République algérienne démocratique et populaire

UNIVERSITE BADJI MOKHTAR
ANNABA

جامعة باجي مختار
عنابة

Faculté des Sciences de l'Ingénieur

Département de l'Electronique

Année : 2006

MEMOIRE

Présenté En Vue De L'obtention Du Diplôme De Magister

Tatouage d'images par paquet d'ondelettes

Option

Systèmes intelligents

Par :

M^{r}: LEMOUCHI KARIM

Directeur de mémoire : **Mr. N. DOGHMANE** Pr U.ANNABA

DEVANT LE JURY

Président:	Mr ABBASSI H.AHMED	Pr.	U. ANNABA
Examinateurs	Mr L. BENNACER	MC	U. ANNABA
	Mr M BENOUARET	MC	U. ANNABA

DÉDICACES

Je dédie ce travail à :

A la mémoire de mon très cher père qui a toujours rêvé pur que je sois d'un haut niveau.

Et la fontaine de l'amoure ma mère qui m'a donné la vie, l'espoir, et la tendresse.

A mes frères et ma sœur et leur neveu né Oussama.

A mes Collègues de labo.

A tous mes amis

A tous ceux qui m'aiment

Remerciements

Ces trois années de thèse ont été jalonnées par des nombreuse rencontres, la plupart du temps heureuses, qui m'ont permis à chaque fois de m'enrichir autant sur le plan humain que sur le plan scientifique.

Mes remerciements les plus distingués s'adressent à mon directeur de thèse, le professeur **N. DOGHMANE** pour le soutien moral qu'il m'a apporté tout le long de ce travail pour sa générosité, ses conseils précieux et l'élaboration de ce document.

Je tiens à remercier les membres du jury pour l'intérêt porté à cette thèse :

- Professeur Mr **ABBASSI H.AHMED** de l'université de Annaba qui m'a honoré par sa présence en qualité président du jury.
- Professeur Mr **M. BEDDA** qui m'a honoré en expertisant **c**e travail en qualité d'examinateur
- Maître de Conférences Mr **M. BENOUARET** qui m'a honoré **en** examinant ce travail en qualité d'examinateur
- Maître de Conférences Mr **L. BENNACER** qui m'a honoré en jugeant **ce** travail en qualité d'examinateur

Résumé

Avec l'apparition et le développement des nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité et sans prise en compte des droits d'auteurs. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le *tatouage*. Le principe des techniques dites de tatouage est d'insérer une marque imperceptible dans les valeurs de la donnée. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée *watermark* correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelles que soient les transformations (licites ou illicites) que la donnée tatouée subie, la marque doit rester présente tant que la donnée reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée).

Mot-cles: tatouage numérique d'image, ondelette, dwt, filigrane, cryptographie, steganographie,

Abstract

Digital image watermarking has attracted a lot of interest in recent years, due in particular to the development of Internet and the World Wide Web. The aim is to protect ownership by including in the image a copyright information. This information, or mark, has to be set in such a way that it is invisible: indeed, it must not alter the viewing content and, in addition, it should not be easy to remove. Furthermore, the mark must be resistant to attacks directed at erasing it. A number of methods have been proposed to insert robust and invisible watermarks. Some operate directly in pixel space, other in a transform domain, such as, *Fourier* or *DCT*. We propose here to study a *DWT* (discrete wavelet transform) for the watermarking procedure.

Key words : watermarking, wavelet, dwt, cryptography, steganography,

ملخص

مع ظهور و تطور التكنولوجيات الرقمية الجديدة, تضاعف معها الغش و التزوير, و هذا راجع إلى نقص التقنيات الخاصة بحماية المعلومات الرقمية. هذه المعلومات في حقيقة الأمر معرضة باستمرار للقرصنة: حيث نستطيع تخزينها, نسخها, تغيرها, ثم يعاد بثها بصفة غير شرعية دون أن تفقد ميزتها و دون أي اعتبار لحقوق الطبع. و لهذا شرع سريعا في تطوير مجال جديد للبحث في هذا الميدان: " الوشم".

المبدأ الأساسي لتقنيات الوشم يتمثل في إدراج علامة غير مرئية بين عناصر المعلومة. إن العلامة المدرجة و التي تسمى " ووتر مارك"" الوشم" , تدخل في إطار قانون حماية المؤلف. هذا النوع من الوشم يجب أن يستجيب إلى متطلبات محكمة من ناحية الصلابة.

في الواقع, مهما كانت التغيرات (شرعية أو غير شرعية) المطبقة على المعلومة الموشومة, فإن العلامة يجب أن تبقى حاضرة مادامت المعلومة تحت الاستغلال. أضف إلى ذلك, فإن المعلومة المدرجة لا يمكن اكتشافها إلا من طرف أشخاص مخولين (يملكون مفتاح اكتشاف خاص).

كلمات مفتاحية : الوشم الرقمي , الموجيات , التشفير

Résumé

Avec l'apparition et le développement des nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité et sans prise en compte des droits d'auteurs. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le *tatouage*. Le principe des techniques dites de tatouage est d'insérer une marque imperceptible dans les valeurs de la donnée. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée *watermark* correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelles que soient les transformations (licites ou illicites) que la donnée tatouée subie, la marque doit rester présente tant que la donnée reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée).

Mot-cles: tatouage numérique d'image, ondelette, dwt, filigrane, cryptographie, steganographie,

Abstract

Digital image watermarking has attracted a lot of interest in recent years, due in particular to the development of Internet and the World Wide Web. The aim is to protect ownership by including in the image a copyright information. This information, or mark, has to be set in such a way that it is invisible: indeed, it must not alter the viewing content and, in addition, it should not be easy to remove. Furthermore, the mark must be resistant to attacks directed at erasing it. A number of methods have been proposed to insert robust and invisible watermarks. Some operate directly in pixel space, other in a transform domain, such as, *Fourier* or *DCT*. We propose here to study a *DWT* (discrete wavelet transform) for the watermarking procedure.

Key words : watermarking, wavelet, dwt, cryptography, steganography,

ملخص

مع ظهور و تطور التكنولوجيات الرقمية الجديدة, تضاعف معها الغش و التزوير, و هذا راجع إلى نقص التقنيات الخاصة بحماية المعلومات الرقمية. هذه المعلومات في حقيقة الأمر معرضة باستمرار للقرصنة: حيث نستطيع تخزينها, نسخها, تغيرها, ثم يعاد بثها بصفة غير شرعية دون أن تفقد ميزتها و دون أي اعتبار لحقوق الطبع. و لهذا شرع سريعا في تطوير مجال جديد للبحث في هذا الميدان: " الوشم".

المبدأ الأساسي لتقنيات الوشم يتمثل في إدراج علامة غير مرئية بين عناصر المعلومة. إن العلامة المدرجة و التي تسمى " ووتر مارك"" الوشم" , تدخل في إطار قانون حماية المؤلف. هذا النوع من الوشم يجب أن يستجيب إلى متطلبات محكمة من ناحية الصلابة.

في الواقع, مهما كانت التغيرات (شرعية أو غير شرعية) المطبقة على المعلومة الموشومة, فإن العلامة يجب أن تبقى حاضرة مادامت المعلومة تحت الاستغلال. أضف إلى ذلك, فإن المعلومة المدرجة لا يمكن اكتشافها إلا من طرف أشخاص مخولين (يملكون مفتاح اكتشاف خاص).

كلمات مفتاحية : الوشم الرقمي , الموجيات , التشفير

Table des matières

Liste des Figures

Liste des Tableaux

Notations et Abréviations

CD-ROM: Compact Disk Read Only Memory.

JPEG : Type de Compression d'Image.

MPEG : Type de Compression Vidéo

MP3 : Type de Compression Audio.

DVD : Disk Verstile Digital.

SVH : Système Visuel Humain

PSNR: Peak Signal to noise Ratio / rapport signal bruit

DCT : La transformée en Cosinus Discrète

TFD : La Transformée de Fourier Discrète

SBPA : Séquence Binaire Pseudo Aléatoire

LBM : Modulation des bits de poids faibles

DIM : Dither Index Modulation

SDQ : Subtractive Dithered Quantization.

DWT : La Transformée d'ondelette Discrète.

IDWT : La Transformée d'ondelette Discrète Inverse.

µ : micro.

B : La Bande passante.

Φ: l'ondelette de synthèse.

ψ (*t*) : l'ondelette mère.

***L*^{2}(R) :** Espaces orthogonaux

EZW : Embedded Zero-tree Wavelet.

JPEG-2000 : Type de Compression d'image dans le domaine d'ondelette.

Signal 2D : signal à deux Dimension L'Image.

TF : la transformée de Fourier.

CWT : Continuous Wavelet Transform.

STFT : Short Term Fourier Transform.

TO : La Transformée en Ondelettes.

TOC : La Transformation en Ondelette Continue.

AMR : Analyse Multi Résolution.

LL : low-low frequency band.

LH : low-high frequency band.

HL : high-low frequency band.

HH : high-high frequency band.

MAP : la méthode du Maximum à Posteriori.

Cropping : Extraire un Morceau d'une Image.

1. Introduction

Avec le développement croissant des échanges des fichier et des données sous forme numérique et avec l'essor récent des moyens de communication et notamment les outils tells que les ordinateurs, les imprimantes et les moyens de communication numérique à haut débit qui sont devenus bon marché et largement accessibles , en plus de la popularité de l'internet à clairement démontrés la formidable potentiel économique du marchés du multimédia digital, et les utilisateurs investissent largement dans la technologies numérique . Malheureusement ces avancées technologiques offrent aussi une opportunité sans précédente pour le piratage des oeuvres protégées par un droit d'auteur (copyright). En effet, les données numériques peuvent être très aisément et rapidement recopiées à l'infini de manière exacte. Donc ces données sont en effet très faciles à pirater on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité.

Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement le tatouage ou watermarking, la sphère des applications du tatouage ne cesse d'augmenter depuis quelque années englobant outre le protection de copyright et l'authentification. Le principe des techniques dites de tatouage est d'insérer une marque imperceptible dans les valeurs de la donnée.

Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée watermarque correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelles que soient les transformations (licites ou illicites) que la donnée tatouée subit, la marque doit rester présente tant que la donnée reste exploitable. De plus, la présence de La Marque ne doit être détectée que par des personnes autorisées. De nombreux algorithmes ont étés présentés récemment et certains produits sont même commercialisés. Cependant, aucun d'eux ne satisfait pleinement au cahier des charges idéal. Alors pourquoi ce type de protection électronique semble t-il tant tarder à se développer ? La réponse est simple : le droit d'auteur. Au siècle dernier, il était à la mode de prétendre que droit d'auteur et l'Internet (ou son cousin multimédia le *World Wide Web*) étaient associés comme l'eau et le feu et qu'en conséquence, le droit d'auteur serait appelé bientôt à s'évaporer ou à s'éteindre.

Ce document ou mémoire est divisé en cinq parties. La première partie présente la problématique et la nécessite de la protection des documents numériques qui sous-tendent notre approche des notions de copyright et le droit d'auteur. La deuxième partie suivante c'est

l'état de l'art, en donne un modèles de protection qui appelle le tatouage à partir d'un système décodage (la cryptographie, la stéganographie) en plus on définir plusieurs types et classements de tatouage que nous avons successivement élaborés. Pour la troisième chapitre sera une partie théorique et mathématique sur l'outil de travail, l'ondelette et DWT. Les méthodes proposées sont expliquées et des résultats expérimentaux sont présentés dans le quatrième chapitre. Quant au dernier chapitre il est consacré aux attaques que peut subir l'image tatouée. Il est question donc d'étudier la robustesse de la marque insérée en présence de telles attaques.

Première chapitre

PROBLEMATIQUE

La protection de la propriété intellectuelle est devenue récemment un besoin pressant surtout avec l'évolution rapide des techniques de transmission numérique.

1. Protection des Droits D'auteur.

1.1 Introduction.

Le développement des réseaux de communication et des supports numériques comme le Compacte Disc, le CD-ROM, le Digital versatile Disc … entraîne une diffusion massive de document stockés a laide de formats numériques, tels **JPEG**, **MPEG**, **MP3**. Ces techniques, qui permettent d'emmagasiner une grande quantité d'information en peut de place; facilitent aussi l'utilisation illégale des documents, il est en effet extrêmement aisé de récupérer un document sur internet ou sur un CD-ROM et de le copier un grand nombre de fois avant de diffuser ces duplications. Non seulement la copier est facile, mais elle est parfaite, alors qu'un document analogique se détériore lorsqu'on le duplique, par contre la copier numérique a exactement les mêmes qualités que l'original.

Ces manipulations si elles débouchent sur la commercialisation des copies, ou sur toute utilisation autre que privée, sont illégales tant que les droits d'auteurs n'ont pas été verses à l'ayant droit du document. L'objectif est d'associer à un document une marque qui protégé les créateurs, est indécelable par l'observateur, Il n'est efficace que s'il résiste aux divers traitements volontaire et involontaire.

1.2 Principes.

Qu'est-ce qui est protégé par le droit d'auteur ?

Le droit d'auteur protège toute œuvre originale et coulée dans une certaine forme [1]. Il en résulte que, pour qu'une création soit protégée par le droit d'auteur, deux conditions doivent être remplies

1.2.1 La Condition d'Originalité :

Il n'existe pas de définition légale du critère de l'originalité, qu'une œuvre est originale si elle apparaît comme le fruit de l'effort intellectuel de son auteur. La question de savoir si une œuvre est « originale » ou non est une question de fait souverainement

appréciée par le juge du fond. La notion d' « originalité », centrale en droit d'auteur, est difficile à définir en pratique. Pour savoir si une œuvre est originale, on vérifiera concrètement si l'auteur a disposé d'un espace de liberté (a-t-il suivi des contraintes techniques précises ? Plus œuvre suit des contraintes techniques, plus l'espace laissé à la créativité de l'auteur sera limité). Dans le même ordre d'idées, on vérifiera si l'auteur a eu l'occasion d'opérer des choix déterminant la forme d'œuvre.

Par conséquent, ne seront pas protégées par le droit d'auteur parce que l'auteur n'aura pas pu exercer sa liberté créative et investir l'œuvre de son empreinte :

- les formes réalisées exclusivement par une machine ou émanant spontanément de la nature : ainsi par exemple, un paysage naturel, la mer, ou un arbre, n'est pas protégé par le droit d'auteur et peut donc être librement reproduit;
- les simples reproductions serviles de ce qui existe (qui ne contiennent rien d'original puisque par hypothèse elles sont serviles) ;
- les informations brutes : les données factuelles échappent au droit d'auteur mais le droit d'auteur s'appliquera à la sélection et à la présentation des données;

1.2.2 La Condition de Mise en Forme :

Pour qu'une œuvre bénéficie de la protection, il faut en outre qu'elle soit coulée dans une certaine forme susceptible d'être appréhendée par les sens (même si cette perception implique l'intervention d'un appareil, comme c'est le cas d'une œuvre accessible en ligne et qui ne peut être perçue que par une personne possédant un ordinateur et un accès Internet).

Il en résulte que le droit d'auteur ne protège pas :

-les simples idées : une idée, aussi « géniale » ou « originale » qu'elle soit, n'est jamais susceptible d'appropriation, ni par le droit d'auteur ni par un autre moyen [2].

- les méthodes ou les styles, même originaux, ne sont pas protégés par le droit d'auteur : on pourra donc s'inspirer, lors de la création d'un site web, des styles utilisés par d'autres, pour autant que l'on ne copie aucun élément formel original.

1.2.3 Durée des Droits D'Auteur :

La protection par le droit d'auteur est limitée dans le temps, la règle générale étant que les droits d'auteur se prolongent pendant toute la vie de l'auteur plus 70 ans après sa mort [3] (ou après la mort du dernier auteur survivant en cas d'œuvre de collaboration).

2. Sécurisation de Documents Electroniques.

La recherche sur la protection des images a motivé de nombreuses recherches sur le tatouage numérique et leur taille importante dans l'étude des algorithmes de développement rapide des applications informatiques s'est accompagné d'un accroissement rapide et massive d'utilisation des documents ou images numériques, notamment dans le domaine des multimédias, des transmissions satellite ou de l'imagerie médicale, la circulation des documents numérique (image, son ,vidéo) sur Internet posent un problème des droits d'auteurs et copyright, nous abordons les techniques de sécurité proprement dites et les standards correspondants, tant sur le plan de la cryptographie, du tatouage d'information que des méthodes intégrées de protection contre les copies illicites . Cela nous amène ensuite à décrier les infrastructures de gestion des droits numériques.

2.1 La Nécessite des Nouvelles Techniques.

La recherche sur la protection des images a principalement débuté ver les années 90, une époque marquante pour le monde de l'image numérique et aujourd'hui les technologies numériques se sont considérablement répondues et imposes entant que vecteurs de données ne cesse de croître, documents, données multimédia (graphiques, audio te vidéo) et œuvres de notre vie quotidienne, se substitutions de plus en plus aux supports analogiques traditionnels.

Les première techniques, comme le contrôle d'accès (destine à autoriser ou à refuser l'accès au document) ou la cryptographie (chiffrer ou signer le document) se sont révélées insuffisantes ou d'un emploi difficile. En effet, les dispositifs de cryptographie protègent l'image lors d'une transaction, mais pas au-delà, le destinataire retrouvé après déchiffrement (ou vérification de la signature) la même version de l'image que celle qui précédait l'envoi, donc sans protection. Une technique complémentaire a alors été envisage : le tatouage, dérivé de la stéganographie.

La stéganographie est l'art de cacher une information, une signature, dans un message que n'importe qui va pouvoir observer. Ce message peut être de diverses natures : texte, image, son… Etc.

L'idée est de cacher dans le document une information propre à son ayant droit sous la forme d'une marque qui ne pourra être enlevée sans une altération importante de ce document (rendant alors son utilisation impossible). Cette marque, dénommée filigrane ou watermark, devra rester imperceptible et faire suffisamment corps avec le document pour rester présente malgré les manipulations que se dernier risqué de subir. Les transformations pouvant altérer

La marque sont des rotations, des changements d'échelle, des symétries, des découpages, des changements de format, l'application de filtres, l'ajout de bruit… etc. La marque peut aussi être dégrade lors d'une impression, renumérotation par scanner. Ces manipulations peuvent avoir pour but la destruction de la marque, ou tout simplement une utilisation facile de document ou l'image (compression JPEG par exemple). On doit reconnaître la marque même quand le contenu numérique de l'image a changé.

Un système de tatouage dépend du contexte de son utilisation , temps d'exécution des programmes de tatouage et de vérification , mémoire disponible et les impératifs de la sécurité, environnement ouvert, fermé, qui va avoir accès à quoi, qui va exécuter les programmes de tatouage, de vérification.

2.2 Cryptographie et Stéganographie.

L'objet de la cryptographie est l'étude des techniques ayant pour but d'assurer la confidentialité, l'intégrité et l'authenticité des informations ou de leur origine. Elle se caractérise, schématiquement, par deux approches principales, qui, pour nombre d'applications, ne s'excluent pas mutuellement, mais peuvent souvent être combinées harmonieusement entre elles.

La sténographie fait partie de ces techniques et consiste en la dissimulation d'un message à l'intérieur d'une information hôte, celle-ci devenant le canal de transmission, son médium. Ce message est inséré dans l'hôte en utilisant une clef de sorte qu'un tiers n'en ayant pas connaissance ne puisse pas détecter sa présence ni l'enlever. Tous les formats hôtes sont possibles et on pourra insérer tout type d'information dans un document texte, dans une image, dans une vidéo, etc.….

La stéganographie se distingue de la cryptographie dans la mesure où l'objectif principal en cryptographie est de rendre illisible un message primaire à toute personne ne possédant pas une information secrète adéquate. De plus, alors que la cryptographie offre une sécurité à priori (contrôle d'accès, par exemple) la stéganographie offre une sécurité plutôt à posteriori, dans la mesure où le message secondaire est supposé rester accessible même après recopies et manipulations du message primaire.

2.3 Tatouage et Stéganographie.

Les techniques de tatouage ont aujourd'hui le vent en poupe, en raison de l'inquiétude croissante des producteurs de contenu numérique qui doivent, pour tirer bénéfice des nouveaux marchés engendrés par ces technologies, mettre en place des mécanismes de protection des œuvres distribuées.

Le format numérique permet en effet des copies de masse à peu de frais et engendre autant de manque à gagner. Ainsi en est-il donc des distributeurs de musique, de films, de livres et de logiciels qui cherchent à inclure dans les fichiers vendus des marques numériques indécelables appelées tatouages ou watermarking.

Les techniques de tatouage ou watermarking et de la stéganographie peuvent sembler proches et dérivent en effet souvent des mêmes idées. Toutefois les utilisations foncièrement différentes font que les implémentations et adaptations des schémas et les questions soulevées par ces deux domaines sont radicalement différentes. Ainsi le watermarking ou tatouage est-il concerné principalement par la protection des droits d'auteur.

Un enjeu majeur aujourd'hui est de pouvoir faire la preuve de l'efficacité d'un schéma de protection d'une œuvre numérique sur des périodes longues à l'échelle des progrès informatiques.

La stéganographie est moins concernée par ces questions de durée. Elle est globalement soutenue par le besoin qu'ont certaines personnes de communiquer de façon sécurisée, communication par définition limitée dans le temps.

3. Principes de Tatouage ou Watermarking.

3.1 Pourquoi Utiliser le Watermarking ?

A une époque qui voit se développer tous les outils de communication, échanger des informations, qu'il s'agisse d'images, de sons, ... est devenu très facile, et beaucoup plus pratique ; avec le développement d'internet, avec le numérique qui remplace l'analogique, la quantité d'images qui transitent est très importante. Cependant, il est de ce fait devenu plus simple pour une tierce personne d'intercepter, de modifier ou de s'approprier ces images. La protection de ces données est donc devenue un enjeu majeur. Restons dans le domaine de l'imagerie médicale et prenons l'exemple de la télémédecine, certaines radiographies transitent via internet, par exemple lorsqu'elles sont examinées par un médecin d'un site distant, ou lorsqu'elles appartiennent à une base de données de radiographies accessibles sur internet.

Pour éviter qu'une tierce personne mal intentionnée n'en modifie le contenu, on y ajoute une marque, qui code par exemple le nom du patient et celui du médecin traitant.

Le watermarking, ou tatouage d'image, propose une solution pour la protection d'images, il consiste à insérer dans une image une marque, qui peut être le logo d'une société, le nom du propriétaire codé dans un masque binaire, ... Elle peut aussi définir des droits ou des interdictions associes à l'image : est-il permis d'imprimer l'image, de la copier, Dans ce cas, les ordinateurs, les imprimantes qui seront en charge de traiter l'image doivent savoir extraire l'information de l'image et l'interpréter.

3.2 Différents Objectifs D'un Algorithme de Marquage.

Les conditions que doit remplir une marque dépendent du problème traité. Un problème de tatouage peut être un problème de copyright, son but est alors de permettre aux propriétaires de l'image de prouver leurs droits sur cette image et également de repérer d'ou proviennent les copies illégales de cette image. C'est dans cette problématique que nous nous placerons.

Mais un algorithme de tatouage d'images peut aussi avoir pour but de repérer toute modification non autorisée de l'image devra, au contraire du cas précédent, être fragile, de sorte que n'importe quel changement de l'image entraîne une modification de la marque et soit donc détecté. On peut aussi marquer une image, de façon aussi discrète

que possible, dans le but d'échanger des messages secrets. Ceux-ci sont caches dans l'image, et nécessitent une clef secrète pour être décodes.

On peut enfin cacher des informations descriptives dans une image ; par exemple, un médecin peut inclure dans une radiographie, de façon discrète afin de ne pas la dénaturer, le nom du patient traité, et son diagnostic, ses observations.

Ce cas est le plus simple, puisqu'une attaque visant à détruire la marque ne présente aucun intérêt et n'est donc a priori pas à craindre.

Mais même en se restreignant au premier cas, les exigences concernant la marque varient avec le problème initial. Dans certains cas, on supposera que la personne qui a le droit d'extraire les marques dispose d'une image originale non marquée pour faire l'extraction ; dans d'autres, on veut pouvoir faire l'extraction sans recourir à l'image originale.

Dans la plupart des problèmes de watermarking, il faut veiller à ce que si plusieurs personnes possèdent des images marquées s'associent, elles ne soient pas capables, en mettant leurs images en commun, de trouver et d'effacer les marques. Signalons enfin qu'il est souvent souhaitable que l'extraction de la marque ne puisse se faire que par des personnes possède une clef privée (cela peut être une série de chiffres, une phrase, etc...). Ainsi, même si l'algorithme

3.3 Définition Du Tatouage D'images.

Le tatouage d’image, plus connu sous le nom de ‘watermarking’, est une discipline apparue au début des années 90 et qui ne cesse de prendre de l’importance en traitement d’image. elle consiste à insérer une signature invisible dans une image, une vidéo ou une séquence audio.

La marque insérée est uniquement connue du propriétaire (problème d’identification) ou du diffuseur (problème de suivi). Ses caractéristiques sont uniques et dépendent des clés fournies par le propriétaire. Les travaux de recherche les plus récents proposants des techniques de tatouage qui permettent de retrouver la marque en aveugle, sans recours à l’image originale.

3.4 Principe Du Tatouage.

3.4.1 Principe Général D'un Système de Tatouage :

Le tatoueur insère une marque (w) dans un médium (m) original. Cette insertion peut se faire suivant une clé secrète (k) qui sera alors nécessaire à l'extracteur. Le médium une fois marqué peut subir diverses attaques, volontaires ou non, qui risquent de supprimer la marque ou la rendre illisible.

L'extracteur a alors pour but d'extraire soit la marque elle-même, soit un indice de présence caractérisant la probabilité de présence de la marque dans le médium, figure1.1.

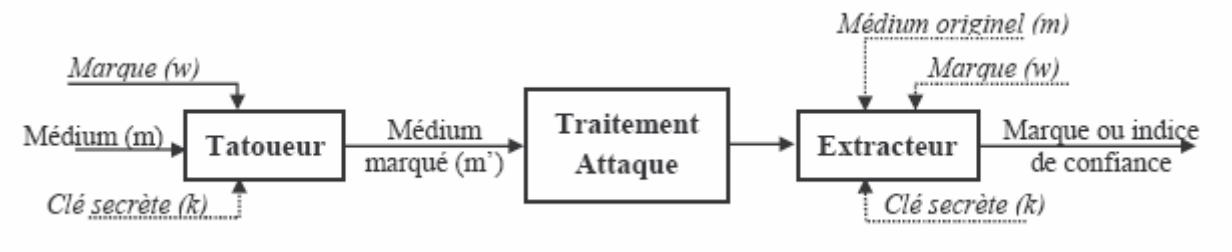


figure1.1 : *système générale de tatouage.*

Le schéma de tatouage d'images se décompose en deux opérations distinctes illustrées figure 1.2 :

3.4.2 La Phase D'insertion :

Elle consiste à introduire une marque dans l'image en vue d'identifier son propriétaire (le nom de l'auteur ou de l'entreprise par exemple). Cette insertion peut se faire dans le domaine spatial ou dans le domaine transformée (transformée de Fourier, en cosinus discrète, en ondelettes …).

3.4.3 La Phase de Détection :

Elle permet de retrouver la marque ou la signature insérée. Cette étape est la plus souvent effectuée en aveugle, c'est à dire sans utiliser l'image originale (utiliser l'image originale donnerait un schéma plus lourd et pourrait poser des problèmes de sécurité). Entre l'insertion et la détection, l'image marquée peut subir des modifications licites ou illicites.

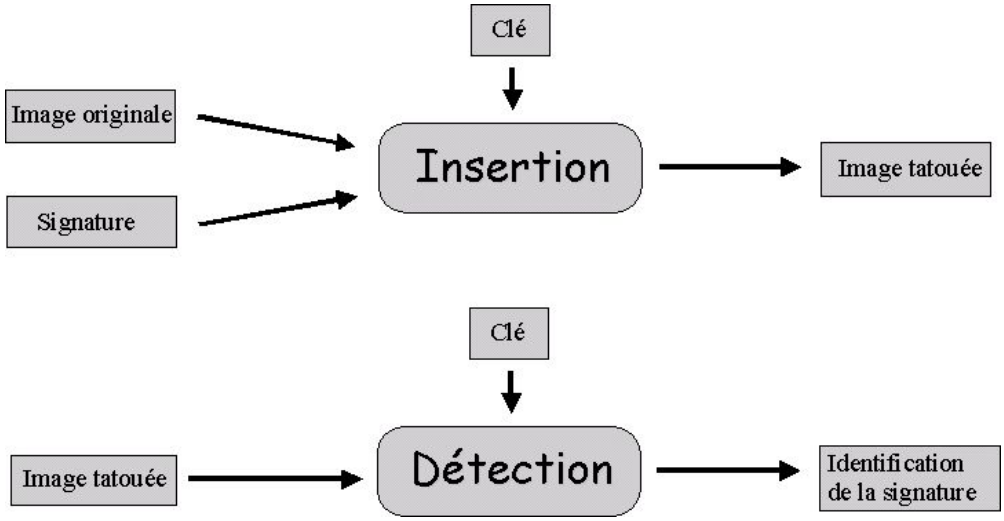


figure 1.2 : *Insertion et détection pour le tatouage d'images*

3.5 Contraintes et Caractéristiques D'un Marquage.

Les performances d'un marquage sont appréciées sous les quatre critères suivants : Imperceptibilité, Robustesse, Complexité, Capacité

3.5.1 Imperceptibilité :

Le tatouage doit être invisible à l'œil humain. Prenons deux exemples très simples pour souligner son importance. Imaginons une image en niveau de gris avec une large zone uniforme. Si l'on rajoute un peu de bruit, ceci va immédiatement se voir dans cette zone. Il faut plutôt mettre le tatouage dans des zones de fort gradient (contour de formes, zones fortement texturées,…) où l'œil est moins sensible. Un autre exemple vient du marquage des images couleurs. Il est connu que l'œil humain n'est pas sensible de la

même façon à toutes les longueurs d'onde. On peut ainsi dissimuler plus ou moins d'informations suivant la teinte considérée.

C'est une condition nécessaire à tout algorithme de tatouage d'images. L'utilisation de masques psychovisuels [4, 5, 6] tend de plus en plus à se généraliser pour insérer une quantité d'information importante tout en gardant la marque invisible.

3.5.2 Robustesse :

On pourrait séparer cette rubrique en deux parties : la *robustesse* et la *sécurité*. Ces deux caractéristiques sont souvent confondues surtout dans le cas du marquage. On parle de robustesse pour définir la résistance du tatouage face à des transformations de l'image tatouée. Ces transformations peuvent être de type géométrique (rotation, zoom, découpage …). Elles peuvent modifier certaines caractéristiques de l'image (histogramme des couleurs, saturation…). Il peut aussi s'agir de tous les types de dégradations fréquentielles de l'image (compression avec pertes, filtres passe haut ou passe bas, passage analogique->numérique
->analogique, impression de l'image, etc.…). Ces attaques sont dénommées « attaques aveugles », car le pirate agit sans réellement savoir ce qu'il fait. Il espère ainsi laver l'image.

La sécurité caractérise la façon dont le marquage va résister à des attaques «malicieuses ». On peut faire des parallèles avec la cryptanalyse. Le pirate va chercher à laver l'image de façon intelligente. Il est sensé connaître l'algorithme et va, en général, chercher la clef qui lit le tatouage. Cela demande souvent une analyse approfondie de la technique de marquage employée.

3.5.3 Complexité :

Dans la pratique, la plupart des opérations de tatouage doivent pouvoir s'effectuer en temps réel (surtout la détection, pour des films par exemple). Ceci implique une contrainte supplémentaire sur la complexité des opérations utilisées pour le marquage et pour la détection.

3.5.4 Capacité :

La capacité d'un système de tatouage numérique désigne le rapport : « nombre de données » à dissimuler sur « taille du document hôte ». Dans le cas du marquage, et comme nous l'avons vu précédemment, la capacité se limite souvent à 1 bit. De façon générale, plus la capacité est faible, plus la robustesse et l'imperceptibilité sont fortes.

Pour être performant et efficace le système de protection des droits d'auteur, le tatouage doit vérifier les trois critères suivants figure 1.3.

Les 3 éléments sont dispositifs pour avoir une meilleure qualité de la protection de droit d'auteur.

