UNIVERSITE IBN ZOHR
FACULTE DES SCIENCES
AGADIR

جامعة ابن زهر
كليـــــة العلـــــوم
أكاديـر

**THÈSE**

*Présentée à*
La Faculté des Sciences d'Agadir

*En vue de l'obtention du*

**THÈSE DE DOCTORAT ÈS-SCIENCES**
**Option** : Mathématiques et Informatique Appliquées

**Spécialité** : Informatique

Par

**MOHAMED EL HAJJI**

TITRE DE LA THÈSE

# LA SÉCURITÉ D'IMAGES PAR LE TATOUAGE NUMÉRIQUE DANS LE DOMAINE D'ONDELETTES

*Soutenu le: 28/01/2012, devant le jury :*

| | | |
|---|---|---|
| Pr. Driss Mammass | (Directeur de l'EST, Univ. Ibn Zohr- Agadir) | Président |
| Pr. Hassan Douzi | (Professeur, FS, Univ. Ibn Zohr- Agadir) | Directeur de thèse |
| Pr. Mohamed Wakrim | (Professeur, FS, Univ. Ibn Zohr- Agadir) | Rapporteur |
| Pr. Bouabid EL Ouahidi | (Professeur, FS, Univ. Med V- Rabat) | Rapporteur |
| Pr. Abdelkarim Zatni | (Professeur, ESTA, Agadir) | Rapporteur |
| Pr. Rachid Harba | (Professeur, Polytech Orléans, France) | Co-Directeur et Examinateur |
| Pr. Karim Afdel | (Professeur, FS, Univ. Ibn Zohr- Agadir) | Examinateur |

# Résumé

Cette thèse présente nos contributions relatives au domaine du tatouage numérique dans le domaine d'ondelettes. Dans ce but, nous avons introduit les notions de base se rapportant au concept du tatouage numérique ainsi que la transformée en ondelettes.

Nous avons proposé deux méthodes «aveugle» de tatouage d'images basée sur le contenu dans le domaine d'une transformée en ondelettes exprimée par le schéma lifting (FSDWT) à échelles mixées. Plus précisément sur les blocs de coefficients significatifs qualifiés par «Blocs dominants» correspondants aux régions autour des contours et les zones texturées. La première méthode est basée sur l'étalement de spectre amélioré (ISS) des coefficients dominants et la deuxième méthode est basée la quantification des blocs dominants. Nous avons aussi présenté une méthode « fragile» d'authentification d'images et de détection des zones altérées, basée sur les blocs dominants et les moments invariants. Nous avons présenté des résultats numériques afin d'évaluer les performances de ces méthodes.

**Mots clés :** Tatouage numérique, Authentification, Transformée en ondelettes, Représentation à échelle mixées, Coefficients dominants, Etalement de spectre amélioré (ISS), la quantification QIM, Descripteurs de forme.

# Abstract

This thesis presents our different contributions relative to digital watermarking in wavelets domain. For this purpose, we have introduced the basic concepts related to the concept of digital watermarking and the wavelet transform.

We proposed two "blind" watermarking images methods based on the content in a wavelet transform expressed by the lifting scheme (FSDWT) in mixed scales. Exactly in blocks of significant coefficients qualified by "dominant Blocks" corresponding to the regions around the edges and textured areas. The first method is based on the improved spread spectrum (ISS) and the dominant coefficients; however the second method is based on quantification of dominant blocs. We also presented an image authentication and tamper detection method "fragile" based on dominant blocs and invariants moments. We have presented numerical results to evaluate the performance of these methods.

**Key Words:** Digital Watermarking, Authentication, Wavelet transform, Mixed scales, dominant coefficients, improved spread spectrum (ISS), Quantification QIM, shape descriptors.

*À mes chers parents*
*À ma chère femme*
*À mon cher fils Reda*
*À mes frères et mes sœurs*

# Remerciements

Je remercie M. Driss Mammass, directeur de recherche du laboratoire IRF-SIC et directeur de l'EST, Univ. Ibn Zohr- Agadir, pour m'avoir accepté dans son équipe et m'avoir fait l'honneur de présider le jury. Je lui suis également reconnaissant pour sa disponibilité, ses qualités pédagogiques et scientifiques. J'ai beaucoup appris à ces côtés et je lui adresse toute ma gratitude.

Mes remerciements les plus sincères à M. Hassan DOUZI, mon directeur de thèse, pour la confiance qu'elle m'accordée et la gentillesse. Pour son inépuisable patience, pour son regard critique et plus généralement pour tout ce que j'ai pu apprendre à son contact durant ces années de thèse. Ces quelques lignes ne peuvent pas exprimer toute ma gratitude.

