme le changement d'échelle (Resize), la rotation est d'une façon particulière le ‘’Cropping’’. Néanmoins, l'algorithme proposé présente une faible robustesse face aux attaques de type compression comme la norme JPEG.

4.3 Tatouages d'images couleurs

4.3.1 Utilisation de l'espace couleur RGB

Certains auteurs ont dissimulé le filigrane que sur le composant Bleu, pour la raison que ce dernier est le moins sensible aux altérations [68]. D'autres auteurs ont proposé d'ajouter la marque dans les trois canaux R, V et B [70][107][108] pour l'augmentation de l'espace d'insertion de l'image , dans [87][109][110] les auteur ont tenté d’incruster La marque à travers autres Systèmes de Représentation Colorimétrique que le RVB (XYZ, YIQ, YUV).

Cette section a fait l’objet d’un article présenté lors de la conférence iceedt'08 [111]. Dans le travail présenté dans cette section, la transformée en ondelettes discrète est appliquée sur les deux composants V et B afin d'imposer une structure fixée par le marque.

La seule raison d'utiliser deux composants est de ne pas dégradé la qualité des canaux de l'image originale.

4.3.1.1 Insertion de la marque

La méthode proposée est basée sur un schéma additif et s'appuie sur le marquage des deux canaux vert et bleu de l'image originale. Les deux canaux sont tout d’abord décomposés en utilisant la *transformée en ondelettes discrète* avec la structure pyramidale. Dans notre système d’inclusion de la marque, la décomposition est performée à travers deux et un niveau de décomposition utilisant le « *Haar filter* » respectivement pour le V et B. Le schéma de la *figure 4.22* montre le diagramme d’inclusion de la watermark Dans cette partie, nous allons détailler l'algorithme; l'image marquée ***X’*** résulte de l'inclusion dans l'image hôte ***X*** de la marque ***W***.

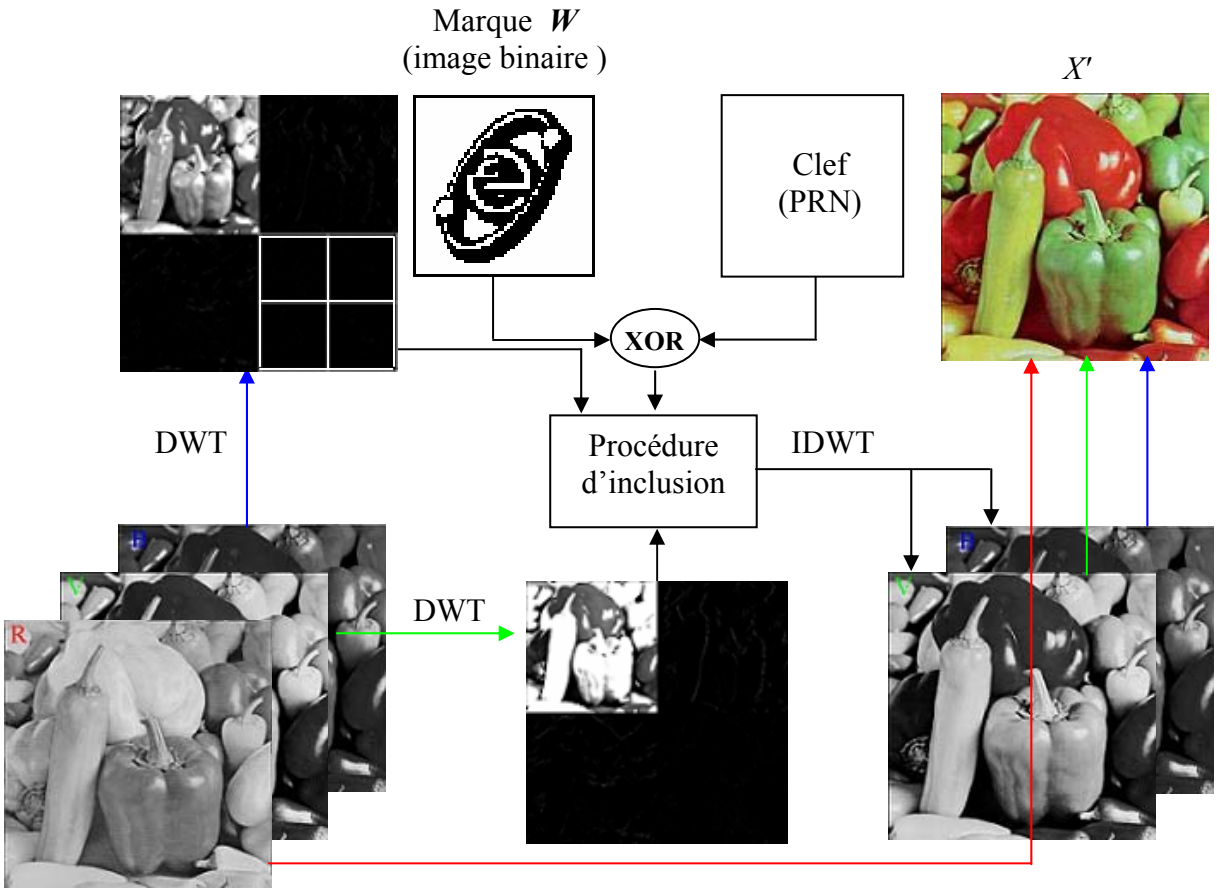


Figure 4.22: *Diagramme de la procédure d'inclusion de la marque.*

Où :

X – les trois canaux (Rouge, Vert et Bleu) de l'image originale.

X' – Image marquée

Pour le canal V la sous-bande de décomposition LL est divisée en blocs de 4x4 (P_V) coefficients chaque pixel de la marque qui est de taille 64 x 64 pixels , est additionnée dans tous les coefficients de chaque bloc du sous-bande LL , de même pour le canal B, après la décomposition du canal B à travers un seul niveau de décomposition de la transformée en ondelettes discrète, la sous-bande HH sera elle-même décomposée utilisant le « *Haar filter* » en quatre bandes fréquentielles , cette décomposition est justifiée par le fait que les détaille de la transformée en ondelettes discrète (LH,HL,HH) sont robustes face à certaine nombres d'attaque tel que le filtrage , ajustent et gamma correction. La soub-bande HH_{H2} est aussi divisée en blocs de 2x2 (P_B) coefficients où tous les coefficients de chaque bloc contiennent le pixel correspondant de la maque à ajouter. La procédure d'inclusion est performée selon les deux formules suivantes :

$$C^{LL}_{W,Pvi} = C_{Pv,i} + \alpha_{LL} W_i, \quad i, P_V = 1,...,64x64. \qquad \textbf{4.16}$$

$$C^{HH\ 2}_{W,Pb,i} = C_{Pv,i} + \alpha_{HH2} W_i, i, P_V = 1,...,64x64. \qquad \textbf{4.17}$$

Où $\boldsymbol{\alpha}$ est la force du tatouage. $w_{ij} \in \{0,1\}$, $1 \leq i \leq 64x64$.

C_{Pv} les coefficients de la sous-bande LL du canal V et C_{PB} les coefficients de la sous-bande HH_{H2} du canal B.

L'image marquée est obtenue en appliquant l'inverse de la transformée en ondelettes discrète (*IDWT*) sur les deux canaux V et R.

4.3.1.2 Extraction de la marque

Dans la procédure d'extraction de la marque, les deux canaux Verts de l'image marquée et l'image originale tous deux décomposés en un niveau par la *DWT,* et les deux canaux bleus de l'image marquée et l'image originale tous deux décomposés en deux niveaux par la *DWT*. Il est supposé que l'image originale est connue pour l'extraction (schéma d'extraction non aveugle). À l'extraction la somme des 16 coefficients de chaque bloc de 4x4 de la sous-bande LL du premier niveau de décomposition de la transformée en ondelettes discrète du canal V est comparée avec la somme correspondantes des coefficients de l'image originale pour extraire un seul bit de la marque. La même méthode est appliquée sur des blocs de 2x2 de la sous-bande HH_{H2} du canal B.

La procédure d'extraction est décrite par les deux formules suivantes:

$$\boldsymbol{w_i = (\sum C_{w,\mathrm{Pv,i}} - \sum C_{Pv,i}) / \alpha_{LL}}, \quad i = 1...64x64 \qquad \textbf{4.18}$$

$$SI\ \boldsymbol{W_{ij} > (\alpha_{LL} * 4x4)}/2,\ Alors\ \boldsymbol{W_{ij}} = 1,\ Sinon\ \boldsymbol{W_{ij}} = 0 \qquad \textbf{4.19}$$

$$\boldsymbol{w_i = (\sum C_{w,\mathrm{Pv,i}} - \sum C_{Pv,i}) / \alpha_{LL}}, \quad i = 1...64x64 \qquad \textbf{4.20}$$

$$SI\ \boldsymbol{W_{ij} > (\alpha_{LL} * 4x4)}/2,\ Alors\ \boldsymbol{W_{ij}} = 1,\ Sinon\ \boldsymbol{W_{ij}} = 0 \qquad \textbf{4.21}$$

Où $\boldsymbol{C_{w,Pv,i}}$ *et* $\boldsymbol{C_{w,PB,i}}$ sont respectivement les coefficients de la DWT des deux canaux Vert et Bleu marqués (et peut être attaqués).

$\boldsymbol{C}_{\mathrm{Pv,i}}$ $\boldsymbol{C}_{\mathrm{PB,i}}$ sont respectivement les coefficients de la DWT des deux canaux Vert et Bleu de l'image originale.

La *figure 4.23* montre le diagramme d'extraction de la marque ;

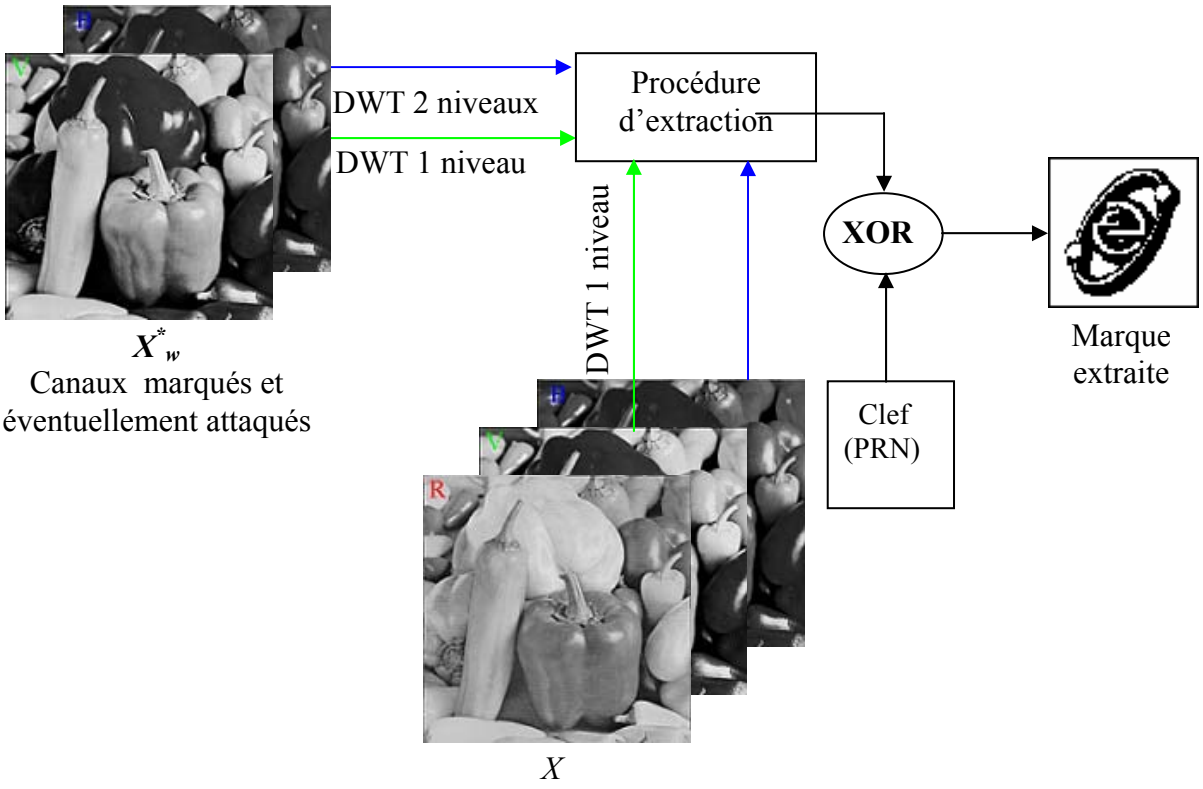


Figure 4.23: *Diagramme de la procédure d'extraction de la marque.*

X - les trois canaux (Rouge, Vert et Bleu) de l'image originale.