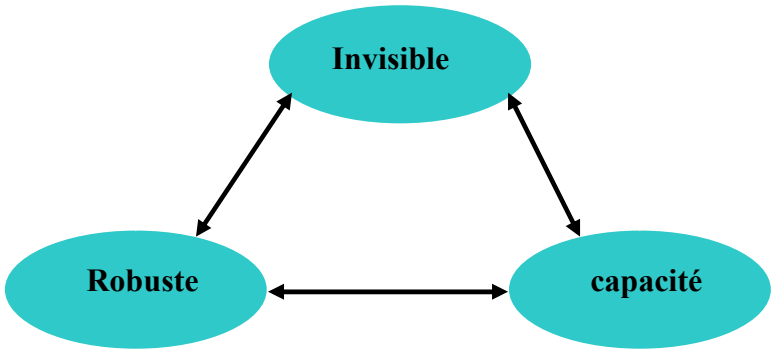


figure 1.3 : *Représentation schématique du compromis entre robustesse, capacité et visibilité*

3.6 Utilisation de Marquage.

Maintenant que nous avons vu les caractéristiques demandées au tatouage numérique, voici des différentes formes de marquage :

:

3.6.1 Le Marquage Faible (ou Fragile) :

Dans ce cas particulier, on demande au tatouage d'avoir une très grande imperceptibilité et une faible robustesse. Ainsi, la marque ne supportera quasiment aucun traitement. On pourra ainsi certifier ou non l'intégrité de l'image.

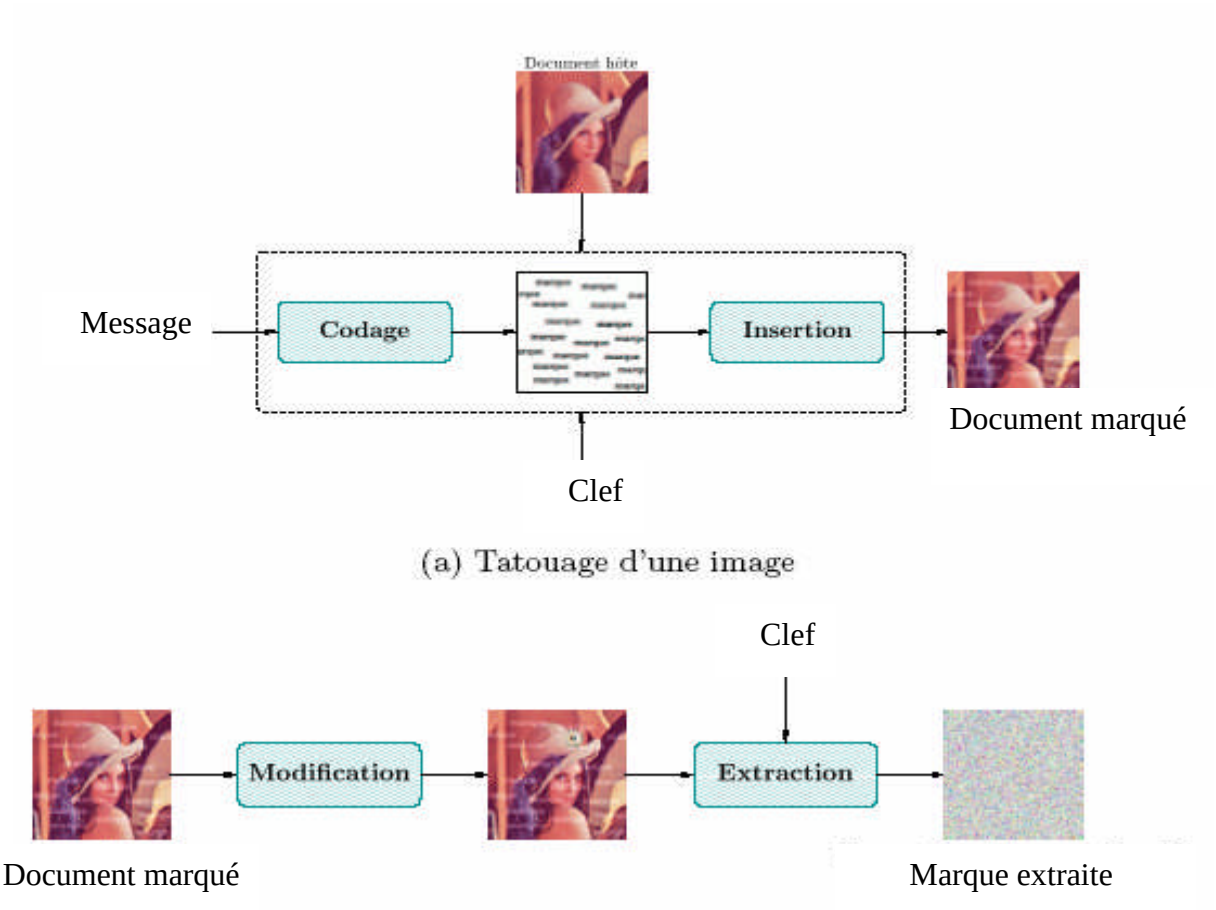
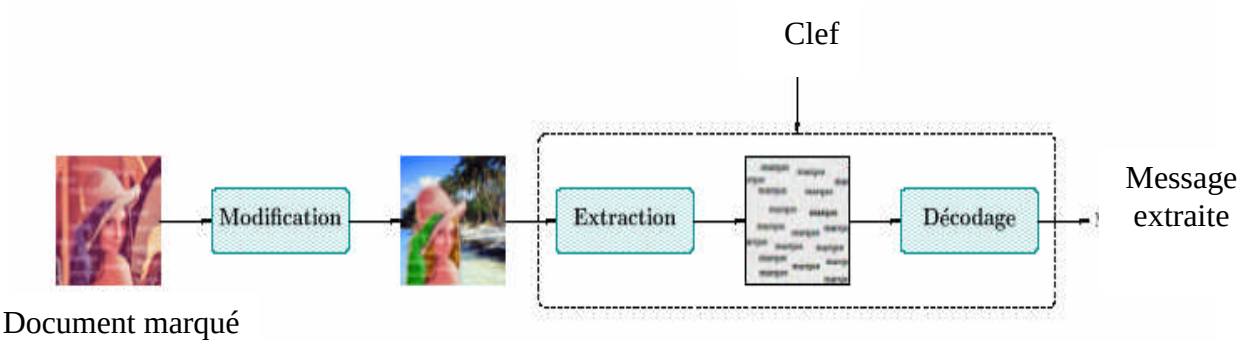


figure 1.4 : *Représentation schématique d'un tatouage fragile.*

La moindre modification du document se répercute fortement sur la marque extraite et on peut en déduire que le document n'est pas authentique.

3.6.2 Le Marquage Fort (ou Robuste) :

Il s'agit de la forme la plus commune de tatouage numérique Elle est en général imperceptible et surtout très robuste. Le cas limite de ce type de marquage est un marquage visible, comme un logo, mais avec une robustesse à toute épreuve (le Vatican a utilisé ce type de marquage pour ses documents.



(c) Tatouage robuste : malgré de fortes modifications, le message doit pouvoir être lu correctement

figure 1.5 : *Représentation schématique d'un tatouage robuste.*

3.6.3 Le Marquage Symétrique (ou Privé) :

On parallèle avec la cryptographie prend ici toute son importance. Le marquage symétrique signifie que l'on utilise la même clef pour insérer et détecter le tatouage.

3.6.4 Le Marquage Asymétrique (ou Publique) :

La clef de marquage et celle de détection sont différentes Outre l'intérêt immédiat (n'importe qui peut lire la signature sans pour autant pouvoir l'enlever ou la modifier), ces techniques récentes sont plus sécurisées Elles portent officieusement le nom de « marquage de seconde génération ».

4. Les Autres Applications Du Tatouage.

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

Il paraît donc nécessaire que la première étape de la conception d'un algorithme de tatouage comprenne la définition des applications auxquelles la méthode sera destinée puisque celles-ci définiront les besoins de la marque. La littérature relative au tatouage décrit abondamment les utilisations possibles du marquage [7] [8] [9] : on distingue généralement la protection de la propriété individuelle (détaillée auparavant), le suivi de

document, la prévention de la redistribution non autorisée, la protection des droits de copie, l'indexation, l'information sur le support et l'intégrité du contenu du document.

4.1 L'intégrité de Données Multimédia.

La marque permet de s'assurer que le contenu du document est authentique : il s'agit d'une marque fragile, qui subit des distorsions si le document a été altéré. Le concept de robustesse est ici différent : à l'inverse des autres applications du tatouage, la marque est conçue de manière à se détériorer dès que le document est modifié. Seules les modifications agressives doivent être prises en compte : la marque idéale en termes d'intégrité n'est pas affectée par des opérations de compression ou par l'ajout de bruit inhérent à la transmission des données. Un exemple d'utilisation est l'authentification de conversations téléphoniques ou de vidéos afin de permettre leur utilisation lors de procès : la marque montrerait si le signal a subi des coupes, ou même les localiserait, permettant de vérifier si le sens premier de la conversation a été respecté.

4.2 Prévention de La Redistribution non Autorisée.

L'objectif est de détecter les possesseurs licites d'un document qui sont à l'origine de sa distribution illicite. Les exemples les plus courants de telles distributions sont les copies (gravées) de CD audio, ou encore la mise à disposition de fichier audio au format mp3 sur les pages web personnelles. Une solution au problème de la redistribution non autorisée consiste à identifier séparément les acheteurs, en leur attribuant un numéro de série personnel.

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

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

4.3 La Réglementation des Copies de Données Multimédia.

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

Des informations relatives à la copie et à l'utilisation sont encodées dans la marque : il peut s'agir d'autorisations du type (pas de copies), (une seule copie), (plus de copies disponibles), ou encore (copie sans restriction). Le dispositif chargé de la lecture et/ou de la copie interroge le support en refusant de le lire ou de le copier si les données encodées ne le permettent pas. Ce dispositif suppose la construction d'une nouvelle génération de lecteurs audio. Les lecteurs DVD de seconde génération (permettant de graver des données vidéo) devraient être équipés d'un tel système de tatouage.

4.5 Information sur Le Support.

La marque peut contenir des données publiques informatives sur l'oeuvre, de type auteur, titre, date, adresse électronique etc. Dans l'éventualité (très probable) où cette application interviendrait en complément d'une protection de la propriété, il s'agirait non pas d'une seconde marque, mais d'informations supplémentaires insérées dans la première marque. On peut aussi envisager l'insertion d'une seconde marque entièrement publique, ce qui autoriserait le client à supprimer ces informations supplémentaires pour minimiser la taille des données stockées. Cette technique à été développée par Digimarc sur les images numériques [10] qui sont alors appelées (smart images).

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

5. Conclusion.

Ce chapitre avait comme objectif de familiariser avec la discipline du tatouage de documents. Après avoir introduite la cryptographique et la stéganographie qui sont des disciplines très proches de tatouage, nous avons vue ensuite ses notions sur les droits d'auteurs et les différents définitions de copyright et en quoi consiste la protection des documents numérique et exactement sur l'image.

Pour une meilleure protection de l'image ou document numérique doit d'être subits des critères et contraintes sur le système comme la robustesse et la masse d'information, et par fois la nature et la structure de l'information, qui adopte un technique de protection équivalent.

Deuxième Chapitre

Etat de l’art

1. Introduction.

Le tatouage des données numériques est une discipline récente qui trouve son origine dans le manque de techniques fiables de protections de ce type de données. En effet, associé à d'autres techniques, cet axe de recherche a pour but de résoudre des problèmes aussi variés que la protection du copyright et des droits d'auteurs, la réglementation des copies, la prévention de la redistribution non autorisée, le suivi de documents et l'intégrité du contenu d'une donnée.

Les différentes applications citées ci-dessus entraînent diverses contraintes qui seront détaillées dans les pages suivants. Nous ne développerons dans la suite de ce rapport que la partie du tatouage ayant trait à la protection du copyright et des droits d'auteurs des images numériques. Les propos généraux peuvent cependant s'étendre aux autres supports (audio ou vidéo). Après avoir présenté les premières définitions et propriétés du tatouage, nous définirons les processus d'implémentation puis de détection de la marque. Nous présenterons alors des techniques permettant d'évaluer une méthode de tatouage, puis nous donnerons les différentes applications de ces méthodes.

Le but dans tout algorithme de tatouage d'images numériques est de pouvoir insérer une marque (ou signature) qui soit liée au propriétaire. Le plus souvent on choisit le nom du propriétaire ou celui de l'entreprise qui souhaite utiliser la méthode. Ce nom appelé label est ensuite codé en un message composé de 0 et de 1.

Les méthodes de watermarking sont très diverses ; elles sont souvent spécialisées pour un type de support (son, image, signal de télévision, etc...), et n'ont pas toutes les mêmes objectifs (comme on l'a vu, elles peuvent simplement servir à vérifier que l'image n'a pas être modifie, ou bien servir à passer un message, ou alors coder le nom du propriétaire de l'image).

Dans cette partie, nous exposons les principes et propriétés générales des processus de tatouage puis nous donnons un aperçu des techniques développées jusqu'à présent. Nous faisons la distinction entre les méthodes dites additives et les méthodes dites (virtuelles). Dans le premier type de techniques, la marque est ajoutée à des caractéristiques de l'image.

2. Principes Généraux de Tatouage pour La Protection du Copyright.

L'objectif du tatouage pour la protection du copyright est d'introduire dans une image originale une marque invisible, appelée tatouage ou watermarking, contenant un code de

copyright. L'image ainsi marquée ou tatouée peut alors être distribuée, elle portera toujours la marque de son propriétaire. Cette image est susceptible de subir diverses transformations. Ces transformations peuvent être licites (comme la compression) ou illicites, elles ont alors pour but de détruire le marquage. Si elles ne dégradent pas trop la qualité de l'image, ces modifications ne doivent pas gêner la détection de la marque.

Dans la plupart des algorithmes de tatouage, le marquage est protégé par un code secret. Seules les personnes ou les organismes autorisés peuvent savoir si une image a été marquée et le cas échéant lire cette marque. Cette exigence se concrétise dans les algorithmes de tatouage par l'usage d'une clef privée cryptographique appartenant au propriétaire de l'image.
La définition la plus globale que l'on puisse donner d'une méthode de tatouage est la suivante

Définition 1 **:** Le principe général d'une méthode de tatouage d'une donnée numérique consiste à transmettre un message en même temps que la donnée, en modifiant directement la valeur des échantillons de cette donnée.
Cette définition est intéressante car elle recouvre toutes les méthodes de tatouages, quelles que soient leurs applications. On remarque aussi que ces méthodes sont voisines de la discipline de la stéganographie. On souligne ainsi les rapports du tatouage avec la théorie de la communication.

Définition 2 **:** Le principe général d'une méthode de tatouage d'une image numérique en vue de la protection du copyright consiste à transmettre une information de copyright en même temps que l'image, en modifiant imperceptiblement la valeur des échantillons de cette image. La détection de l'information de copyright doit être possible tant que l'image transmise est de qualité proche de celle de l'image originale. La mise en oeuvre de la détection doit nécessiter l'emploi d'une clef privée.

Nous présentons figure 2.1 un schéma illustrant la définition 2. Le signal d'entrée I, appelé signal hôte (medium) sera modifie par une application **E**. Cette étape est l'incrustation de la marque **W** dans **I**, avec l'intervention de la clef privée **K**. Le signal sortant $\mathbf{I}^*$, est diffusé. Il est alors soumis à des transformations licites ou illicites
de nature inconnue, cette version attaquée est notée **I'**. A la détection **D**, la marque est extraite (on obtient alors une marque $\mathbf{W}'$) ou sa présence est contrôlée (une variable booléenne indique si la marque est présente dans l'image testée). Tous les processus de détection n'ont pas les mêmes entrées.

Les pages suivants présents les différentes versions de ce processus et la terminologie associée. Nous allons maintenant présenter plus en détail les schémas d'implémentation et de détection de la marque. Nous accompagnerons ces schémas du formalisme donné par Petitcolas et al. Dans [11] et généralement utilisé par la communauté des tatoueurs. Ils ont l'avantage de pouvoir modéliser tous les algorithmes de tatouage.

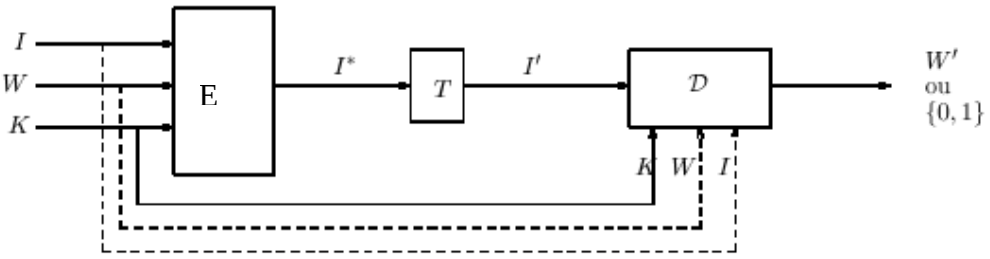


figure. 2.1 - *Schéma général d'un processus de tatouage. L'image tatouée* ***I***** est obtenue par application de la fonction d'implémentation* ***E*** *sur la clef* ***K****, la marque* ***W*** *et l'image originale* ***I****,* ***I'*** *subit alors des transformations* ***T****, l'image résultante est testée par un processus de détection* ***D****, qui extrait la marque ou détecte sa présence.*

3. Processus D'Implémentation de La Marque.

3.1 Schéma Général.

La figure 2.2 présente le schéma général d'implémentation de la marque. Une image hôte (medium) **I** est tatouée d'une marque **W** par un propriétaire possédant une clef privée **K**. L'image résultat **I*** est perceptuellement similaire à **I** et contient le code de copyright **W**.

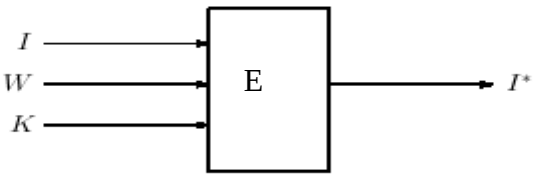


figure 2.2 : *schéma général du processus d'implémentation d'une marque. I est l'image hôte,* ***K*** *la clef privée,* ***W*** *la watermarque,* ***I**** *est l'image tatouée résultat de l'application* ***E****.*

3.2 Formalisme.

L'implémentation de la marque est une application **E** de l'espace des clefs **k**, de l'espace des marques **w** et de l'espace des images **i** dans ce dernier espace. Elle fait correspondre à une clef **K**, une watermarque **W** et une image hôte **I**, une image tatouée $\mathbf{I}^*$

$$(w,k,i) \longrightarrow i \qquad (2.1)$$

$$(W,K,I) \longrightarrow I^* \qquad (2.2)$$

Ce formalisme, très général, représente le processus d'implémentation de la marque pour tous les processus de tatouage. Nous allons maintenant préciser les propriétés que l'application **E** doit satisfaire et définir les espaces de départ et d'arrivée **w**, **k** et **i**.

3.3 La Fonction D'Implémentation.

3.3.1 Contrainte D'Imperceptibilité :

Le marquage doit être imperceptible, c'est à dire qu'un utilisateur quelconque ne doit pas pouvoir différencier visuellement l'image marquée de l'image originale. Cette propriété est importante pour deux raisons. La première est évidente : le marquage ne doit pas empêcher la compréhension de l'oeuvre, celle-ci doit garder toute sa qualité artistique ou commerciale .une autre raison est, qu'ainsi cachée, la marque est plus difficilement détruite par piratage.

Dans la plupart des algorithmes proposés, l'imperceptibilité du tatouage s'obtient en utilisant diverses propriétés du Système Visuel Humain (SVH). Ces propriétés, souvent trouvées à partir d'heuristiques, proposent des modélisations du comportement psychovisuel humain. En général, un seuil de perceptibilité est calculé à partir de l'image originale, les modificatins de l'image ne peuvent se faire qu'à concurrence de ce seuil. Cette contrainte pose un problème d'évaluation. En effet, une fois l'image tatouée, on doit pouvoir assurer que les distorsions causées sont imperceptibles.

On utilise couramment le PSNR (pour *Peak Signal to noise Ratio*) pour quantifier ces dégradations Nous expliquerons dans les pages suivants que cette mesure n'est pas adaptée à notre propos.

3.3.2 Sûreté du Tatouage, Inversibilité de E :

Comme dans toutes les disciplines proches de la cryptographie, la sûreté du système est

assurée uniquement par la confidentialité de la clef **K**. En effet, on ne peut pas garantir la confidentialité des algorithmes mis en œuvre. Cette exigence correspond au deuxième principe de Kerckhoffs [12]. Si **K** est inconnu, aucun utilisateur ne doit pouvoir retrouver l'image originale. Cette contrainte est souvent remplacée par la suivante, plus réaliste : Ne connaissant pas la clef secrète, un pirate ne doit pas pouvoir retrouver l'image originale sans pour cela mettre en oeuvre des moyens plus coûteux que ceux correspondant à l'achat des droits de copyright.

L'inversibilité de l'application **E** est donc conditionnée par la connaissance de laclef. Cette inversibilité n'est pas obligatoire. Elle peut être recherchée si les ayant- droits de l'image veulent enlever la marque pour en ajouter une autre (si par exemple, le statut de copyright a changé).

L'inversibilité de **E** est impossible si des informations inhérentes à l'image originale ont disparu dans la version tatouée. Certains processus d'implémentation sont par exemple fondés sur une substitution ou une quantification des valeurs de l'image qui sont alors irrémédiablement modifiées. Ces derniers schémas assurent plus de sécurité dans le cas où la clef est divulguée et peuvent alors servir pour des algorithmes dits à clef publique, où aucun secret n'est requis pour la détection de la marque [13].

L'inversibilité est comprise ici en son sens mathématique (certains auteurs l'appellent réversibilité). En tatouage d'images, le terme d'inversibilité est souvente mployé pour définir une attaque, appelée *dead lock attack* ou impasse. Nous verrons dans le paragraphe suivant que cette attaque, proposée par Craver et al. [14], utilise un défaut d'injectivité de l'application **E**.

3.3.3 Injectivité de L'Application E :

Si une image marquée correspond à deux propriétaires différents, c'est à dire deux couples (**W**,**K**)on se retrouve dans la position dite de l'impasse : On ne peut pas conclure sur l'appartenance de l'image à l'un ou l'autre des propriétaires. Cette situation arrive si l'application E n'est pas injective.

Craver and al. [14] ont utilisé un défaut d'injectivité de la fonction **E** pour invalider le processus de marquage. A partir d'une image tatouée, $\mathbf{I^* = E\ (W_A, K_A, I_A)}$, un attaquant, exhibe un triplet $\mathbf{(W_B, K_B, I_B)}$ tel que $\mathbf{I^* = E(W_B, K_B, I_B)}$. Cette attaque invalide le processus de marquage, puisque, quelque soit la méthode de détection, le double marquage est présent, on ne peut pas conclure quand à la propriété de l'image.

La solution proposée pour éviter ce problème est de restreindre les espaces de départ en impose une structure fixée à la clef et à la marque. Si on impose de plus que la clef soit fonction de l'image originale, l'attaquant aura alors beaucoup plus de mal à générer le triplet solution (W_B, K_B, I_B). En général, un tiers de confiance intervient dans le protocole de tatouage, il délivre par exemple la clef privée, pour chaque image.

3.3.4 Surjectivité de L'Application E :

E est surjective si et seulement si, il existe pour toute image I, un triplet (W_A, K_A, I_A) tel que :

$$I = E(W_A, K_A, I_A) \qquad (2.3)$$

Pour notre application, ceci signifie que toutes les images (originales ou non) possèdent une marque à l'état naturel. Il suffirait à un pirate de trouver le code et la marque pour s'approprier les images originales en circulation. Le danger de cette attaque, très proche de celle mentionnée ci-dessus est évité de la même manière : On restreint les ensembles de départs et on introduit un tiers de confiance dans le protocole de tatouage.

3.3.5 Conclusion :

Si l'on veut donner un formalisme mathématique rigoureux de l'application E, les deux contraintes d'injectivité et de surjectivité présentées ci-dessus imposent de redéfinir les ensembles de départs et d'arrivée de cette application. Soit Io l'ensemble des images originales et Im, l'ensemble des images tatouées. L'application E est alors définie comme une injection de l'espace d'entrée sur l'espace de sortie :

$$(w, k, Io) \longrightarrow Im \qquad (2.4)$$

$$(W, K, I) \longrightarrow I^* \qquad (2.5)$$

Cette définition est impossible à utiliser pratiquement, l'espace Io ne peut en effet être ni défini ni connu, il est en constant changement. Nous garderons donc comme définition de l'application E celle donnée dans (2.3). Les solutions envisagées pour résoudre les situations explicitées ci-dessus seront d'ordres protocolaires. On considérera par la suite que le processus de tatouage est associé à un modèle fonctionnel et que les clefs sont distribuées par un tiers de confiance.

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

4. Processus de Détection de La Marque.

4.1 Schéma Général.

La figure 2.3 présente le schéma général de détection **D** de la marque. L'entrée du processus est constituée d'une image test $\mathbf{I^0}$ et de la clef **K** de détection. Certains algorithmes nécessitent en plus la connaissance de l'image originale **I** et de la marque implantée **W** (en pointillés sur le schéma). La sortie du détecteur peut être la watermarque extraite $\mathbf{W}'$ ou un résultat de décision indiquant si la marque **W** a été retrouvée dans $\mathbf{I}'$.

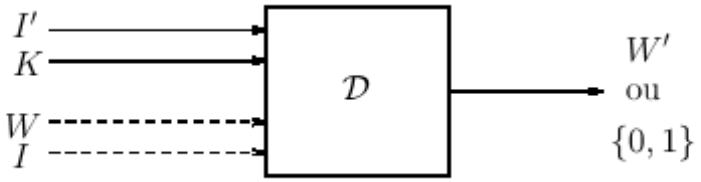


figure. 2.3 : *Schéma général du processus de détection d'une marque. I^o est l'image test, K la clef privée, W la watermarque, I est l'image originale. Le résultat de la détection D peut être une marque ou une décision*

.

4.2 Formalisme des Différents Types de Détection.

Nous avons vu dans la présentation du schéma général du processus de détection que les entrées et les sorties du système peuvent varier selon les algorithmes. Nous allons ici nommer et caractériser ces différents processus.

4.2.1 Les Schémas Privés :

La détection est dite privée si l'image originale est nécessaire

- Si le détecteur extrait la marque, il est dit de Type I, on a alors :

$$(K, I, I') \longrightarrow W' \qquad (2.6)$$

- Si le détecteur est une mesure de présence de la marque (sa sortie sera 1 si la marque est détectée 0 sinon), la détection est alors une application de type II avec:

$$(W, K, I, I') \longrightarrow 0,1 \qquad (2.7)$$

La présence de l'image originale à la détection facilite la création du schéma général

De tatouage (implémentation et détection) et apporte beaucoup de robustesse à ce schéma. Cependant, ceux ci ne sont pas adaptés à toutes les applications pour des raisons évidentes (comme dans le cas de la réglementation de copies) ou des raisons techniques (comme dans le cas du suivi de document).

4.2.2 Les Schémas Semi-Privés :

Une détection semi-privée n'utilise pas l'image originale et donne une réponse sur la présence de la marque

$$(K, I, I') \longrightarrow 0,1. \qquad (2.8)$$

4.2.3 Les Schémas Aveugles :

Une détection aveugle (appelée parfois publique) extrait la watermarque insérée sans l'image originale.

$$(K, I') \longrightarrow W \qquad (2.9)$$

La robustesse du schéma ne repose ici que sur la connaissance de la clef **K**, on ne peut plus s'appuyer sur le caractère privée de la connaissance de l'original ou de la marque : Il faut donc apporter beaucoup de soin à anticiper les attaques possibles. Ce schéma est utilisable dans tous les cas de tatouage nécessitant une clef privée.

4.2.4 Les Schémas Asymétriques :

La détection par algorithmes asymétriques ou à clef publique peut être schématisée comme une détection aveugle, la clef secrète de détection étant connue de tous. Une des principales difficultés de ce type de tatouage est d'empêcher la destruction de la marque ou son invalidation alors que tous les utilisateurs connaissent l'algorithme employé et la clef. C'est pour cela que l'on utilise des algorithmes asymétriques où la clef d'implantation de la marque n'est pas la clef de détection.

4.2.5 Commentaires :

Pour la protection du copyright, la marque est supposée connue, les algorithmes de figure2.4 présente cette détection par extraction sont alors suivis d'une étape de vérification. détection globale. La marque extraite $\mathbf{W}'$ est comparée à une. La marque prédéfinie **W** par mesure de corrélation ou par mesure de distance de Hamming.

finalement seuillée pour obtenir la valeur de décision : 1 si l'image I^o Cette mesure est

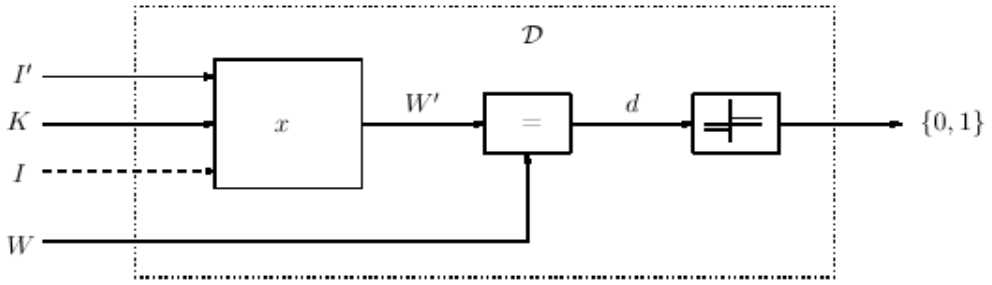


figure 2.4 : *Schéma général du processus de détection par extraction x de la marque W' puis comparaison avec la marque prédéfinie W puis enfin seuillage du résultat pour obtenir la valeur de décision*

Dans la suite de ce rapport, nous nous appuierons sur le formalisme des schémas semi-privés (voir la relation (2.8)).

4.3 *Propriétés du processus de détection.*

4.3.1 Robustesse aux attaques :

Une fois tatouées, les images diffusées peuvent être soumises à des transformations quelconques. Ces transformations, qu'elles soient licites ou illicites, constituent des attaques sur le processus de tatouage. Le chapitre des attaques donne des exemples d'attaques possibles. Si ces attaques ne dégradent pas trop la qualité de l'image, elles ne doivent pas gêner la détection de la marque, le détecteur est dite robuste à ces attaques.

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

$$\text{Si } \mathbf{t\,(I^*)} \sim \mathbf{I}^* \qquad \text{Alors } \mathbf{D\,(W, K, t\,(I^*))=1} \qquad \mathbf{(2.20)}$$

Où $\sim$ est l'opérateur (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 à priori sur l'attaque t, la seconde est la difficulté d'évaluation de la similarité perceptuelle.

4.3.2 Sûreté de La Détection :

Conformément au principe de Kerckhoffs, la connaissance de l'algorithme de détection utilisé ne doit pas permettre de retrouver la clef **K**. En effet, c'est sur la confidentialité de cette information que repose le protocole de tatouage.

4.3.3 Fiabilité de La Détection :

Un processus de détection fiable doit minimiser la probabilité de faux négatifs (une marque présente n'est pas détectée) et interdire les probabilités de fausses alarmes (une marque est détectée à tort). Pour toute transformation t, on peut noter la probabilité de faux négatifs :

$$P_{fn} = P(D(W, K, I') = 0| \quad I' = t(I^*), \quad I' \sim I^*) \tag{2.21}$$

Et de même la probabilité de faux positifs :

$$P_{fa} = P(D(W, K, I') = 1| \quad I' \neq t(I^*)) \tag{2.22}$$

Avec P (A/B) signifiant (probabilité de A sachant B). Ces deux probabilités sont appelées respectivement probabilités d'erreurs de type I et de type II.

5. Les Méthodes de Tatouage Existantes.

Dans la plupart des présentations générales, les différentes méthodes sont classées selon le domaine dans lequel les transformations sont faites. P. Bas [15], les différencie selon la façon dont la marque est inscrite dans l'image : il distingue deux grands ensembles de méthodes, les additives et les substitutives.

5.1 Schémas Additives .

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter un (bruit) à l'image. La figure 2.5 montre le schéma complet d'une méthode additive. La première étape est la génération d'une marque $\mathbf{W}'$ qui est composée d'un bruit blanc modulant parfois un message **M.** La seconde étape est la pondération de cette marque grâce à la prise en compte de critères psychovisuels et de caractéristiques propres à l'image. La troisième étape est l'addition de la marque dans les valeurs de l'image. Cette

incrustation peut se faire directement sur l'image (dans le domaine spatial) ou dans un domaine transformé. Cette section nous permettra de donner un aperçu de ces différentes étapes à travers des exemples de schéma de tatouage.