Je remercie également M. Rachid Harba du labo LESI à Polytech Orléans en France, pour les remarques constructives qu'il m'a fournie ainsi que pour leurs précieux conseils, pour la collaboration que nous avons eu ces quatre années qui fût pour moi une grande source d'expérience, mais aussi pour son rôle en temps que membre du jury.

Je voudrais remercier les rapporteurs de cette thèse M. Mohamed Wakrim, Professuer à la faculté des sciences Ibn zohr, M. Bouabid El Ouahidi, Professeur à la faculté des sciences d'Univ. Med V- Rabat et M. Abdelkarim Zatni professeur à EST d'Agadir, pour l'intérêt qu'ils ont porté à mon travail.

J'associe à ces remerciements M. Karim Afdel, professeur à la faculté des sciences Ibn zohr pour avoir bien voulu juger ce travail.

Sincères remerciements à toute l'équipe du laboratoire IRF-SIC mais aussi à ceux qui sont passés parmi nous durant mon doctorat. Ils sont nombreux et je ne peux tous les citer ici (par peur d'en oublier) mais tous par leur gentillesse ou leurs conseils m'ont apporté quelque chose et je les en remercie. Je salue particulièrement Mustapha Amrouch. Merci à Youssef Es Saady pour son soutien sans faille.

Ma reconnaissance va aussi à ma mère et à mon père dont l'éducation, la confiance, l'appui moral et financier m'ont permis de m'épanouir. Je suis également fort reconnaissant à ma femme qui a supporté mes humeurs changeantes avec dévouement et attention. À mes frères et à mes sœurs, je dis merci pour tous ces moments où vous m'avez fait ressentir la chaleur fraternelle.

Enfin, Je remercie tous ceux qui ont contribué, de prés ou de loin, à la réalisation de ce travail.

# Table des matières

# Liste des tableaux

# Liste des figures

# Introduction générale

Ces dernières décades, les documents multimédias sont devenus un élément central dans les différents domaines d'applications grâce au développement des technologies liées à l'informatique. En effet, elles sont des outils de travail essentiel en biomédical, en imagerie satellitaire et astronomique, en production cinématographique, ou encore en informatique industrielle. Ce développement phénoménal ne s'est pas fait sans entraîner des inquiétudes de manipulations illicites puisque n'importe quelle personne peut facilement copier, modifier et distribuer les images numériques sans risque de les détériorer. Ces manipulations illicites sont un problème central pour la sécurité d'un système, quel que soit : un état, une entreprise ou un particulier. D'où, l'importance de protéger ces documents multimédias contre un accès ou une distribution non autorisée.

Les techniques de cryptage constituent la première solution pour empêcher l'accès non autorisé à des données numériques. Elles répondent aux besoins des utilisateurs en matière de sécurité comme la confidentialité, l'intégrité et l'identification. Néanmoins, ces techniques se sont révélées insuffisantes ou d'un emploi difficile. En effet, les outils de cryptographie protègent l'image uniquement lors d'une transmission, mais une fois l'image est déchiffrée, il n'y a plus de contrôle pour empêcher une manipulation illégale.

Dans ce contexte, le tatouage numérique (Digital Watermarking en anglais) apparaît comme étant une alternative pouvant s'avérer efficace et complémentaire pour aider à établir une sécurité supplémentaire, à assurer un accès autorisé, à faciliter l'authentification du contenu ou empêcher la reproduction illégale. L'idée est de cacher dans une image (ou dans un document multimédia numérique) une marque invisible. Un algorithme de détection ou d'extraction est nécessaire pour approuver la présence de cette marque.

Il est possible de faire un parallèle entre le tatouage et les techniques utilisées pour la sécurisation des billets de banque, par exemple l'insertion d'un message en filigrane. La

figure 1 montre la marque visible en filigrane dans un billet de 200 dirhams. Lorsque l'on regarde le billet dans des conditions normales d'utilisation, la marque est invisible, alors que dans des conditions d'observation du billet par transparence, la marque devient visible.