X^*_w - Canaux (Vert et Bleu) marqués et éventuellement attaqués

4.3.1.3 Robustesse de l'algorithme

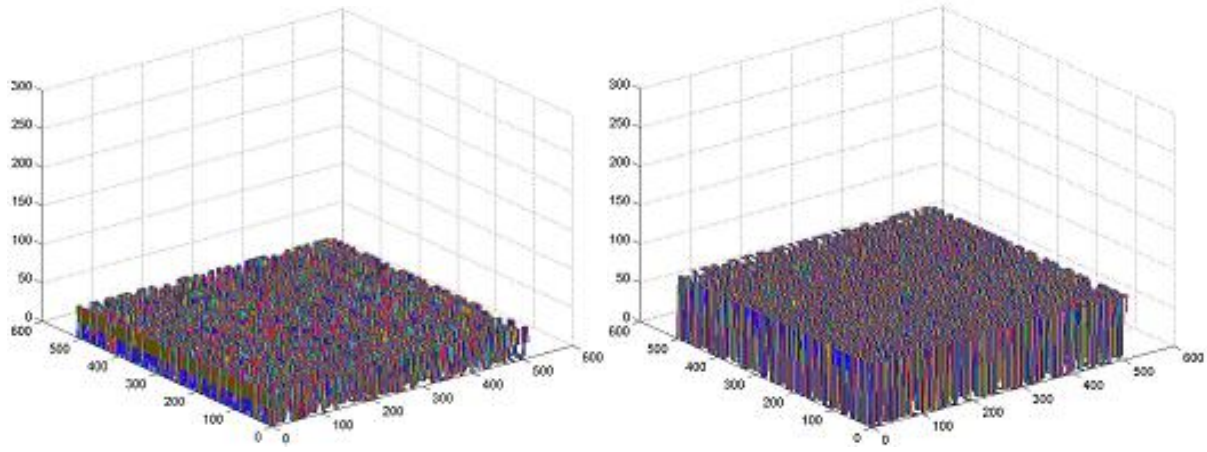
Les tests présentés ici sur l'image ''Peppers-color'' (*Figure 4.24 (a)*) ont été effectués avec un facteurs de robustesse $\alpha = 8$ pour la sous-bande fréquentielle LL pour le canal vert et 6 pour la sous- bandes fréquentielles HH_{H2} pour le canal bleu. Le message inséré est une image binaire de taille MxM, ou M = 64.

Par raison d'incohérence du PSNR (Peak Signal to Noise Ratio) dans le cas des images couleur [107][108] (les valeurs du PSNR restent élevées alors que les dégradations sont visibles pour l'image tatouée); Le PSNR est calculé pour chaque canal à part, les PSNR mesurés pour les canaux tatoués V et B sont respectivement 39.19 db, 47.37 db.

a: Image originale . **b :** Image marquée .

Figure 4.24: *Application de la méthode proposée sur l'image ''Peppers-color'' de taille 512x512 avec α = 8 pour LL du canal V et 6 pour HH_{H2} du canal B.*

La *figure 4.25 (a*) représente la différence *absolue* entre le canal vert de l'image originale et celui de l'image tatouée fortement amplifiée par un facteur de 20, le même facteur d'amplification est utilisé pour représenter la différence *absolue* entre le canal bleu de l'image originale et celui de l'image tatouée.



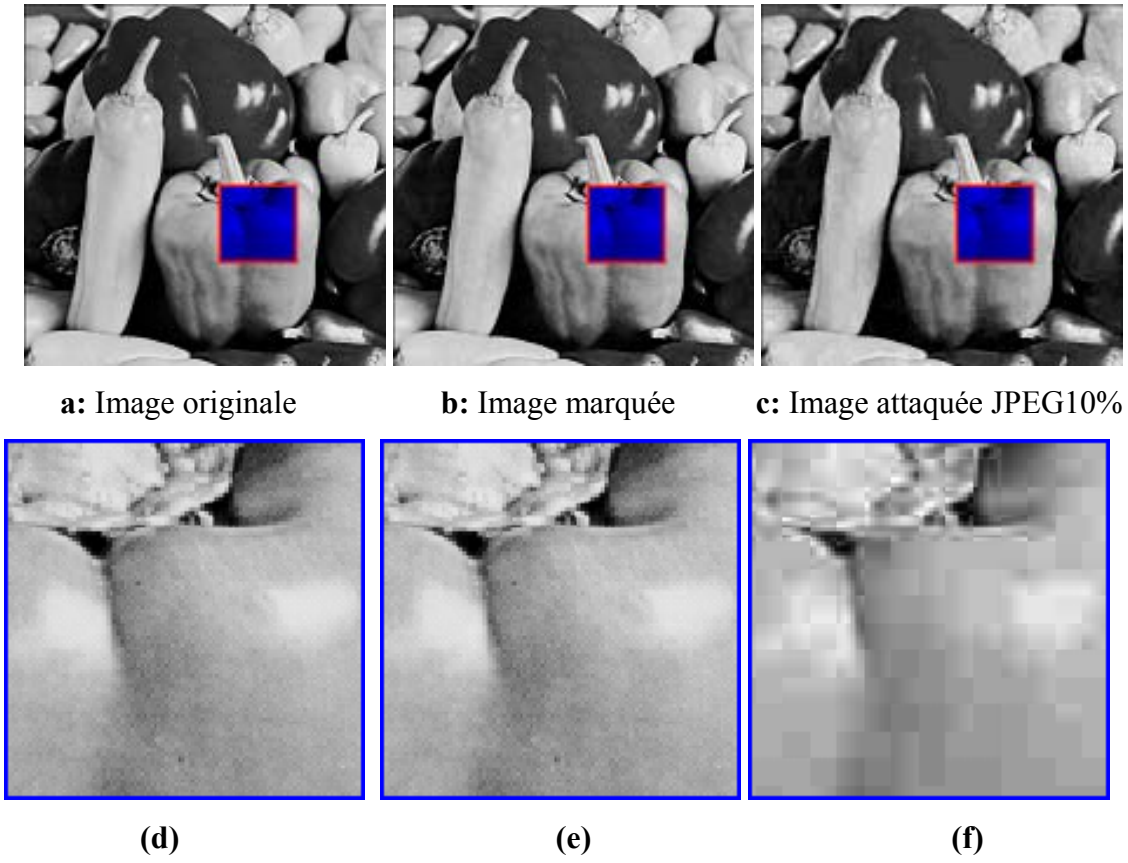
(a) **(b)**

Figure 4.25: *Différence absolue entre les canaux (V et B) de l'image originale et les canaux (V et B) de l'image marquée, amplifiée par un facteur de 20.*

Afin de montrer l'influence de différentes attaques sur la lecture de la marque, nous choisissons d'illustrer nos résultats sur la seule image ''Peppers-color'', sachant que des résultats similaires ont été obtenus sur d'autres images de même taille. Nous avons décidé de

valider l'algorithme face à des attaques de type « traitement du signal » (filtrage, ajout de Bruit Gaussien, modifications de l'histogramme, etc).

La *figure 4.26* présente le canal V de l'image ''Peppers-color'' tatouée avant et après compression JPEG de 10% de qualité. Les artefacts apparaissent nettement. Pour ce taux, le tatouage donne des résultats positifs.



a: Image originale **b:** Image marquée **c:** Image attaquée JPEG10%

(d) **(e)** **(f)**

Figure 4.26: *Invisibilité et robustesse de l'algorithme même après une compression de 10% de qualité.*

L'image de zoom présentée dans la *figure 4.26 (e)* montrant la contrainte d'invisibilité de notre algorithme même si le facteur de robustesse α est plus au mois élevé, la *figure 4.26 (f)* montre que les artefacts apparaissent nettement, pour ce taux, et la marque toujours existe (*figure 4.27 (d)*).

Notre algorithme de tatouage offre dans l'ensemble de bonnes performances en termes de robustesse face à certains nombres d'attaques. On constate que le tatouage reste très résistant aux modifications de luminance et de contraste, ainsi qu'aux ajustements et compression JPEG. La *figure 4.27* illustre quelques traitements effectués sur l'image

‘’Peppers-color’’ ainsi que les marques extraites. L’algorithme permet d’insérer 64x64 bits dans chaque canal (V et B) de l'image originale à travers la transformée en ondelettes discrète et satisfait les propriétés de transparence et de robustesse.

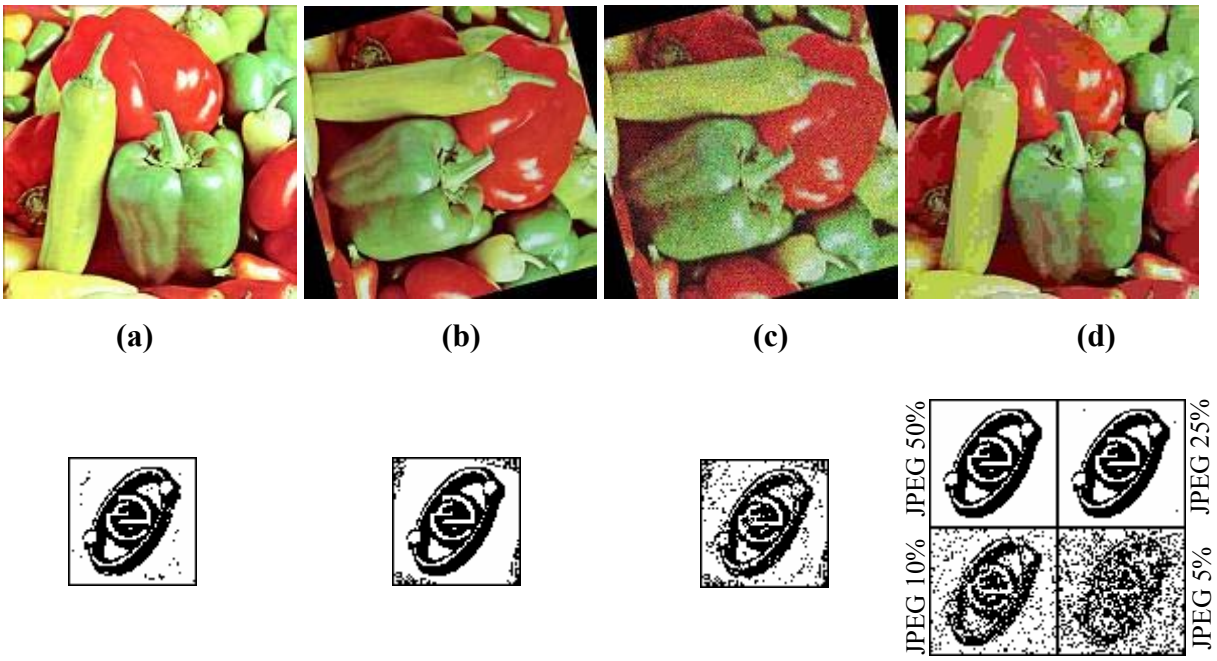


Figure 4.27:*L'image ‘’Peppers-color’’ marquée et attaquée et les marques extraites après attaques.*

La méthode proposée montre sa robustesse même si l'image tatouée subi plusieurs attaques successives comme le montre la *figure 4.27 (c*) ou l'image est attaquée par quatre traitement de différente type (compression JPEG de 25% de qualité, filtrage, Bruit Gaussien et Rotation -75%). Après ces quatre traitements successifs la marque extraite reste visible.