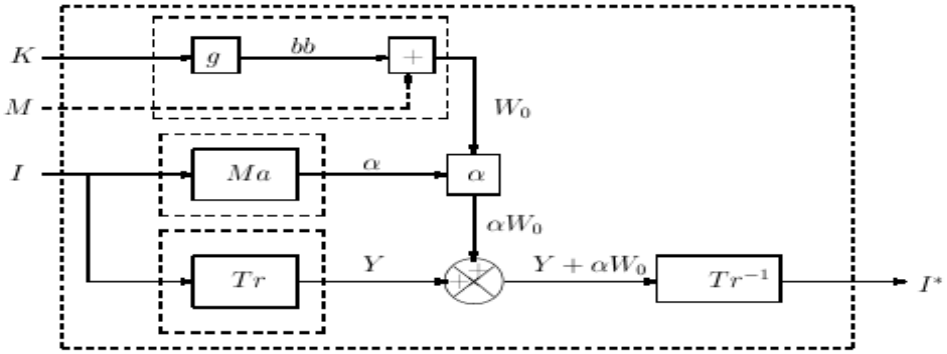


figure 2.5 : *Schéma d'une méthode additive. La marque* W^0 *est construite en modulant le message* ***M*** *par un bruit blanc bb de générateur* ***K.*** W^0 *est ensuite pondéré par un gain α, issu du calcul d'un masque Ma psychovisuel. Cette marque est ajoutée à l'image ou à une transformée Tr de celle-ci*

.

Dans les schémas additifs la signature ajoutée a des composantes de l'image.

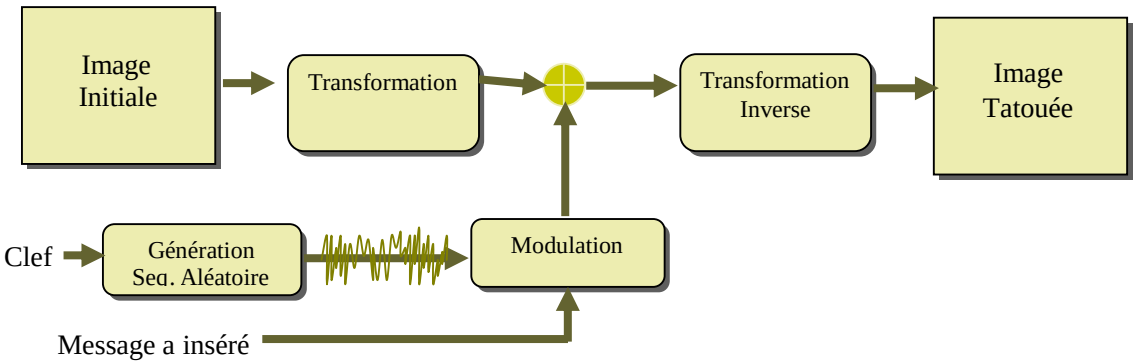


figure2.6 : *insertion de la marque dans le schéma additif.*

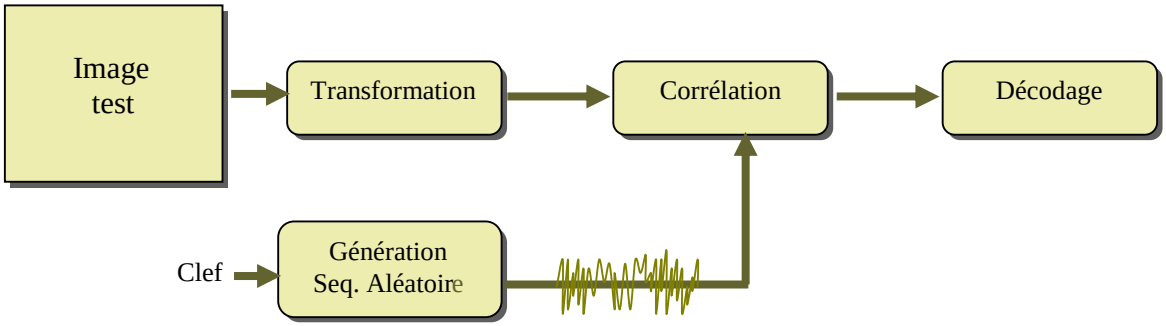


figure2.7 : *Détection de la marque dans le schéma additif.*

5.2 *Schémas Substitifs.*

La signature ou l'information est substituée à des composantes de l'image, l'information ne remplace pas des valeurs de l'image.

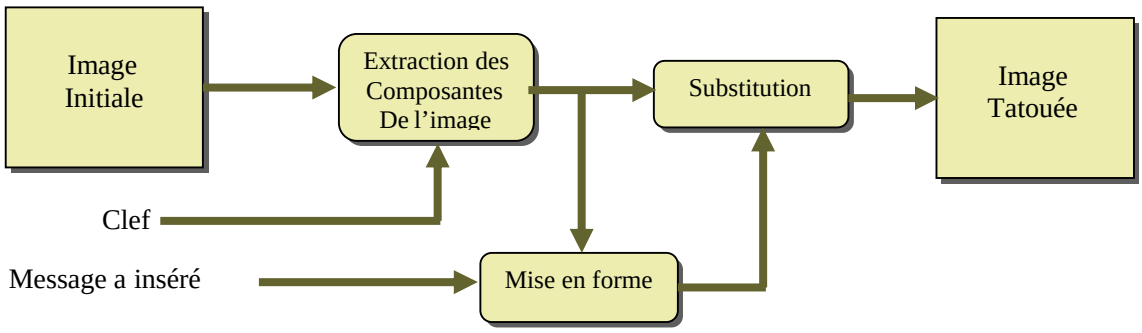


figure2.8 : *Insertion de la marque dans le schéma substitif.*

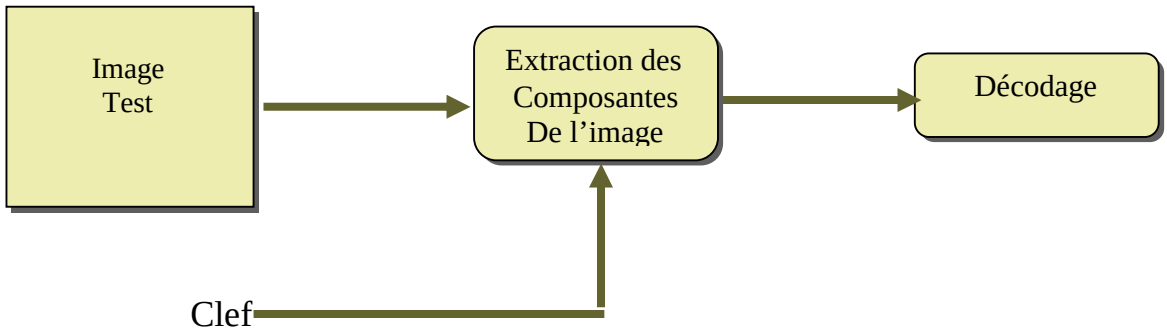


figure2.9 : *Détection de la marque dans le schéma substitif.*

5.3 Schémas virtuelles.

Nous appelons tatouage virtuel, un tatouage où la marque n'est pas ajoutée sur les données mais où la marque impose des contraintes aux valeurs de l'image. Ces méthodes de tatouages ne sont pas additives : l'information n'est pas ajoutée à l'image, ni substitutives l'information ne remplace pas des valeurs de l'image.

Considérons un exemple simple pour illustrer cette définition :

- la clef secrète **K** détermine un ensemble de **N** paires de pixels $(ai, bi)_{i=}$ [1 : N].
- La watermarque **W**, de longueur **N** est exprimée en modifiant la relation d'ordre

Liant les pixels entre eux. Soit (a^*_i, b^*_i) les pixels modifiés.

$a^*_i = a_i$ et $b^*_i = b_i$. - si $\mathbf{W_i} = 1$ et si $a_i \leq b_i$

si $a_i > b_i$ a^*_i et b^*_i sont choisis tels que $a^*_i < b^*_i$.

- si $\mathbf{W_i} = -1$ et si $ai \leq bi$ a^*_i et b^*_i sont choisis tels que $a^*_i > b^*_i$.

si $a_i > b_i$ $a^*_i = a_i$ et $b^*_i = b_i$.

-Les pixels modifiés sont réintégrés à leurs places dans l'image, la détection consiste à lire le message en regardant comment les paires de pixels (trouvées grâce à **K**) sont ordonnées. Au travers de cet exemple très simple apparaissent les avantages d'utiliser ce type de méthode. D'une part, on peut transmettre une marque de longueur non négligeable.

D'autre part, l'image n'est plus ici considérée comme un canal bruité pouvant créer des interférences avec la marque mais comme le support du marquage. En outre, on a une grande liberté sur la façon de modifier les composantes. Dans notre exemple, ces composantes ne seront pas toujours modifiées (une fois sur quatre pour une marque centrée) et on peut le faire de multiples façons : ajouter un coefficient, multiplier par un autre... Ces algorithmes ne sont jamais inversibles, l'information initiale étant perdue. Ainsi, les attaques malignes ne consisteront pas à enlever la marque (on ne peut pas enlever de relation d'ordre) mais à la brouiller (l'attaquant inversera la relation). Chen et al. [13] ont présenté une étude de ce dernier type d'attaque et ont quantifié la dégradation nécessaire au brouillage de la marque. Plus généralement les schémas de tatouage virtuels peuvent être décrits par les étapes présentées ci-dessous :

- La clef privée K sélectionne des composantes de l'image. Elles peuvent être des pixels, des coefficients issus de domaines transformés ou encore des propriétés de l'image.
- La watermarque W est exprimée en modifiant les caractéristiques des composantes Pointées par K. Cela peut être une relation d'ordre, un critère de similarité, une propriété géométrique de l'image ou encore l'appartenance à un certain espace fonctionnel.
- Ces composantes sont ensuite réintégrées dans l'image Comme on l'a vu dans l'exemple, la détection consiste à récupérer les composantes secrètes et à examiner leurs caractéristiques.

On peut parler ici de lecture de la marque. Dans les paragraphes suivants, nous présenterons des exemples de méthodes de tatouage virtuels.

Donc Les différents algorithmes de tatouages d'images numériques se distinguent ensuite essentiellement selon les critères suivants :

- **Le type de schéma d'insertion de la signature :** soit un schéma additif (la marque est ajoutée sans modifier l'image originale) soit un schéma substitutif (on supprime dans l'image certaine de ses composantes, cette substitution formant le support de la marque)
- **La stratégie sur la marque :** la manière de transformer la signature (ou le message) en marque numérique et la mise en forme de celle-ci vis-à-vis de l'image à marquer (utilisation d'un masque psycho visuel adaptant la marque à l'image à tatouer, sélection de sites prépondérants dans l'image pour l'insertion).
- **Le choix de l'espace de travail :** la marque peut soit être insérée dans le domaine spatial, soit dans le domaine transformée (DCT, TFD, Ondelettes, fractales)**.**

Pour décrire les différentes méthodes de tatouage d'images, nous traitons séparément les méthodes spatiales et les méthodes fréquentielles. Comme indique la figure 2.10.

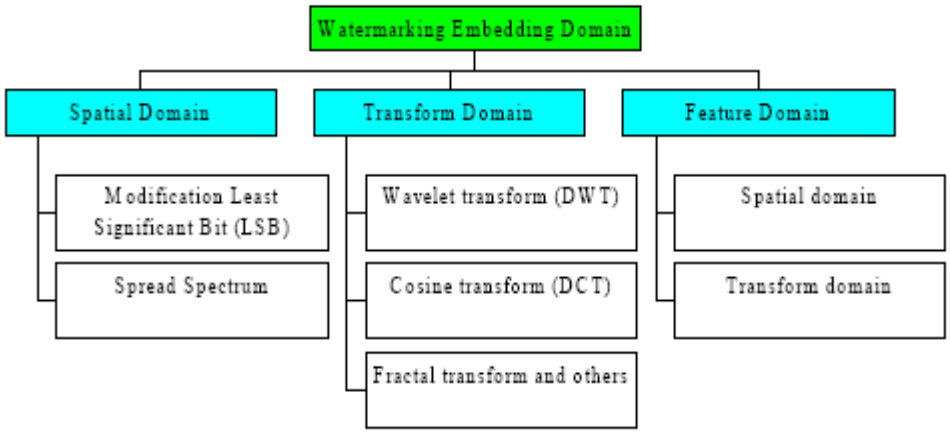


figure 2.10 : *classements des algorithme sur les domaines de travails*

5.4 Méthodes spatiales.

Les méthodes spatiales consistent à insérer la marque directement dans l'image. Elles ont l'avantage d'être facilement implantables mais sont pour le moment peu robustes aux attaques géométriques.

5.4.1 Insertion et détection :

L'insertion et la détection dans le domaine spatial suivent dans la majorité des algorithmes le schéma classique décrit ci-dessous :

- D'une part on génère une Séquence Binaire Pseudo Aléatoire S (une m-sequence ou une gold sequence par exemple) à l'aide d'une clé secrète, uniquement connue du propriétaire. Cette séquence est composée uniquement de +1 et de –1 et a une moyenne nulle (c'est à dire autant de –1 que de +1).
- Le message à insérer composé de +1 et –1 (par exemple M = {+1, -1, -1, +1}) est ensuite modulé par la Séquence S puis transformé en un signal à deux dimensions : pour cela on remplit ligne par ligne ce signal 2D. Pour une image 12*12, il faudra donc une séquence S de 144 échantillons. Cette marque est ensuite ajoutée directement à l'image comme le décrit la figure 2.11.

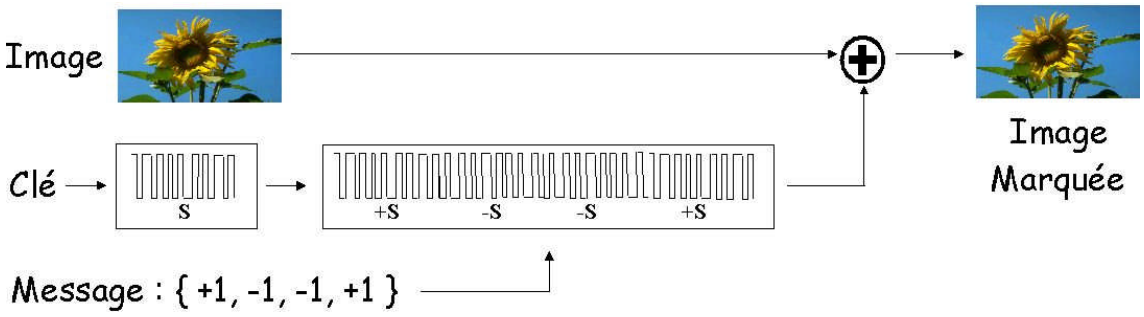


figure 2.11 : *Processus d'insertion pour la méthode spatiale.*

- La détection se fait le plus souvent par corrélation : en effet la marque ayant une moyenne nulle, on peut considérer que l'intercorrélation de la marque avec l'image est négligeable par rapport à l'autocorrélation de marque. Pour détecter la signature, il suffit donc de calculer l'intercorrélation de la marque avec l'image marquée. Ce calcul se fait simplement en multipliant pixel par pixel les deux images et en faisant ensuite la somme des produits. Le processus est répété pour chaque bit inséré pour obtenir à la fin le message détecté.

Appelons I l'image initiale, W la marque, W_1 une marque différente et I_w l'image marquée et supposons que toutes ces images sont de taille 100*100. La détection suit alors le schéma ci-dessous :

- On forme l'image marquée $\mathbf{I_w = I + W}$

- On calcule l'intercorrélation $\langle I_w,W\rangle = \langle I+W,W\rangle = \langle I,W\rangle + \langle W,W\rangle$

$= \varepsilon + 10\,000$ (avec $\varepsilon << 10\,000$)

- Pour une marque différente on aurait $\langle I_w, W1\rangle = \langle I, W\rangle + \langle W_1, W\rangle$

On prend donc une décision sur la présence ou non d'une signature si l'intercorrélation est supérieure à un seuil préalablement fixé, comme le résume le schéma de la figure 2.12 :

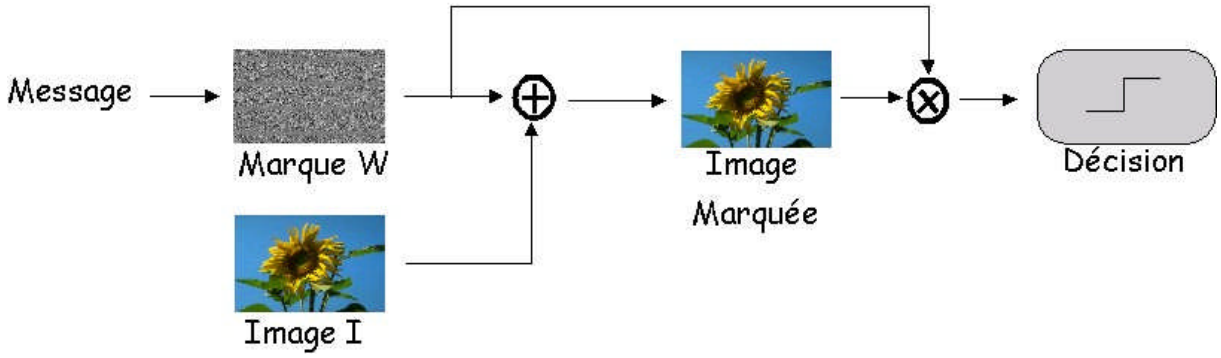


figure 2.12 : *Détection de la marque par corrélation*

5.4.2 Exemples d'algorithmes :

Dans cette section nous présenterons divers algorithmes de tatouage d'images dans le domaine spatial. Ce résumé non exhaustif a pour but de se familiariser avec les différentes techniques utilisées actuellement.

La numérisation des images introduit un bruit de quantification qui modifie principalement les bits les moins significatifs de chaque pixel. Il est alors possible d'ajouter à ce bruit la marque que l'on veut insérer. Tanaka et al. [16] remplacent ce bruit par un signal à l'aide d'un quantificateur prédictif, tandis que Wolfgang et al. [17] ajoutent un motif à deux dimensions créé à partir de SBPA. Toutes les deux opèrent une détection par corrélation.

Bender et al. [18] introduisent une méthode statistique appelée Patchwork qui consiste tout d'abord à sélectionner, selon une clé secrète, une séquence de n paires de pixels (a_i,b_i). Ensuite on augmente chaque a_i de 1 et on diminue chaque b_i de 1, la somme des différences donne 2n. Pour le pirate qui ne connaît pas les 2n paires choisies, la somme des différences pour 2n paires quelconques donnera, pour n assez grand, un résultat proche de 0.

De nombreux algorithmes cherchent à rendre la marque la moins visible possible en adaptant celle-ci à l'image qui doit être tatouée [19,20]. Pour cela ils modulent la marque par un masque adapté qui contient de nombreuses caractéristiques de l'image : ce masque peut être

obtenu en se basant sur la variance de l'image ou sur un modèle psychovisuel. L'objectif est à chaque fois d'insérer la marque dans les zones adéquates : parties de l'image très texturées, contours, parties très sombres. La figure 2.13 donne un exemple de marque modulée par un masque psycho visuel

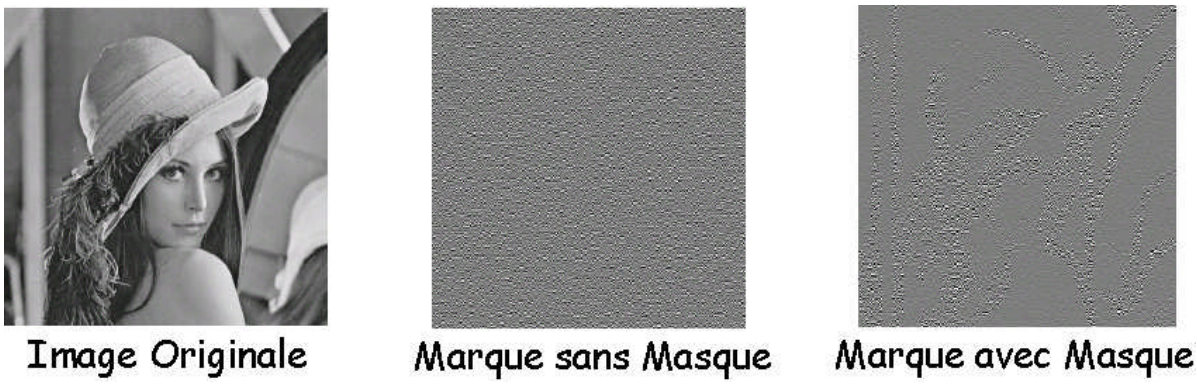


figure 2.13 : *différents types de marquages*

Delaigle et al. [21] ont développé un modèle perceptif permettant d'évaluer analytiquement la visibilité ou l'invisibilité d'une marque afin de pouvoir éventuellement rétroagir sur l'algorithme de tatouage. Partant de l'idée que le système visuel humain réagit comme un ensemble de canaux par lesquels sont transmis différents types d'information au cerveau, leur algorithme propose de décomposer l'image originale en canaux. La détermination de chaque canal est faite sur la base de caractéristiques fréquentielles (module et phase) ainsi que de la localisation dans le champ de vision. Toute la difficulté consiste à identifier des canaux en adéquation avec les critères perceptifs humains. L'hypothèse sous-jacente consiste à admettre que deux signaux à l'intérieur d'un même canal ne pourront être distingués par l'œil humain.

Quelque Différente techniques dans le domaine spatial

- Modulation des bits de poids faibles (LBM)
  - Tirkel [1993]: 1ère notion de watermark
- W. Bender [1995]: Méthode du Patchwork
  - Différences de luminances entre 2 ensembles de pixels
- Méthode par quantification
  - B. Chen : Dither Index Modulation (DIM)
  - J. Eggers : Subtractive Dithered Quantization (SDQ)
- Modulation d'amplitude 2D
  - Kutter [1996] : 1er essai d'une marque robuste aux transformations géométriques

5.5 Méthodes fréquentielles.

Les méthodes fréquentielles sont des méthodes plus récentes dont le principe est d'insérer la marque non pas directement dans l'image mais dans le domaine transformée : DCT, TFD, Ondelletes et DWT, fractales. Pour retrouver l'image marquée, on effectue la transformée inverse. Ces méthodes résistent mieux aux attaques géométriques.

La figure 2.14 décrit le schéma d'insertion dans le domaine DCT.

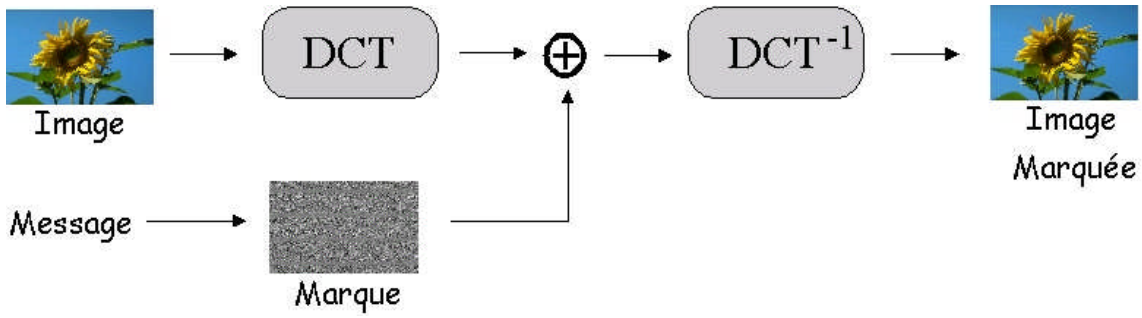


figure 2.14 : *Insertion d'une marque dans le domaine DCT.*

5.5.1 Insertion dans le domaine DCT :

Cox et al. [22] proposent une méthode qui utilise la transformée en cosinus discrète (DCT) pour insérer la marque dans l'image. Ils appliquent la DCT à toute l'image et insèrent la signature dans les basses fréquences, c'est à dire dans les composantes les plus significatives. Ils modifient les μ fréquences de plus grande amplitude, excepté la composante continue, suivant l'une des formules suivantes :

$$v'i = v_i + \alpha.x_i .$$
$$v'_i = v_i . (1 + \alpha.x_i)$$
$$v'_i = v_i . e^{\alpha.xi}$$

Avec :

v'_i : Coefficient DCT de l'image marquée.
v_i : Coefficient DCT de l'image originale.
α : Coefficient d'invisibilité.
x_i : Coefficient réel issu d'une distribution gaussienne centrée normée.

L'extraction se fait en inversant le processus d'insertion et en utilisant l'image originale pour retrouver la marque. La suite x'_i extraite est comparée à la suite x_i par un calcul de corrélation. La décision est de type « tout ou rien ».

5.5.2 Insertion dans le domaine TFD :

Csurka et al. [23] ont présenté une approche de tatouage d'images basée sur la transformée de Fourier Discrète (TFD). La marque ajoutée au domaine de la TFD est obtenue en encodant le message à l'aide de SBPA telles que les m-séquences ou les gold-séquences. Afin de pouvoir compenser une attaque basée sur des transformées géométriques, Csurka et al. ajoutent des pics de référence qui permettent de modifier les amplitudes de la TFD. Grâce à cette technique, il est possible de synchroniser le signal en détectant les pics insérés, la marque peut alors être extraite et décodée. Pour s'assurer de l'identité du propriétaire même si le message n'a pas été correctement décodé, ils utilisent une approche bayesienne pour calculer la probabilité qu'un filigrane ait été généré avec une clé donnée.

5.5.3 Insertion dans le domaine ondelettes :

Les transformées en ondelettes ont, comme la DCT ou la TFD, été utilisées par la communauté du tatouage d'images [15, 16, 17]**.** L'intérêt de cette transformée repose d'une part sur les analyses en termes psychovisuels menées afin d'optimiser les tables de quantification des codeurs, d'autre part sur l'aspect multi-échelle qui est propice à une répartition plus robuste du tatouage. Ce gain en robustesse apporté par l'usage d'une transformée en ondelettes est particulièrement significatif si l'on considère les algorithmes de compression de type EZW *(Embedded Zero-tree Wavelet*) qui seront vraisemblablement intégrés dans la nouvelle norme de compression JPEG-2000.

5.5.4Utilisation de la Transformée de Fourier-Mellin :

Les transformations géométriques sont actuellement les attaques les plus efficaces pour empêcher la détection de la signature dans l'image marquée. Ce constat a conduit les tatoueurs d'images à chercher un espace transformée invariant aux transformées géométriques. O Ruanaidh et al. [24] préconisent l'usage de la Transformée de Fourier-Mellin pour assurer la restitution du tatouage après que l'image a subi une translation, une rotation ou

encore un changement d'échelle. L'espace invariant est obtenu d'une part grâce à la propriété de la transformée de Fourier qui répercute une translation de l'image exclusivement sur la phase et laisse invariant l'amplitude, d'autre part par un changement de repère de cartésien vers logarithmique polaire qui ramène les opérations de rotation et de changement d'échelle à une translation.

Les transformations géométriques sont actuellement les attaques les plus efficaces pour empêcher la détection de la signature dans l'image marquée. Ce constat a conduit les tatoueurs d'images à chercher un espace transformée invariant aux transformées géométriques. O Ruanaidh et al. [24] préconisent l'usage de la Transformée de Fourier-Mellin pour assurer la restitution du tatouage après que l'image a subi une translation, une rotation ou encore un changement d'échelle.

5.6 Autres approches.

De nombreuses autres techniques sont étudiées ou en cours d'investigation. Des chercheurs s'intéressent notamment au domaine fractal [25], l'objectif étant de mettre à profit certaines propriétés d'invariance propres aux fractales afin de pouvoir prévenir certaines attaques et récupérer la marque sans recourir aux documents originaux.

Coltuc et al. Proposent d'insérer une signature dans l'image par modification de son histogramme. L'insertion de la marque s'effectue en substituant l'histogramme de l'image originale par un histogramme arbitraire de forme périodique. La détection de la marque s'effectue par simple calcul de l'histogramme de l'image marquée. Ce schéma est peu robuste à une manipulation de pixels mais par contre résiste bien aux transformations géométriques.

Actuellement un intérêt grandissant est porté aux schémas dits substitutifs qui représentent les méthodes pour lesquelles la marque est formée par la suppression de certaines composantes de l'image. Ces composantes sont choisies, comme pour le schéma additif, par une clé secrète ; la signature est ensuite adaptée à l'image originale

(Par un masque psychovisuel par exemple). La détection de la signature s'effectue en examinant la répartition des caractéristiques extraites. Si la répartition est proche (au sens d'un critère de similitude) d'une répartition propre à une signature, la signature est détectée comme présente.

5.7 Classification des méthodes de marquage :

Cette figure 2.15 montre les classements des méthodes de tatouage.

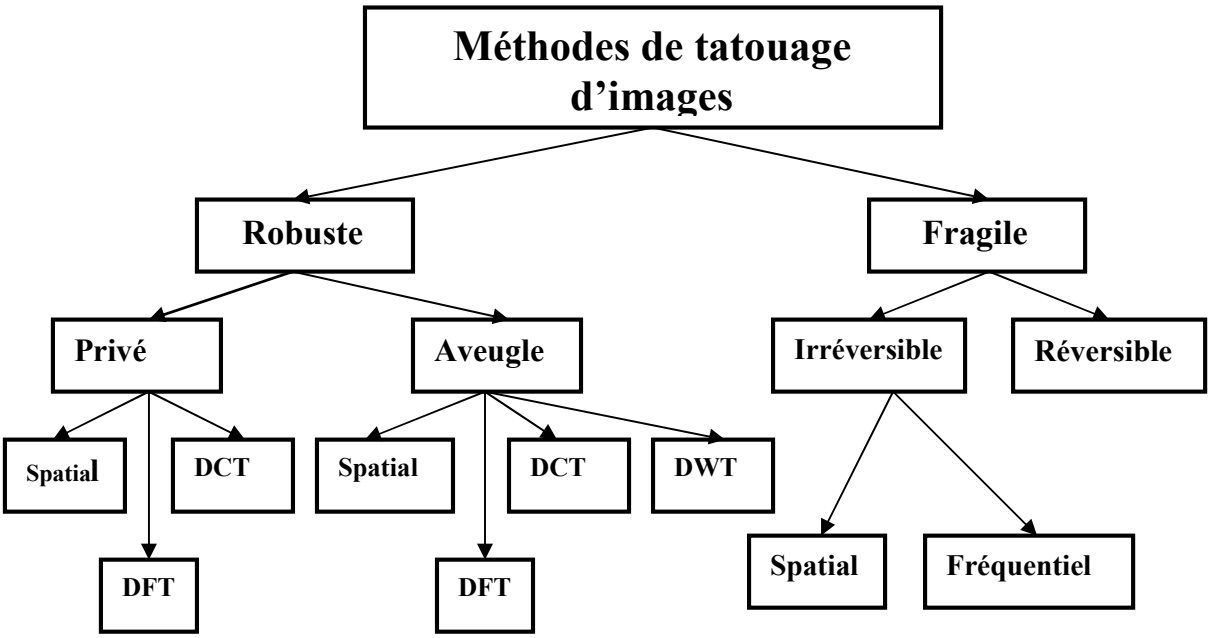


figure 1.15 : *Classification des méthodes de tatouage.*

6. Conclusion.

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

Il paraît donc nécessaire que la première étape de la conception d'un algorithme de tatouage comprenne la définition des applications auxquelles la méthode sera destinée puisque celles-ci définiront les besoins de la marque.

Troisième chapitre

Ondelettes et DWT

L'objet de ce chapitre est de présenter les ondelettes et DWT en forme théorique ou mathématique que nous allons utiliser dans la suite de ce travail. Nous les situerons dans le panorama plus large de l'analyse du signal 2D par les ondelettes, puis nous rappellerons leurs propriétés fondamentales ainsi leur paquet d'ondelette.

1. Introduction .

Comme déjà mentionné auparavant, les deux principaux domaines de représentation utilisés en traitement du signal sont le temps et la fréquence. L'outil désormais classique permettant de passer d'un domaine à l'autre est la transformée de Fourier (TF). La TF permet d'estimer les fréquences présentes dans un signal, mais pas de localiser l'endroit ou ces fréquences apparaissent ou disparaissent, car elle agit sur la totalité du signal.

Pour disposer d'une information de type temps- fréquence, c à d à la fois en temps et en fréquence, il faut calculer la TF d'une fenêtre de petite taille que l'on fait « glisser » d'un bout à l'autre du signal. On obtient alors une représentation temps-fréquence de type spectrogramme. L'inconvénient de cette procédure, outre sa faible résolution conjointe temps/fréquence est que la taille de la fenêtre est constante. Il serait plus pertinent d'adapter la taille de la fenêtre d'analyse aux caractéristiques locales du signal : petite fenêtre lorsque le signal varie rapidement (hautes Fréquences) et plus grande fenêtre lorsque ses variations sont lentes (basse fréquences).

L'analyse en ondelettes vise à apporter une solution à ce problème en décomposant le signal sur une base de signaux élémentaires, les ondelettes obtenues par dilatation et décalage d'une ondelette de base. En modifiant ainsi par dilatations on contractions successives la taille de l'ondelette analysante.

Les ondelettes c'est d'abord une théorie mathématique récente d'analyse du signal développée dans les années 80. On peut considérer qu'il s'agit d'une extension de l'analyse de fourier. On a un signal continu et on le décompose en une série de nombres qui décrivent des courbes qui s'additionnent pour reconstruire le signal. L'intérêt de cette théorie est au départ l'analyse des signaux et elle a déjà de nombreuses applications.