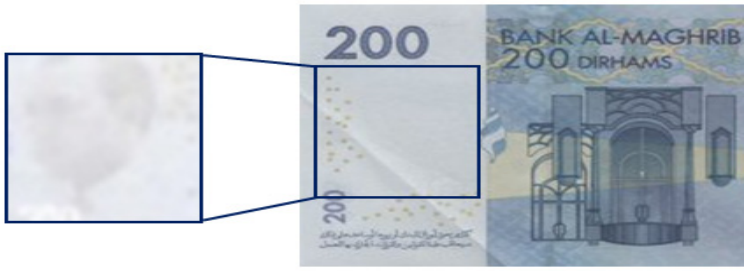



*Figure 0.1: Filigrane d'un billet de 200 Dirhams*

Depuis quelques années, le domaine de tatouage d'image connaît un extraordinaire développement et plusieurs techniques ont vu le jour, mais chacune suit un cahier de charges spécifique. Celui-ci se détermine généralement en ces termes : invisibilité, capacité, robustesse et sécurité. Il est naïf de croire qu'une seule technique de tatouage peut répondre aux différentes spécificités de chaque application. De même, il est inutile d'inventer une multitudes de techniques de tatouage en ignorant les contraintes du cadre d'utilisation visé et du document utilisé.

**Contributions**

L'objectif de cette thèse est d'étudier et de proposer des nouvelles méthodes de tatouage numériques dans le domaine d'ondelettes. Nous utiliserons la transformée d'ondelettes de Faber-Schauder qui représenté à échelles mixées. En effet, cette transformée se distingue par sa simplicité (schéma lifting, opérations arithmétiques, sans traitement aux bords) et par sa grande capacité à détecter les zones texturés et les régions autour des contours (qui représentent les régions les plus intéressantes pour l'insertion des tatouages numériques). En plus, la représentation des coefficients d'ondelettes dans une distribution à échelles mixées permet de sélectionner facilement les zones adéquates pour le tatouage.

Quatre contributions seront présentées :

La première contribution a porté sur la sélection automatique des blocs dominants des coefficients de la transformée en ondelettes de Faber-Schauder (FSDWT). Ces blocs dominants vont servir dans les méthodes développées dans cette thèse. Cette sélection se base sur les caractéristiques statistiques des coefficients de la transformée FSDWT. Nous montrons que ces blocs correspondent aux régions autour des contours et aux zones texturées où l'insertion permet de développer des méthodes de tatouage efficaces.

La deuxième et la troisième contribution concernent la proposition de deux méthodes robustes qui sont basées sur la transformée FSDWT. Ces deux méthodes sont utilisées pour les images en niveaux de gris mais elles peuvent être modifiées pour être appliquées aux images couleurs. La première méthode est basée sur l'utilisation de l'étalement de spectre amélioré. Le principe consiste à ajouter aux blocs dominants une séquence aléatoire suivant le bit de la marque à cacher. La détection est effectuée par un calcul de la corrélation entre les blocs dominants de l'image reçue et la séquence utilisée lors de la phase d'insertion. La seconde méthode est basée sur la modulation d'index (QIM). Cette méthode consiste à quantifier les coefficients des blocs dominants. La détection repose sur le calcul de la distance minimale entre les blocs dominants et les quantificateurs. L'originalité de ces deux méthodes réside dans l'utilisation de la représentation des coefficients d'ondelettes à échelles mixées et les blocs dominants. Les performances obtenues montrent que ces deux méthodes offrent une haute qualité d'images tatouées et une robustesse contre plusieurs attaques conventionnelles.

La quatrième contribution est la proposition d'un algorithme original d'authentification d'images. Cet algorithme est basé sur les coefficients dominants et les moments invariants. Cet algorithme est hybride, il opère dans le domaine de la transformée FSDWT et le domaine spatial. Le principe de cet algorithme consiste à combiner les coefficients dominants et un vecteur descripteur obtenu à partir des moments invariants de l'image. Le vecteur descripteur est utilisé pour vérifier si l'image tatouée a été altérée durant sa transmission. Alors que les blocs dominants sont utilisés pour détecter les zones altérées d'une image attaquée. L'insertion est effectuée par la substitution de plan des bits LSB par une marque cryptée obtenue à partir des informations d'identification (par exemple les

informations sur le patient dans le cas des images médicales), les emplacements des blocs dominants de l'image et le vecteur descripteur de l'image. Les résultats obtenus montrent que cette nouvelle méthode est efficace en termes d'imperceptibilité et en termes de détection des zones altérées.

**Organisation de la thèse**

Le manuscrit sera composé de deux parties et sera organisé comme suit:

La première partie établit un état de l'art des différentes terminologies dans lesquelles s'inscrivent nos travaux de mémoire. Cette première partie se décompose en deux chapitres:

Le chapitre 1 décrit les aspects principaux et les terminologies liés aux évolutions des technologies du tatouage invisible des images numériques. Ces terminologies sont nécessaires pour les chapitres suivants pour éclairer des points tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle. Nous présenterons aussi une classification des techniques de tatouage selon différents critères et quelques métriques pour l'évaluation de la qualité perceptuelle des images.