La figure 4.28 présente les réponses du détecteur à 1000 marques générées aléatoirement, la distance de Hamming est 0.

La marque w^* pour la sous-bande LL du première niveau de décomposition de la transformée en ondelette discrète du canal V apparaît en position 200 et en positions 800 pour la sous-bande HH_{H2} du deuxième niveau de décomposition du canal B, elle est parfaitement détectée, la distance de Hamming est nulle.

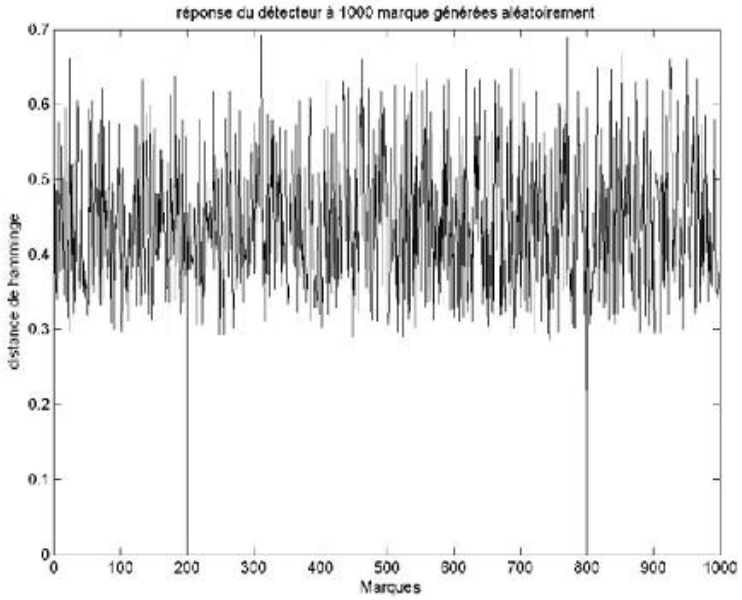
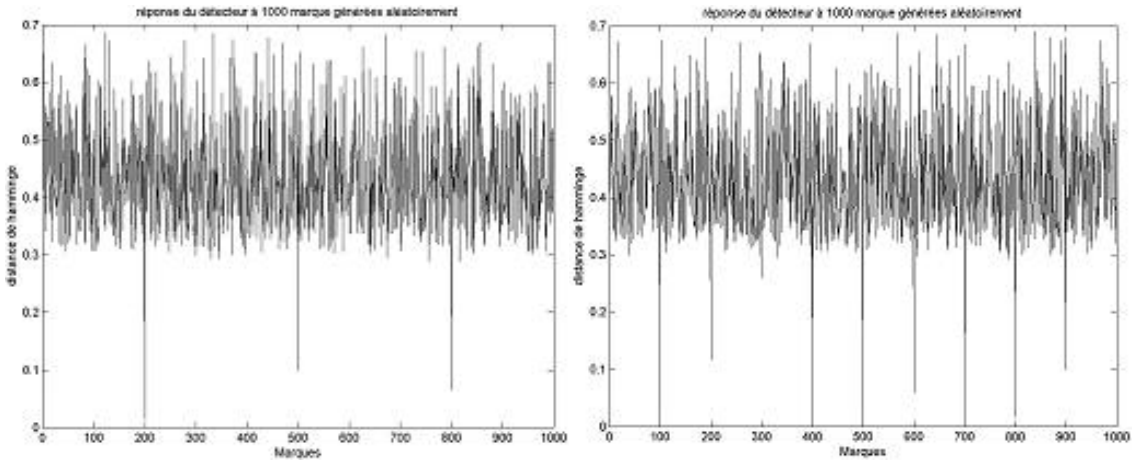


Figure 4.28: *Réponse du détecteur à 1000 marques générées aléatoirement, notre marque apparaît en position 200 pour LL bande et en positions 800 pour* HH_{H2}.

*La figure 4.*29 *(a)* montre le comportement du détecteur après les types d'attaques suivantes: JPEG20%, JPEG10%, JPEG5%, Bruit Gaussien, Filtering, Rotate-75% avec Cropping, Resize 150%, JPEG25% et Bruit Gaussien, JPEG25% et Filtering et Bruit Gaussien et Rotation -75%.

La détection est excellente et la marque est reconnue que pour la compression de qualité 5%.

Ces marques sont extraites de la sous-bande LL, la détection des marques extraite de la sous-bande HH_{H2} (*figure 4.29 (b))* après les trois type d'attaques suivantes: Intensity Adjustment, Gamma Correction, Intensity Adjustment et Gamma Correction, est excellente et les marques sont reconnues pour les trois types ce qui explique que la bande fréquentielles LL, est robuste que face certain type d'attaque, et la sous-bande HH_{H2} est aussi robuste que face certain autre type d'attaque *(figure 4.30)*.



(a) **(b)**

Figure 4.29: *Réponse du détecteur après attaque. (a) marques extraites de LL, (b) marques extraites de* HH_{H2}.

Les attaques présentées ci-dessus dégradent plus ou moins l'image. La *figure 4*.30 présente la variation de la valeur de la réponse du détecteur en fonction du type d'attaque pour les deux bandes fréquentielles LL et HH_{H2} des deux canaux vert et bleu respectivement.

Les abscisses représentent les différentes attaques selon l'ordre que nous avons donné ci-dessus.

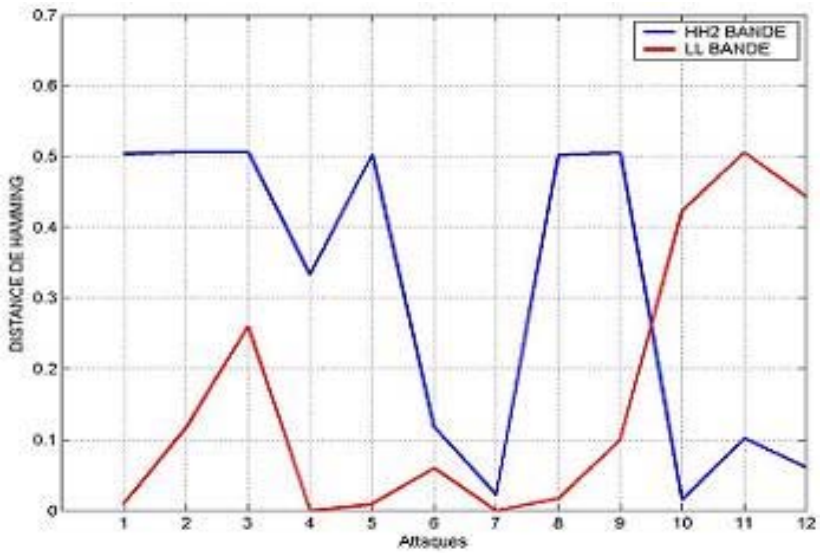
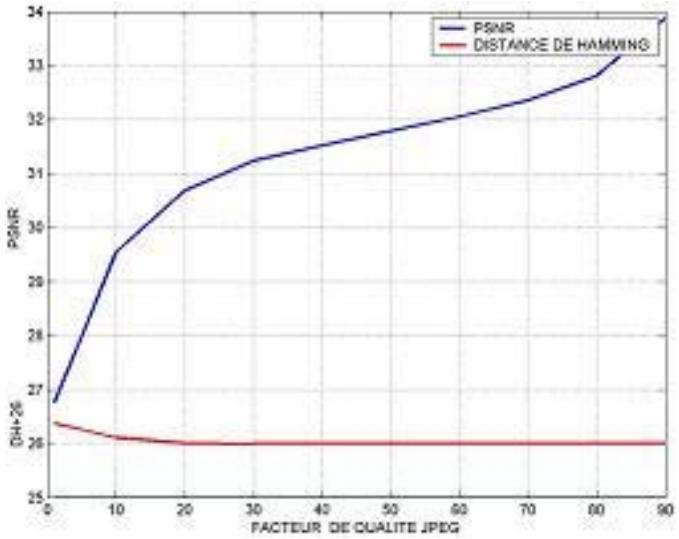


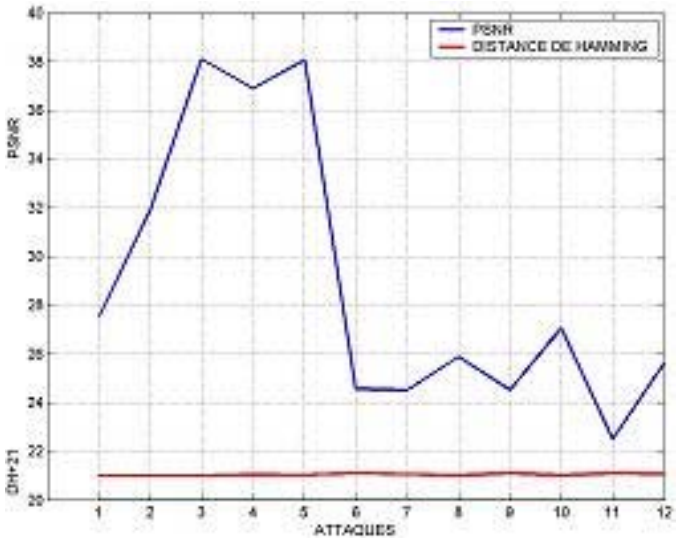
Figure 4.30: *la réponse du détecteur en fonction du type d'attaque pour les deux (LL,* HH_{H2}*) bandes fréquentielles.*

Nous présentons dans La *figure 4.31* des résultats obtenus face à différent type d'attaque. Le premier graphique de la *figure 4.31 (a)* représente la variation des réponses du détecteur et PSNR calculé entre l'image hôte et celle marquée et attaquée en fonction du taux de compression, le second *(b)* représente la variation des réponses du détecteur et PSNR en fonction des types d'attaques ci-dessous: Bruit Gaussien, Filtrage, Resize 150%, Resize 50%, Resize 90%, Rotation avec Cropping-45%, Rotation avec Cropping-75%, Intensity Adjustment, Gamma Correction, Bruit Gaussien et JPEG25%, Rotaion-75 et JPEG25% et Bruit et filtrage, Intensity Adjustment et Gamma Correction.

On a constaté que même si l'image marquée subit une dégradation visible après une compression JPEG ou filtrage ou même plusieurs attaques en même temps, il est toujours possible d'extraire une marque de bonne qualité.



(a)



(b)

Figure 4.31: *Robustesse vis-à-vis plusieurs types d'attaques*.

Nous avons proposé une méthode de tatouage additive, non aveugle basé sur la modification des Deux canaux vert et bleu du Systèmes de Représentation Colorimétrique RVB, pour le canal vert la modification été à travers la sous-bandes LL du premier niveau de décomposition de la transformée en ondelettes discrète, et dans la sous-bande HH_{H2} du deuxième niveau de décomposition de la transformée en ondelettes discrète le deuxième niveau de décomposition été appliqué sur la sous-bande HH et non pas a la sous-bande LL du premier niveau pour être plus robuste au modification de l'histogramme et au 'Intensity Adjustment'' ainsi qu'au ''Gamma Correction''.

La méthode permet d'insérer une information très importante (64x64x2 bits) tout en assurant les propriétés de transparence et de robustesse. Nous avons inséré la marque d'une façon redondante dans les deux bandes de décomposition pour assuré la robustesse de l'algorithme face à plusieurs nombres d'attaques.

Notre algorithme a prouvé sa robustesse face aux différents types d'attaques tels que la compression JPEG et les attaques géométriques locales. La *figure 4.30* montre que chaque bande de décomposition est robuste face à certaine nombre d'attaques où:

LL bande robuste face à : JPEG compression, ajout de Bruit Gaussien, Rotation, Cropping et Resize …etc

HH bandes robustes face à : Intensity Adjustment, Gamma Correction …etc

4.3.2 Amélioration par l'espace couleur YCbCr

4.3.2.1 Choix de l'espace d'insertion

Dans un objectif de satisfaire un compromis invisibilité/robustesse, dès lors qu'une image marquée risque de subir un ensemble de traitements et/ou attaques, nous proposons dans cette section une nouvelle approche de tatouage additif. Cette technique est basée sur l'utilisation de l'espace de représentation colorimétrique YCbCr dits antagonistes. L'objectif est d'assurer simultanément, à l'aide de l'utilisation de ces deux composantes, une invisibilité maximale et une grande robustesse face aux différents types d'attaques.