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. La décomposition en paquets d'ondelettes est une extension de la transformée en ondelettes discrète permettant de choisir le pavage du plan temps-fréquence. Ce choix est réalisé à travers la sélection d'une base de paquets d'ondelettes. En général, la base est sélectionnée selon le signal traité et selon un critère répondant aux contraintes de l'application. Cette base sera appelée meilleure base. Nous allons présenter dans cette partie les différents outils cités ci-dessus. Dans le premier chapitre, nous introduirons la transformée en ondelettes continue puis nous parlerons de la transformée en ondelettes discrète et de l'analyse multi résolution permettant de générer certaines de ces ondelettes. En particulier, nous présenterons le critère que nous utiliserons dans la méthode de tatouage proposée.

Dans cette partie, nous nous sommes volontairement limités aux notions nécessaires à la compréhension de la méthode décrite dans la suite du rapport. La bibliographie de ce chapitre est fondée sur [26] [27] [28] [29] [30] [31] [32].

2. Principe des Ondelettes.

La transformation de Fourier est en fait une projection de la fonction signal sur l'espace (continu) des exponentielles complexes. Elle n'est pas bien adaptée aux signaux non stationnaires ou transitoires parce que les exponentielles complexes s'étalent régulièrement en temps de $-\infty$ à $+\infty$.

L'idée des ondelettes est donc de projeter la fonction signal sur un espace de fonction à support temporel limité, de façon à pouvoir étudier ce qui se passe localement. En fait, cela consiste à projeter le signal **x** sur une famille de fonctions à valeur moyenne nulle (les ondelettes mères) par des translations et des dilatations :

$$\mathbf{T}x(t,a,\psi)=\int_{-\infty}^{+\infty} x(s)\,\psi^{*}_{t,a(s)}ds,\ \psi_{t,a(s)} = (\,|\,a\,|^{-1/2}\,)\,\psi((s-t)/a) \qquad (3.1)$$

On obtient ainsi ce qu'on appelle la transformation continue en ondelettes (*Continuous Wavelet Transforrm*, CWT).

La variable « **a** » est un facteur d'échelle, car si | **a** | **>1** l'ondelette **ψ** est dilatée, et si | **a** | **<1** elle est comprimée.

La CWT est donc une représentation plutôt temps échelle que temps-fréquence. Toutefois si elle est bien localisée autour d'une fréquence $\mathbf{f_0}$, une interprétation temps–fréquence est possible avec une identification formelle

$$\mathbf{f_0=f/a.} \qquad \mathbf{(3.2)}$$

Notons que la différence principale vis- à- vis de la STFT (Short Term Fourier Transform) est que lorsque « **a** » est changé, la forme de l'ondelette ne change pas, mais sa durée et sa largeur de bande changent toutes deux.

La STFT utilise la même largeur de fenêtre pour toutes les fréquences. La CWT utilise une fenêtre courte aux fréquences élevées et une fenêtre longue aux fréquences basses. Ceci permet de résoudre au moins partiellement le problème du compromis temps/fréquence. La bande passante **B** est proportionnelle à la fréquence **f**, et donc **B/F=φ** une constante. On parle de bande passante car la CWT peut être vue comme une opération de filtrage de **x** par un ensemble (banc) de filtres. La CWT est invariante par translation en temps et en échelle.

$$\mathbf{Y(t)= | a_0 |^{1/2}\ x[a_0(t-t_0)]} \qquad \mathbf{(3.3)}$$

$$\mathbf{=>\quad Ty(t, a, \psi)= Tx\ (a_0*(t-t_0), a/a_0\ ;\psi)} \qquad \mathbf{(3.4)}$$

Le signal peut être retrouvé à partir de sa transformée par :

$$\mathbf{X(t)=} \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \mathbf{Tx(s, a, \psi)\Phi s,a(t)ds\ da/a^2.} \qquad \mathbf{(3.5)}$$

Φ: est l'ondelette de synthèse.

Ceci est possible si :

$$\int_{-\infty}^{+\infty} \mathbf{\psi\ (f)\Phi^*(f)df/|\ f\ |=1} \qquad \mathbf{(3.6)}$$

2.1 Les Propriétés de La Transformée En Ondelette.

Bien que les propriétés de la transformée en ondelettes (TO) continue soient discutées et utilisées tout au long de ce mémoire, nous en rappellons ici l'essentiel sous une forme stynthétique.

- ***Linéarité***

La linéarité de la TO vient de la linéarité du produit interne

- ***Propriété de translation***

Si ***f*(x)** a pour TO continue alors la fonction translatée ***f'(x) = f(x-b)*** a pour TO.

- ***Propriété d'échelle***

Si ***f*(x)** a pour TO continue alors la fonction ***f '* (*x*) = (1/ *s*) *f* (*x* / *s*)** a pour TO

.

2.2 Transformation en Ondelettes Continue.

2.2.1 Définitions :

Les représentations temps-échelle ont été conçues pour un objectif initialement différent : si on recherche dans un signal de forme complexe une forme d'onde connue, susceptible d'avoir subi des translations en temps, et des dilatations (ou contractions) temporelles, il est naturel de rechercher une corrélation entre le signal et cette forme, dilatée et translatée. On introduit ainsi la Transformation en Ondelette Continue (TOC) :

$$C(a,\tau) = \frac{1}{\sqrt{a}} \int_{\Re} x(t).\psi\left(\frac{t-\tau}{a}\right)^{*} dt \qquad \textbf{(3.7)}$$

$$C(a,\tau) = \sqrt{a} \int_{\Re} X(f)\Psi(af)^{*}.e^{+i2\pi f\tau} df \qquad \textbf{(3.8)}$$

$$avec\ \Psi(f) = TF\left[\psi(t)\right]$$

La 1ère ligne est la définition même de la TOC, tandis que la 2ème en est une expression obtenue par l'application du théorème de Parseval. La forme d'onde **ψ (*t*)** est l'ondelettemère, ou l'ondelette analysante. On conçoit que la présence d'une forme proche de **ψ (*t*),** dilatée par un facteur ***a*** et décalée (retardée) de ***τ*** entraîne un pic de

corrélation dans le plan correspondant : c'est cette approche qui a conduit l'analyse de signaux sismique à introduire la TOC.

Cependant, la 2ème ligne de l'équation permet une interprétation spectrale de la TOC la fonction $\Psi(af)$ peut être interprétée comme la transmittance d'un filtre (donc définie par l'ondelette-mère), dilatée le long de l'axe des fréquences d'un facteur a. Cette dilatation ne doit pas être confondue avec la translation en fréquence, car elle conduit à une variation de la largeur de bande du filtre équivalent : on se trouve donc en présence d'une analyse temps-fréquence, non plus à bande constante, mais à bande relative constante. Ceci est en fait très familier à divers métiers : acoustique, analyse des vibrations, …etc. On se référera aux notions d'analyse en bande d'octave, familières dans ces domaines.

- Localisation en temps
- Localisation en fréquence
- Régularité R

$$\int_{\Re} t^r \psi(t)dt = 0 \text{ pour } r = 0,1, \ldots, R \qquad \textbf{(3.9)}$$

- Conservation de l'énergie :

$$\int_{\Re} [x(t)]^2 dt = \int_{\Re^2} |C_X(\alpha,\tau)|^2 d\alpha d\tau \qquad \textbf{(3.10)}$$

2.3 Transformation en Ondelette Discrète.

L'une des façons simples d'aborder le problème de la transformation en Ondelettes Discrète est de considérer er la discrétisation en position $\tau=k.\tau$ $k \in Z$, et en échelle $a=a_o^j$ $j= 0,1,...$. On remarque que la discrétisation en échelle est choisie en progression géométrique de pas a_o .alors que celle en position est en progression arithmétique de raison τ_o.

$$\psi(t) \rightarrow \frac{1}{a_o^{j/2}} \psi\left(a_o^{-j} t - k\tau_o\right) \qquad \textbf{(3.11)}$$

l'échantillonnage dyadique. Par contre la DWT perd la propriété d'invariance par translation temporelle :

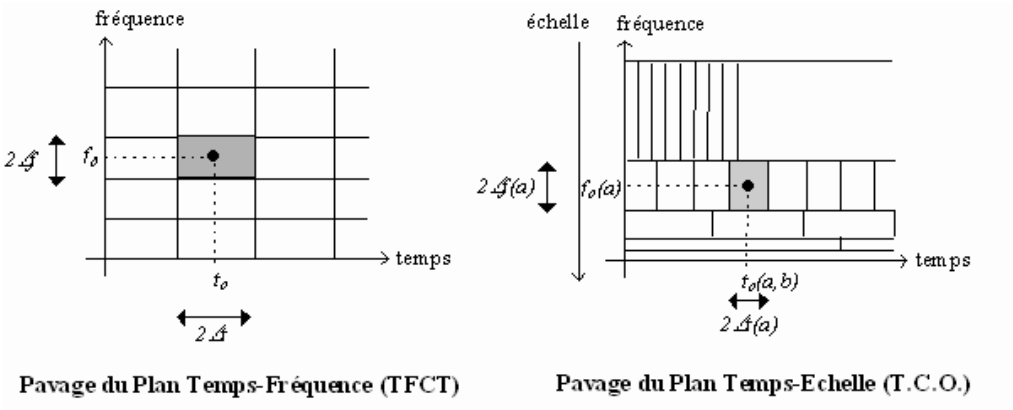


figure 3.1: *différents représentations ou partage du signal*

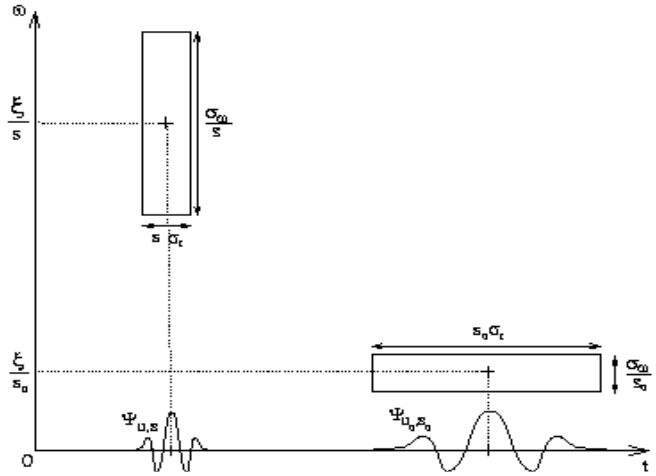


figure3.2 : *Le plan temps/fréquence et les boites d'Heisenberg*

La DWT est une projection sur un ensemble de fonctions non orthogonales. L'un des résultats majeurs de la théorie des ondelettes a été le développement de bases ortho normales d'ondelettes, avec les avantages qui en découlent.

Toutefois cette approche a été surtout appliquée dans le contexte de la compression (tout particulièrement les images), et dans celui de dé bruitage. Mais on peut bien sur utiliser une base orthonormale d'ondelettes pour l'analyse de signaux.

2.4 Quelques Exemples D'Ondelettes.

Montrons maintenant quelques exemples d'ondelettes a titre indicatif.

2.4.1 Ondelette de Haar :

Est assez classique, elle se caractérise par sa fonction d'échelle.

$$w(t) = \begin{cases} 1 & 0 \le t \le 1/2 \\ -1 & 1/2 < t < 1 \\ 0 & \text{Ailleurs} \end{cases} \qquad W(f) = je^{-j\pi f}\frac{\sin^2(\pi f/2)}{\pi f/2}$$

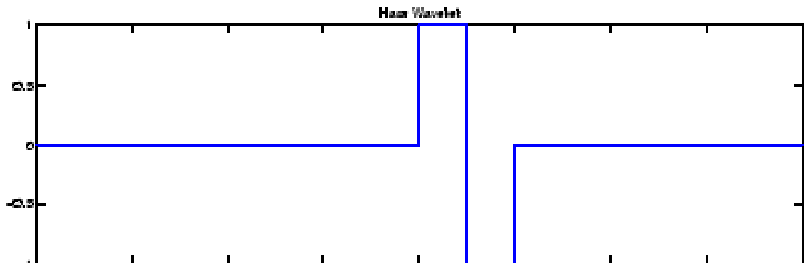


figure 3.3 : *représentation de l'ondelette de haar*

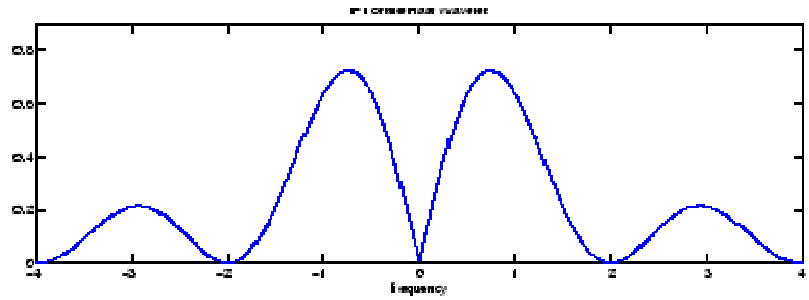


figure 3.4 *: représentation de l'ondelette de haar dans le domaine fréquentiel*

2.4.2 Ondelette de Morlet :

Est également souvent utiliser :

$$w(t) = e^{-t^2/2}\cos(5t) \qquad W(f) = \sqrt{2\pi}e^{-(2\pi f-5)^2/2} + \sqrt{2\pi}e^{-(2\pi f+5)^2/2}$$

$$\Psi(x) = \mathrm{EXP}\left(\frac{x2}{2}\right)\mathrm{EXP}(-\iota\omega ox)$$

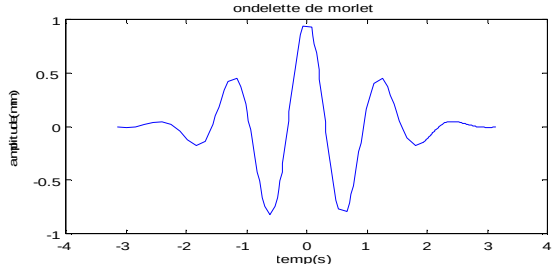


figure 3.5 :*representation de l'ondelette de morlet*

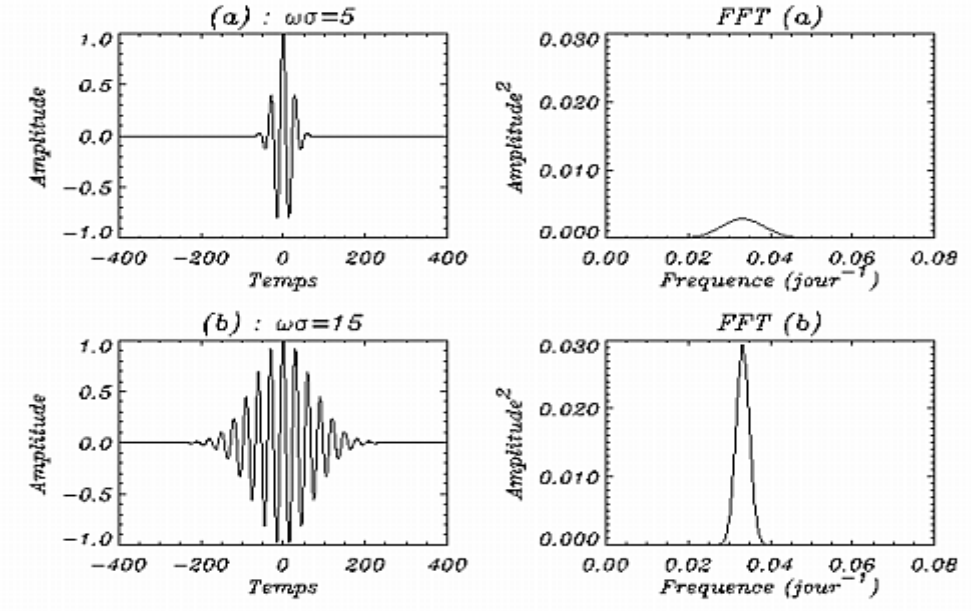


figure3.6 : *Ondelettes Morlet.*

deux ondelettes de meme periode sont répresentées, mais la largeur à demi-hauteur de la seconde et trois fois plus grande que celle de la premiere, le spectre correspondant aux ondelettes est dessiné à droits.

2.4.3 Ondelette de Mexican Hat:

$$w(t) = (1-t^2)e^{-t^2/2} \qquad W(f) = \sqrt{2\pi}(2\pi f)^2 e^{-(2\pi f)^2/2}$$

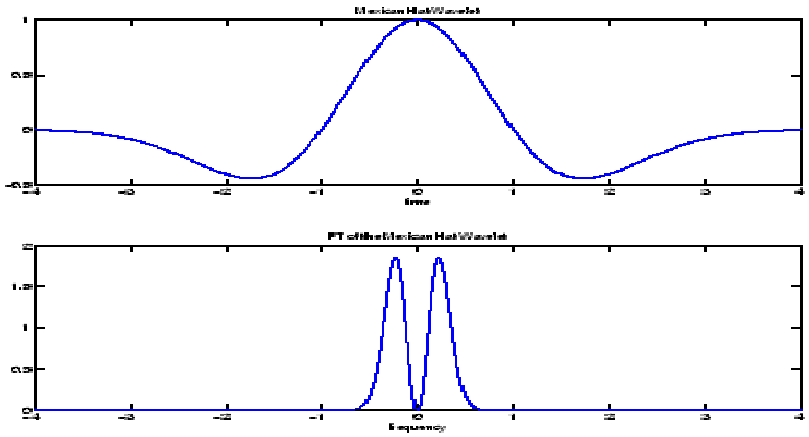


figure 3.7 *: représentation de ondelette de chapeau mexicaine dans deux domaines*

2.4.4 ondelette de Shannon :

$$w(t) = \mathrm{sinc}(t/2)\cos(3\pi t/2) \qquad W(f) = \begin{cases} 1 & .5 \le |f| \le 1.0 \\ 0 & \text{otherwise} \end{cases}$$

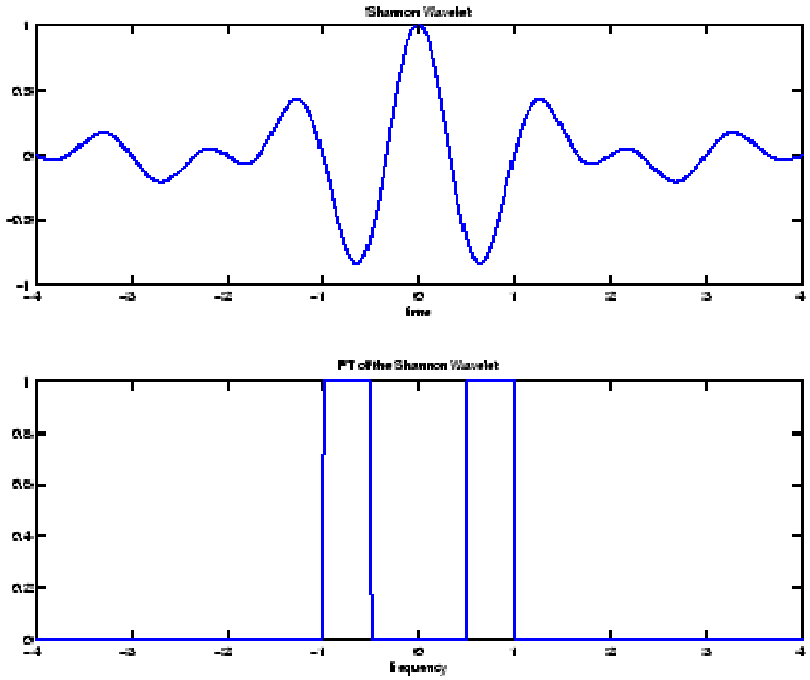


figure 3.8: *représentation de ondelette de Shannon dans deux domaines*

3. Les Ondelettes et Paquets D'Ondelettes.

La transformation en ondelettes permet l'analyse multi-résolution des signaux dans le plan temps-fréquence. Elle peut être réalisée à l'aide d'un banc de filtres octave composé de filtres passe bande avec une largeur de bande relativement constante proportionnelle à la fréquence. Ce type de filtre peut être utilisé pour la modélisation de la réponse fréquentielle des oreilles. De plus, il est aussi adopté à l'analyse de signaux constitués d'un mélange de signaux hautes fréquences de durée courte et de signaux de basses fréquences de longue durée.

La transformation en paquets d'ondelettes est la généralisation de la transformation en ondelettes. Elle permet de choisir un compromis entre la résolution fréquentielle et la résolution temporelle dans chaque sous-band. Chaque décomposition possible correspond à une base différente.

Cette transformation peut être utilisée pour l'analyse adaptative des signaux en cherchant toujours la meilleure base de décomposition. De plus, les paquets

d'ondelettes peuvent être considérés comme une alternative à la quantification vectorielle, évitant les computations complexes associées à la recherche dans le dictionnaire.

3.1 L'Analyse Multi Résolution.

Le cadre d'analyse de ces ondelettes qui s'expriment à l'aide de filtres discrets s'est considérablement développé ces dernières années, et nous disposons de tout un jeu de théorèmes reliant les propriétés des ondelettes et celles de filtres discrets. Par ailleurs, il existe plusieurs familles classiques d'ondelettes qui portent en général soit le nom de leur créateur, soit celui d'une propriété.

Les ondelettes dyadiques sont des ondelettes dont la dilatation vérifie une propriété spécifique, Cette propriété permet d'implémenter les transformées par des bancs de filters.

L'analyse multi résolution consiste à projeter le signal x sur une série de sous espaces orthogonaux de $L^2(\mathbf{R})$ (les espaces d'approximations V_i et de détails W_i). Nous verrons que la projection d'un signal sur les espaces de détails fournit sa *transformée en ondelettes discrète*. Les espaces de projections du signal sont entièrement caractérisés par la donnée de deux filtres (passe haut et passe bas). Ces filtres permettent le calcul rapide des coefficients de la transformée en ondelettes discrète via un algorithme itératif.

3.1.1 Théorie de la AMR :

- ***Définition 1*** : Une analyse multi résolution de $\mathbf{L^2(R)}$ est une suite $\{\mathbf{V_m}\}$ de sous espaces fermés de $\mathbf{L^2(R)}$ ayant les propriétés suivantes :

(1) $\cap_m \mathbf{V_m} = \{0\}$, $\mathbf{U_m}\ V_m$ est dense dans $\mathbf{L^2(R)}$ et $\mathbf{V_{m+1} \subset V_m}$

(2) Pour toute fonction $\mathbf{x(t)}$ de $\mathbf{L^2(R)}$ et tout m de $\mathbf{Z}$, $\mathbf{x(t) \in V_m \leftrightarrow x(2^m t) \in V_0}$

(3) Pour toute fonction $\mathbf{x(t)}$ de $\mathbf{V_0}$ et tout k de $\mathbf{Z}$, $\mathbf{x(t-k) \in V_0}$

(4) Il existe une fonction $\boldsymbol{\phi}\mathbf{(t)}$ de $\mathbf{V_0}$ telle que l'ensemble $\{\boldsymbol{\phi}\mathbf{(t-k)}\}_{k \in Z}$, constitue une base inconditionnelle ou base de Riesz de $\mathbf{V_0}$. C'est à dire qu'il existe

deux réels **A** et **B** avec **A > 0**, tels que : pour toute fonction **f** de V_0, $f = \sum_k g_k \phi(t-k)$, *et*

$$A\|f\|^2 \leq \sum g_k^2 \leq B\|f\|^2 \qquad \textbf{(3.12)}$$

- ***Interpretations :***

(1) Les V_m sont appelés espaces d'approximations. La première relation ($V_{m+1} \subset V_m$) traduit le fait que la projection dans V_{m+1} est une approximation plus grossière du signal que sa projection dans V_m, c'est à dire que l'information contenue dans V_m est plus riche que celle contenue dans V_{m+1}.

(2) Montre que l'on peut passer d'un espace d'approximation à un autre par changement d'échelle.

(3) Est l'invariance par translation temporelle.

(4) Montre que l'on peut engendrer V_0 par translation d'un même motif et assure la stabilité numérique de la décomposition d'une fonction sur V_0.

3.2 Ondelettes et Fonctions D'échelle.

Les Ondelette et fonctions d'échelles biorthogonales sont caractérisées par un banc de filtres à reconstruction parfaite.

La fonction ϕ est appelée fonction d'échelle car elle permet de passer d'un espace d'approximation à un autre, c'est à dire d'une échelle à une autre.

La fonction ϕ et ses versions translatées engendrent l'espace V_0. Un simple changement d'échelle, montre que les sous-espaces V_j sont engendrés par la dilatée $\phi_j(t) = \phi(2^{-j}t)$ et ses translatées. Cette famille constitue une base de Riesz de V_j. En général, on normalise ces fonctions : si $\|\phi\|^2 = 1$ alors il en est de même pour $\{\phi_{j,k}(t) = 2^{-j/2}\phi(2^{-j}t - k)\}$, les fonctions génératrices de l'espace d'approximation V_j.

Pour un signal x d'énergie finie, les coefficients d'approximations sont définis par :

$$a_x(j,k) = < x, \phi_{j,k} > \qquad \textbf{(3.13)}$$

L'approximation du signal x à la résolution 2^{-j} correspond à sa projection dans V_j :

$$A_j x(t) = \sum_k a_x(j,k)\check{\phi}_{j,k}(t) \tag{3.14}$$

3.2.1 Espaces de détails :

On définit $\{W_i\}$, les ensembles tels que :

$$W_i \oplus V_i = V_{i-1} \tag{3.15}$$

Les W_i représentent les espaces de « détails » (ce sont les complémentaires orthogonaux des espaces d'approximations). Cette construction implique directement que les W_i sont orthogonaux entre eux et que leur somme directe recouvre $L^2(\mathbf{R})$:

$$L^2(\mathbb{R}) = \oplus_{j\in\mathbb{Z}} W_j \tag{3.16}$$

En fréquence, on observe mieux la complémentarité des deux ensembles ainsi que leur finalité (basses fréquences correspondant à approximation, hautes fréquences à détail) :

Soit $f \in V_1$, soit g tel que $g(t) = f(2t) \in V_0$, alors en transformée de Fourier on a :

$$G(\omega) = \int f(2t)e^{-i\omega t}dt$$
$$G(\omega) = \frac{1}{2}F(\frac{\omega}{2}) \tag{3.17}$$

La *figure 3.3* montre la géométrie de ces espaces dans le long de l'axe des fréquences.

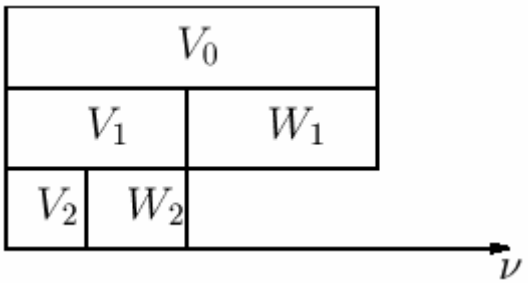


figure 3.9 : *Schéma de la géométrie des espaces de détails et d'approximations*
Relation à deux échelles

Cette relation est appelée ainsi car elle fait intervenir deux échelles distinctes dans son écriture, c'est à dire qu'elle fait le lien entre deux espaces consécutifs.

V1$\subset$**V0**, alors $\phi_{1,0} = \phi(t/2) \subset V_1$ est combinaison linéaire des $\phi(t-k)$ (base de V_0), d'où :

$$\forall l \in \mathbb{Z}, \exists g(l), \forall t \in \mathbb{R}, \phi(\frac{t}{2}) = \phi_{1,0} = \sum g(l)\phi(t-l) = g * \phi(t) \qquad \textbf{(3.18)}$$

La fonction ψ respecte aussi la relation à deux échelles : En effet, $\psi(t/2) \in W_1 \subset V_0$ est combinaison linéaire des $\phi(t-k)$.

$$\forall l \in \mathbb{Z}, \exists h(l), \forall t \in \mathbb{R}, \psi(\frac{t}{2}) = \psi_{1,0} = \sum h(l)\phi(t-l) = h * \phi(t) \qquad \textbf{(3.19)}$$

Ces relations mettent en évidence l'existence d'un filtre passe haut *h* et d'un passe bas *g* dont la donnée est équivalente à celle des fonctions ondelette et échelle.

3.2.2 *Bancs de filtres à reconstruction parfaite et algorithme à trous :*

On peut de même effectuer la décomposition du signal a_1 en un signal $\mathbf{a_2}$ et un signal $\mathbf{d_2}$; en répétant cette opération on crée un signal à basse résolution $\mathbf{a_j}$ et une suite de signaux de détails $\mathbf{d_1}$ .... $\mathbf{d_j}$.

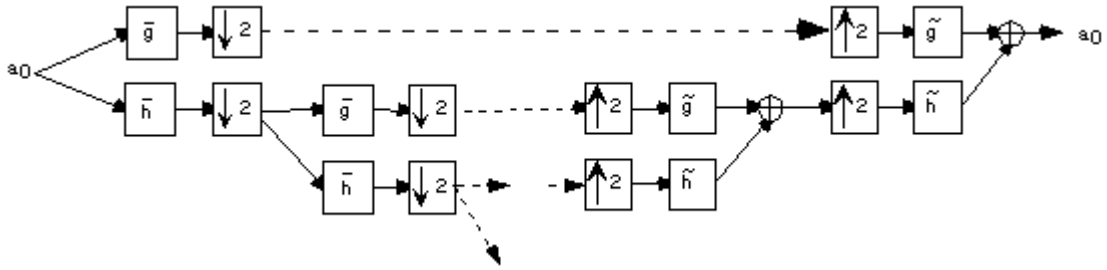


figure 3.10 : *Schéma d'un ensembles des filtres*

On peut faire une décomposition récursive analogue en utilisant l'algorithme et engendrer ainsi un signal à basse résolution $\mathbf{A_j}$ et une suite de signaux de détails $\mathbf{D_1}$ .... $\mathbf{D_j}$. Les deux décompositions sont liées par la relation suivante : deux décomposions

$$\mathbf{a_j[n] = A_j[2^j n]} \qquad \mathbf{d_j[n] = D_j[2^j n]} \qquad \textbf{(3.20)}$$

De l'algorithme à trous aux fonctions d'échelle

Dans le domaine fréquentiel, le transfert de a_0 à A_j vaut

$$\left(\prod_{p=0}^{j-1} \hat{h}(2^p \omega)\right) \quad \textbf{(3.21)}$$

Effectuons un changement d'échelle $\mathbf{T = 2^{-j}t}$ de sorte que l'intervalle entre les échantillons non nuls du filtre le plus large soit 1 quelque soit j. Alors l'intervalle entre les coefficients non nuls du filtre le plus étroit est $\mathbf{2^{-j}}$. Le transfert devient

$$\left(\prod_{p=1}^{j} \hat{h}(2^{-p} \omega)\right) \quad \textbf{(3.22)}$$

Faisons tendre j vers l'infini. Si le transfert ci-dessus converge dans L^2, alors sa limite est la transformée de Fourier d'un signal d'énergie finie qui vérifie nécessairement une équation d'échelle :

$$\phi\left(\frac{t}{2}\right) = 2\sum_{k\in\mathbb{Z}} h[k]\,\phi(t-k) \quad \textbf{(3.23)}$$

De telles fonctions sont au cœur des analyses multi résolutions, qui sont elles-mêmes à la base des ondelettes dyadiques.

3. *3* Algorithme.

Au lieu de décomposer le signal en ondelettes en le comparant à chaque échelles , aux ondelettes de tailles appropriées, on commence par étudier le signal à la résolution la plus fine, qui constitue le point de départ. On commence par séparer le signal en deux composantes : l'allure générale du signal, et l'ensemble des petits détails. L'image lisse est le signal tel qu'on le voit à la moitié de la résolution la plus fine, avec deux fois moins d'échantillons. On obtient cette image à l'aide de la fonction d'échelle

(filtre passe-bas). Les détails encodes par les ondelettes sont les retouches qu'il faut apporter à l'image lisse pour reconstituer le signal initial, on les obtient à l'aide d'un

filtre passe-haut. L'algorithme consiste à répéter la procédure à une résolution demie de la précédente tant que le signal n'a pas perdu sa substance.

4. Avantages et Applications.

Le fait que la transformée utilise des fonctions bien localisées dans le plan temps/fréquence lui donne beaucoup d'avantages.

– La résolution en fréquence de la transformée dépend du facteur de dilatation *s* par le principe d'Heisenberg, on peut donc choisir arbitrairement celle-ci suivant ce que l'on désire analyser.

– Pour des signaux physiques présentant des variations très rapides, des sauts, des marches, bref des discontinuités ; l'analyse en ondelettes est adaptée car l'ondelette va détecter ces singularités et analyser celles ci. Cette particularité rend l'analyse en ondelettes complémentaires à l'analyse de Fourier. En effet, avec cette dernière, les discontinuités d'un signal ne sont pas facilement analysables, car les coefficients des fréquences correspondantes sont étalés dans toute la transformée.