Le chapitre 2 expose une description de la transformée d'ondelettes puis la transformée rapide de Faber-Schauder exprimée par un schéma lifting et la représentation des coefficients d'ondelettes à échelles mixées. Nous exposons également dans ce chapitre, le principe du tatouage d'images utilisant la transformée en ondelettes. En particulier, nous présentons quelques algorithmes très connus qui utilisent cette transformée.

La seconde partie est composée de deux chapitres. Elle présente les trois méthodes de tatouage développées durant cette thèse de doctorat. Cette partie se décompose aussi en deux chapitres :

Dans le chapitre 3, nous présenterons les deux méthodes robustes de tatouage. Dans premier lieu, nous décrivons la méthode basée sur l'étalement de spectre. Puis, nous dérivons la deuxième par la quantification QIM. Les deux méthodes développées sont testées et validées sur un ensemble d'images test et un résumé des résultats obtenus est présenté au cours du chapitre.

Le chapitre 4 décrit la méthode élaborée pour l'authentification d'images. Dans un premier temps, nous présenterons la technique utilisée pour extraire le vecteur descripteur. Puis, nous décrivons les différentes phases de la méthode. Enfin, les résultats obtenus seront présentés.

# Partie 1

# Chapitre 1 Introduction au Tatouage numérique d'image

## 1.1 Introduction

Les documents multimédias (image, audio, vidéo) sont devenus un moyen de communication à part entier de plus en plus présent dans notre vie quotidienne. Ils sont également des outils de travail essentiels dans les domaines du biomédical, de l'imagerie satellitaire et astronomique, de la production cinématographique, ou encore de l'informatique industrielle. L'intérêt récent du grand public pour les documents multimédia et surtout l'image, au travers du grand développement des technologies de communication et des outils de traitement d'images, a apporté quelques problèmes liés à la distribution illégale, la duplication, la falsification et l'authentification.

Dans ce contexte, le tatouage numérique a été introduit comme étant une alternative à la cryptographie pour établir une sécurité supplémentaire afin d'assurer un accès autorisé, de faciliter l'authentification du contenu et d'empêcher la reproduction illégale. Ce contexte s'est rapidement élargi à d'autres types d'applications que nous développerons dans la section 1.2 ci-dessous.

La conception d'une méthode de tatouage repose en générale sur la théorie de l'information et des communications numériques (capacité, codes orthogonaux, codes correcteurs, multi-porteuses - OFDM, partage de canaux, CDMA, interférences, model de Costa…), sur le traitement et l'analyse du signal (représentations temps-échelle, transformations multi-résolutions, ajout de bruit, filtrage et estimation de paramètres, segmentation, détection), sur les statistiques (corrélation, décision, tests d'hypothèses, processus stochastique, mesures de confiance, reconnaissance), et sur la cryptographie. Cette conception repose aussi sur la prise en compte le système visuel humain(SVH) ainsi que les différents types d'attaques pouvant altérer la marque.

Ce chapitre décrit les aspects principaux et les terminologies liés au tatouage des images numériques. Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle des images. Nous présenterons aussi une classification des techniques de tatouage selon différents critères. La Figure 1.1 présente un organigramme de cette classification.