Nous avons choisi d'insérer la même marque dans les deux bandes fréquentielles :

- La bande LL (*Low Low*) du premier niveau de décomposition de la transformée en ondelettes discrète de la composante luminance Y.

- La bande HH_2 (*High High 2*) du second niveau de la DWT de l'une des deux composantes de chrominances en l'occurrence la composante Cr.

4.3.2.2 Insertion de la marque

Les composantes Y et Cr de l'espace YCbCr sont ainsi décomposées respectivement en un et deux niveaux de décomposition par la DWT avec la structure pyramidale, en utilisant les filtres de Haar. Une marque, définie préalablement par l'utilisateur, est ajoutée (schéma additif) dans les deux sous-bandes, la sous bande LL de la composante Y et la sous bande HH_2 de la composante Cr. Ainsi, chaque pixel de la marque correspondra à un bloc de coefficients pour chacune de ces deux sous bandes. Cette section a fait l'objet d'un article présenté lors de la conférence cifa'08 [112].

Le choix de marquer la composante de luminance est motivé par des raisons de robustesse, vis-à-vis d'une attaque involontaire due à la compression en particulier, comme la norme JPEG par exemple. En effet, ce type d'attaque dégrade relativement plus les deux composantes de chrominance par rapport à la composante de luminance. Néanmoins, l'insertion de la marque dans l'une des deux composantes achromatiques assurera la robustesse de la méthode face à d'autres types d'attaques, tel que ''Intensity Adjustment'' et ''Gamma Correction''.

Le schéma de la *figure 4.32* montre le diagramme d'inclusion de la marque.

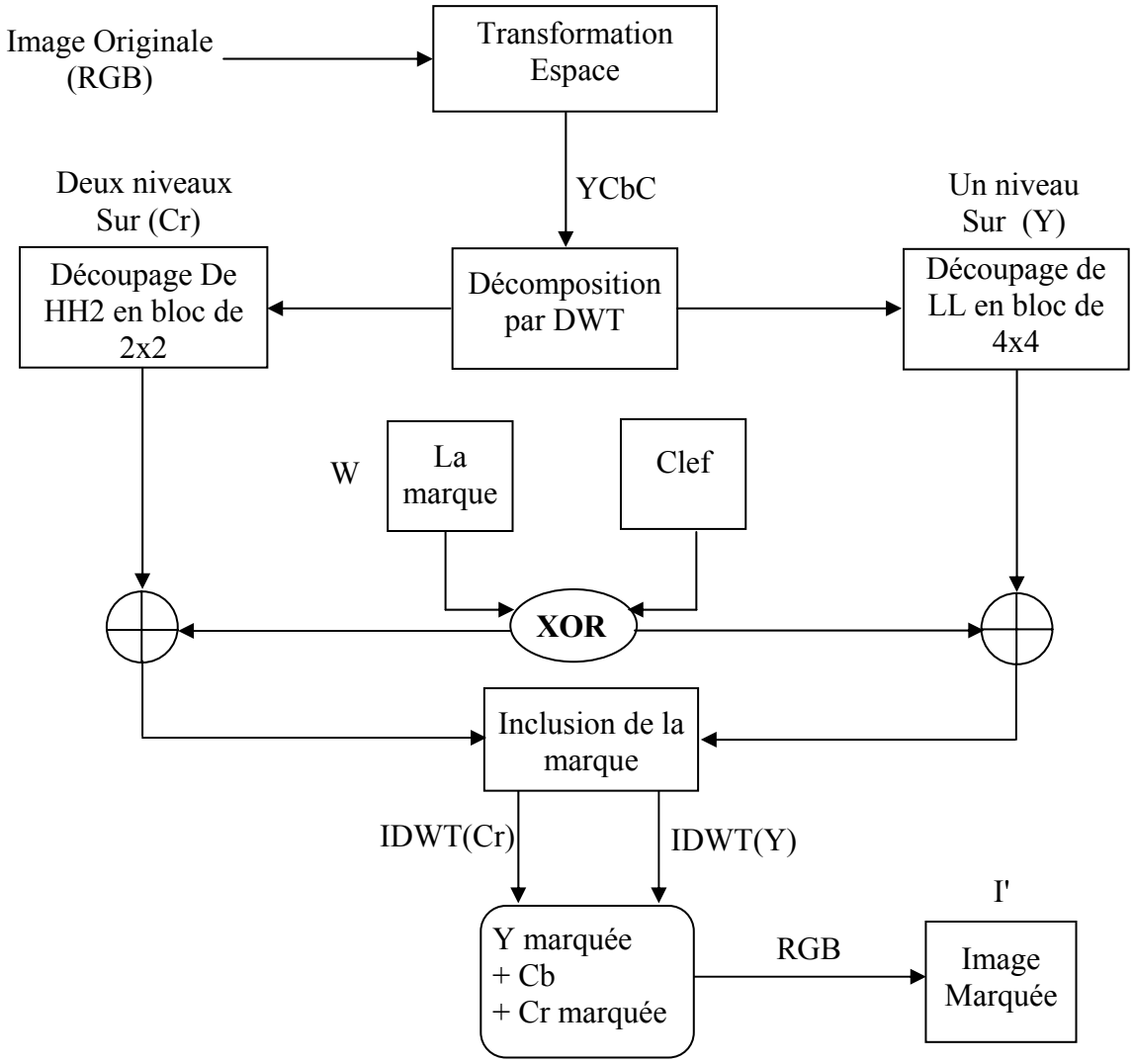


Figure 4.32 : *Schéma proposé pour l'inclusion de la marque.*

Chaque pixel de la marque, sous forme d'une image binaire de taille 64 x 64 pixels, est ajouté simultanément aux 16 coefficients d'un bloc 4x4 (B_Y) de la composante de luminance Y, et aux 4 coefficients d'un bloc 2x2 (B_{Cr}) de la composante achromatique Cr.

La procédure d'inclusion est donnée par les deux expressions suivantes :

$$C^{LL}_{w,B_{Y,i}k} = C^{LL}_{B_{Y,i}k} + \alpha_{LL} * W_i, \qquad \textbf{4.22}$$

$$\text{i} = 1,\ldots,64\text{x}64.\ \text{k} = 1,...,4*4.$$

$$C^{HH2}_{w,B_{Cr,i}k} = C^{HH2}_{B_{Cr,i}k} + \alpha_{HH2} * W_i, \qquad \textbf{4.23}$$

$$\text{i} = 1,\ldots,64\text{x}64.\ \text{k} = 1,...,2*2.$$

Où α est la force du tatouage. $w_i \in \{0,1\}$, $1 \le i \le 64x64$.

C_{By} sont les coefficients de la sous-bande LL du composante Y. C_{BCr} sont les coefficients de la sous-bande HH2 du composante Cr.

L'image marquée est obtenue en appliquant l'inverse de la transformée en ondelettes discrète (*IDWT*) sur les deux composantes Y et Cr puis une transformation au RGB.

4.3.2.3. Extraction de la marque

Dans la procédure d'extraction de la marque, les deux composantes de luminance, celle de l'image marquée et celle de l'image originale, sont toutes les deux décomposées en un seul niveau par la DWT. Quant aux deux composantes de chrominance Cr, de l'image marquée et de l'image originale, elles sont toutes les deux décomposées en deux niveaux par la DWT.

Dans la phase de l'extraction, la somme des 16 coefficients, de chaque bloc de 4x4 de la sous-bande LL du premier niveau de décomposition, de la composante Y est comparée avec la somme correspondantes aux mêmes coefficients de l'image originale pour extraire un seul bit de la marque. La même méthode est appliquée sur des blocs de 2x2 de la sous-bande HH_2 de la composante Cr.

La procédure d'extraction est décrite par les deux expressions suivantes:

$$W_i^{*LL} = \left(\sum_{k=1}^{4*4} C_{w,B_{Y,i}k}^{*LL} - \sum_{k=1}^{4*4} C_{B_{Y,i}k}^{LL}\right) / \alpha_{LL}\ , \qquad \textbf{4.24}$$

$$i = 1,\ldots,64x64.\ \text{Si } W_i^{*LL} > (\alpha_{LL} * 4x4)/2,$$
$$Alors\ W_i^{*LL} = 1\ Sinon\ W_i^{*LL} = 0. \qquad \textbf{4.25}$$

$$W_i^{*HH2} = \left(\sum_{k=1}^{2*2} C_{w,B_{Cr,i}k}^{*HH2} - \sum_{k=1}^{2*2} C_{B_{Cr,i}k}^{LL}\right) / \alpha_{HH2}\ , \qquad \textbf{4.26}$$

$$i = 1,\ldots,64x64.\ \text{Si } W_i^{*HH2} > (\alpha_{HH2} * 2x2)/2,$$
$$Alors\ W_i^{*HH2} = 1\ Sinon\ W_i^{*HH2} = 0. \qquad \textbf{4.27}$$

Où $C_{w,B_{Y,i}k}^{*LL}$ et $C_{w,B_{Cr,i}k}^{*HH2}$ sont respectivement les coefficients de la DWT des deux composantes Y et Cr marquées (et peut être attaquées).

$C_{B_{Y,i}k}^{LL}, C_{B_{Cr,i}k}^{HH2}$ Sont respectivement les coefficients de la DWT des deux composantes Y et Cr de l'image originale (YCbCr).

La *figure 4.33* montre le diagramme d'extraction de la marque ;

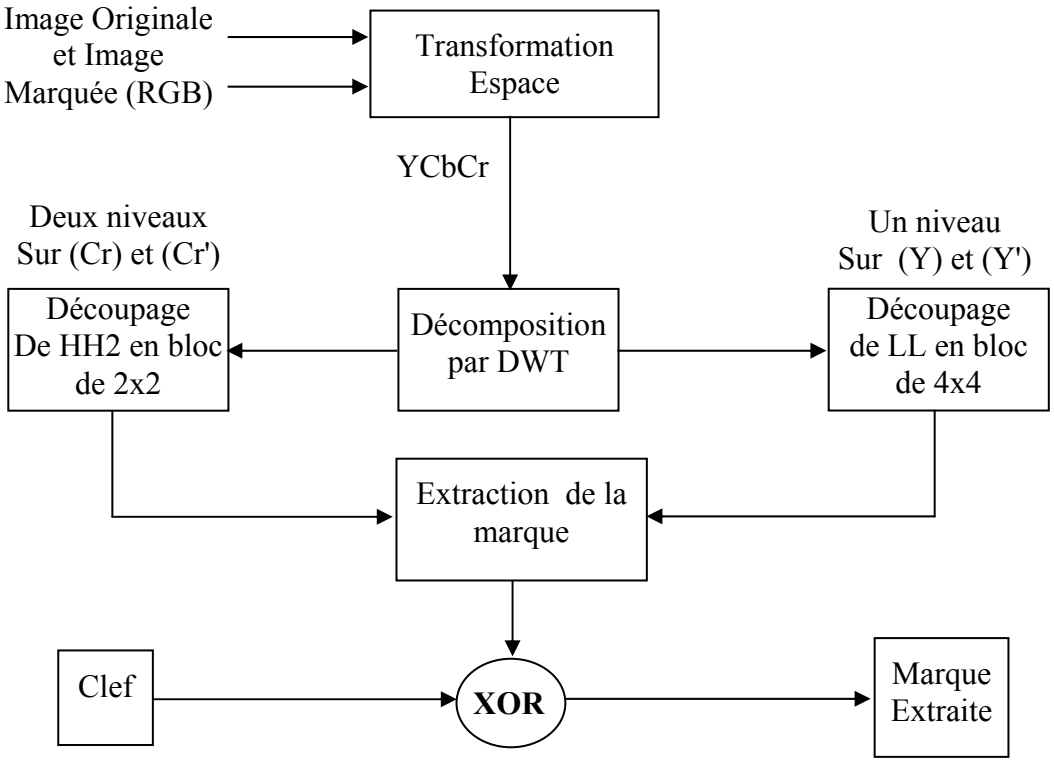


Figure 4.33: *Diagramme de la procédure d'extraction de la marque.*

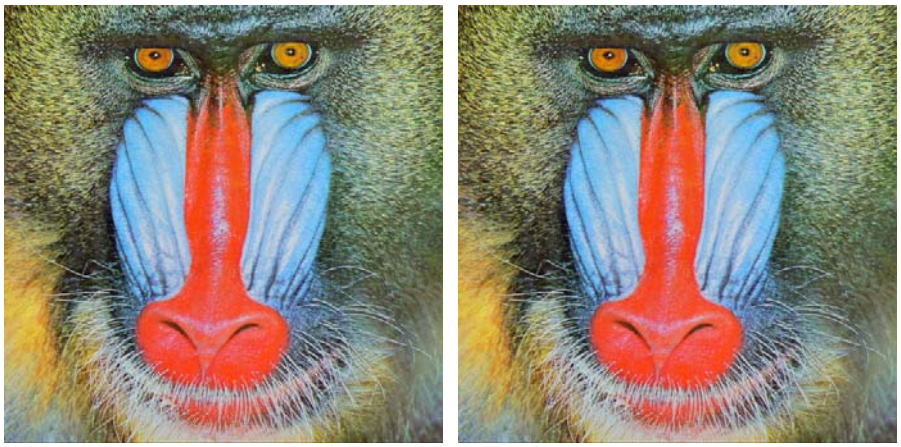
Ou Y' et Cr' sont les deus composantes marquées et éventuellement attaquées.