– On peut représenter complètement et efficacement un signal quelconque en peu de coefficients.

4.1 Application aux Images.

En deux dimensions, la représentation en ondelettes peut être vue de la même manière qu'une représentation en ondelettes sur chacun des axes *x* et *y* (ondelettes séparables*)*. On utilise donc une extension de l'algorithme pyramidal à une dimension. a chaque étape on décompose.

4.1.1 Algorithme pyramidal :

Nous avons vu que l'AMR d'un signal revient à le décomposer à différentes échelles, en approximations et en détails. S. Mallat [27] propose un algorithme rapide permettant de calculer les coefficients de détails et d'approximations en utilisant des filtrages et décimations successifs.

La figure 3.10 présente cet algorithme : Les coefficients de détails correspondant à l'espace $\mathbf{W_1}$ sont obtenus par filtrage passe haut (**filtre *h1***) puis décimation par 2, les approximations sont obtenues de la même manière par filtrage passe bas (**g1**). Pour

obtenir les coefficients de détails aux résolutions supérieures, il suffit de réitérer ces étapes sur les coefficients d'approximations.

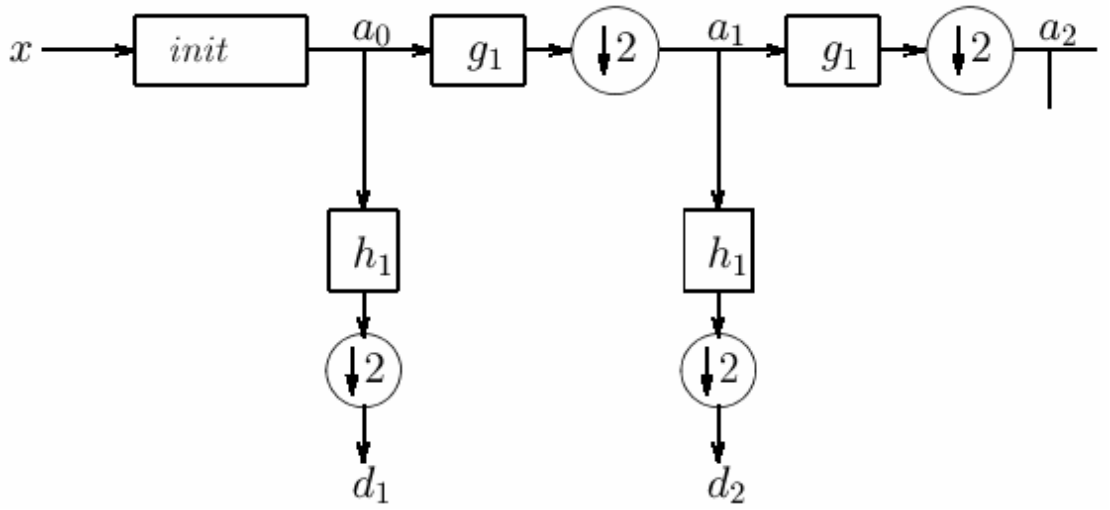


figure 3.11: *Algorithme pyramidal de Mallat où les a_i sont les coefficients d'approximation les d_i ceux de détails.*

On peut reconstruire le signal grâce à des filtres $\boldsymbol{h_2}$ et $\boldsymbol{g_2}$ selon l'algorithme présenté à la figure3.11**.** L'approximation a_n à un niveau donné n est la somme des coefficients de détails $\boldsymbol{d_{n+1}}$ et d'approximations $\boldsymbol{a_{n+1}}$ du niveau supérieur préalablement filtrés et réechantillonés.

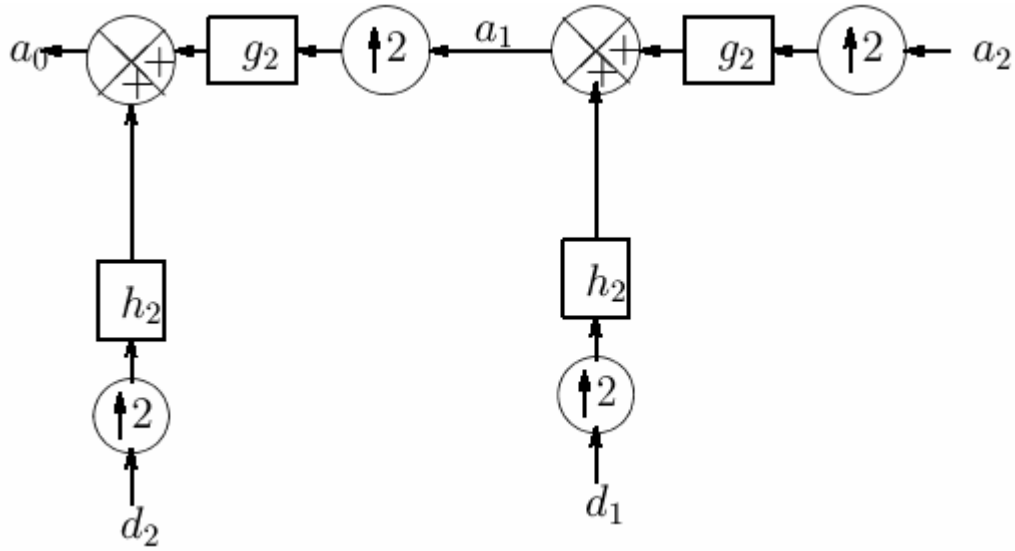


figure3.12 : *Algorithme de reconstruction du signal*

4.1.2 Filtrage par bande :

D'un point de vue fréquentiel, le signal apparaît comme décomposé suivant différentes bandes la figure 3.12 présente ce point de vue.

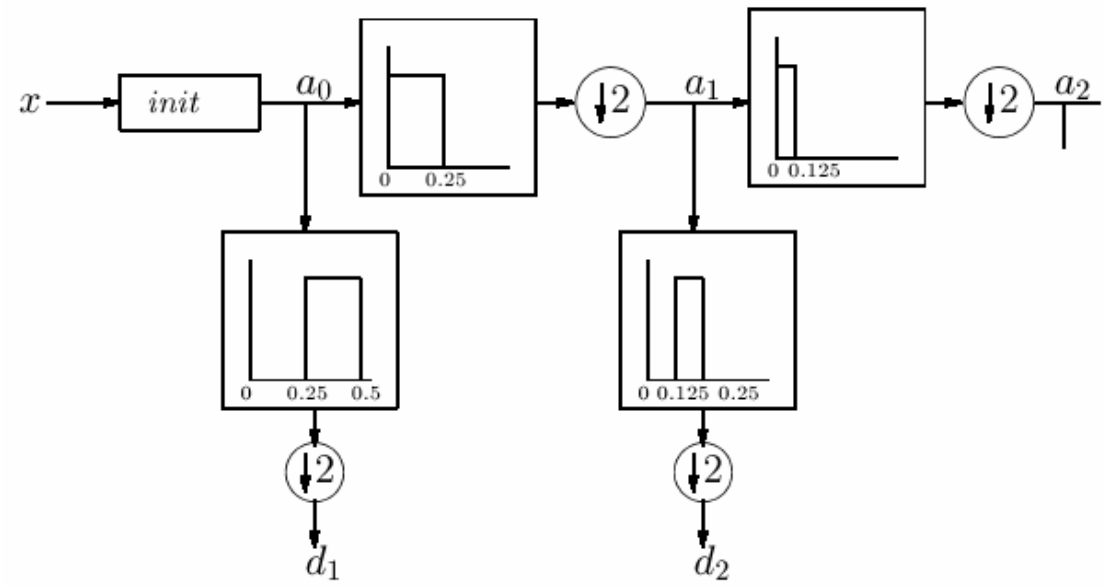


figure 3.13 : *Algorithme pyramidal de Mallat : point de vue fréquentiel*

(3.24)

$\mathbf{A^d_{2\hat{}j+1}\ f}$ **en** $\mathbf{A^d_{2\hat{}j}\ f}$, $\mathbf{D^1_{2\hat{}j}\ f}$, $\mathbf{D^2_{2\hat{}j}\ f}$, $\mathbf{D^3_{2\hat{}j}\ f}$, où:

$\mathbf{A^d_{2\hat{}j}\ f = ((f(x, y)* \phi_{2\hat{}j}(-x)\ \phi_{2\hat{}j}(-y))\ (2^{-j}n, 2^{-j}m))}$ pour (m, n) appartenant à Z^2

$\mathbf{D^1_{2\hat{}j}\ f = ((f(x, y)* \phi^j(-x)\ \psi^j(-y))\ (2^{-j}n, 2^{-j}m))}$ pour (m, n) appartenant à Z^2 **(3.25)**

$\mathbf{D^2_{2\hat{}j}\ f = ((f(x, y)* \psi_{2\hat{}j}(-x)\ \phi_{2\hat{}j}(-y))\ (2^{-j}n, 2^{-j}m))}$ pour (m, n) appartenant à Z^2 **(3.26)**

$\mathbf{D^3_{2\hat{}j}\ f = ((f(x, y)* \psi_{2\hat{}j}(-x)\ \psi_{2\hat{}j}(-y))\ (2^{-j}n, 2^{-j}m))}$ pour (m, n) appartenant à Z^2 **(3.27)**

On convolue d'abord les colonnes de $\mathbf{A^d_{2\hat{}j+1}\ f}$ avec un filtre à une dimension, on garde toutes les autres colonnes, on convolue les colonnes du signal résultant avec un autre filtre à une dimension, on retient les autres colonnes. Les filtres utilisés dans cette décomposition sont les filtres miroir en quadrature ***H*** et ***G***. On itère le procédé ci-dessus en faisant varier **j**. Ceci correspond à une décomposition en filtres miroirs conjugués séparables. Les coefficients d'ondelettes ainsi obtenus ont une grande amplitude au voisinage des contours et dans les textures selon une orientation spatiale

donnée. Les expressions (3.24)-(3.27) montrent qu'en deux dimensions $\mathbf{A^d_{2^j}}$ **f** et $\mathbf{D^k_{2^j}}$f sont calculés à l'aide de filtres séparables selon les abscisses et les ordonnées. La décomposition en ondelettes peut alors être vue comme la décomposition d'un signal en un ensemble de bandes de fréquences orientées dans l'espace. $\phi(x)$ peut être considéré comme un filtre passe-bas parfait et ψ comme un filtre passe-bande. La décomposition de $\mathbf{A^d_{2^{j+1}}}$ **f** est telle que :

- $\mathbf{A^d_{2^j}}$ **f** correspond aux basses fréquences,

- $\mathbf{D^1_{2^j}}$ **f** donne les hautes fréquences verticales (contours horizontaux),

- $\mathbf{D^2_{2^j}}$ **f** donne les hautes fréquences horizontales (contours verticaux),

- $\mathbf{D^3_{2^j}}$ **f** donne les hautes fréquences dans les deux directions (les coins),

Cette décomposition est illustrée dans la figure ci-dessous :

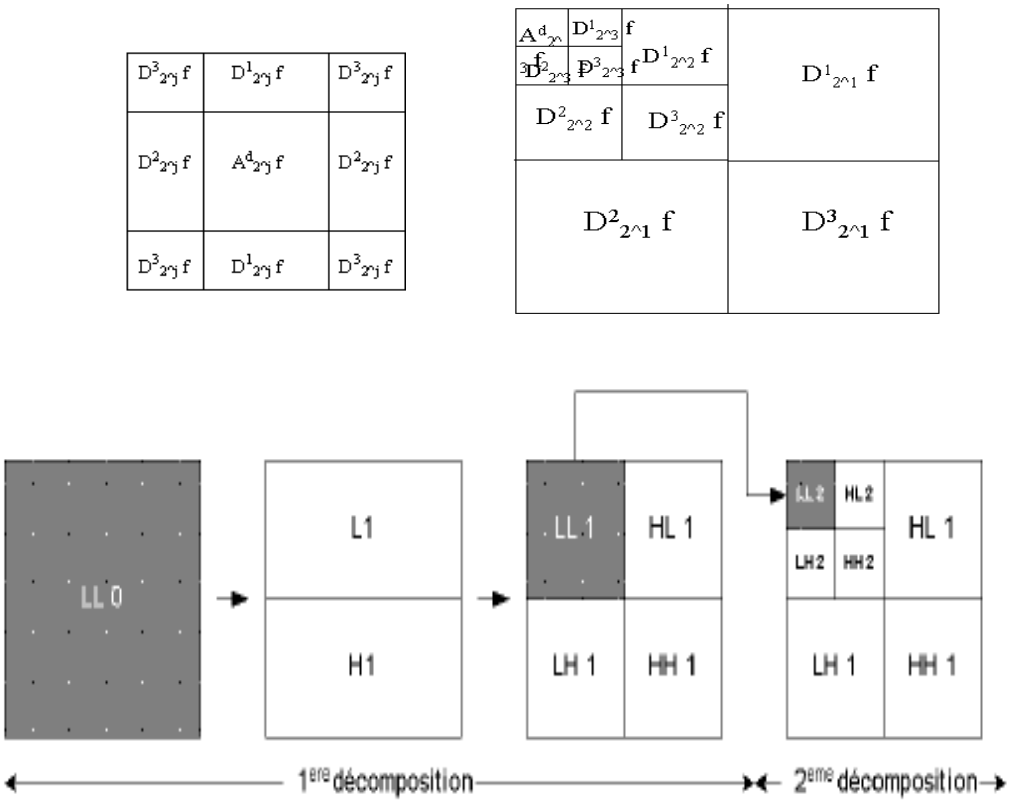


figure 3.14 : *Décomposition en ondelettes à plusieurs niveaux*

figure 3.15 : *Exemple de décomposition en ondelettes*

5. Conclusion

Dans ce chapitre nous avons présenté quelques définitions, propriétés des images numériques, et une introduction à la théorie des ondelettes classiques, puis nous avons introduit la transformée en ondelettes discrète d'un signal et d'une image. Ces ondelettes, comme nous l'avons vu, sont largement utilisées aujourd'hui dans maintes applications, non seulement en analyse d'images ou de vidéos, mais aussi dans beaucoup d'autres domaines (audio, statistiques...).Leur popularité et leur facilité d'utilisation en ont fait un outil indispensable, au même titre que l'analyse de Fourier.

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

Méthodologie adoptée

Méthode proposée

1. Introduction.

Les bases obtenues par l'application de l'algorithme exposé dans le troisième chapitre représentent des composantes significatives de l'image ondelette. Le principe de la méthode de tatouage que nous présentons dans ce chapitre consiste à modifier les valeurs fréquentielles de l'image et des pixels afin d'imposer une structure fixée par la watermarque.

Dans ce chapitre, nous allons détailler les différentes étapes du processus de tatouage d'images. Nous détaillerons ensuite les étapes d'implémentation et de détection de la marque de façon conceptuelle et schématique.

Enfin, nous allons présenter un exemple simple de l'application de notre processus en donnant quelques résultats de tatouage des images tests.

2. Objectifs.

L'objectif principal de ce travail est de trouver une méthode robuste contre les attaques permettant d'insérer une quantité d'information importante dans l'image sans pour autant la dégrader visuellement. L'accent a donc été mis sur le compromis à faire entre insérer le maximum de bits (la marque) dans l'image et à garder la marque invisible. Notre critère de référence a donc été de trouver une méthode qui résiste aux traitements d'image (filtrages, compression, rééchantillonnage, lissage …) et notamment à une compression JPEG de X % qui détériore déjà considérablement l'image.

3. Contexte.

Notre travail a été consacré au tatouage d'images et plus spécifiquement au tatouage dans le domaine fréquentiel. Ce domaine est en effet plus accessible pour un novice que peut l'être les domaines spatial ou fractal par exemple.

Il a été décidé de ne s'intéresser qu'à des images codées en 256 niveaux de gris. Ce choix est judicieux à plusieurs égards :

- Les images codées en 256 niveaux de gris sont la base de travail de la plupart des algorithmes de traitement d'images.

- Il est préférable d'obtenir des résultats sous certaines contraintes et de rendre ensuite l'algorithme générique que d'essayer d'obtenir directement un algorithme générique sans jamais y parvenir.
- Pour passer d'images codées en niveaux de gris à des images couleurs une première approche consiste à appliquer l'algorithme à la luminance des images couleurs.

4. Principe de la Méthode.

Le tatouage d'images que nous proposons suit un schéma classique d'insertion dans le domaine transformé, la détection étant effectuée en utilisant des méthodes de corrélation. Le paragraphe suivant décrit cette méthode.

4.1 Algorithmes de Tatouage ou Watermarking Proposés.

Le figure 4.1 rappelle le principe d'un algorithme de watermarking : inclure, de façon discrète, une marque dans une image, et être capable de l'extraire, même si l'image marquée est attaquée entre temps.

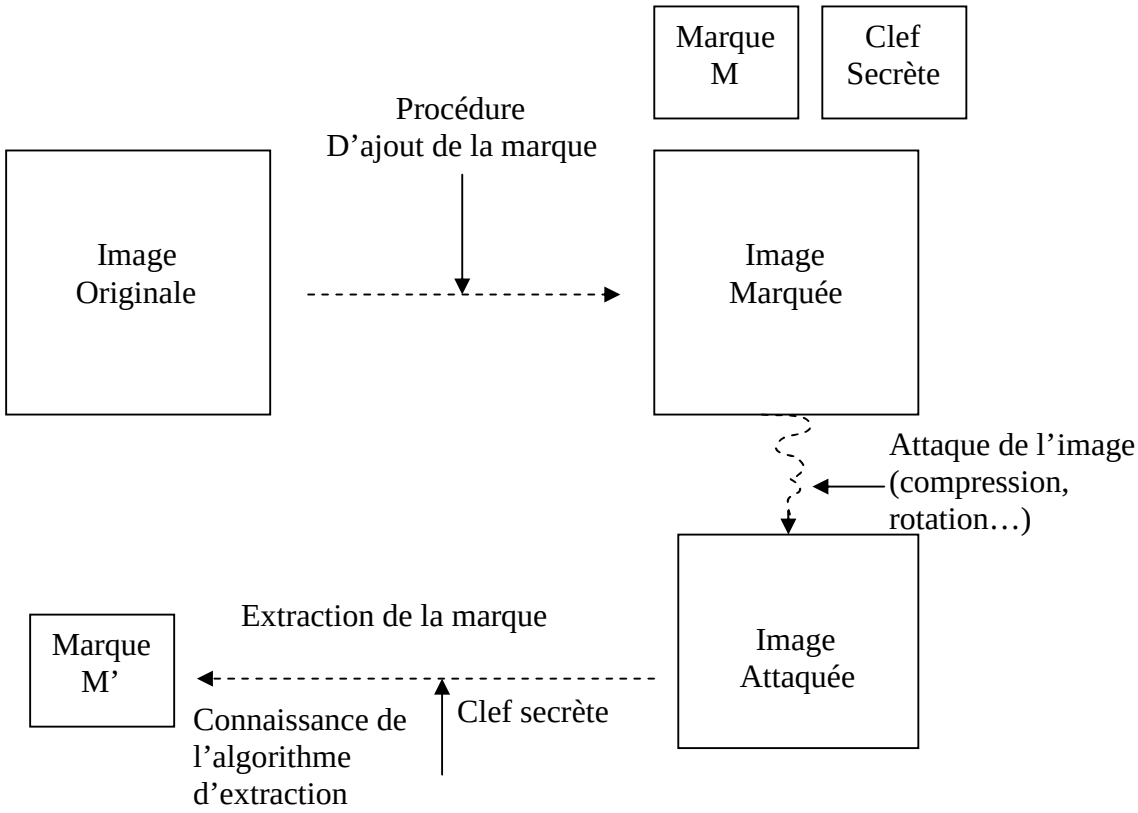


figure. 4.1 : *Principe d'un algorithme de watermarking : la marque incluse dans l'image originale, M, et la marque extraite après attaque de l'image marquée, M', doivent être aussi semblables que possible.*

Nous allons utiliser ici l'algorithme défini dans le troisième chapitre pour insérer une marque dans une image de 512x512 pixels comme référence, figure 4.2. Nous verrons également comment l'extraire, et estimerons les performances de l'algorithme.

figure 4.2 : *L'image Lena (512 x 512 Pixels)*

4.2 Tatouage par le domaine de la DWT (Discret wavelet transform).

Dans le domaine de la DWT bidimensionnel, chaque niveau de décomposition produit quatre bandes de données, une correspondante à des basses fréquences (low-pass band) (LL), et trois autres correspondent à des hautes fréquences Horizontale (HL), verticale (LH), et diagonale (HH) (high pass band), voir la figure 4.3.

L'image ainsi décomposée montre une image grossière danse le coin supérieur à gauche correspond à la basse résolution (low pass band LL), et trois images détaillées en hautes fréquences.

La bande passe bas LL peut de plus être décomposée pour obtenir d'autres niveaux de décomposition. La figure (4.4-4.5) illustre clairement les niveaux de décomposition sur l'image Lena.

<table>
<tr><td>LL2</td><td>HL2</td><td rowspan="2">HL1</td></tr>
<tr><td>LH2</td><td>HH2</td></tr>
<tr><td colspan="2">LH1</td><td>HH1</td></tr>
</table>

figure 4.3 : *Transformée en ondelette discrète (DWT) d'une image (avec deux niveaux)*

Où:

LL: low-low frequency band.

LH: low-high frequency band.

HL: high-low frequency band.

HH: high-high frequency band.

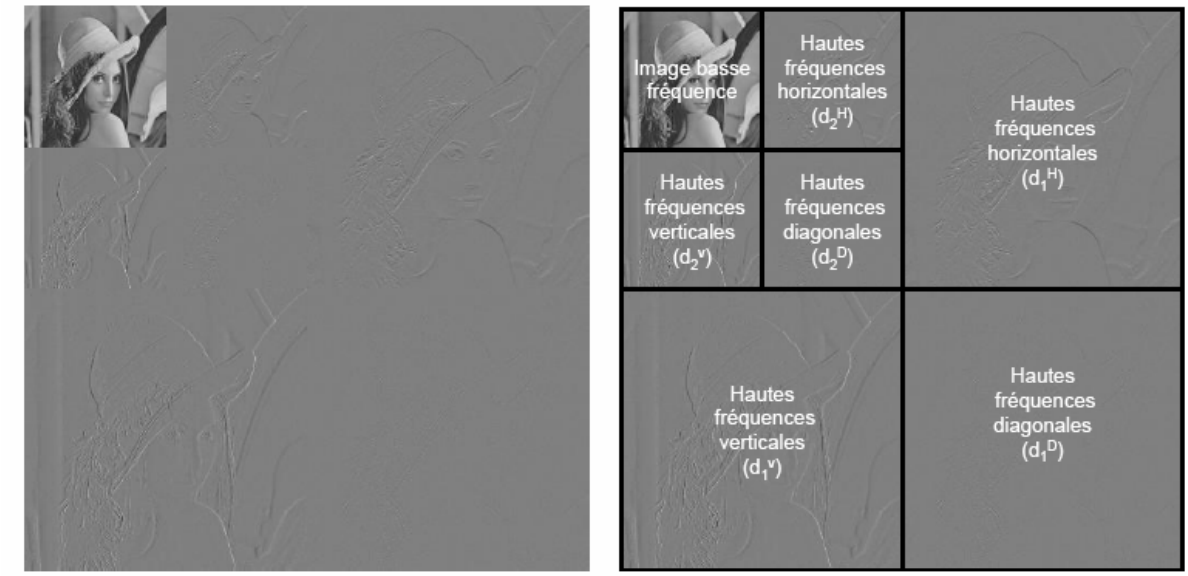


figure 4.4 : *Transformée en ondelette discrète (DWT) pour l'image Lena 512x512 pixels.*

d_1^D : détail niveau 1 hautes fréquences diagonales.

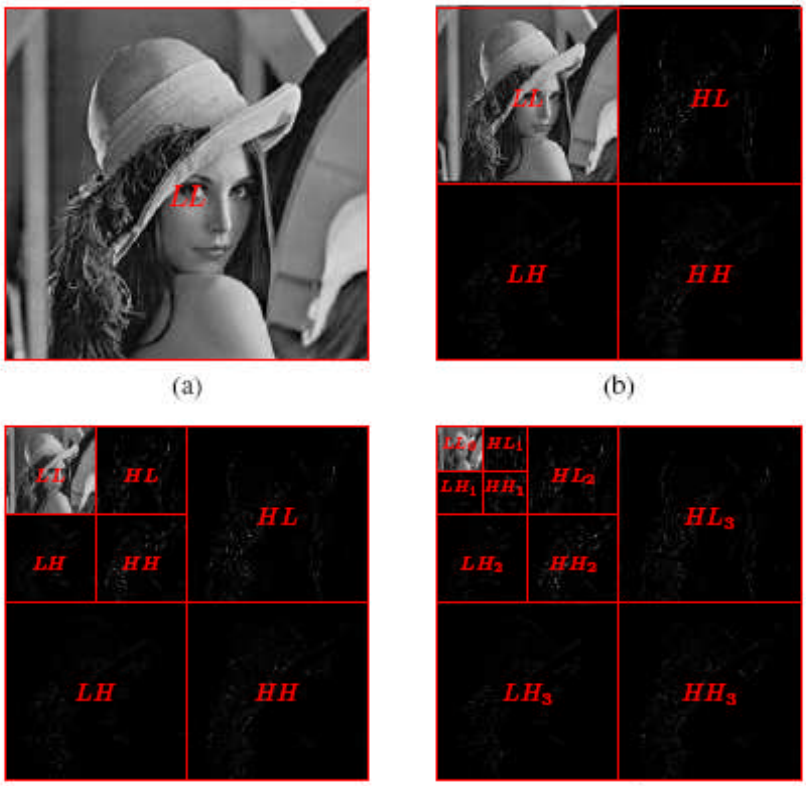
d_1^H : détail niveau 1 hautes fréquences horizontales.

d_1^V : détail niveau 1 hautes fréquences verticales.

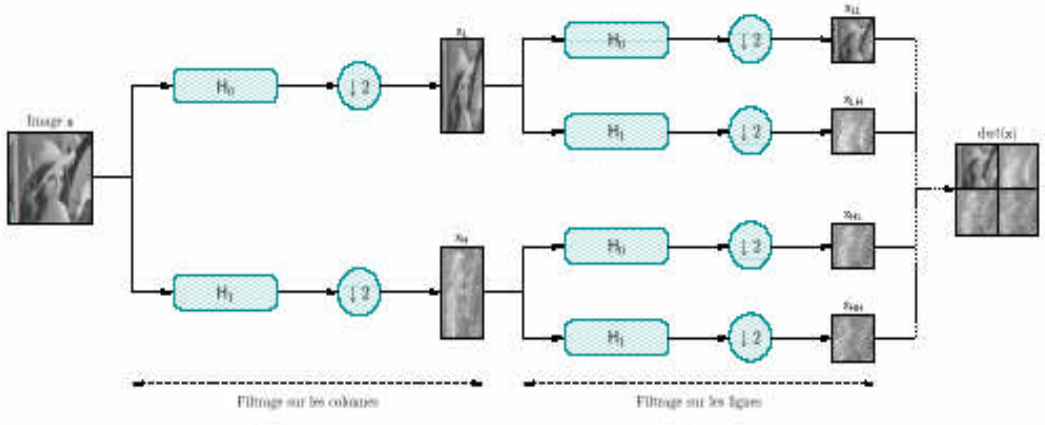
d_2^D : détail niveau 2 hautes fréquences diagonales.

d_2^H : détail niveau 2 hautes fréquences horizontales.

d_2^V : détail niveau 2 hautes fréquences verticales.



(1) Transformée en ondelettes de l'image Lena sur trois niveaux



(2) Principe de la transformée en ondelettes vue par l'approche bancs de filtres, appliqué sur une image

figure 4.5 : *Exemples de transformée en ondelettes pour l'image Lena.*

(a) représente l'image originale.

(b) décomposition en niveau 1 de l'image.

(c) décomposition en deuxième niveau de l'image.

(d) décomposition en troisième niveau de l'image.

4.3 Diagrammes du système de tatouage proposé.

4.3.1 Méthode de tatouage basée sur la DWT :

Le tatouage dans le domaine DWT peut être divisé en deux procédures : l'inclusion de la marque et l'extraction de la marque.

- **La procédure d'inclusion de la marque**

Le schéma de la figure 4.6 montre le diagramme d'inclusion de la watermark.

Dans cette partie, nous allons détailler l'algorithme (voir le tableau 4.1); l'image marquée X' résulte de l'inclusion dans l'image hôte X de la marque W.

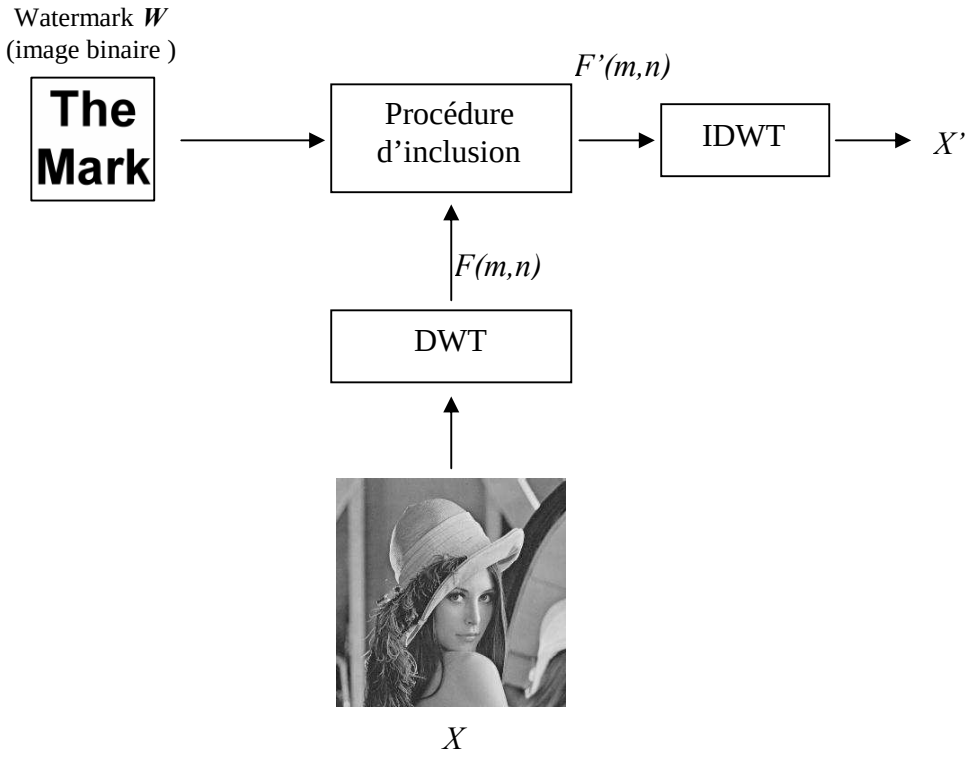


figure 4.6 *: Diagramme de la procédure d'inclusion de la marque.*

Où:

X – Image originale
X' – Image marquée

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 un seul niveau 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, LH, HL et HH), voir la figure 4.7. F(m,n) dénote les coefficients de la DWT de l'image originale. La procédure d'inclusion est performée selon la formule suivante :

$$X_{w,ij} = X_{ij}^{k} + \alpha_k W_{i,j}^{k}, \quad i,j = 1,\ldots,n/2, \text{ et } \quad k = 1,2,3,4.$$

Où α 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*).

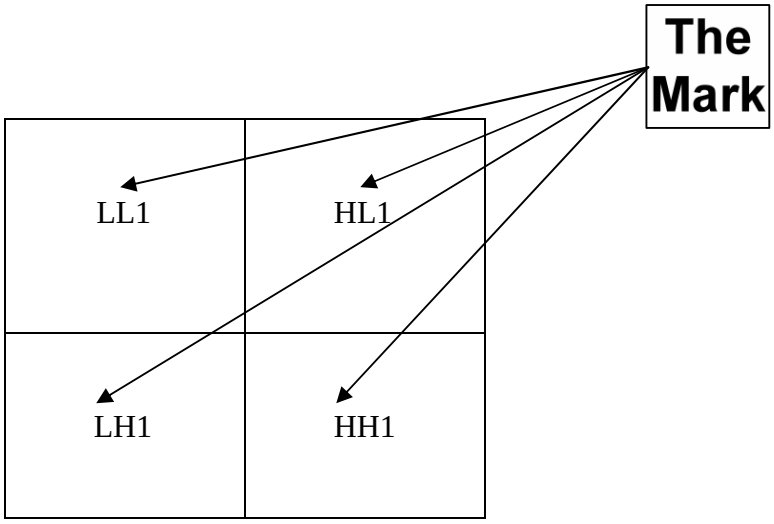


figure 4.7 : *Inclusion de la marque dans les quatre bandes fréquentielles de l'image.*

- **La procédure d'extraction de la marque**

Dans la procédure d'extraction de la marque, l'image marquée et l'image originale toutes deux décomposées en un niveau par la DWT. Il est supposé que l'image originale est connue pour l'extraction.