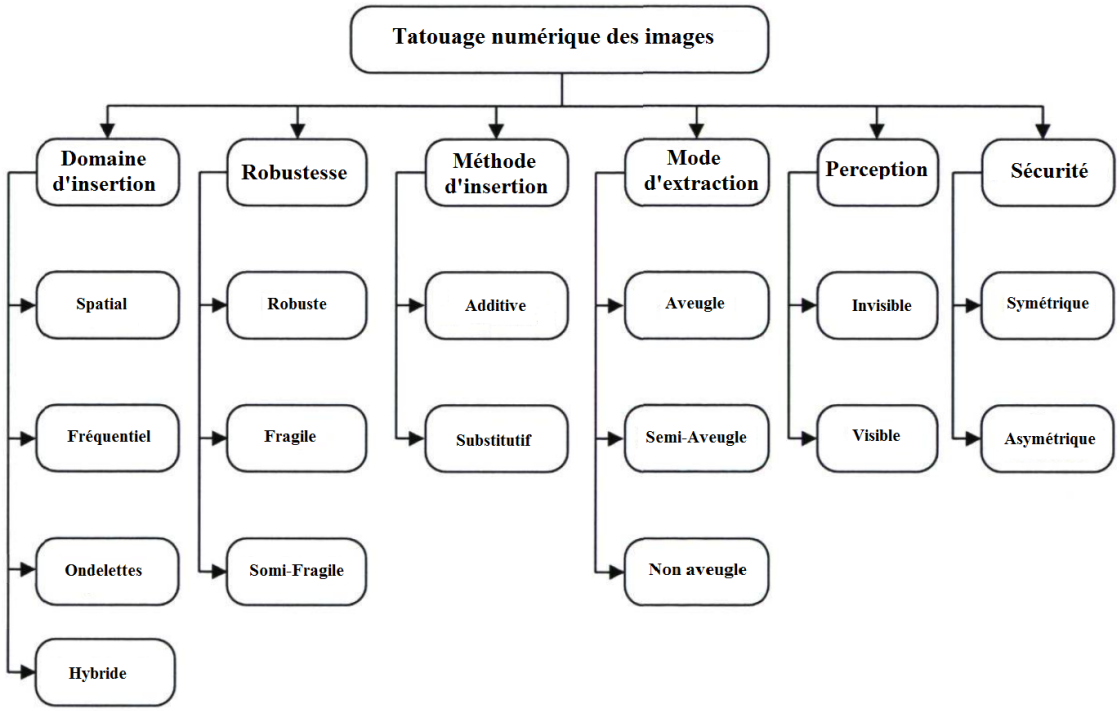



*Figure 1.1: Classification des méthodes de tatouage numérique des images*

## 1.2 Applications du tatouage numérique

Plusieurs applications industrielles de tatouage numérique sont proposées dans la littérature. Cox et al présentent dans leur livre [Cox07] une description détaillée des différentes applications du tatouage numérique. Ainsi, DWA[1] [DWA10] proposent dans leurs papiers blancs une liste des applications. Parmi celle-ci, on cite :

**La protection du copyright :**

[1] Digital Watermarking Alliance: Un groupe d'industriels réunis aux seins une douzaine d'acteurs de watermarking, dont Thomson, Philips et Digimark.

La protection du copyright constitue la première application pour laquelle le tatouage numérique a été utilisé. La technique traditionnelle consiste à mettre sur le document une information textuelle généralement sous forme " © *Auteur Date*". Cette technique a montré quelques limites :

Dans le cas d'un livre, il est facile de retirer le copyright lors de la copie de quelques pages.

Pour les images, le copyright textuel est souvent inséré d'une manière visible sur l'un des coins de l'image, ce qui peut cacher une partie de l'image et peut être retiré en utilisant un logiciel de retouche d'image (par exemple une opération de recadrage).

Pour l'audio, le copyright textuel est souvent mentionné sur le support physique, d'où l'importance d'une technique alternative pour les formats audio numérique qui sont souvent placés sur les sites web.

L'objectif de tatouage numérique dans ce type d'application est d'insérer une information d'identification du propriétaire d'une manière imperceptible et inséparable aux documents multimédias.

Plusieurs systèmes ont été proposés, nous citons par exemple celui proposé par la société Digimark [Dig10] qui propose d'utiliser une base de données centrale pour identifier le propriétaire de watermark (qui doit payer un droit de garder l'information dans la base de données). Un autre système d'identification de contenu est proposé dernièrement par Youtube [You11] pour identifier et interdire l'enregistrement dans leur système les vidéos ayant des droits.

**Authentification :**

Le tatouage permet de vérifier qu'une image n'a pas été modifiée. Ce type de tatouage permet d'assurer l'intégrité du document. Il est utilisé aussi bien dans l'authentification des images médicales, la télé-surveillance ainsi que la sécurité des papiers d'identité. Le processus de tatouage numérique consiste à cacher des informations servant à détecter une éventuelle modification ou un découpe de l'image par une personne non autorisée et à localiser précisément les régions manipulées, voir éventuellement à les restaurer.

A titre d'exemple, nous avons développé un algorithme de tatouage des images numériques dans un but d'authentification. Le principe de cet algorithme sera détaillé dans le chapitre 4. Cette méthode permet à la fois d'authentifier l'image mais aussi, le cas échéant, de localiser les zones ayant subi une attaque.

**Indexation**

Le tatouage peut avoir une application dans le domaine de l'indexation de documents. Le tatouage numérique repose sur l'insertion une description caractéristique de l'image afin de faciliter sa recherche de manière plus simple dans une base de données. En effet, on peut envisager de compléter la signature du créateur par une description sommaire de l'image pour permettre son indexation de manière plus simple.