4.3.2.4. Robustesse luminance-chrominance

Les tests présentés sur l'image ''Baboon'' (*figure 4.34 (a)*) ont été effectués avec:

- Un facteur de robustesse $\alpha = 8$ pour la sous-bande LL et $\alpha = 6$ pour la sous-bande HH_2.
- Le message inséré est une image binaire de taille MxM, ou M = 64.

La robustesse est toujours évaluée en calculant, pour les différentes images utilisées, le PSNR entre l'image originale et l'image marquée. Dans notre travail, le PSNR pour les images en couleurs, est calculé pour chaque composante (R,V et B) séparément. Les PSNR mesurés pour ces composantes sont respectivement 39.19 dB, 39.87 db, 38.92 dB.

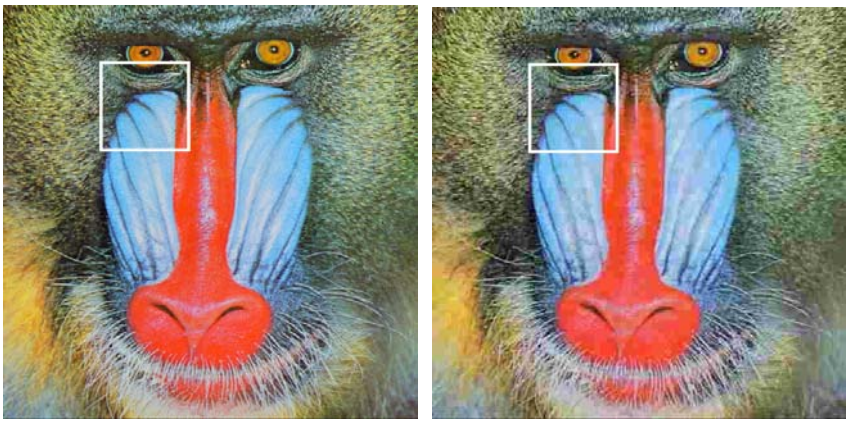


a: Image originale . **b :** Image marquée .

Figure 4.34: *Application de la méthode proposée sur l'image ''Baboon'' de taille 512x512 avec α = 8 pour LL et 6 pour HH_2.*

Dans l'objectif de montrer l'influence de différentes attaques sur la lecture de la marque, nous avons choisis de nous contenter des résultats obtenus sur la seule image ''Baboon''. Sachant que des résultats similaires ont été obtenus sur d'autres images de même taille (les images de tests). L'algorithme proposé est validé face à des attaques de type ''traitement du signal'', et quelques attaques visant la falsification de l'image tatouée.

La *figure 4.35* présente l'image originale ''Baboon'' (RGB) avant et après compression JPEG de 10% de qualité. Les artefacts apparaissent nettement. Pour ce taux, le tatouage donne des résultats appréciables.



(a) (b)

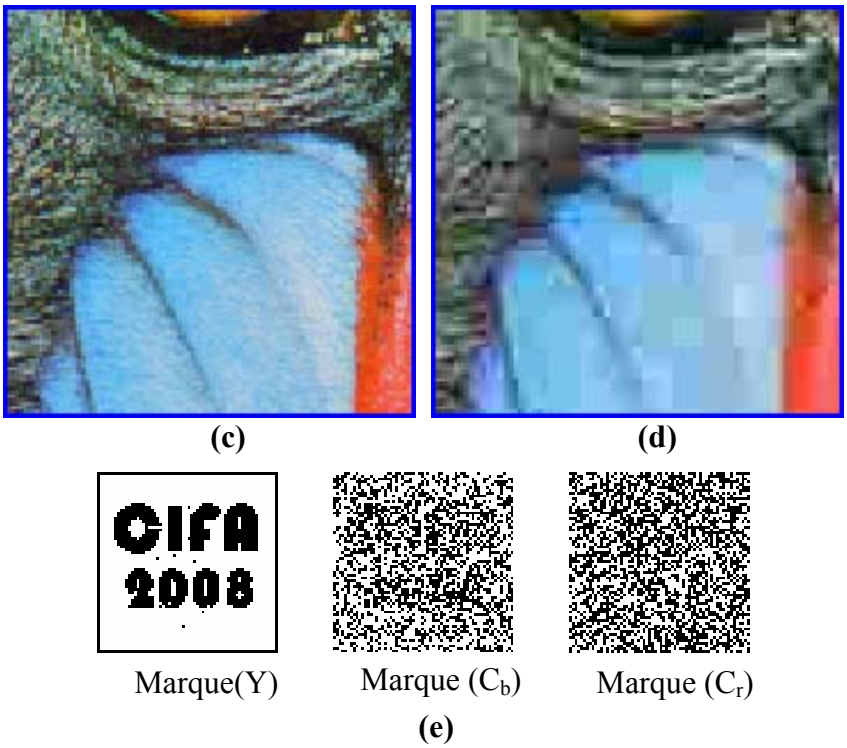


Figure 4.35: *Robustesse de l'algorithme après une compression de 10% de qualité.*

Le zoom de l'image ‘’Baboon’’, présenté dans la *figure 4.35 (d)*, montre bien la robustesse de l'algorithme de tatouage proposé même pour des taux de compression relativement élevés. En effet, la marque extraite, (*figure 4.35 (e))* est de bonne qualité même si le facteurs de compression est de qualité dégradante (Les artefacts apparaissent nettement). Ce qui montre que la composante de luminance est très robuste à la compression JPEG, même pour des taux de compressions très dégradants.

Le tatouage réalisé résiste bien aux modifications de luminance et de contraste, ainsi qu'aux ajustements et compression JPEG. La *figure 4.36* illustre certains exemples de traitements effectués sur l'image ‘’Baboon’’ ainsi que les marques extraites. La méthode permet d'insérer 64x64 bits dans chaque composante (Y et Cr) de l'image originale à travers la transformée en ondelettes discrète tout en assurant les propriétés de transparence et de robustesse.

Nous avons également utilisé la composante Cb, afin d'évaluer sa robustesse par rapport à la luminance. Pour la composante Cb la marque est ajoutée au niveau de la sous bande LL à travers un niveau de décomposition de la DWT.

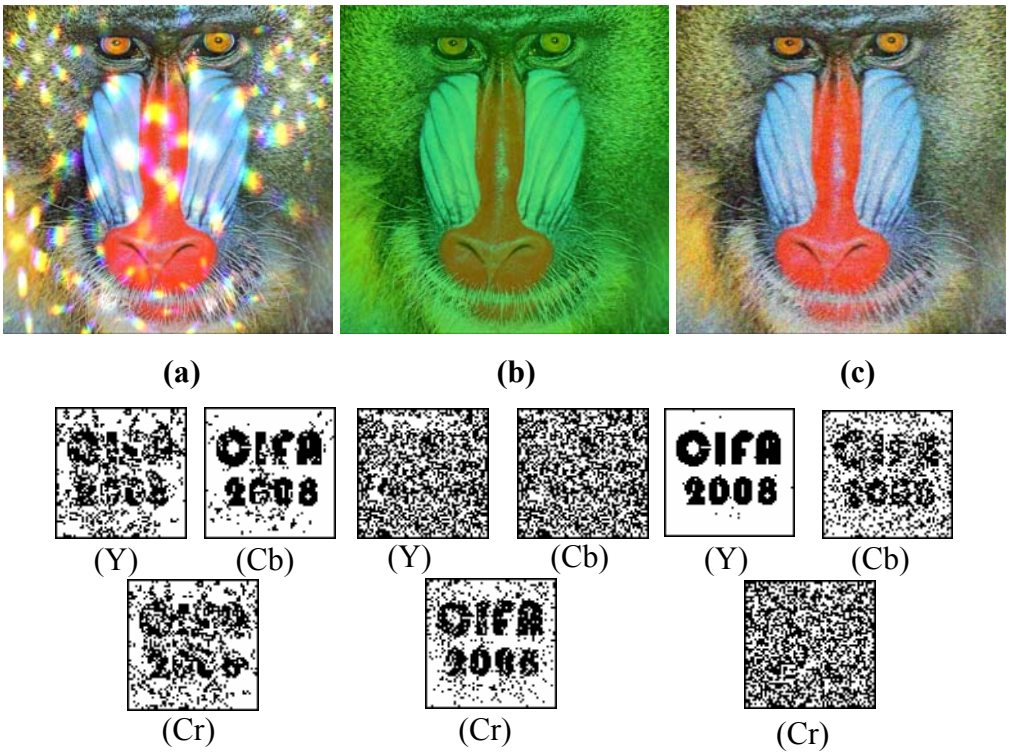


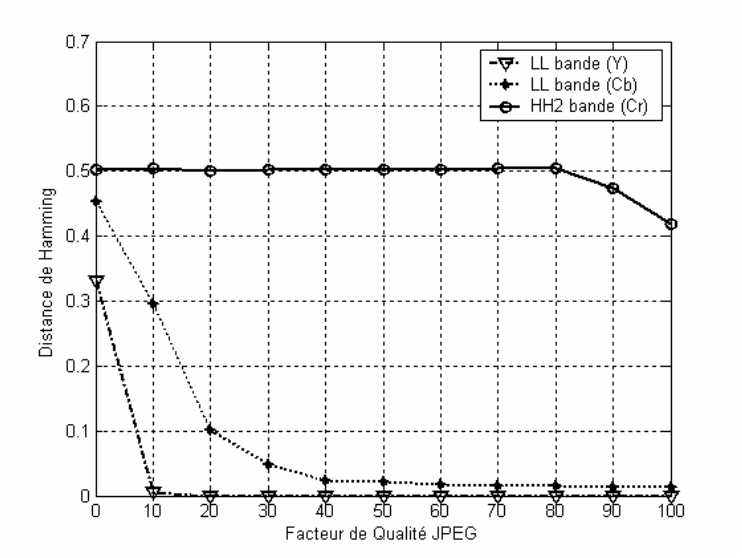
Figure 4.36: *L'image ''baboon'' marquée et attaquée et les marques extraites après attaques.*

La méthode proposée est relativement robuste même si l'image tatouée subie plusieurs attaques successives. La *figure 4.36 (c)* présente le cas d'une image attaquée par trois traitements de différents types (compression JPEG de 20% de qualité, filtrage, Bruit Gaussien 0.004). La marque extraite reste visible pour la composante Cb et elle est de bonne qualité pour Y.