La procédure d'extraction est décrite par la formule :

$$w_{ij} = (X_{w,ij} - X_{\mathbf{w,ij}}^{*\mathbf{k}}) / \alpha_k, \qquad i,j = 1..n/2, \text{ et } k = 1,2,3,4.$$

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

La figure 4.8 montre le diagramme d'extraction de la marque ;

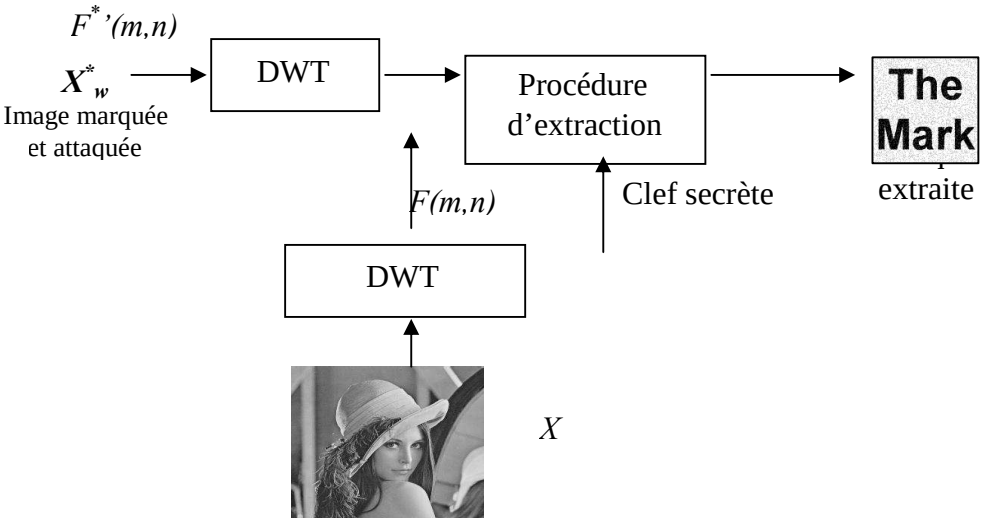


figure 4.8 : *Diagramme de la procédure d'extraction de la marque.*

Où :

X - Image originale.

X^*_w - Image marquée et attaquée.

Premier niveau de décomposition
Inclusion de la marque
Entrée : image originale, $\boldsymbol{I} = (a_{ij},\ 1 \le i,j \le n)$, et la marque sous forme d'image binaire, $\boldsymbol{W} = (w_{ij} \in \{0,1\}, 1 \le i,j \le n/2)$. **Processus :** 1. effectuer une DWT bidimensionnelle sur l'image, obtenir le premier niveau de décomposition de l'image hôte $\boldsymbol{I}$. 2. Modifier les coefficients de la DWT X_{ij} dans les bandes fréquentielles LL, HL, LH, et HH : $$\overset{k}{X}_{w,ij} = \overset{k}{X}_{ij} + \alpha_k W_{i,j}, \quad i,j = 1,\ldots,n/2, \text{ et } k=1,2,3,4.$$ 3. Appliquer IDWT pour obtenir l'image marquée, $\boldsymbol{I}_w$. **Sortie:** image marquée.
Extraction de la marque
Entrée: image marquée. **Processus :** 1. effectuer une DWT bidimensionnelle sur l'image, obtenir le premier niveau de décomposition de l'image marquée (et qui peut être attaquée) $\mathbf{I}^*_w$.

2. Extraire la marque (sous forme d'une image binaire) à partir bandes fréquentielles LL, HL, LH, et HH :

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

3. si $W_{ij} > 0.5$, alors $W_{ij} = 1$, si non $W_{ij} = 0$.

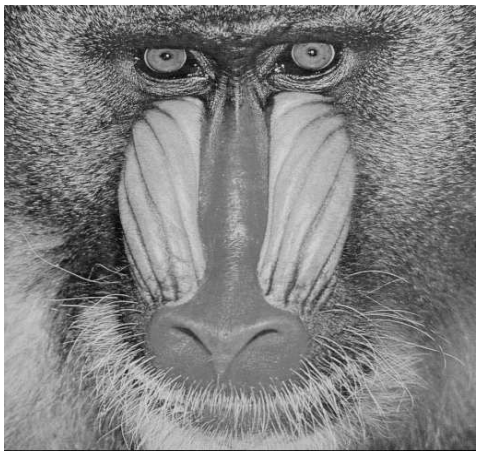
Sortie : Marque sous forme d'image binaire.

Tab. 4.1 : *algorithme de tatouage.*

4.3.2 Plateforme des tests numériques :

Nous avons effectué des tests sur un ensemble de trois images de référence: Lena, boat, mandrill. Ces images classiques sont toutes de dimension 512X512 et codées sur 8 bits par pixel. Pour pouvoir évaluer plus aisément les résultats, la signature insérée consistait en une petite image binaire constituant le sigle (copyright).

a- *Image de test « lena» de taille 512X512*



b*-Image de test «mandrill» de taille 512X512*

c- *Image de test «boat» de taille 512X512*

d- *Marque insérée de taille 20X50*

e- *Petite Marque insérée de taille 12X9*

figure4.9 : *base d'images utilisées pour les tests*

Voici un schéma simplifié pour le mécanisme de tatouage pour le deux sens, insertion et détection de la marque.

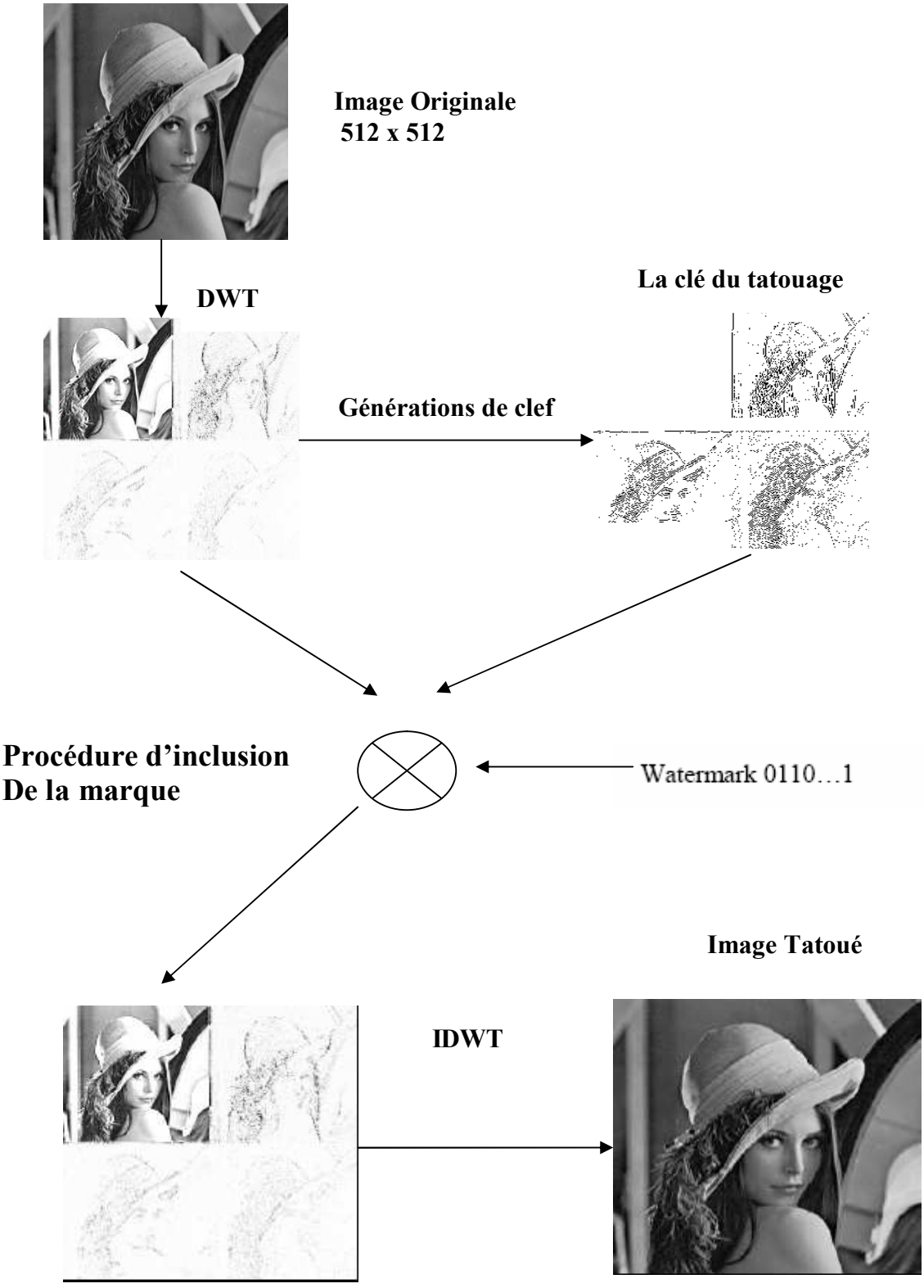


figure 4.10: *les étapes d'insertion de la marque sur l'image Lena 512x512.*

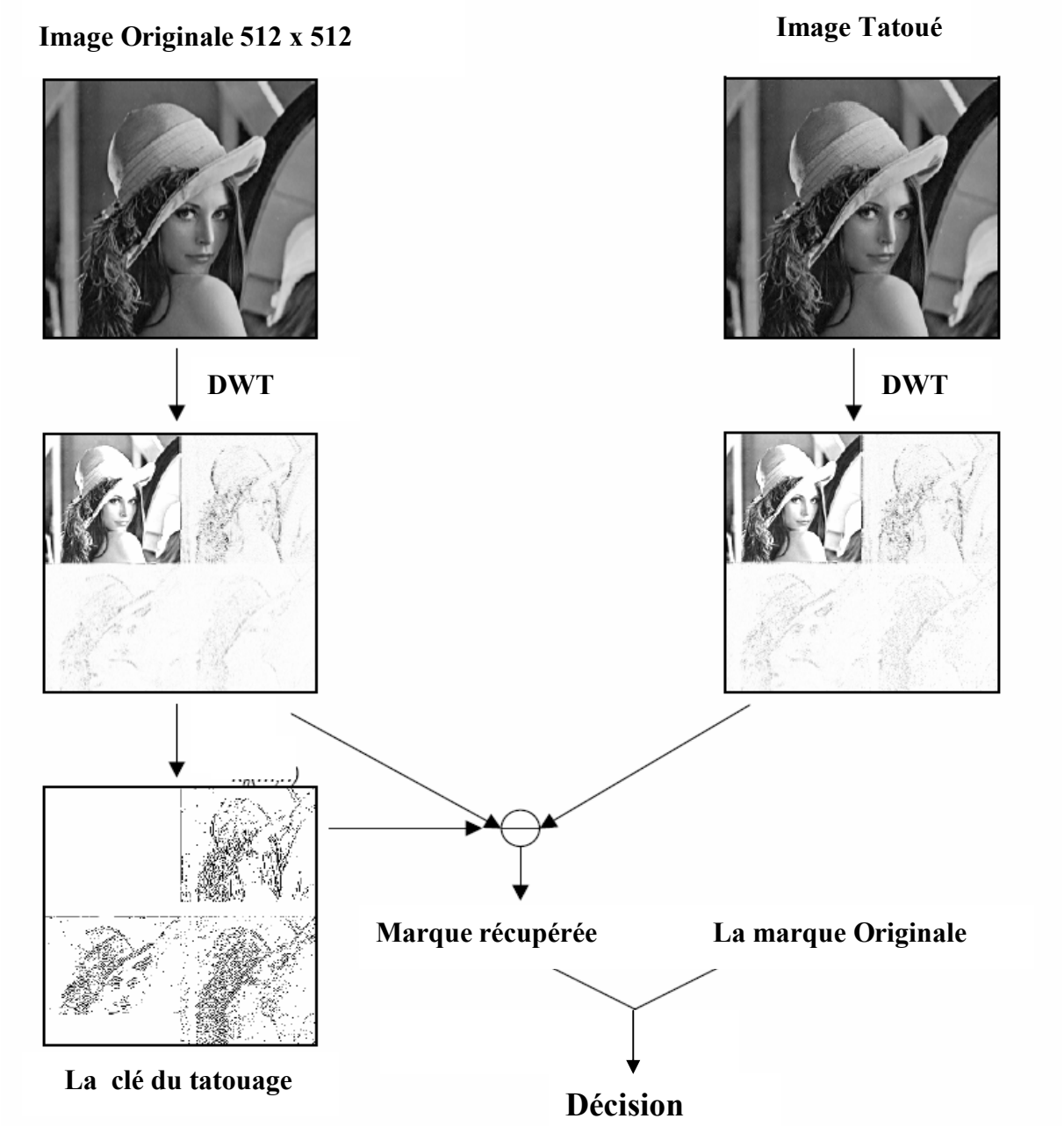


figure 4.11 :*les étapes d'extraction de la marque sur l'image Tatouée*

La phase d'extraction est duale de la phase d'insertion. On extrait ainsi une marque qui est ensuite corrélée avec la marque originale afin d'établir un score de corrélation qui permet de déterminer la présence ou la non présence de la marque.

4.3.3 Etude sur les clés en cryptographie en général :

Le tatouage est donc une technique permettant d'insérer une marque sans qu'elle soit perceptible et pouvant être extraite. Pour cela il est indispensable d'utiliser une clef privée et/ou publique exactement comme dans le cas du chiffrement et du déchiffrement.

Crypter ne se justifie que relativement à l'existence d'attaquants ou cryptanalystes dont le travail est plus ou moins difficile.

L'objectif de l'attaque c'est de trouver la clé. C'est plus fort que trouver le clair associé à un chiffré donné, puisque la donnée de la clé fournit la possibilité de calculer tous les clairs associés à tous les chiffrés. On considère qu'une attaque est efficace si elle a une probabilité non négligeable de réussir en un temps inférieur ou égal à quelques années (voir plus !) sur une plusieurs machines puissantes.

4.3.3.1 Les méthodes de cryptographie actuelle :

4.3.3.1.1 Le chiffrement actuel :

Le chiffrement est l'action de transformer une information claire, compréhensible de tout le monde, en une information chiffrée, incompréhensible. Le chiffrement est toujours associé au déchiffrement, l'action inverse. Pour ce faire, le chiffrement est opéré avec un algorithme à clé publique ou avec un algorithme à clé privée.

4.3.3.1.2 Les algorithmes à clé privé ou à clé secrète :

Les algorithmes à clé privée sont aussi appelés algorithmes symétriques. En effet, lorsque l'on crypte une information à l'aide d'un algorithme symétrique avec une clé secrète, le destinataire utilisera la même clé secrète pour décrypter.

Le marquage symétrique signifie que l'on utilise la même clef pour insérer et détecter le tatouage.

4.3.3.1.3 Les algorithmes à clé publique :

En effet, les algorithmes à clé publique sont aussi appelés algorithmes asymétriques. C'est à dire que pour crypter un message, on utilise la clé publique (connue de tous) du destinataire, La clef de marquage et celle de détection sont différentes Outre l'intérêt immédiat (n'importe qui peut lire la signature sans pour autant pouvoir l'enlever ou la modifier), ces techniques récentes sont plus sécurisées Elles portent officieusement le nom de « marquage de seconde génération ».

4.3.3.1.4 La préparation au cryptage :

Une information de type texte, ou n'importe quel autre type d'information a besoin d'être codée avant d'être cryptée à l'aide d'un algorithme à clé publique ou privée. En

d'autres termes, il faut fixer une correspondance entre une information et un nombre, puisque les algorithmes à clé (publique ou privée) ne peuvent crypter que des nombres. Le problème se résout facilement, puisque la plupart du temps, ce type de cryptographie est essentiellement utilisé sur des machines. Et comme de toute façon les informations sur une machine sont une suite de nombres, le problème est déjà très simplifié.

4.3.3.2 Les Méthodes basées sur les registres LFSRS :

Un système de chiffrement à clef secrète à flot (par opposition aux chiffrements par blocs) consiste à additionner bit à bit au texte clair une suite aléatoire de même longueur, appelée suite chiffrante. Ce système assure une sécurité parfaite sous la condition que la suite chiffrante soit une suite complètement aléatoire de la même taille que le message à chiffrer. Cependant, comme il n'est en général pas envisageable de partage une clef secrète qui soit aussi longue que le message à chiffrer, on utilise dans la pratique une ***suite pseudo aléatoire*** générée de façon déterministe à partir d'un secret commun court qui, lui, peut être échangé plus facilement.

Une méthode classique pour générer une suite binaire pseudo aléatoire est d'utiliser un registre à décalage à rétroaction linéaire (**LFSR** pour *Linear Feedback Shift Register*).

Un **LFSR** de longueur L est composé d'un registre à décalage contenant une suite de L bits $(s_i,\ldots,s_{i+L-1})$, et d'une fonction de rétroaction linéaire : $s_{i+L} = c_1\, s_{i+L-1} + c_2\, s_{i+L-2} + \ldots + c_L\, s_i$.

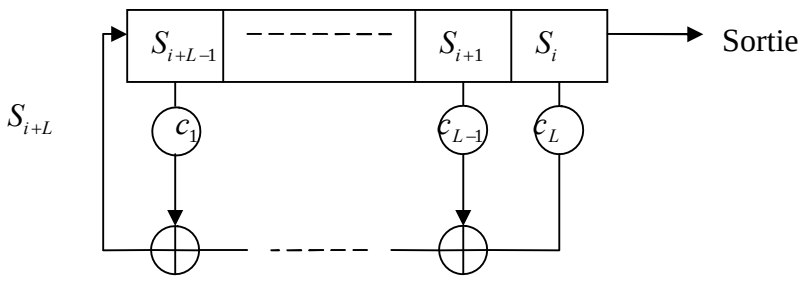


figure 4.12 : *le registre à décalage à rétroaction linéaire LSFR*

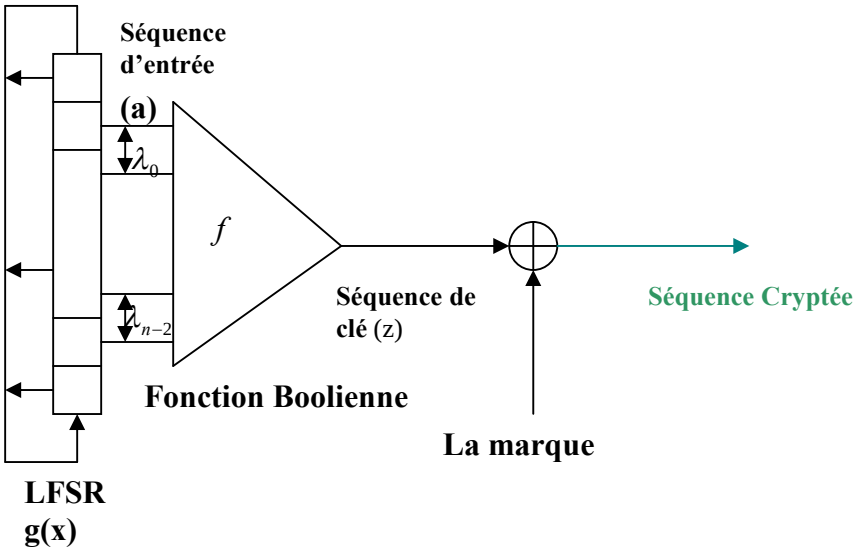


figure 4.13 : *système de générateur d'un clef LSFR*

4.3.4 Évaluation des algorithmes du tatouage :

4.3.4.1 Qualité :

L'efficacité d'un algorithme de tatouage d'images est jugée sur sa capacité à résister aux attaques mais aussi sur l'invisibilité de la marque. Cependant il est assez difficile de pouvoir quantifier numériquement la visibilité d'une marque. Pour remédier à ce problème, la première idée est de calculer le rapport signal à bruit PSNR : Le PSNR quantifie l'intensité de la marque. Cependant il s'adapte aux caractéristiques de l'image.

Mesure de la qualité d'une image (PSNR) :

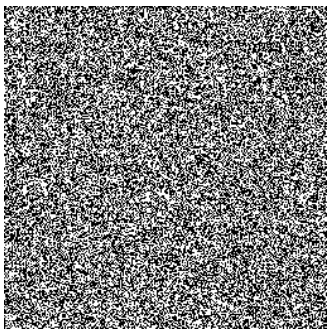
$$(PSNR)_{dB} = 10\log_{10}(MN \max_{m,n} I_{m,n}^2 / \sum_{m,n}(I_{m,n} - \tilde{I}_{m,n})^2)$$

Où I(m,n) est la valeur du pixel (m,n) de l'image référence et Ĩ(m,n) celle de l'image à tester, les deux images étant de taille [M x N] .

Avec le seul PSNR comme juge, on ne peut donc différencier les deux images.

a- image originale Lena 512*512

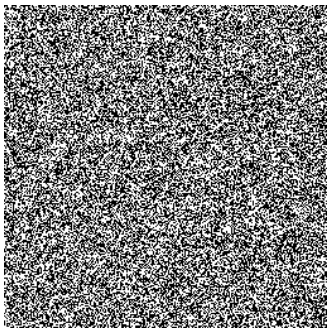
b- image Lena tatouée



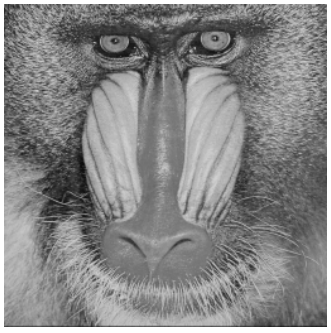
c-la différence avant et après tatouage Amplifier par facteur 20

a- image originale boat 512*512

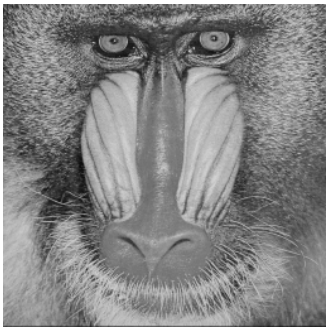
b- image boat tatouée



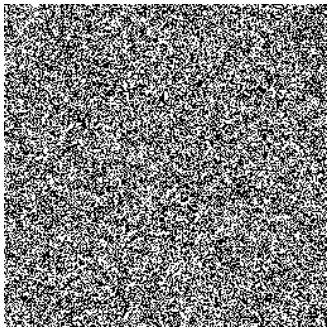
c-la différence avant et après le tatouage Amplifiée par un facteur de 20.



a- image originale mandrill 512*512



b- image mandrill tatouée

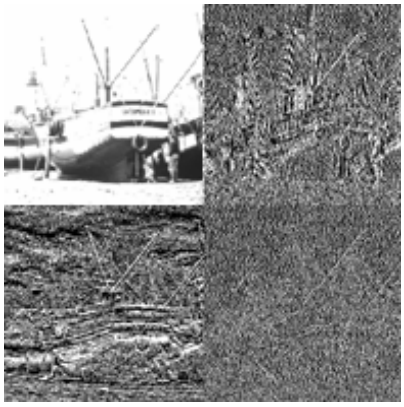


c-la différence avant et après le tatouage Amplifiée par un facteur 20

figure 4.11 : *résultat de la méthode pour filtre haar dans le niveau 1 entre deus images (a) image originale 512*512, (b) image tatoué et (c) la différence amplifier.*

a- image décomposé par DWT sur niveau 1 pour Lena 512* 512

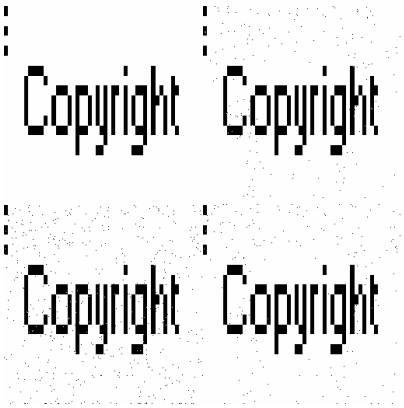
b- les marques extrais de chaque composant de l'image Lena (message256*4)



a- image décomposé par DWT sur niveau 1 pour boat 512* 512

b- les marques extrais de chaque composant de l'image boat (message256*4)

a- image décomposé par DWT sur niveau 1 pour Mandrill 512* 512



b- les marques extrais de chaque composant de l'image Mandrill (message256*4)

figure 4.12 : *résultat d'extraction de la marque avant l'attaque.*

Image	PSNR (dB)		
Résolutions	**512*512**	**256*256**	**128*128**
Lena	**42.34**	**42.20**	**42.06**
Boat	**42.14**	**42.28**	**42.04**
Mandrill	**41.80**	**41.60**	**40.85**

Tab. 4.2 : *Mesure du PSNR pour chaque image tatouée pour différent résolutions.*

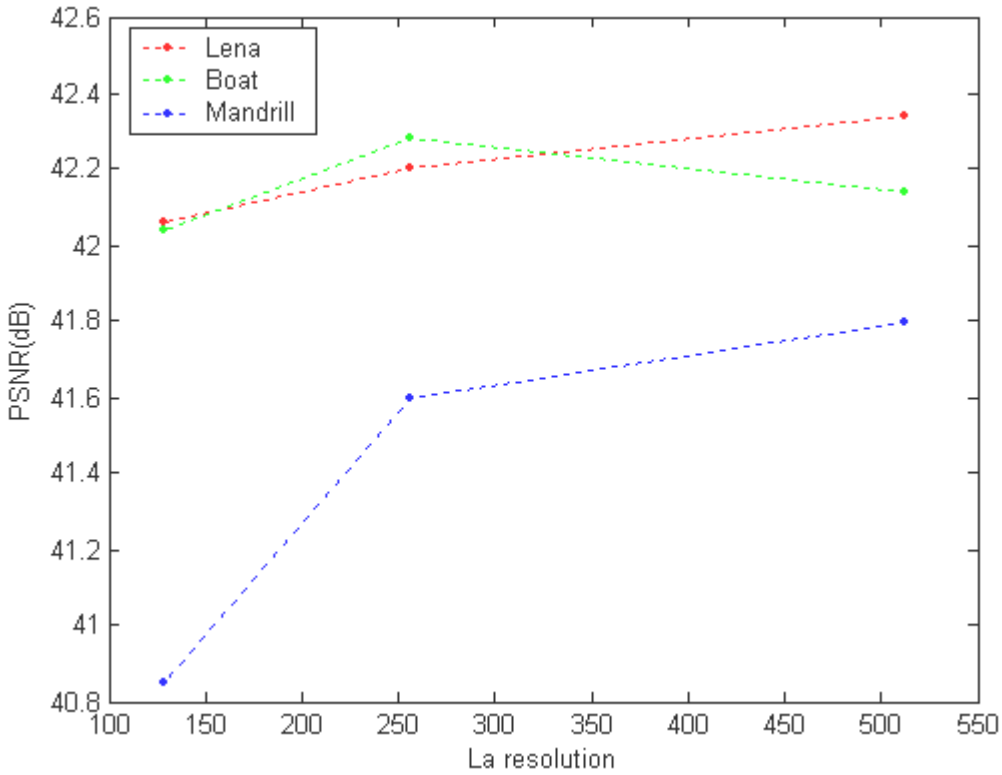


figure4.13 *: les courbes de PSNR en fonction de la résolution pour des images tatouées avant l'attaque.*

Nous avons effectué le calcul selon le tableau **Tab.4.2** c'est-dire 3 nœuds **(**512, 256, 128) qui représente différents taille ou résolution d'image pour savoir le rapport bruit signale PSNR en

fonction de la taille et plusieurs type d'image, l'image de Lena et Boat sont proches l'un de l'autre mais le rapport bruits signal grande devant l'image de Mandrill.

5. Seconde méthode de tatouage.

Ici, nous appliquons l'algorithme de tatouage sur l'image de Lena, sur plusieurs niveaux et avec différents types de filtres. La figure 4.14 montre le système de tatouage pour différentes couches de bandes de fréquences (2 couches) et l'insertion et la détection de la marque.

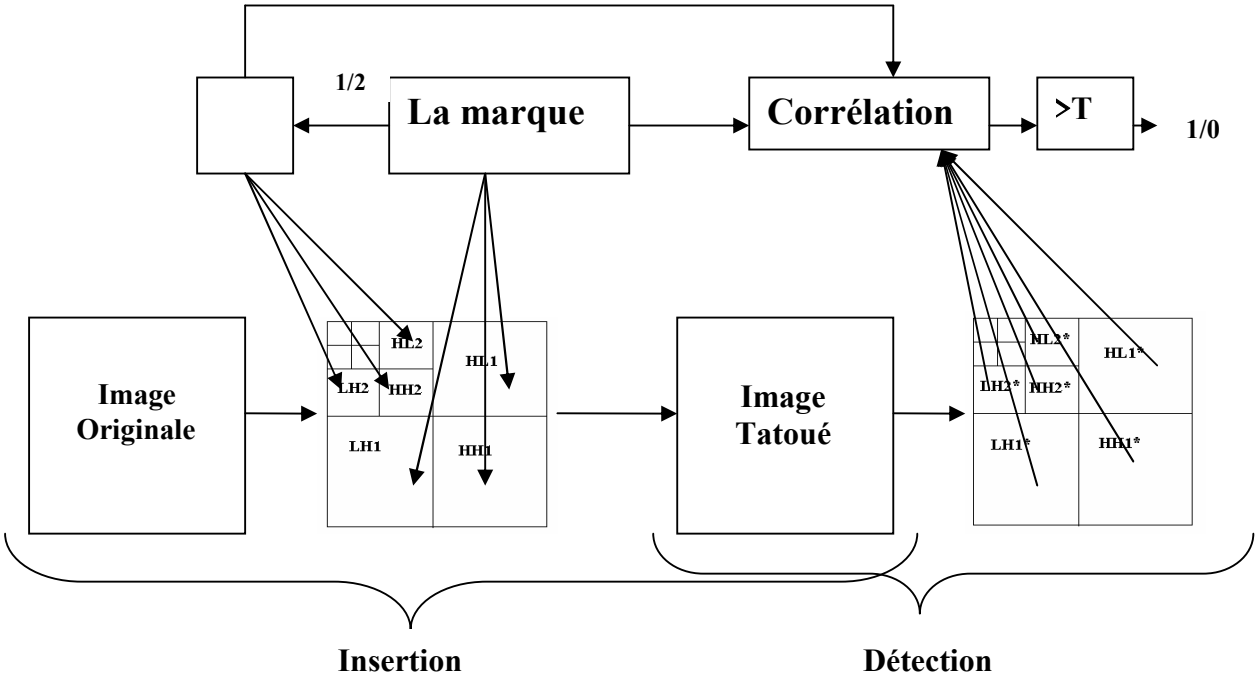


figure 4.14 : *Deuxième algorithme de marquage par la méthode de DWT*

Deuxième niveau de décomposition
Inclusion de la marque
Entrée : image originale, **I** = (a_{ij}, $1 \le i,j \le n$) , et la marque sous forme d'image binaire, **W** = ($w_{ij} \in \{0,1\}$, $1 \le i,j \le n/2$). **Processus :** 1. effectuer une DWT bidimensionnelle sur l'image, obtenir le premier niveau de décomposition de l'image hôte **I**. 2. effectuer une DWT bidimensionnelle sur les coefficients de la bande LL1 obtenir le deuxième niveau de décomposition de l'image hôte **I** 2. Modifier les coefficients de la DWT X_{ij} dans les bandes fréquentielles, HL1, LH1, HH1,LL2 , HL2, LH2 et HH2 : $X^{k}_{w,ij} = X^{k}_{ij} + \alpha_k W_{i,j}$, $i,j = 1,\ldots,n/2$, et k=1,2,3,4.

3. Appliquer IDWT pour obtenir l'image marquée, $\mathbf{I}_w$.

Sortie: image marquée.

Extraction de la marque

Entrée: image marquée.
Processus :
1. effectuer une DWT bidimensionnelle sur l'image, obtenir le premier niveau de décomposition de l'image marquée (et qui peut être attaquée) $\mathbf{I}^*_w$.
2. Extraire la marque (sous forme d'une image binaire) à partir bandes fréquentielles LL2, HL2, LH2, HH2, HL1, LH1, et HH1 :

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

3. si $W_{ij} > T = 0.5$, alors $W_{ij} = 1$, si non $W_{ij} = 0$.

Sortie : Marque sous forme d'image binaire.

Tab 4.3 : *système de tatouage de second algorithme*

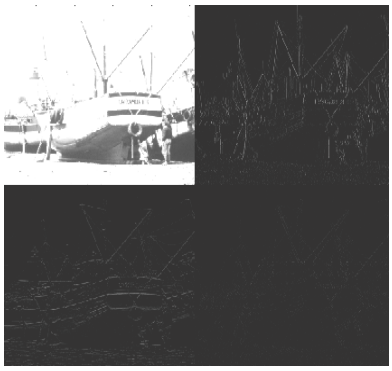
5.1 Décomposition en deux niveaux.