On peut aussi envisager d'insérer un tatouage représentant un lien vers une autre source d'information (un lien vers un site Internet) afin d'obtenir des renseignements complémentaires sur l'image. Un exemple d'un système d'intégration de tatouage numérique pour améliorer les requêtes dans les systèmes de gestion de base de données (SGBD), est proposé dans [Wil05] et [Gro03].

**Le contrôle de diffusion (Monitor Broadcasts)**

Cette application permet aux propriétaires ou aux distributeurs de contenu de suivre la diffusion des émissions sur la télévision ou sur Internet de leur contenu. Le tatouage numérique est utilisé pour prouver que le contenu a été joué dans son intégralité en générant des rapports sur l'état de diffusion dans un marché donné à un moment précis. Des informations complémentaires peuvent être fournies, y compris la conformité d'utilisation, de la licence et la détection d'une utilisation illégale. Une description de ce système est présentée par Kalker dans [Kal99].

**Contrôle de copie**

L'objectif est de détecter la présence d'un copyright (une marque) pour contrôler ou rendre la copie de l'œuvre extrêmement difficile. Protégeant ainsi les droits et les bénéfices des détenteurs des droits d'auteur. Ce principe a été utilisé dans les vidéos où la marque indique si la vidéo peut être recopiée ou non. En effet, le détenteur d'un DVD a le droit de

réaliser des copies de sauvegarde, mais non de diffuser des copies à d'autres personnes. Les systèmes de reproduction conformes doivent donc tolérer les copies de première génération (réalisées à partir d'un original) mais interdire les copies de copies. Cette application a besoin de la création d'une architecture matérielle adaptée au schéma de tatouage.

**Contrôle d'Accès Sécurisé et Communiquant (CASC)**

Les documents d'identité, tels que les cartes d'identité, les passeports, les permis de conduire et le badge magnétique, contiennent des informations textuelles, une image d'identité, et éventuellement quelques autres caractéristiques biométriques comme les empreintes digitales ou une signature manuscrite. Aujourd'hui, avec le développement des nouvelles technologies, un contrefacteur peut aisément remplacer une photo ou modifier les informations sur ces documents dans la mesure où il est très difficile à le différencier de l'original. Dans le but de renforcer la sécurité, le tatouage numérique nous permet de marquer la photo d'identité par des informations liées au document (les empreintes digitales, la signature manuscrite, …) de manière à lier l'image aux autres composantes du document et ainsi d'élever significativement les performances du système d'accès.

**Autres applications** : Il existe d'autres applications de tatouage numérique [DWA10] telle que la gestion des transactions (Fingerprinting), e-commerce, l'ajout des informations publicitaires, etc.

La Figure 1.2 suivante présente les champs d'application du tatouage numérique classés en trois catégories suivant l'architecture de matériels utilisée.

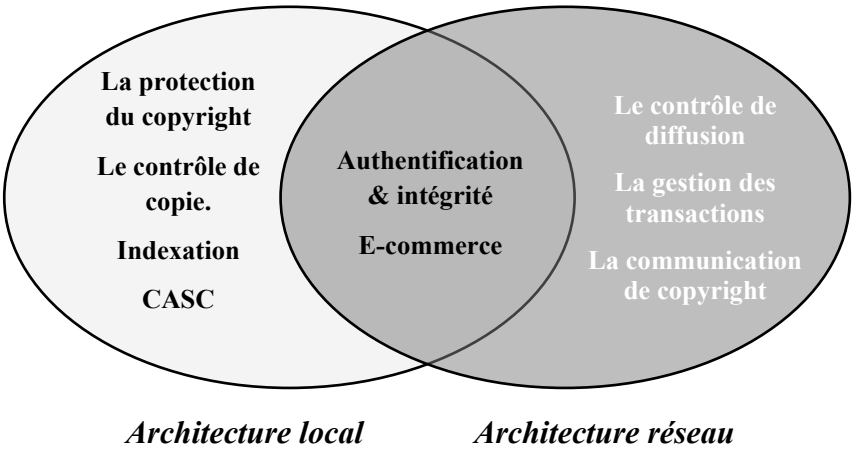



*Figure 1.2 : Les catégories d'applications de tatouage numérique*

## 1.3 La cryptographie

Les techniques de cryptage constituent la première solution pour empêcher l'accès non autorisé à des données numériques. Elles répondent aux besoins des utilisateurs en matière de sécurité comme la confidentialité, l'intégrité et l'authentification. On distingue deux familles de système de cryptographie: symétriques et asymétriques :

### 1.3.1 La cryptographie symétrique

Dans la cryptographie symétrique, les correspondants partagent la même clé pour chiffrer et déchiffrer les documents électroniques. Les algorithmes de chiffrement symétriques sont utilisés pour construire différents mécanismes cryptographiques comme les générateurs pseudo-aléatoires de nombres, les fonctions de hachage ou encore les codes d'authentification de messages. L'avantage de ce type d'algorithmes est qu'ils sont conçus pour chiffrer très rapidement des données de grande taille avec des clés relativement courtes.