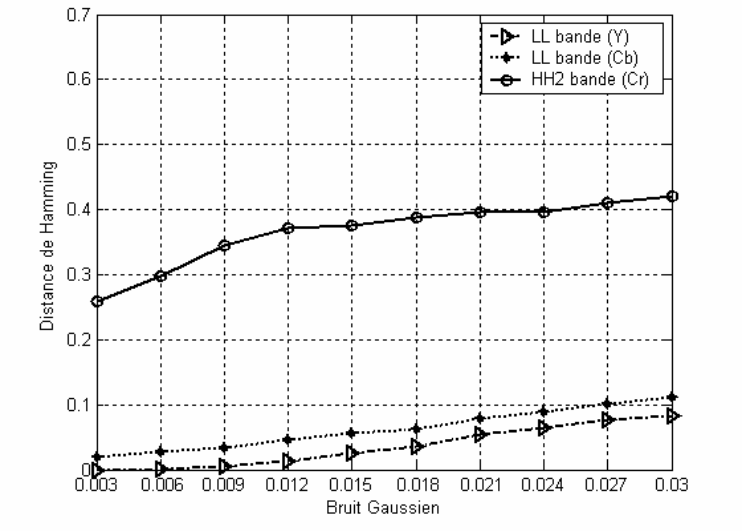
Cependant, elle est complètement invisible pour la composante Cr qui n'est pas robuste face à des attaques successives de type compression et de Bruit Gaussien.

Dans un souci d'évaluer les performances de cet algorithme, en comparant la marque extraite avec la marque originale, nous avons utilisé la distance de Hamming.

La *figure 4.37* montre la robustesse de l'algorithme proposé face à des attaques de types compression JPEG (*figure 4.37 (a)*) et Bruit Gaussien (b) pour les trois marques extraites à partir des trois composantes Y, Cb, Cr.



(a)



(b)

Figure 4.37 : *Robustesse vis-à-vis de la ''Compression'' et le ''Bruit Gaussien''.*

Les résultats (distance de Hamming) obtenus pour les différents types d'attaques utilisées dans cet algorithme sont portés sur le *tableau 4.7*.

Attaques	Y	Cb	Cr
JPEG 0 %	0.331	0.452	0.502
JPEG 10 %	0.004	0.296	0.503
JPEG 20 %	0.000	0.100	0.500
Filtrage	0.001	0.011	0.469
Bruit Gaussien 0.003	0.000	0.019	0.258
Gamma Correction	0.498	0.068	0.004
Intensity Adjustment	0.501	0.096	0.063
jpeg20%+filtrage+bruit 0.004	0.014	0.133	0.498
Intensity - A + Gamma - C	0.344	0.152	0.054
Gamma Correction + JPEG50%	0.496	0.447	0.500

Tableau 4.7: *Distance de Hamming des marques extraites à partir des trois composantes(Y, Cb et Cr).*

4.3.2.5 Comparaison entre luminance-chrominance

La composante luminance Y et donc très robuste face à des attaques de compression et de Bruit Gaussien, en comparaison avec les composantes achromatiques. Cependant, les composantes achromatiques sont relativement plus robustes dans le cas des modifications de luminance et de contraste tel que ‘’Intensity Adjustment’’ et ‘’Gamma Correction’’ (*figure 4.38).* Dans cette figure, nous représentons la variation de la robustesse en fonction des différents types d'attaques :

Gamma Correction, Intensity Adjustment, Filtrage, JPEG 20% et Bruit Gaussien 0.004 et Filtrage, Gamma Correction et Intensity Adjustment, Gamma Correction et JPEG 50%.

Même si l’image marquée subit une dégradation visible après une compression JPEG, un filtrage ou dans le cas de plusieurs attaques simultanées, il est toujours possible d’extraire une marque de bonne qualité. Le seul inconvénient de l’algorithme proposé, vis à vis des attaques étudiées dans cette section, est sa relative faiblesse face à une attaque multiple de type Gamma Correction + JPEG 50%, (*figure 4.38*). Cet inconvénient est dû au tatouage de la composante Y qui n'est pas robuste face à des attaques de type gamma correction, et celui de la composante Cr qui n'est pas robuste face à la compression.

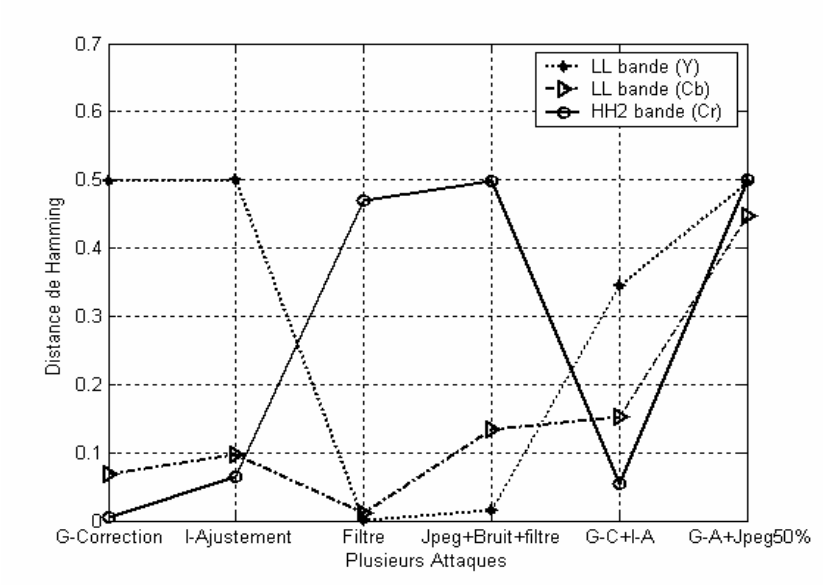


Figure 4.38 : *La distance de Hamming (corrélation) en fonction du type d'attaque pour les trois composantes Y, Cb et Cr.*

La *figure* 4.*39* présente les résultats obtenus dans le cas où la compression JPEG, est appliquée au trois composantes R, G et B et aussi à la composante de luminance Y. La composantes Y et donc plus robuste face à la compression ce qui justifie bien notre choix.

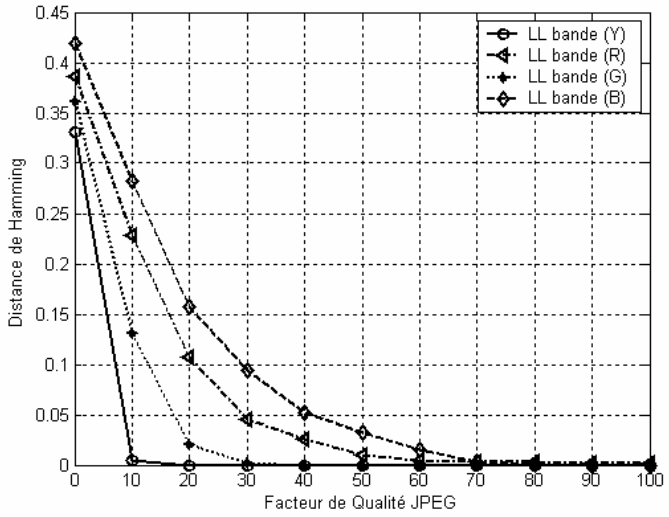


Figure 4.39: *La robustesse vis-à-vis de la compression pour les trois composantes R, V et B et la composante luminance Y.*

Nous avons présenté dans cette section une méthode de tatouage additive, non aveugle basée sur la modification des deux composantes Y et Cr du Système de Représentation Colorimétrique YCbCr. La méthode permet d'insérer une information de taille relativement

importante (64x64x2 bits) et de satisfaire les propriétés de transparence et de robustesse. Nous avons inséré la marque d'une façon redondante dans les deux bandes de décomposition (LL et HH_2) pour assurer la robustesse de l'algorithme face à plusieurs types d'attaques pouvant être simultanées. Cet algorithme a prouvé sa robustesse face à des attaques comme la compression JPEG, le Bruit Gaussien, le Filtrage, Intensity Adjustment et Gamma Correction ainsi que d'autre traitements comme la falsification. La *figure 4.38* montre que chaque bande de décomposition est robuste pour un certain nombre d'attaques. Ainsi, la bande LL de la luminance est robuste face à : JPEG compression, Filtrage, Bruit Gaussien et la bande HH_2 de la chrominance est robuste face à :
Intensity Adjustment, Gamma Correction.

Les résultats présentés dans cette section montrent que l'insertion basée sur les composantes de luminance chrominance est plus robuste vis à vis de la compression JPEG par rapport à l'insertion basée sur les canaux du SRC RVB. Il suffit donc d'utiliser une seule composante achromatique (Cr ou Cb) pour assurer la robustesse de l'algorithme face aux '' Intensity Adjustment'' et ''Gamma Correction''.

4.4 Conclusion

Nous avons présenté dans ce chapitre les algorithmes de tatouage par la transformée en ondelettes discrète que nous proposons. Où chaque algorithme est constitué de deux étapes principales : l'inclusion de la marque et l'extraction de la marque.

Nous avons ainsi présenté les résultats obtenus les méthodes que nous proposons. Ces résultats montrent un excellent comportement de notre détecteur face à des compressions JPEG (allant de 100% a 10%), et un bon comportement face aux différentes types d'attaques que nous avons présentées.

Nous n'avons pas fait ici une description exhaustive de toutes les attaques existantes. En particulier, nous n'avons pas présenté les attaques spécifiques à certains algorithmes.

Conclusion et perspectives

Nous avons présenté dans ce mémoire différentes méthodes de tatouage d'images numériques. Après avoir souligner des différents principes qui définissent le tatouage d'image, nous avons présenté une classification des différents schémas que l'on peut rencontrer dans la littérature, nous avons choisi de travailler sur les techniques d'implémentation de la marque dites additives.

Après avoir présenter quelques définitions et propriétés des images numériques, ainsi que la transformée en ondelettes discrète d'un signal et d'une image, Nous avons présenté les quatre schémas de tatouage proposés, qui utilisent chacun largement les propriétés et les point forts de la transformée en ondelettes discrète, appliquée que ce soit, sur des images en niveaux de gris ou des images en couleurs.

La principale contribution développée dans ce mémoire repose sur le développement d'un schéma de tatouage additif qui insère les marques en fonction des coefficients de la DWT afin d'imposer un espace d'insertion fixé par la marque. Nous avons utilisé dans la première proposition les quatre bandes (LL_2, LH_2, HL_2, HH_2) fréquentielles du deuxième niveau de décomposition par la DWT, afin d'assurer la robustesse de l'algorithme face à un grand ensemble d'attaques. Nous avons choisi dans la deuxième approche d'insérer la marque d'une façon parallèle et redondante pour augmenter sa robustesse face aux distorsions géométriques, dans cette approche l'insertion été à travers un seul niveau de décomposition par la DWT, ce choix peut permettre l'utilisation d'une marque de taille importante.

Nous avons aussi proposé deux schémas pour les images en couleurs, basés sur la décomposition de l'espace d'insertion en blocs de coefficients. Nous avons aussi présenté les résultats obtenus à la fin de chaque section, ces résultats visent à analyser les comportements des schémas proposés face à un grand ensemble d'attaques.

Les approches adoptées, offrent dans l'ensemble, de très bonnes performances, en termes de robustesse, soit face aux attaques non volontaire (Compression, Filtrage, Bruit Gaussien, Intensity Ajistement, Gamma Correction, transformations géométriques,…etc.), ou même face aux attaques volontaires comme la falsification par exemple.

Enfin, nous pouvons envisager d'adapter les méthodes de tatouage proposées par la *transformée en ondelettes discrète* à d'autres applications que la protection du copyright et à d'autres supports que les images fixes.