*a- image Lena 512*512*

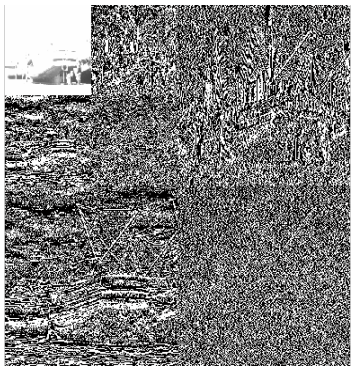
b-décomposition par dwt à 1 niveau

c- décomposition par dwt à 2niveaux

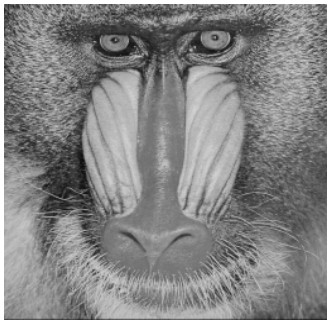
*a- image Boat 512*512*



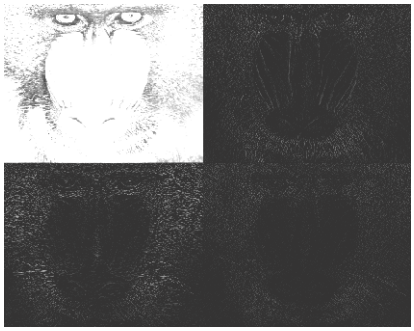
b-décomposition par dwt à 1 niveau



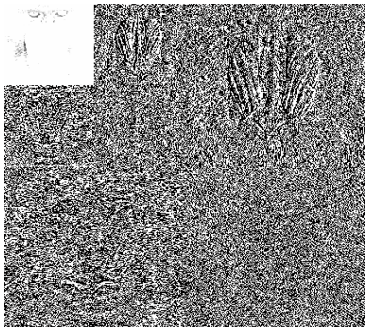
c- décomposition par dwt à 2 niveaux



*a- image Mandrillt 512*512*



b-décomposition par dwt à 1 niveau



c- décomposition par dwt à 2 niveaux

figure 4.15 : *des images résultats de la méthode DWT avec ondelette Haar par passage de niveaux*

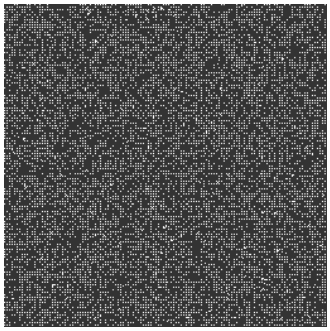
Image	**PSNR (dB)**
Lena 512*512	**50.86**
Boat 512*512	**50.57**
Mandrill 512*512	**50.20**

Tab. 4.4 : *Mesure du PSNR pour chaque image tatouée pour différentes images de la même taille après la marquage et avant l'attaque.*

5.2 La différence entre deux images :

a- image originale Lena 512*512

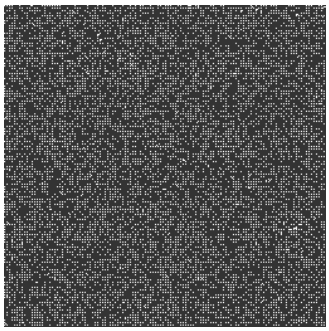
b- image Lena tatouée dans le niveau 2 de dwt



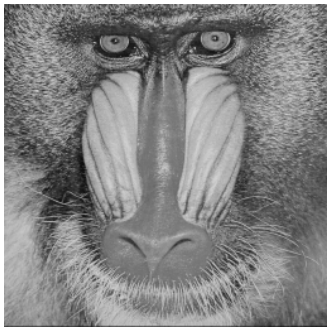
c-la différence avant et après le tatouage Amplifier par facteur 20

a- image originale Boat 512*512

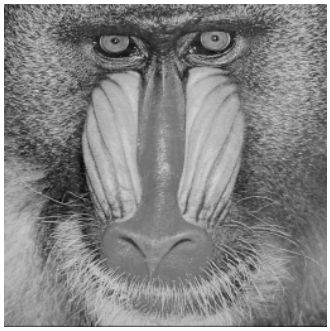
b- image Boat Lena tatouée dans le niveau 2 de dwt



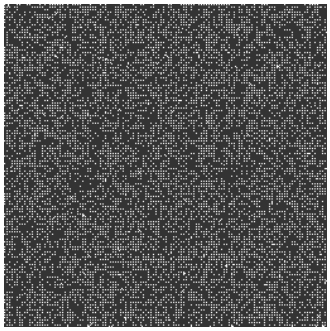
c-la différence avant et après le tatouage Amplifier par facteur 20



a- image originale Mandrill 512*512



b- image Boat Lena tatouée dans le niveau 2 de dwt



c-la différence avant et après le tatouage Amplifier par facteur 20

figure 4.16 : *résultat de la méthode pour filtre haar dans le niveau 2 entre deus images (a) image originale 512*512, (b) image tatoué et (c) la différence amplifier.*

6. Conclusion.

Dans ce chapitre nous avons mis l'accent sur les méthodes de tatouage à base des ondelettes. Nous avons mis en œuvre une technique permettant d'insérer des marques dans le domaine transformé et ceci pour une ou plusieurs bandes. L'évaluation de cette technique sur des images testes, de plusieurs natures et de résolutions, a permis de mettre en évidence son efficacité et aussi ses limites. Plusieurs critères ont été utilisés pour cette validation comme par exemple le PSNR. Cependant, dans ce chapitre nous avons tenté d'évaluer les performances de la méthode de tatouage sans prendre en compte les éventuelles attaques. En effet, le problème majeur de ces techniques est les attaques. Généralement, ces marques, qui sont la preuve de l'appartenance d'une donnée à une personne, peuvent subir des dégradations irréversibles si la donnée est attaquée. Ces attaques peuvent être volontaires, par une personne tierce malintentionnée, ou involontaire comme dans le cas d'une compression indispensable lors d'une transmission ou un stockage ou encore des bruits perturbateurs dus aux canaux ou aux capteurs …etc.

Il est donc indispensable de vérifier la robustesse de ces techniques de tatouage vis-à-vis d'éventuelles attaques. L'objectif du chapitre suivant est donc la vérification de la robustesse de la technique proposée quant aux attaques. Nous nous sommes limités essentiellement aux quelques attaques involontaires (bruits et compression JPEG) compte tenu de leurs effets et leur large présence.

Cinquième Chapitre

LES ATTAQUES

1. Introduction.

Pour être robuste, l'algorithme de tatouage doit permettre de pouvoir retrouver la marque du propriétaire dans l'image tatouée dans tous les cas, même si celle-ci a subi des attaques malveillantes de la part de pirates. On distingue plusieurs cas d'attaques qui ont toutes comme objectif d'empêcher la bonne détection de la marque. Les attaques tiennent une place très importante dans le cahier des charges d'un processus de tatouage puisqu'elles définissent la robustesse d'un système. Une façon simple de classer les attaques serait de quantifier les dégradations qu'elles font subir à l'image. Ceci permet de vérifier directement que le cahier des charges est respecté. Nous avons vu ci-dessus les problèmes posés par la caractérisation de la qualité d'une image. Nous n'avons pas pour le moment de critère assez performant pour classer les Attaques de cette façon . Classiquement, on peut séparer les attaques de la manière suivante. La transformation usuelles de l'image comme la compression, ne visent pas forcément à attaquer le tatouage, ce sont des attaques non-intentionnelles. Le deuxième groupe d'attaques est constitué des attaques (génériques) qui ne visent pas un algorithme en particulier. Le troisième ensemble concerne les attaques ciblées sur une méthode de tatouage déterminée. Enfin, les dernières attaques invalident les protocoles associés au tatouage, comme par exemple l'attaque de l'impasse.

Une autre idée est d'étudier les attaques selon l'étape du tatouage qu'elles mettent en défaut. En effet, si des pirates tentent par exemple d'enlever la marque, c'est l'étape d'implémentation qui est visée. Ils peuvent aussi vouloir invalider le marquage, en noyant par exemple le message dans du bruit, c'est alors l'étape de détection qui est visée. Nous allons maintenant détailler certaines de ces attaques et donner si possible des solutions pour leur résister.

2. Traitement d'Images.

Ces attaques cherchent à estimer l'image originale à partir de l'image marquée, en lui appliquant divers traitements :

filtrages, compressions, échantillonnage, requantification, lissage, manipulation d'histogrammes, conversion analogique/numérique. Langelaar et al. [33] ont par exemple proposé une méthode qui successivement appliquait à l'image un filtrage médian, un filtrage passe-haut et une troncature non-linéaire pour faire disparaître la

marque. Voloshynovsky et al. [34] ont au contraire cherché à estimer la marque par la méthode du maximum à posteriori
(MAP) pour ensuite la retrancher à l'image marquée.

3. Les Attaques et Leurs Classifications.

A l'heure actuelle; la plupart des attaques s'attaquent au signal lui-même pour retires la marque ou en ajoutant une sur marque qui va masquer la première et les attaques moins courantes, il s'agit de déterminer des informations sur les clés à partir des images marquées ces attaques suivent le modèle des attaques courantes en cryptologie.
On distingue principalement deux types d'attaques : celles liées au signal, et les attaques cryptographies.

3.1 Les Attaques Géométriques.

Ces manipulations malveillantes ne cherchent pas à ôter la marque mais plutôt à la désynchroniser ou à la déplacer pour qu'elle ne soit plus détectable. On peut citer les opérations de réduction, compression, d'agrandissement, de fenêtrage, les translations ou encore les rotations. Le logiciel Stirmark [35] combine ces différentes opérations et jusqu'à maintenant aucun schéma de tatouage ne résiste à cette attaque. Le logiciel Unzign [36] effectue des modifications de pixels (déplacement, suppression et/ou duplication de lignes et colonnes) qui est très efficace sur les schémas concernant le domaine spatial, dans ce type d'attaque on distingue deux types de calasse selon la position de l'attaque. Le tableau 5.1 donne une classification des diverses attaques selon cette distinction.

Attaques sur l'implémentation	Attaques sur la détection
cropping	applications affines
filtrage	ajout de bruit
compression	jitter attack
débruitage	passage à l'analogique
moyennage	Stirmark
impasse	Unsign
	mosaïque
	collusion
	surmarquage
	copiage
	fausses alarmes naturelles

Tab5.1 : *Classifications des attaques.*

***Symétrie horizontale :** Certaines images peuvent être "flipper" sans perdre de leur sens (par exemple un paysage). Bien qu'il ne s'applique qu'à peu d'images, lorsqu'il se produit, très peu de marquages lui survivent. Ce serait une grave erreur de penser que l'on ne peut pas appliquer ce genre d'attaque à un film. En effet, essayez vous même de regarder un film qui a subit cette transformation, et vous ne vous apercevrez de rien du tous (sauf dans les scènes ou de l'écriture intervient).

***Rotation :** C'est une transformation qui est très utilisée après avoir (intervient scanné une image. Elle sert à réaligner des images (avec des petits angles) et peut être fatale à certains types de marquages.

***Le recadrement :** Dans certains cas, les personnes ne sont intéressées que par un morceau de l'image (par exemple le centre). Elle recadre (en anglais "crop") alors l'image, ce qui peut détruire le marquage.

***Changement d'échelle :** Ce genre de transformations peuvent être séparées en deux groupes : les transformations uniformes (pour lesquelles on conserve les proportions, l'échelle en X varie comme l'échelle en Y) et bien sûr les transformations non uniformes (où l'échelle en X ne varie pas comme l'échelle en Y)

***Transformations géométriques:** On se contente de faire un mélange de rotations, changements d'échelles non uniformes.

***Filtres passe-bas :** Encore une fois, on utilise pour travailler dans l'espace des fréquences de l'image et dans on ne laisse alors passer que les basses fréquences. En fait, dans des termes un peu plus mathématiques, il ne s'agit ni plus ni moins que d'un produit de convolution du signal (ici l'image) avec une fonction passe bas (dont la transformée de Fourier est une Gaussienne, une fonction porte …etc.).

***Accentuation des contours :** Ou encore appellé filtre "passe-haut" (car il supprime les basses fréquences), ou "*Sharpen*". Il s'agit de l'inverse du filtre passe-bas (encore appellé "*Blur*"). L'intérêt d'une telle attaque est assez faible, sachant que l'on conserve le bruit (et les forts gradients de l'image), et que c'est souvent à ce niveau la que se situe le tatouage (car c'est dans ces zones ou l'on cache de préférence de l'information).

***Attaque par Mosaïque:** Il s'agit ici d'utiliser le "*crop*" d'une façon beaucoup plus violente et qui se prête assez bien aux pages HTML. Il suffit de découper l'image en autant de morceaux que l'on désire (plus il y a de morceaux plus l'attaque à des chances d'aboutir), puis de recoller cette image au moment de l'affichage en créant par

exemple en HTML un tableau dont chacune des cellules contiendra un morceau de l'image. Cette attaque est très peu applicable en pratique, et heureusement car elle est d'une rare efficacité si l'on se donne les moyens de bien découper l'image.

3.1.1 Les Attaques du Processus d'Implémentation de La Marque :

Faire le cropping d'une image consiste à en extraire un morceau. Pour être résistant à ce type d'attaque, le tatouage doit être présent sur toute l'image. La même situation se produit dans le domaine fréquentiel de l'image où la marque doit être partout présente afin d'éviter une destruction par filtrage passe bande.

Les algorithmes de compression sont particulièrement dangereux pour les processus de tatouage puisque leur objectif est exactement l'opposé de celui du tatouage. On veut en effet, par l'utilisation de ces algorithmes ne garder de l'image que les composantes essentielles à leur compréhension (une marque invisible n'est évidement pas essentielle).

C'est pourquoi Cox et al [37] proposent d'insérer la marque dans des endroits (perceptuellement significatifs) de l'image. Ces lieux de marquage seront souvent choisis directement dans les domaines transformés utilisés par les algorithmes de compression.

La marque insérée dans l'image ressemble souvent à du bruit, c'est donc tout naturellement que les pirates appliquent au document marqué des méthodes classiques de débruitage (filtres de Wiener, filtre de Kalman, estimation du maximum a posteriori, ondelettes, multifractal) pour lui retrancher l'estimée de la marque. Sous certaines conditions, le signal résultant sera proche du signal original. Ces attaques par cropping, filtrage, compression et débruitage font parties des attaques dites non-intentionnelles. Si un pirate utilise l'une d'elles, la principale dificulté qu'il rencontrera sera qu'il ne pourra pas savoir (ne disposant pas de la clef de détection) si cette attaque est une réussite.

Des méthodes plus complexes cherchent à retirer _chirurgicalement_ la marque du signal tatoué. Cette opération peut être très facile dans un cas particulier : si l'implémentation de la marque ne dépend pas de l'image. Dans ce cas, un pirate possédant plusieurs images différentes contenant la même marque pourra enlever celle-ci. En effet, un simple moyennage des images donnera une estimée de la marque, qu'il pourra alors retrancher aux images tatouées. Cette situation peut par

exemple avoir lieu si l'on marque une séquence de film. On imposera donc que l'étape d'implémentation de la marque soit dépendante de l'image, on dira que le tatouage est statistiquement imperceptible.

3.1.2 Les Attaques du Processus de Détection de La Marque :

Une attaque très simple et très dangereuse pour la plupart des schémas de tatouage consiste à désynchroniser la transmission du document. Dans cette attaque, la marque est décalée, le détecteur ne la retrouve pas aux endroits attendus et conclut à l'absence de la marque. Pour la protection des images digitales, cette désynchronisation se fait la plupart du temps par le biais d'applications affines, telles que la translation ou la rotation.

Nous verrons dans le chapitre suivant, lorsque nous détaillerons les différentes méthodes existantes, les remèdes à cette attaque. Le passage du numérique à l'analogique avec retour au numérique constitue une attaque intéressante car c'est le moyen le plus evident de détourner des données payantes (chaînes de télévision à péage ...). Cette opération est souvent considérée comme composée de l'ajout d'un bruit et d'une attaque appelée en anglais jitter attack consistant à enlever des lignes et des colonnes et à en dupliquer d'autres.

Ces attaques bien que dangereuses n'ont pas été créees intentionnellement pour invalider le tatouage. Dans le logiciel Stirmark [35], il existe une attaque appelée du même nom qui consiste à appliquer des petites déformations géométriques invisibles sur l'image. Ces déformations désynchronisent le détecteur qui ne retrouve plus la marque (bien que celle-ci soit présente). Unsign [36] est un logiciel dont seuls les exécutables sont disponibles sur Internet, il permet également d'effectuer des déformations invisibles sur l'image afin de craquer une marque.

Une autre attaque proposée dans [38] permet d'invalider la détection sans pour autant supprimer la marque. Cette attaque utilise le fait qu'on ne peut pas tatouer d'images de trop petite taille. Un pirate appelé Bob vole une image appartenant à Alice2 afin de la mettre sur son site Internet. Il décompose cette image en petites imagettes qu'il accole en mosaïque sur sa page Internet. Un utilisateur visitant le site de Bob verra l'image globale portant le tatouage d'Alice mais un robot traqueur équipé d'un détecteur ne reconnaîtra pas la watermarque. Cette attaque très simple est imparable.

L'attaque dite de collusion a lieu lorsque plusieurs utilisateurs sont en possession du même document portant différentes watermarques. La mise en commun de ces documents permet de nombreuses opérations : moyenne, recherche de propriétés statistiques communes dans différents domaines, recherche d'informations sur la localisation de la marque... Décrivons une attaque par moyenne : l'image résultante de la moyenne des images tatouées en circulation aura la même qualité que ces dernières. Elle contiendra toutes les marques, leurs amplitudes étant fortement diminuées. La détection sera alors perturbée à la fois par cette baisse d'amplitude et de possibles interférences entre les marques. L'attaque par surmarquage consiste à tatouer à nouveau une image déjà tatouée.

Pour certains schémas, en particulier si les lieux de tatouages sont fixés, cette attaque peut être très dangereuse. Certains protocoles de tatouage se protègent en vérifiant, avant de distribuer une clef, que l'image originale proposée n'est pas tatouée. Cette protection n'est utile que si le schéma de tatouage demeure inconnu. En effet, s'il est connu, un pirate peut ajouter une marque de sa fabrication qui invalidera la détection.

L'image ne lui appartiendra pas (le tiers de confiance n'étant pas le distributeur de la clef) mais le pirate possédera une version non tatouée de l'image. Les protocoles se protégeant en distribuant uniquement des clefs pour les images non tatouées ne respectent donc pas le principe de *Kerckhoffs*. C'est le cas du processus de tatouage public de *Digimarc* [39]. De plus cette protection peut être contournée. C'est le principe d'une attaque [38] visant particulièrement l'algorithme de tatouage de *Digimarc.* Dans celle-ci, les pirates commencent par contourner l'interdiction au surtatouage : une image est dégradée jusqu'à ce que l'on puisse la surtatouer (la première watermarque n'étant plus lisible). On ajoute à l'image originale l'image ainsi surtatouée (en diminuant son amplitude pour que les dégradations n'apparaissent plus). L'image résultante porte alors les deux tatouages, mais le détecteur n'en lit qu'un, le nouveau : le pirate s'est donc approprié l'image. L'attaque par copiage consiste à recopiesur une image non marquée. Le détecteur validera alors la nouvelle image comme étant tatouée. Cette attaque s'applique naturellement aux problèmes d'intégrité, puisqu'elle rend possible la présentation de faux qui seront authentifiés par le détecteur.

Un schéma de détection recherche un motif (la marque) présent dans l'image. Ce motif est soit implanté dans la donnée de façon licite (c'est le but de l'étape

d'implémentation), soit de façon illicite comme pour l'attaque de copiage ou d'impasse, mais il peut aussi arriver que ce motif soit présent (à l'état nature) dans une image originale. Les fausses alarmes naturelles déclenchées ainsi sont statistiquement très nombreuses et représentent un vrai problème pour l'intégrité des schémas de tatouager une marque obtenue préalablement (par exemple par estimation).

3.2 Les Attaques Cryptographiques.

Ces attaques s'inspirent largement du domaine de la cryptographie et en utilisent ses principes. Par exemple la plupart des schémas de tatouage utilisent des clés secrètes uniquement connues du propriétaire ; pour être en parfaite sécurité il est donc déjà nécessaire d'avoir à sa disposition un jeu de clés conséquent. Une autre manipulation utilise une méthode de collusion et de moyennes statistiques : le principe est de faire une moyenne de différentes images marquées. Plus le nombre d'images sera grand et plus on aura de chances de faire disparaître la marque.

3.3 Autres Attaques.

D'autres attaques ne cherchent pas à détruire la marque mais au contraire ont pour but de fausser l'identification du propriétaire. Craver et al. [40] proposent d'insérer une autre marque dans l'image marquée dans le but de créer un litige lors de l'authentification du propriétaire : deux personnes sont alors en droit de revendiquer la propriété du support numérique.

D'autre part**,** Kutter et al. [41] proposent d'estimer une marque sur l'image marquée par des méthodes de prédiction connues (*MAP, Wiener …*), et d'ensuite insérer cette marque sur une image tampon (*Watermark Copy Attack*). Le but est toujours de créer un litige lors de l'authentification du propriétaire : en effet lors de la confrontation avec le propriétaire, le pirate pourra répondre que le logiciel de détection retrouve la marque sur beaucoup d'autres images qui n'appartiennent cette fois qu'au pirate.

4. Choix des Attaques.

Les attaques utilisées sont les transformations présentes dans notre travail, pour plus de détailles, elles sont présentées dans ce chapitre, mais on utilise la compression d'image comme choix d'attaque, c'est une attaque majore (non intentionnelle), elle modifiée le contenu de l'image, donc est une attaque directements sur la marque qui

rendre plusieurs méthodes de tatouage spatial plus fragile même dans le tatouage en transformer comme la DCT.

4.1 Compression d'Image.

La compression d'image est l'une des branches de cette discipline que s'set emparée de la plus grand part des attaques sur l'image, elle couvre des domaines d'applications variés depuis les images numériques diffusées dans l'internet et dans les medias numériques de stockage massive jusqu'au HDTV (HIGH Définition Télévision) , notre algorithme de travail proposée à l avantage majeur qui est la protection d'image contre la compression numérique non intentionnelle.

5. Résultats et discussion.

Robustesse à la compression JPEG, une attaque non intentionnelle :

Le tatouage de l'image Lena, par exemple, résiste à des compressions JPEG même pour des taux de compression élevés. Cependant, pour toutes les images utilisées dans nos tests, le tatouage est suffisamment robuste pour des taux de compression moyens. La figure 4.14 présente l'image Lena obtenue après une compression JPEG de 1%, 3%, 7%, 10%, 20%, 50%, 70%, 100% de qualité.

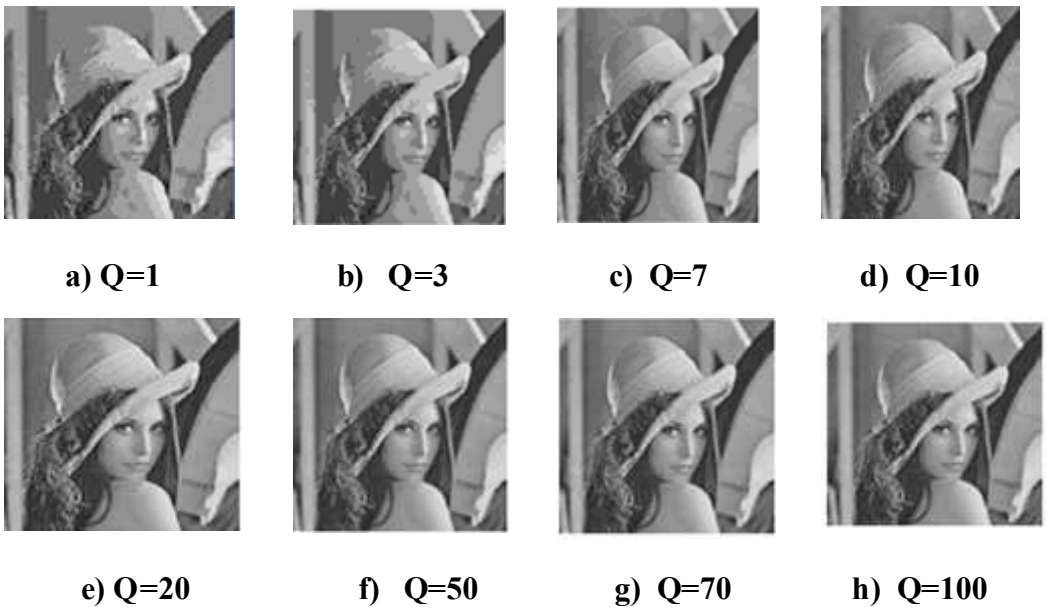


figure5.1 *: les images de Lena 512*512 tatouée et compressé par différents taux de compression*

Après une attaque par compression jpeg nous avons extrait le message caché dans les 4 bandes de l'image Lena (LL, HL, LH, HH), figure 5.2. Les figures a, b, c, d, e, f, g et h représentent les message s extraits pour plusieurs qualités de compressions. Nous remarquons que dans la bande (low low) LL le message est présent et net, alors qu'il l'est moins dans les autres bandes HL, LH, HH. Par contre si le taux de compression utilisé est réduit [75-80] % le message est très clair dans les 4 bandes Nous avons choisi trois images de la même taille 512*512 pixels de comparaison pour différentes taux de compression. Nous remarquons que les courbes figure 5.3 convergent vers le même résultat avec une petite différence en terme de PSNR.

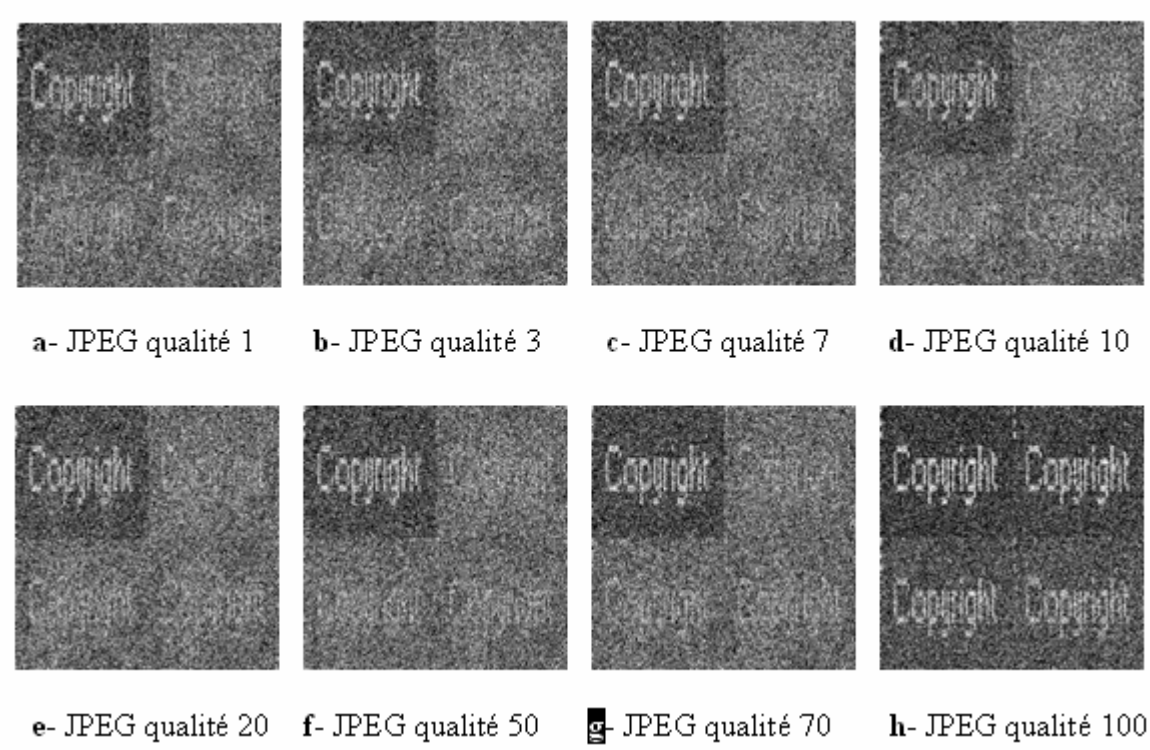


figure5.2 *: extraction de la marque dans l'image Lena 512*512 après une attaque par compression par différents types de qualité de compression.*

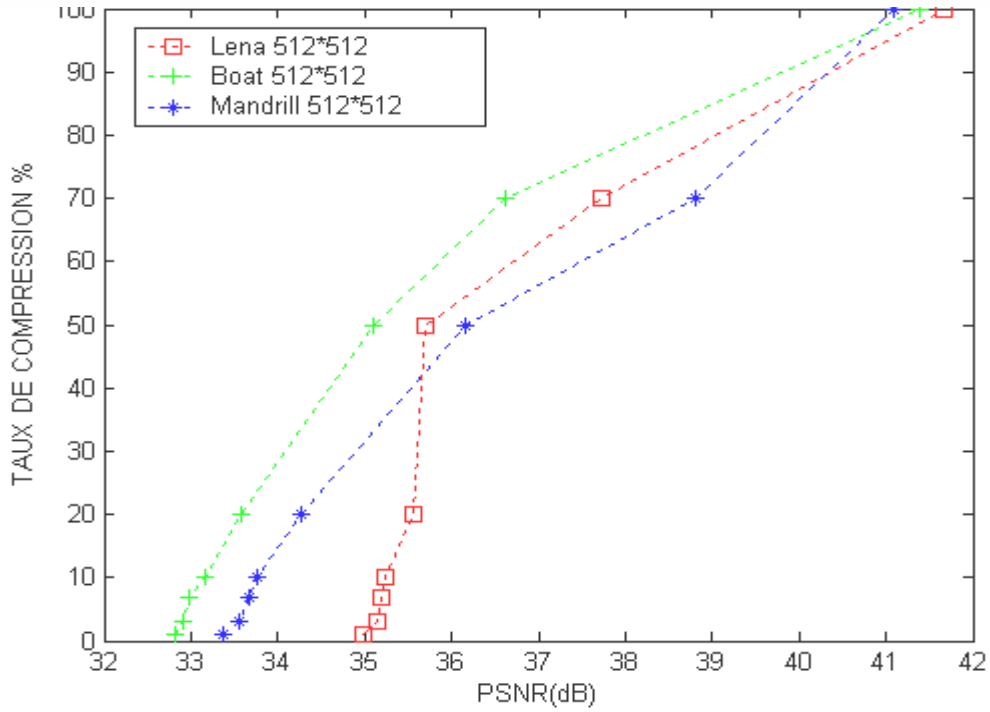


figure 5.3 *: comparaison de différentes images de la même taille après une attaque par compression jpeg*

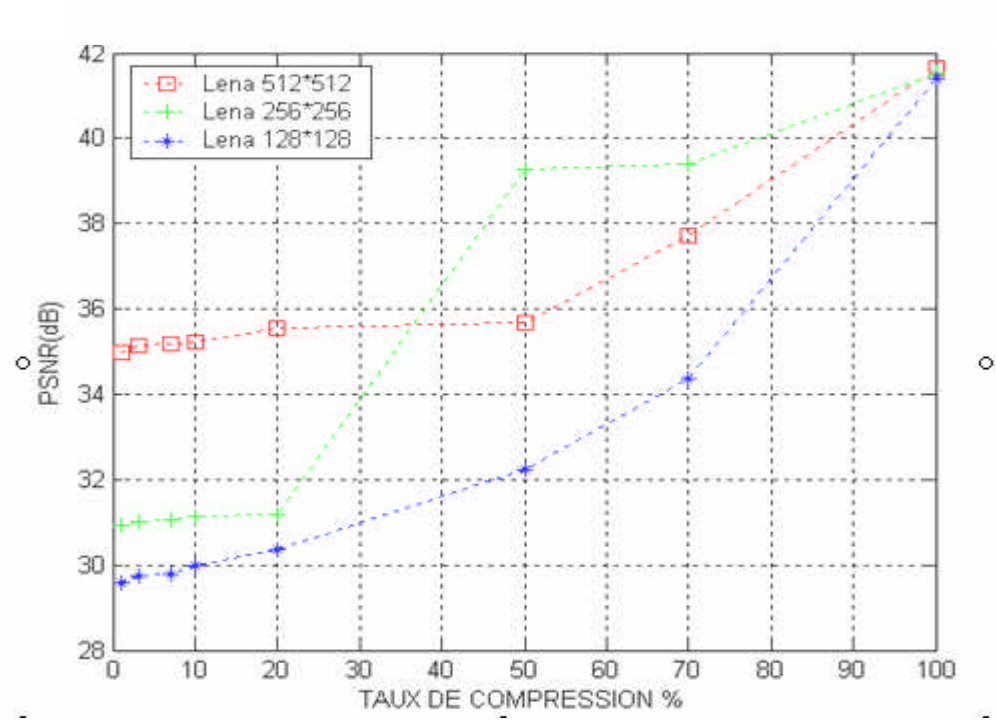


figure5.4 *: On compare ici le PSNR pour les différentes tailles de l'image Lena en fonction de taux de compression jpeg*