Nous distinguons trois grandes familles de chiffrements symétriques :

**Le chiffrement par blocs** : Dans ce type de chiffrement, il y a une séparation du texte clair en blocs d'une longueur fixe. On peut les voir comme un chiffrement par substitution où

chaque bloc de taille fixe est substitué par un autre bloc. Le DES2 [FIPS99] [Fei73] est un algorithme de chiffrement par bloc de 64 bits utilisant des clés de 56 bits. Il a été remplacé par le triple-DES (3-DES). L'AES[3], le successeur du DES, est issu de la même famille.

**Le chiffrement par flots :** Le principe de ce type d'algorithmes est de chiffrer une suite de caractères (bit/bit ou octets/ octets), à l'aide d'une transformation qui varie au fur et à mesure du flux. Ils ont souvent recours un générateur de nombres pseudo-aléatoires.

**Les fonctions de hachage :** Elles sont utilisées comme un outil de vérification d'intégrité d'un document numérique [Wol96]. Une fonction de hachage opère généralement sur un message M de longueur arbitraire pour fournir une valeur de hachage h de taille fixe. Selon Rey et al [Rey01], pour qu'une telle fonction soit considérée comme sûre elle doit vérifier les propriétés suivantes:

- Il est *facile* de calculer $h$ connaissant $M$,
- Il est *difficile* de retrouver $M$ connaissant $h$,
- Il est *difficile* de trouver un message M' (différent de $M$) ayant comme valeur de hachage $h' = h$.

Parmi les fonctions de hachage utilisées, on cite : MD-4, MD-5 (Message Digest), SHA-1 (Secure Hash Algorithm) [FIPS10], etc.

### 1.3.2 La cryptographie asymétrique

Le problème de la cryptographie symétrique est que la clé doit être transmise entre l'expéditeur et le destinataire d'une manière sûre. Pour palier à ce problème, Whitffie Diffie et Martin Hellman [Dif76] ont inventé le concept de la cryptographie asymétrique (appelée aussi à clé publique). Ce type de chiffrement repose sur un schéma asymétrique qui utilise une paire de clés pour le chiffrement: une clé publique, qui chiffre les données, et une clé privée correspondante, aussi appelée clé secrète, qui sera utilisée pour le déchiffrement. Des exemples d'algorithmes asymétriques sont RSA [Bel94], DSA (Digital

[2] Data Encryption Standard
[3] Advanced Encryption Standard

Signature Algorithm) [Gol01]. Le principal inconvénient des algorithmes à clé public est leur grande lenteur par rapport aux algorithmes à clé secrète.

## 1.4 Principe de tatouage numérique

L'idée de base du tatouage numérique est de créer des métadonnées contenant des informations (par exemple le propriétaire de l'objet, le nombre de copies autorisées, le n° d'identification…) sur le document à protéger. Ces informations d'identification (ou signature) sont ensuite cachées de manière intime et résistant aux données (i. e, invisible ou inaudible suivant la nature du document). L'insertion s'effectue dans les composantes perceptibles (comme la luminance des pixels d'une image), et non dans l'en-tête du fichier [Fur05] [Cox98]. De ce fait, le tatouage est théoriquement indépendant du format de fichier. Il peut être détecté ou extrait même si le document a subi des modifications ou s'il est incomplet.

La Figure 1.3 représente un modèle générique d'un système de tatouage numérique. Ce modèle se découpe en deux phases fondamentales : l'insertion et la détection (ou l'extraction) de la marque (l'information d'identification).