Bibliographie

[1] http://www.iipa.com

[2] S.Voloshynovskiy, S.Pereira, T.Pun, J.J.Eggers, J.K.Su**.** Attacks on digital watermarks: classification, estimation based attacks, and benchmarks**.** *Communications Magazine, IEEE*, Vol 39, No 8, pages 118 –126, 2001**.**

[3] D.Kirovski, F.A.P.Petitcolas**.** Blind pattern matching attack on watermarking systems**.** *IEEE Transactions on signal processing*, Vol 51, No 4, pages 1045 – 1053, 2003**.**

[4] P.Moulin, J.A.O'Sullivan**.** Information-theoretic analysis of information hiding**.** *IEEE Transactions on Information Theory*, Vol 49, No 3, pages 563 – 593, 2003**.**

[5] A.Kerckhoffs**.** La cryptographie militaire. Journal des sciences militaires**.** Vol 9 :5 – 38, Jan 1883**.**

[6] M.L.Miller, G.J.Doërr, I.J.Cox**.** Applying informed coding and embedding to design a robust high-capacity watermark**.** *IEEE Transactions on image processing*, Vol 13, No 6, pages 792 – 807, 2004**.**

[7] I.J.Cox, M.L.Miller, J.A.Bloom**.** *Digital Watermarking.* Morgan Kaufmann Publisher, Inc., San Francisco, 2002**.**

[8] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn**.** Information hiding a survey**.** *Proceedings of the IEEE (USA),* Vol 87, No 7, pages 1062 – 1078, 1999**.**

[9] V.Sedallian, G.Mathias**.** Les problèmes posés par la législation française en matière de chiffrement**.** *droit de l'informatique et des télécoms*, Vol 4, pages 23 – 45 1998**.**

[10] D.Kundur, D.Hatzinakos**.** Digital watermarking for telltale tamper proofing and authentication**.** *Proceedings of the IEEE,* Vol 87, No 7, pages 1167 – 1180, Jul 1999**.**

[11] J-L.Dugelay, C.Rey**.** Tatouage d'images pour des services d'intégrité**.** Technical report, réseau national de la recherche en télécommunication, projet Aquamars, paris, Aug 1999**.**

[12] M.Kutter, S.Voloshynovskiy, A.Herrigel**.** Watermark copy attack**.** *In ping wah wong and edward J.Delp, editors, ISET/SPIE's 12th Annual Symposium, Electronic Imaging : Security and Watermarking of Multimedia Contenu II,* Vol 3971 , pages 23 – 28, San Jose, California USA, Jan 2000**.**

[13] D.L.Robie, R.M.Mersereau**.** Video Error Correcting Using Data Hiding Techniques**.** In *IEEE Fourth Workshop on Multimedia Signal Processing*, pages 59 – 64, Cannes, France, Oct 2001**.**

[14] F.Bartolini, A.Manetti, A.Piva, M.Barni**.** A Data Hiding Approach for Correcting Errors in H.263 Video Transmitted over a Noisy Channel**.** In *IEEE Fourth Workshop on Multimedia Signal Processing*, pages 65 – 70, Cannes, France, Oct. 2001**.**

[15] B.Chen, G.Wornell**.** An information theoretic approach to the design of robust digital watermarking systems**.** In *International Conference on Acoustic, Speech and Signal Processing (ICASSP)*, pages 2061 – 2064, Phoenix, AZ, March 1999**.**

[16] F.Hartung, J.K.Su, B.Girod**.** Spread spectrum watermarking: Malicious attacks and counterattacks**.** In *Security and Watermarking of Multimedia Contents, Proceedings of SPIE* , Vol 3657, pages 147 – 158, 1999**.**

[17] H.Stone**.** Analysis of attacks on image watermarks with randomized coefficients**.** Technical report TR 96-045, NEC Research Institute, Princeton, NJ, USA, May 1996**.**

[18] G.C.Langelaar, R.L.Lagendijk, J.Biemond**.** Removing spatial spread spectrum watermarks by non-linear filtering**.** In *9th European Signal Processing Conference (EUSIPCO'98)*, pages 2281 – 2284, Island of Rhodes, Greece, 1998**.**

[19] S.Pereira, S.Voloshynovskiy, M.Madueno, S.M-Maillet, T.Pun**.** Second generation benchmarking and application oriented evaluation**.** *I. S. Moskowitz, éditeur, Information Hiding*, Vol 2137 de *Lecture Notes in Computer Science*, pages 340–353, Springer, 2001**.**

[20] B.Vassaux, P.Nguyen, S.Baudry, P.Bas, J.M.Chassery**.** Survey on attacks in image and video watermarking**.** *Applications of Digital Image Processing XXV,* Vol 4790, pages 169 – 179, 2002**.**

[21] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn**.** Attacks on copyright marking systems**.** In *Information Hiding, Second International Workshop,* pages 219 – 239, 1998**.**

[22] F.A.P.Petitcolas**.** Watermarking schemes evaluation**.** *IEEE Signal Processing*, Vol 17, no. 5, page 5864, 2000**.**

[23] Z.Wang, A.C.Bovik, L.Lu**.** Why is image quality assessment so dificult?**.** In *IEEE Conference on Acoustics, Speech and Signal Processing*, Vol 4, pages 3313 – 3316, May 2002**.**

[24] W.Bender, D.Gruhl, N.Morimoto, A.LU**.** Techniques for data hiding**.** *IBM systems journal*, Vol 35, No 3 – 4, pages 313 – 336, 1996**.**

[25] O.Bruyndonckx, J.J.Quisquater, B.Macq**.** Spatial Method for Copyright Labeling of Digital Images**.** In *IEEE Workshop on Nonlinear Signal and Image Processing (NSIP'95)*, pages 456 – 459, 1995**.**

[26] M.Kutter, F.Jordan, F.Bossen**.** Digital Watermarking of Color Images using Amplitude Modulation**.** *Journal of Electronic Imaging*, Vol 7, No 2, pages 326 – 332, Avr 1998**.**

[27] I.Pitas**.** A Method for Watermark Casting in Digital Images**.** *IEEE Transactions On Circuits and Systems on Video Technology*, Vol 8, No 6, pages 775 – 780, Oct 1998**.**

[28] J.Brassil, S.Low, N.Maxemchuk, L.O'Gorman**.** Electronic marking and identification techniques to discourage document copying**.** *IEEE Journal on Selected Areas in Communications,* pages 1278-1287, 1994**.**

[29] M.Barni, F.Barolini, V.Cappellini, A.Piva**.** A DCT- domain system for robust image watermarking**.** *Signal processing, Publisher Elsevier North-Holland,* Vol 66, No 3, pages 375 – 372, 1998**.**

[30] J.P.DUBUS**.** Analyse Multirésolution Et Psychovisuelle**.** *technique de l'ingénieur Mesures et contrôle*, Vol RE1, No R632, pages 1 – 21, 1998**.**

[31] X.Xia, C.Boncelet, G.Arce**.** A Multiresolution Watermark for Digital Images**.** In *Processing IEEE International Conference on Image Processing*, Vol 3, pages 548 – 551, Oct 1997**.**

[32] M.Kutter**.** Watermarking resisting to translation, rotation and scaling**.** In *Processing of SPIE* : *Multimedia systems and applications*, Vol 3528, pages 423 – 431, Boston, Nov 1998**.**

[33] J.R.Hernandez, F.P-Gonzalez**.** Statistical analysis for watermaking schemes of copyright protection of images*. Proceedings of the IEEE*, Vol 87, No 7, pages 1142 – 1143, Jul 1999**.**

[34] J.R. Hernández, M.Amado, F.P-gonzález**.** Dct-domain watermarking techniques for still images: Detector performance analysis and a new structure**.** *IEEE Transactions on Image Processing*, Vol 9, No 1, pages 55 – 68, 2000**.**

[35] I.Pitas, T.H.Kaskalis**.** Applying signatures on digital images**.** In *IEEE Workshop on Nonlinear Image and Signal Processing*, pages 460 – 463, Neos Marmaras, Greece, Jun 1995**.**

[36] G.C.Langelaar, J.C.A. van der Lubbe, J.Biemond**.** Copy protection for multimedia data based on labeling techniques**.** *Proceedings of the 17th Symposium on information Theory in the Benelux*, pages 33 – 39, Enschede, The Netherlands, 1996**.**

[37] A.Z.Tirkel, G.Rankin, R.Schyndel, C.F.Osborne**.** Electronic water mark**.** In *DICTA,* pages 666 – 672, Austin (TX), Usa, Dec 1993**.**

[38] R.G.Schyndel, A.Z.Tirkel, C.F.Osborne**.** A digital watermark**.** ln *IEEE, editor, ICIP'94,* Vol 2, pages 86 – 90, Austin (TX), Usa, 1994**.**

[39] F.Hartung, B.Girod**.** Watermarking of uncompressed and compressed video**.** *Signal Processing,* Vol 66, No 3, pages 283 – 333, 1998**.**

[40] 1.Cox, J.Killian, T.Leighton, T.Shamoon**.** Secure spread spectrum watermarking for multimedia**.** *IEEE Transactions on Image Proceessing, Vol* 6, No 12, pages 1673 – 1687, Dec 1997**.**

[41] I.J.Cox, J.Killian, T.Leighton, T.Shamoon**.** Secure spread sprectrum watermarking for multimedia**.** Technical report, Nec Research Institute, Princeton, NJ, USA, Oct 1995**.**

[42] A.Piva, M.Band, F.Bartolini, V.Capellini**.** DCT based watermark recovering without resorting to the uncorrupted original image**.** ln *Proceedings ICIP,* Vol 3*,* pages 520 – 523, 1997**.**

[43] M.Barni, F.Bartolini, V.Cappellini, A.Lippi, A.Piva**.** A dwt-based technique for spatio-frequency masking of digital signatures**.** *Security and Watermarking of Multimedia Contents (Electronic Imaging '99)*, Vol. 3657 of *Proceedings of SPIE,* pages 31 – 39*,* san jose california USA, Jan 1999**.**

[44] D.Kundur, D.Hatzinakos**.** A robust digital image watermarking scheme using the wavelet based fusion**.** ln *IEEE-ICIP'97,* volume 1**,** pages 544 – 547, Santa Barbara, Usa, 1997**.**

[45] W.Zhu, Z.Xiong, Y.Zhang**.** Multiresolution watermarking for images and video: a unified approach**.** ln *IEEE-ICIP'98,* Vol l**,** pages 465 – 469, Chicago (IL, USA), Oct 1998**.**

[46] D.Coltuc, P.Bolon**.** Watermarking by histogram specification**.** *Security and Watermarking of Multimedia Contents (Electronic Imaging '99),* Vol 3657 of *Proceedings of SPIE,* pages 252-263, San Jose, California USA, Jan 1999**.**

[47] M.J.J.Maes, C.W.A.M.Overveld**.** Digital watermarking by geometric warping**.** ln *IEEE-ICIP'98,* Vol 2, pages 424 – 429, Chicago (IL, US), Oct 1998**.**

[48] E.Koch, J.Zhao**.** Embedding robust labels into images for copyright protection**.** Technical report, Fraunhofer Institute for Computer Graphies, Darmstadt, Germany, 1994**.**

[49] A.Bors, I.Pitas**.** Image watermarking using dct domain constraints**.** ln *Proceedings ICIP,* Vol 3, pages 231 – 234, Lausanne, 1999**.**

[50] G.C.Langelaar, J.C.A.van der Lubbe, R.L.Lagendijk**.** Robust labeling methods for copy protection of images**.** ln *SPlE Conference,* pages 298-309, San Jose (Cal), 1997**.**

[51] D.Kundur, D.Hatzinakos**.** Digital watermarking using multiresolution wavelet decomposition**.** ln *IEEE ICASSP'98,* Vol 5, pages 2659 – 2662, Seattle (USA), May

1998.

[52] A.Manoury, J.L-Vehel, M.F.Lucas. Watermarking d'images par paquets d'ondelettes. ln *GRETSI'99,* pages 275 – 278, Vannes, France, 1999.

[53] M.M.Yeung, F.Mintzer. An Invisible Watermarking Technique for Image Verification. In *Proceedings of IEEE International Conference on Image Processing*, Santa Barbara, USA, Vol 2, No 26–29, pages 680 – 683, Oct. 1997.

[54] S.Walton. Information Authentification for a Slippery New Age. *Dr. Dobbs Journal*, Vol 20, No 4, pages 18 – 26, Apr 1995.