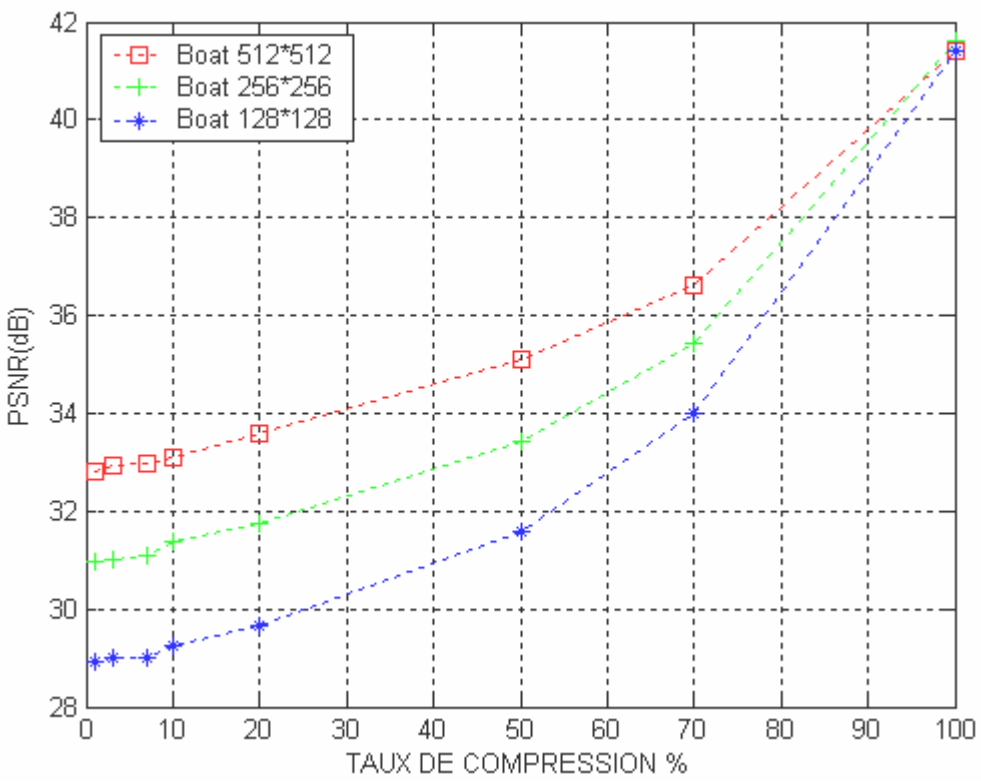


figure5.5 *: On compare ici le PSNR pour les différentes tailles de l'image Boat en fonction de taux de compression jpeg*

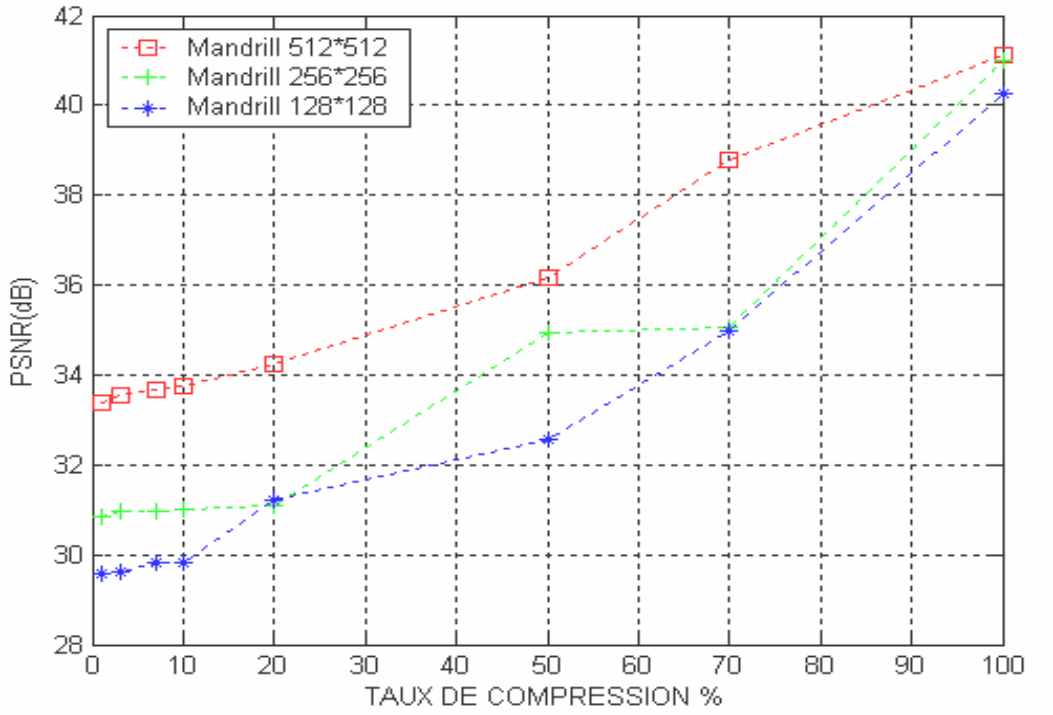


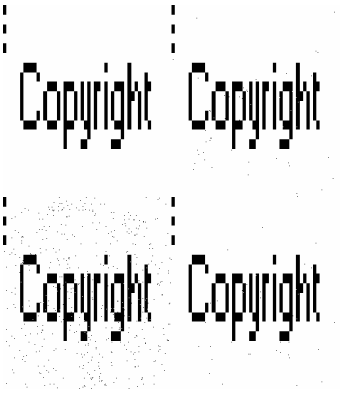
figure5.6 *: On compare ici le PSNR pour les différentes tailles de l'image Mandrill en fonction de taux de compression jpeg*

Les courbes ci-dessus sur les figures 4.17, 4.18 et 14.19 montrent les variations de PSNR pour la même image teste mais pour différentes résolutions. Nous avons alors choisi trois tailles standards 512, 256, 128 pixels et on fait varier le taux compression.

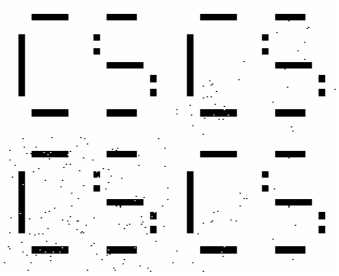
Pour les images ‘’Boat’’ et ‘’Mandrill’’ l’augmentation de la taille assure une augmentation du PSNR sur tout l’intervalle de compression. Par contre l’image Lena après 50% taux de compression, il existe une petite variation dans le PSNR.

5.1 Comparaisons entre deux marques de tailles différentes.

Les figures (figure 5.7) ci-dessous montrent le rapport de la taille de la marque devant une attaque par bruit, la taille de la marque joue un rôle devant ce type d’attaque, (attaque par bruit ou compression) ,



a- la marque extrait de taille 50x20



b- la marque extrait de taille 12x9

figure 5.7 : *extraction de deux marques de tailles différentes avant l’attaque.*

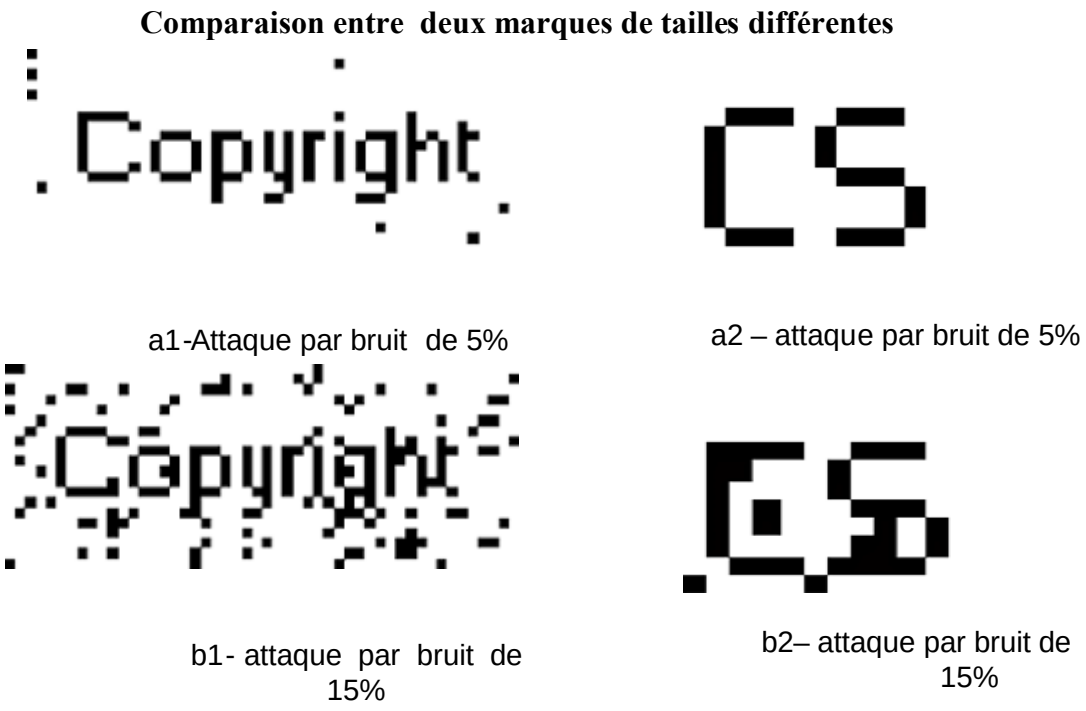


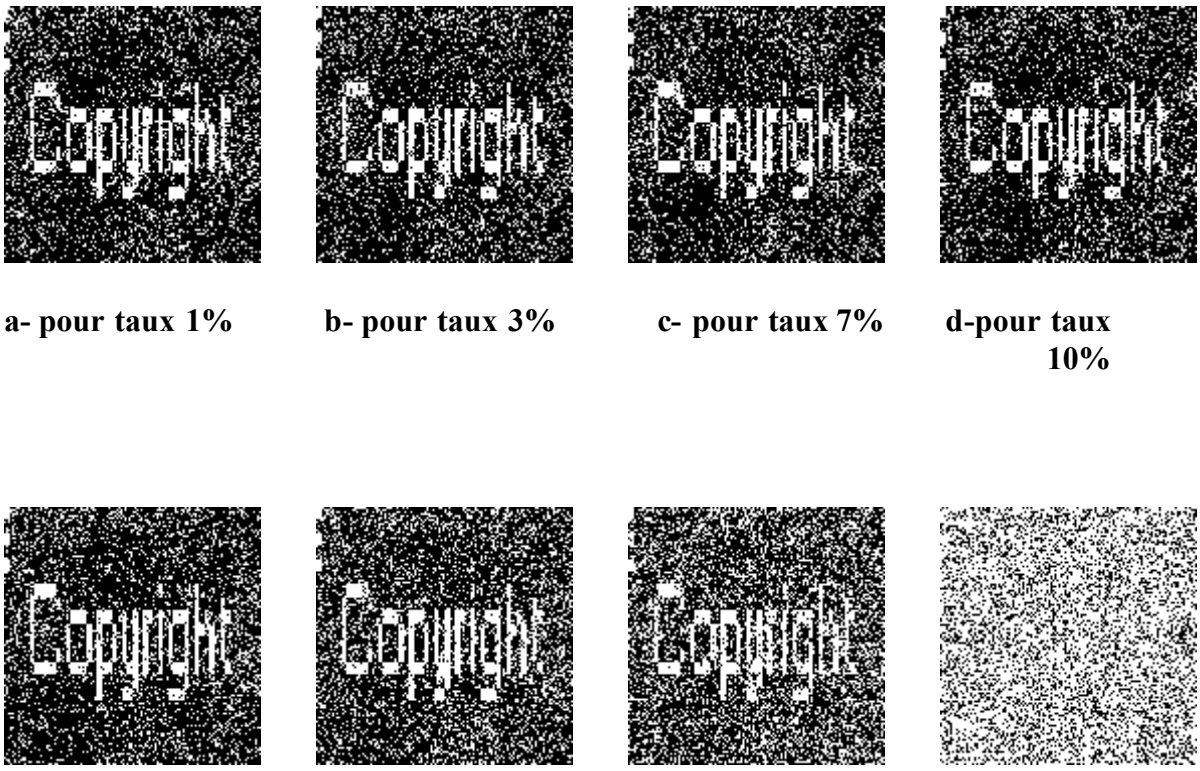
figure 5.8 *: extraction de deux marques de tailles différentes après une attaque par bruit*

D'après les résultats figure 5.8 obtenus nous remarquons que cette méthode de tatouage est relativement résistante pour des attaques dues à des bruits additifs. Il est vrai que cette méthode devient de plus en plus sensible lorsque la puissance du bruit est plus importante. Cependant, pour des amplitudes de bruits jugées élevées l'extraction de la marque est possible avec une certaine dégradation.

5.2 Evaluation du Second algorithme de marquage appliqué.

5.2.1 Extraction de la marque après l'attaque par compression jpeg :

L'image ci-dessous montre la marque après une attaque par compression pour différentes taux et dans niveau 2 pour la transformer on ondelette discret DWT. Pour a, b, c, d et e c-a-dire de [1-20]% les marques sont visibles et supérieur à 50% la marque perde leur visibilité



a- pour taux 1% **b- pour taux 3%** **c- pour taux 7%** **d-pour taux 10%**

e- pour taux 20% **f- pour taux 50%** **g- pour taux 70%** **d-pour taux 100%**

figure 5.9 *: extraction de la marque dans la bande LL2 l'image Lena 512*512 après une attaque par compression par différents types de qualité de compression*

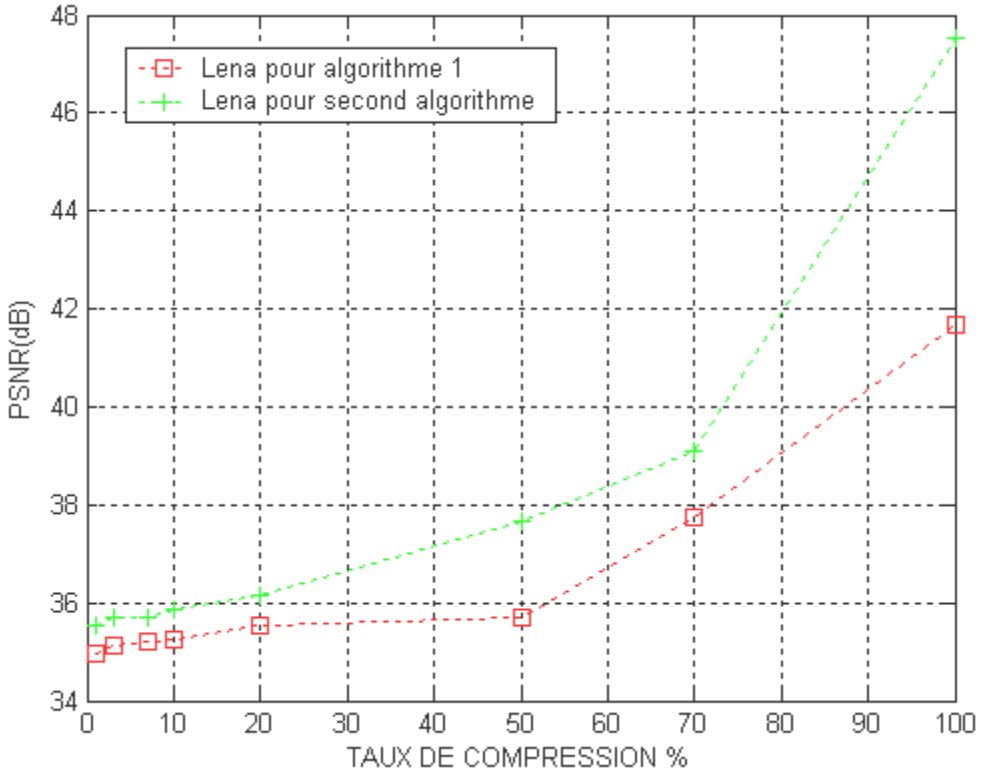


figure 5 10 *: Comparaison du PSNR entre deux algorithmes en fonction de taux de compression jpeg sur l'image Lena*

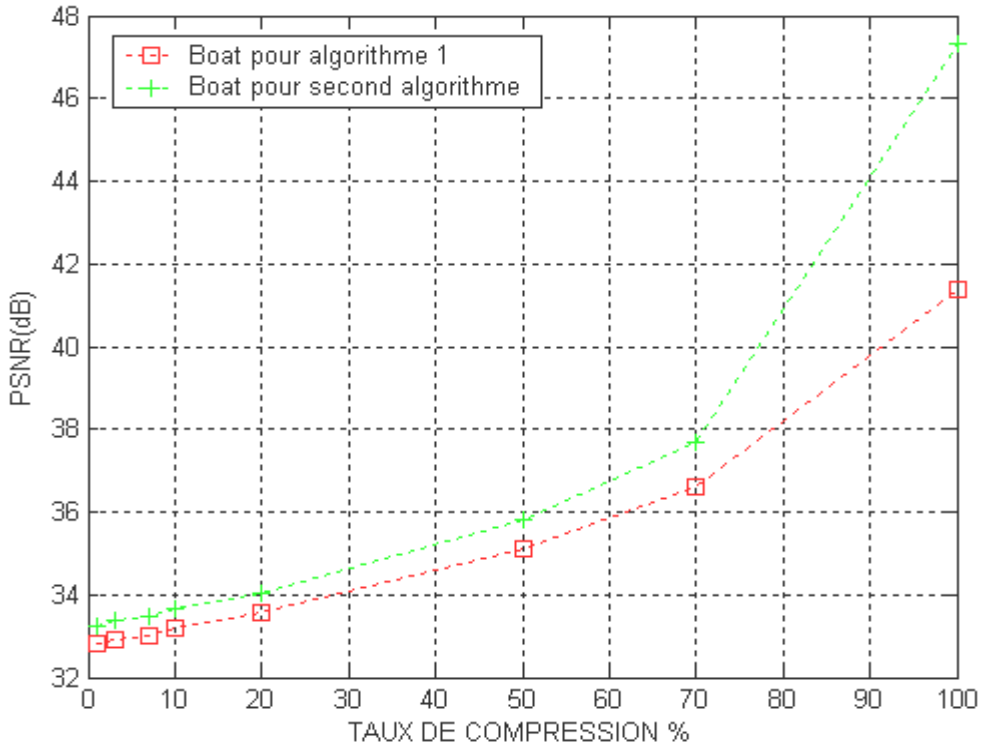


figure 5.11 *: Comparaison du PSNR entre deux algorithmes en fonction du taux de compression jpeg sur l'image Boat*

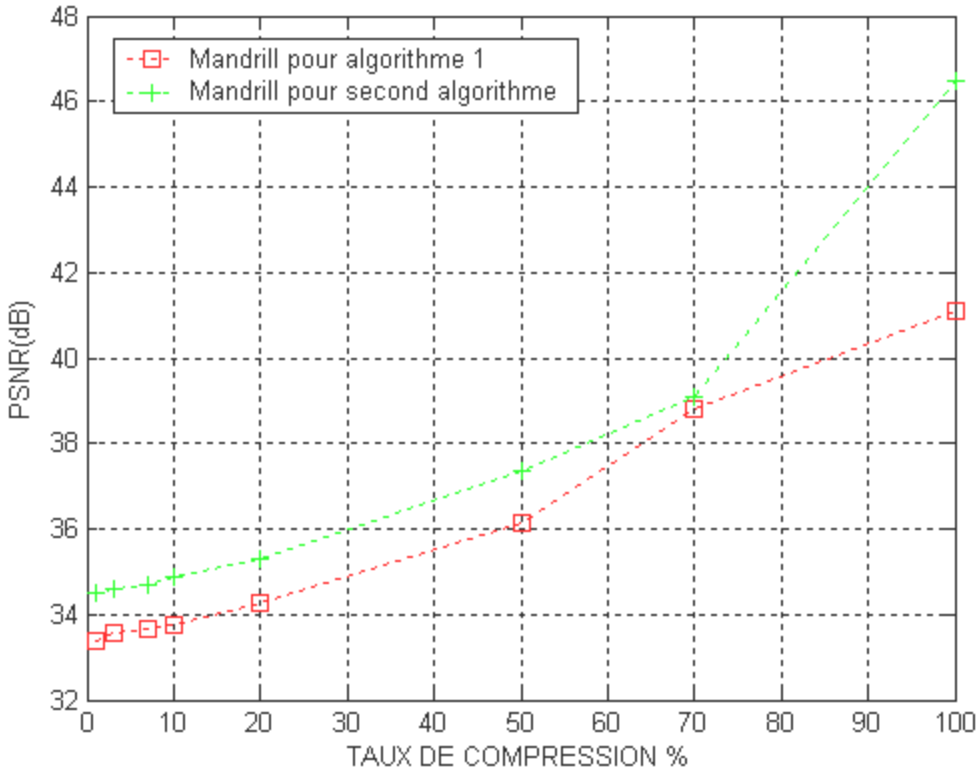


figure 5.12 *: Comparaison du PSNR entre deux algorithmes en fonction du taux de compression jpeg sur l'image Mandrill*

Pour les trois figure ci-dessus figures 5.10, 5.11, 5.12 les courbes sont la même allure pour chaque image mais le PSNR pour second algorithme un peut grand devant le premier algorithme jusqu'à 70% de taux de compression et ou de-là le PSNR augmente avec une valeur considérable, donc notre second algorithme est robuste pour taux de compression inferieure [75-80]% et supérieure de cette valeur le marque est invisible.

6. Conclusion .

Nous avons pu, à travers les exemples et les tests, effectuer et étudier les performances et la robustesse de la technique de tatouage adoptée, vis-à-vis d'une attaque involontaire. En effet, le principe de base du tatouage est de pouvoir extraire la marque insérée sans qu'elle soit visible. Seulement, cette marque peut être altérée ce qui va conduire inévitablement à sa perte. Il est donc primordial de s'assurer de sa robustesse en présence de perturbation, de compression ou même d'une attaque volontaire visant à détruire cette signature.

Dans ce chapitre nous nous sommes limités uniquement à l'étude des performances de cette technique de tatouage en présence d'une attaque volontaire de type compression Jpeg ou bruit perturbateur. Ceci pour plusieurs raisons : la compression et aussi les bruits sont inévitables dans toute transmission ou stockage ; la facilité relative de la mise en œuvre des algorithmes de compression.

Les résultats obtenus montrent la robustesse de cette technique quant à ce type d'attaque. En effet, les résultats ont montré que pour certains types d'images les performances sont meilleures que pour d'autres et aussi pour certaines résolutions. Ceci est du à la quantité d'information contenues dans certaines images par rapport à d'autres. Certaines images, présentent plus de variations aussi bien en luminosité qu'en couleurs par rapport à d'autres. Ceci joue inévitablement un rôle primordial lorsqu'on utilise des décompositions par les ondelettes.

Conclusion et Perspectives

Conclusion finale.

Nous avons introduit ce travail en présentant et en définissant les objectifs du tatouage d'images numériques. Nous avons insisté pour considérer une approche globale du problème, elle nous a conduit à choisir un domaine applicatif : la protection du copyright et à en établir le cahier des charges. Après avoir présenté quelques méthodes génériques, nous avons choisi de travailler sur les techniques d'implémentation de la marque dite robuste.

Nous avons alors présenté la méthode développée pendant cette thèse, elle consiste à représenter une image par une structure d'ondelettes. La marque sera implémentée en déformant cette structure. La suite de notre travail vise à analyser les comportements de notre méthode face à un grand ensemble d'attaques puis à trouver des stratégies visant à diminuer l'effet de ces attaques. Nous nous sommes en particulier attaché à des attaques de compression pour rechercher le seuil optimum définissant la meilleure base de protection d'images.

Nous avons alors présenté la méthode développée dans ce mémoire (la *DWT*), où chaque niveau de décomposition produit quatre bandes de données, une correspondante à des basses fréquences (*low-pass band ou baseband*) (LL), et trois autres correspondent à des hautes fréquences Horizontale (HL), verticale (LH), et diagonale (HH) (*high pass band*). La marque est additionnée dans les quatre bandes fréquentielles de l'image (*LL, LH, HL et HH*). La suite de notre travail vise à analyser les comportements de notre méthode face à un grand ensemble d'attaques. Enfin, afin de respecter le cahier des charges, nous avons mis en oeuvre une méthode permettant de certifier que le tatouage ne dégrade pas l'image marquée. L'avant dernière partie de ce mémoire permet d'analyser la méthode proposée.

A ce propos, nous avons présenté diverses solutions à des attaques intentionnelles. Une méthode dite *clef privée* dite aussi par « leurres » a été mise en œuvre.

Les deux dernières parties de ce rapport présentent les résultats que nous avons obtenus. Ces résultats sont très hétéroclites selon les attaques testées et montrent en particulier les problèmes dus à la non-invariance de l'approche utilisée aux transformations géométriques.

Enfin, on peut envisager d'adapter la méthode de tatouage par la *transformée en ondelette discrète* à d'autres applications que la protection du copyright et à d'autres supports que les images fixes et vidéos comme par exemple l'audio.

Bibliographie

[1] **M. BUYDENS**,
Protection de la quasi-création
p.86 , Bruxelles, Larcier, 1992.
A. BERENBOOM,

[2] **M. Buydens** , La protection de la quasi-création,
p.67 , Bruxelles-Pa ris 1992,
Propriété littéraire et artistique,
n° 24, Paris 1994

[3] L'article L123-1 CPI précise en son alinéa 2 qu'au décès de l'auteur, ce droit persiste au bénéfice de ses ayants droit pendant l'année civile en cours et les soixante-dix années qui suivent".

[4] **BORTOLONI.F**, **BARNI. M**, **CAPPELINI V.** & **PIVA. A**
Mask Building for perceptually hiding frequency embedded watermarks. Proc. of the Int. Conf. Image Processing (ICIP 98),
Vol. 1, pages 450-454. Chicago Illinois US, Octobre 1998.

[5] **VOLOSHYNOVSKY S.**, **HERRIGEL. A**, **BAUMGAERTNER. N** & **PUN.T** A
Stochastic Approach to Content Adaptative Digital Image Watermarking. In Proceeding of International Workshop on Information hiding,
Dresden, Deutschland, Septembre 1999.

[6] DELAIGLE J.F., DE VLEESCHOUVER C., MACQ B.
Watermarking Algorithm Based on a Human Visual Model, In Signal Processing, Vol. 66, pp. 319-335, 1998.

[7] S. Karzenbeisser and **F.A.P. Petitcolas**.
Information hiding techniques for steganography and digital watermarking.
Artech House, 1999.

[8] **F. A. P. Petitcolas, R. J. Anderson,** and **M. G. Kuhn**.
Information hiding _ a survey. Proceedings of the IEEE (USA), 87(7) :1062-1078. 1999.

[9] F. Hartung and **M. Kutter**.
Multimedia watermarking techniques. Proceedings of the IEEE, 87(7) :1079-1107. jul 1999.

[10] A.M. Alattar.
Smart images using digimarc's watermarking technology. In SPIE,editor, Security and Watermarking of multimedia contents,
volume 3971, pages 246-263, San-Jose (CA, USA), January 2000.

[11] F. A. P. Petitcolas, **R. J. Anderson** and **M. G. Kuhn**.
Information hiding a survey.
Proceedings of the IEEE (USA), 87(7) :1062-1078
1999.

[12] A. Kerckhofs.
La cryptographie militaire. Journal des sciences militaires,
IX :5-38, Janvier 1883.

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

[13] B. Chen and **G. Wornell**.
An information_theoretic approach to the design of robust digital watermarking systems. In International Conference on Acoustic, Speech and 0Signal Processing (ICASSP),
Phoenix, AZ, March 1999.

[14] S. Craver, **N. Memon**, **B.L. Yeo,** and **M.M. Yeung**.
Can invisible watermarks resolve rightful ownerships ?
Technical report,
IBM, 1996.

[15] P. Baq.
Méthodes de tatouage d'images fondées sur le contenu. PhD thesis, Institut National Polytechnique de Grenoble,
Octobre 2000.

[16] TANAKA. K, **NAKAMURA.Y** & **MATSUI.K**
Embedding secret information into a dithered multi-level image. In Proc. Military communications Conference,
IEEE, pages 216-220, 1990

[17] WOLFGANG R.B. & **DELP E.J. A**
Watermarking technique for digital imagery: further studies. In Int. Conf. on Imaging Science, Systems and Technology,
Las Vegas, Nevada, Juillet 1997.

[18] BENDER W., **GRUHL D**. & **MORIMOTO**.
Techniques for data hiding. In Proc. of SPIE,
volume 2420, page 40, Février 1995,

[19] BORTOLONI. F, **BARNI. M**, **CAPPELINI.V,** & **PIVA .A**
Mask Building for perceptually hiding frequency embedded watermarks. Proc. of the Int. Conf. Image Processing (ICIP 98),

Chicago Illinois US, Vol. 1 pages 450-454, Octobre 1998,

[20] VOLOSHYNOVSKY S., **HERRIGEL A.**, **BAUMGAERTNER N.** & **PUN T.**
A Stochastic Approach to Content Adaptative Digital Image Watermarking. In Proceeding of International Workshop on Information hiding,
Dresden, Deutschland, Septembre 1999

[21] DELAIGLE J.F., **DE VLEESCHOUVER. C**, **MACQ. B**
Watermarking Algorithm Based on a Human Visual Model, In Signal Processing, Vol. 66, pp& 319-335, 1998.

[22] COX. I.J, KILLIAN .J, LEIGHTON.T & **SHAMOON. T**
Secure spread spectrum watermarking for images, audio and video.
In Int Conf. On Image Processing,
Florence, Février 1996,

[23] CSURKA.G, DEGUILLAUME.F, ORUANAIDH J.J.K & **PUN.T**.
Tatouage d'images basé sur la Transformée de Fourier Discrète.
Coresa 1999, 9-10 Juin 1999

[24] ORUANAIDH J.J.K. & **PUN T**.
Rotation, translation and scale invariant digital image watermarking.
IEEE Signal Processing Society 1997 Int. Conf. on Image Processing (ICIP'97), Santa Barbara, CA, vol.1, pages 536-539, Oct. 1997

[25] ROCHE S. & **DUGELAY J.L.**
Image Watermarking based on the Fractal Transform. IEEE Multimedia Signal Processing .
LA., CA, pages 358-362. 1998

[26]E. Hitti.
Sélection d'un banc optimal de filtres à partir d'une décomposition en paquets d'ondelettes. Application à la détection de saut de fréquences dans des signaux multicomposantes.
PhD thesis, Université de Nantes, 1999.

[27] S. Mallat.
A wavelet tour of signal processing.
Academic Press, 1998.

[28] P. Abry.
Transformée en ondelettes, analyse multirésolution et signaux de pression en turbulence.
PhD thesis, Université C. Bernard Lyon I, 1994.

[29] Y.T. Chan.
Wavelet basics.
Kluwer Academic Publisher, 1995.

[30] G. Strang.
Wavelet and filter bank.
Wellesley Cambridge Press, 1996.

[31] M. Vetterli.
Wavelet and filter banks : Theory and design.
IEEE trans. on signal processing 41(8) :2207-2232,
1990

[32] M.V. Wickerhauser.
Lectures on wavelet packet algorithms.
INRIA, pages 31-99, 1991.

[33] LANGELAAR G., LAGENDIJK R. & BIEMOND J.
Removing spatial spread spectrum watermarks by non-linear filtering. In Proceedings
EUSIPCO98, volume 4, pages 2281-2284, 1998.

[34] VOLOSHYNOVSKY. S, HERRIGEL.A , BAUMGAERTNER. N & PUN. T
Generalized wadermarking attack based on watermark estimation and perceptual remodulation. In Proceedings of SPIE : Security and Watermarking of Multimedia Content II, San Jose, CA, USA, Janvier 2000.

[35] KUHN M. & PETITCOLAS F.
Stirmark,
http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/
Novembre 1997

[36] UnZign.
http://www.altern.org/watermark
Juillet 1997

[37] I.J. Cox, J. Kilian, F.T. Leighton, and **T. Shamoon**.
Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12) :1673-1687,
1997.

[38] S. Karzenbeisser and **F.A.P. Petitcolas**.
Information hiding techniques for steganography and digital watermarking. Artech House, 1999.

[39] Digimarc.
http: //www.digimarc.com.

[40] TANAKA K., NAKAMURA Y. & MATSUI K.
Embedding secret information into a dithered multi-level image. In Proc., Military communications Conference,
IEEE, pages 216-220,1990.

[41] WOLFGANG R.B. & DELP E.J. A
watermarking technique for digital imagery : further studies. In Int. Conf. on Imaging Science, Systems and Technology,
Las Vegas, Nevada, Juillet 1997.