[55] J. Fridrich. Robust Bit Extraction from Images. In *Proceedings of the IEEE International Conference on Multimedia Computing and Systems* (*ICMCS'99)*, Vol 2, pages 536 – 540, Florence, Italy, june 1999.

[56] J.Fridrich, M.Goljan. Protection of Digital Images using Self Embedding. *The Symposium on Content Security and Data Hiding in Digital Media*, New Jersey Institute of Technology, Mar. 1999.

[57] C.Y.Lin, S.F.Chang. Semi-Fragile Watermarking for Authenticating JPEG Visual Content. In *SPIE International Conference. on Security and Watermarking of Multimedia Contents II*, Vol 3971, No 13, San Jose, USA, Jan 2000.

[58] R.B.Wolfgang, E.J.Delp. A watermark for digital images. In *Proceedings of the International Conference on Image Processing*. Vol 3, pages 219 – 222, Lausanne, Switzerland, Sep. 1996.

[59] R.B.Wolfgang, E.J.Delp. Fragile Watermarking Using the VW2D Watermark. In *SPIE International Conference. on Security and Watermarking of Multimedia Contents*, Vol 3657, No. 22, San Jose, USA, Jan. 1999.

[60] J.G. Proakis. *Digital Communications.* Third Edition, McGraw Hill, New York, 1995.

[61] J.Fridrich. Image Watermarking for Tamper Detection. *In Proceedings of IEEE International Conference on Image Processing (ICIP'98)*, Vol 2, pages 404 – 408, Chicago, USA, Oct. 1998.

[62] J.Fridrich. Methods for detecting changes in digital images. In *Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems*, pages 173 – 177, Melbourne, Australia, Oct. 1998.

[63] J.J.K.ÓRuanaidh, T.Pun. Rotation, translation and scale invariant digital image watermarking. In *IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97)*, Vol 1, pages 536 – 539, Santa-Barbara, CA, Oct. 1997.

[64] D.Kundur, D.Hatzinakos**.** Towards a Telltale Watermarking Technique for Tamper-Proofing**.** In *IEEE International Conference on Image Processing (ICIP'98)*, Vol 2, pages 409 – 413, Chicago, USA, Oct. 1998**.**

[65] C.Y.Lin, S.F.Chang**.** A Watermark-Based Robust Image Authentication Using Wavelets**.** ADVENT Project Report, Columbia University, Apr 1998**.**

[66] C.Rey**.** *Tatouage d'image : Gain en robustesse et intégrité des images***.** Thèse Doctorat de l'Université d'Avignon et des Pays de Vaucluse, Feb 2003**.**

[67] J.C.Broudin, G.Seifert**.** Filtrage médian des images couleur**.** Mars 1999**.**

[68] M.Kutter, F.Jordan, F.Bossen**.** Digital signatures of color images using amplitude modulation**.** *Processing of SPIE storage and retrieval for image and video databases, ,* pages 518 – 526, San Jose, California USA, Feb 1997**.**

[69] D.Fleet, D.Heeger**.** Embedding invisible information in color images**.** ln *IEEE ICIP'97,* Vol 1**,** pages 532 – 535, Santa Barbara (Cal) Usa, 1997**.**

[70] A.Piva, M.Barni, F.Bartolini, V.Cappellini**.** Exploiting the cross-correlation of rgb-channels for robust watermarking of color images**.** ln *IEEE-ICIP'99,* Vol l, pages 306 – 310, Kobe (Japan), Oct 1999**.**

[71] P.Flandrin**.** *Temps-fréquence.* Hermès, 1993**.**

[72] H.Reinhard**.** *Éléments de mathématiques du signal. tome 1 - Signaux déterministes* Dunod, 1995**.**

[73] D.Declercq, A.Quinquis**.** *Détection et estimation des signaux.* Hermès, 1996**.**

[74] F.Truchetet**.** *Traitement linéaire du signal numérique.* Hermès, 1998**.**

[75] P.Robert, A.Rey, J.R.Debove, H.Cottez**.** *Le Petit Robert - Dictionnaire de la langue française.* Société du nouveau Littré, Le Robert, paris, 1994**.**

[76] A.Trémeau, C.F-Maloigne, P.Bonton**.** *Image numérique couleur, De l'acquisition au traitement.* Dunod - Cours et applications, 2004**.**

[77] P.Colantoni, A.Trémeau**.** 3d visualization of color data to analyze color images**.** In *Proceedings of PICS Conference*, pages 500 – 505, Rochester, USA, 2003**.**

[78] CIE. Colorimetry. Rapport Technique. 15, Bureau Central de la CIE, 1971**.**

[79] D.Gabor**.** Theory of communications**.** *Journal I.E.E.*, Vol 93, No 26, pages 429 – 457, London , 1946**.**

[80] A.Grossmann, J.Morlet**.** Decomposition of hardy functions into square integrable wavelet of constant shape**.** *SIAM Journal of Mathematical Analysis*, Vol 15, No 4, pages 723 – 736, Jul 1984**.**

[81] P.Lemarié, Y.Meyer**.** Ondelettes et bases hilbertiennes**.** *Revesta Mat, Iberoamericana*, 2 , pages 1 – 18, 1986**.**

[82] G.Battle**.** A block spin construction of ondelettes, Part I : Lemarié functions**.** In *Communications on Mathematical Physics*, Vol 110, No 4, pages 601 – 615, 1987**.**

[83] Y.Meyer**.** *Ondelettes et Opérateurs, I : Ondelettes, II : Opérateurs de Calderón-Zygmund, III :* (with R. Coifman)*, Opérateurs multilinéaires.* Hermann, English translation of first volume is published by Cambridge University Press, Paris, 1990**.**

[84] S.Mallat**.** A theory for multiresolution signal decomposition : The wavelet representation**.** *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol 11, No 7, pages 674 – 693, Jul 1989**.**

[85] B.B-Hubbard**.** *Ondes et ondelettes, la saga d'un outil mathématique.* Pour la science, paris, 1995**.**

[86] S. Mallat**.** A Wavelet Tour of Signal Processing. Academic Press, 1999**.**

[87] E.ELBASI, M.Ahmet**.** PRN based watermarking scheme for color images**.** *Istanbul commerce university journal of science,* 2006.

[88] E.Elbasi, A.M.Eskicioglu**.** A DWT-based Robust Semi-blind Image Watermarking Algorithm Using Two Bands**.** In *IS&T/SPIE's 18th Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference,* Vol 6072, pages 777 – 787, San Jose, CA, Jan 2006**.**

[89] S.P.Maity, M.K.Kundu**.** A Blind Cdma Image Watermarking Scheme In Wavelet Domain**.** In *International Conference on Image Processing (ICIP 04)*, Vol 4, No 24–27, pages 2633 – 2636, Oct 2004**.**

[90] C.Temi, S.Choomchuay, A.Lasakul**.** A Robust Image Watermarking Using Multiresolution Analysis of Wavelet**.** *Proceedings of ISCIT, IEEE, Vol 1, pages 623 – 626, 2005.*

[91] I.Hisashi, A.Miyazaki, T.Katsura**.** An Image Watermarking Method Based on the Wavelet Transform**.** In *International Conference on Image Processing (ICIP'99),* Vol 1, pages 296 – 300, 1999**.**

[92] C-C.Chen**.** Watermarking Experiments Based On Wavelet Transforms**.** *SPIE, Electronic Imaging and Multimedia Technology III,* Vol 4925, pages 60 – 68, 2002**.**

[93] N.Corina**.** *Filigranage dans le domaine des ondelettes Watermarking in the wavelet domain.* Mémoire de diplôme pour obtenir le degré de M.Sc. L'université Politehnica Timisoara Faculté d'Electronique et Télécommunications, 2004**.**

[94] P.Y.Chen, H-J.Lin**.** A DWT Based Approach for Image Steganography**.** *International Journal of Applied Science and Engineering*, Dec 2006**.**

[95] A.Bakhouche, N.Doghmane**.** A Robust and Non-Blind Watermarking Scheme for Gray Scale Images Based on the Discrete Wavelet Transform Domain**.** In *1st Mediterranean Conference on Intelligent Systems and Automation (CISA '08), Published by the American Institute of Physics (AIP).* pages 565 – 570, annaba, Algeria , jul 2008**.**

[96] S.Chouchane, W.Puech**.** Intégration d'un Nouveau Marqueur dans le Codeur d'Images EZW basé sur les Ondelettes**.** In *CORESA* . 2005**.**

[97] J.L.Toutant, W.Puech, C.Fiorio**.** Amélioration de l'invisibilité par adaptation de la quantification aux données à insérer**.** In *Proceedings 20th GRETSI'05*, Louvain-la-Neuve, Belgique, Sep 2005**.**

[98] L.Guillemot, J-M.Moureaux**.** Tatouage d'images : une nouvelle approche basée sur une méthode de compression**.** In *Proceedings CORESA*, Lyon, France, Jan 2003**.**

[99] M.Ossonce, G-L.Guelvouit, C.Delpha, P.Duhamel**.** Paramètrage par la théorie des jeux d'un schéma de tatouage d'images robuste aux rotations et mises à l'échelle**.** In *Proceedings CORESA,* Rennes, France, Nov 2005.

[100] P.Artameeyanant**.** Tabu searching for Watermarking Robust Against Compression and Cropping. In *International Joint Conference*, *IEEE* , Vol pages 4461 – 4463, Oct 2006**.**

[101] B.Verma, S.Jain, D.P.Agarwal, A.Phadikar**.** A New Color Image Watermarking Scheme**.** *INFOCOMP – Journal of Computer Science,* Vol 5, No 2, pages 37 – 42, Jun 2006**.**

[102] Z.Lu, X.P.Zhang**.** Robust image watermarking based on the wavelet contour detection**.** In *Acoustics, Speech, and Signal Processing, IEEE International Conference*, Vol 2, pages 1165 – 1168, Mar 2005**.**

[103] F.Drira, F.Denis, A.Baskurt**.** Image watermarking technique based on the steerable pyramid transform**.** *Proceedings SPIE*, USA, Vol 5607, pages 165 – 176, 2004**.**

[104] A.Bakhouche, N.Doghmane**.** Nouvelle approche de tatouage des images résistante aux distorsions géométriques**.** In *mcseai'08*, oran, algeria, apr 2008**.**

[105] M.I.Mahmoud, M.I.M.Dessouky, S.Deyab, F.H.Elfouly**.** Comparison between Haar and Daubechies Wavelet Transformions on FPGA Technology**.** *International Scientific Journal of Computing,* Vol 6, No 3, pages 23 – 29, *2007.*

[106] M.S.Raval, P.P.Rege**.** Discrete Wavelet Transform Based Multiple Watermarking Scheme**.** In *Conference on Convergent Technologies for Asia-Pacific Region, IEEE*, Vol 3, pages 935 – 938, 2003**.**

[107] A.Parisis, P.Carré, C.F-Maloigne, N.Laurent**.** Tatouage d'images couleur avec adaptation locale des forces de marquage**.** In *Proceedings of CORESA*, pages 105 – 108, Lille, France, Mai 2004**.**

[108] G.Lo-varco, W.Puech, M.Dumas**.** Tatouage d'images couleurs avec CCE : application a la Sécurité routière**.** In *Proceedings Colloque CORESA*, Lyon, France Jan 2003**.**

[109] A.Parisis, P.Carré, C.F-Maloigne**.** Colour watermarking: study of different representation spaces**.** In *CGIV'02*, pages 390 – 393, Poitiers 2002**.**

[110] P.Bas, B.Roue, J-M.Chassery**.** Tatouage d'images couleur additif : vers la sélection d'un Espace d'insertion optimal**.** In *Proceedings CORESA'03*, pages 124 – 127, Lyon, France 2003**.**

[111] A.Bakhouche, N.Doghmane**.** A Novel Color Image Watermarking Scheme Using DWT**.** In *iceedt'08*, 2008**.**

[112] A.Bakhouche, N.Doghmane**.** Nouvelle approche de tatouage d'images Couleurs basée sur la DWT**.** In *cifa'08*, 2008**.**