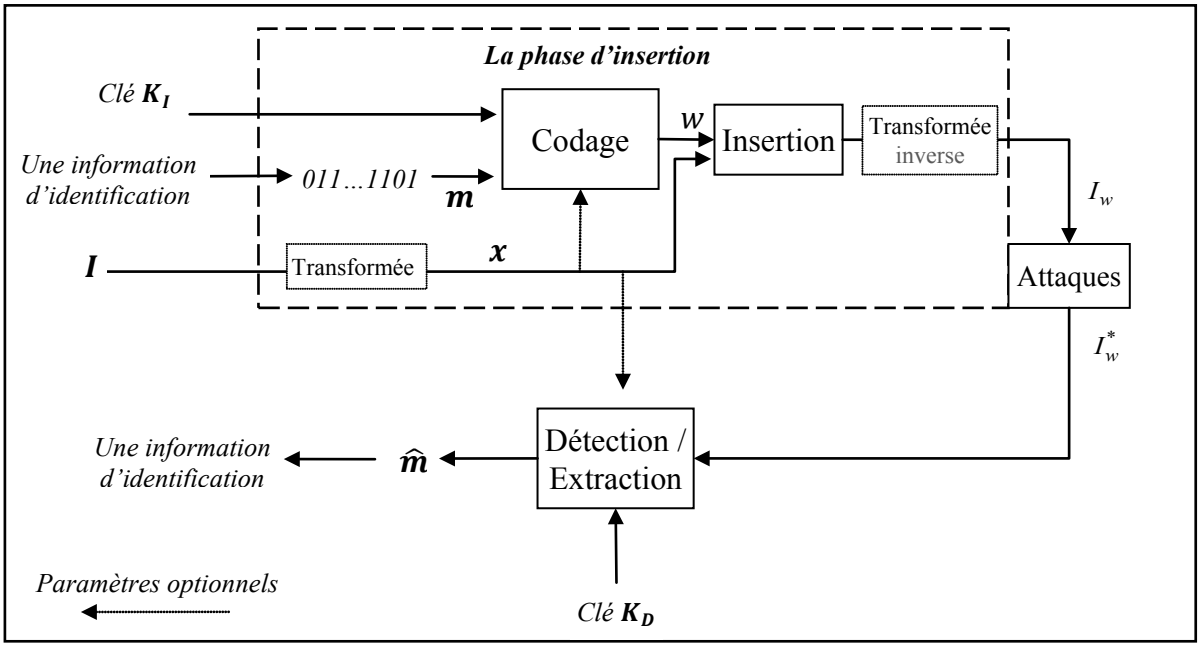



*Figure 1.3 : Le Modèle générique d'un système du tatouage*

La phase d'insertion consiste à insérer de manière imperceptible une information binaire *m*, de longueur *L* bits, dans le document original $I$ . Cette phase peut être modélisée par la fonction suivante :

$$I_w = \varepsilon(I, m, K_I) \qquad (1.1)$$

Pour être précis, nous devons distinguer entre le filigrane w (Watermark), qui est le signal réel ajouté aux données d'origine, et le message m qui constitue les informations véhiculées par le watermark.

Cette phase se décompose aussi en deux étapes principales: le codage de la marque et l'insertion :

Le codage consiste à générer le watermark $w$ à partir de $m$ et une clé $K_I$ par un opérateur de génération que nous appellerons $g : w = g(m, K_I)$.

Cette génération est effectuée soit par une modulation, codes correcteurs d'erreurs (e.g. BCH, Reed-Muller, Turbo Codes, etc.) ou autres techniques (cryptage, randomisation…).

L'étape d'insertion consiste à cacher w dans l'image d'entrée $I$. Cette insertion est effectuée dans le domaine d'une transformée $T$ appropriée (cf. la section 1.8 ci-dessous), possédant des propriétés d'invariance ou de dispersion facilitant l'insertion et rendant le watermark robuste et invisible. Cette transformation est suivie de l'extraction d'un vecteur caractéristique $x$ appelé également le signal hôte puis de la modification de ce vecteur suivant l'information *m* à cachée.

L'image sortant *Iw* est diffusée. Il est alors soumis à des attaques (des perturbations) licites ou illicites de nature inconnue (cf. la section 1.9). Dans la terminologie courante de tatouage numérique, une attaque est un traitement qui peut nuire à la détection du watermark ou à la communication de l'information véhiculée par le watermark. Cette version attaquée est notée $I_w^*$.

La détection, sert à vérifier l'existence ou non d'un tatouage dans un document numérique. Puis si la marque existe nous précédons à l'extraire (on obtient alors une estimation du message inséré).

Le tatouage est qualifié **informé** si l'image originale est utilisée pour générer la marque *w*. Il est dit **aveugle** si la détection de l'information cachée est effectuée directement à partir du signal tatoué, sans avoir connaissance du signal original. Dans le cas contraire, si l'image originale est utilisée, le tatouage est qualifié **non aveugle** (ou à décodeur informé).

Les clés $K_I$ et $K_D$ permettent de sécuriser le schéma de tatouage par l'application des techniques de cryptographie (cf. la section 1.3). La clé $K_I$ permet de crypter la marque. Une autre clés secrète est utilisée par des techniques pour localiser l'endroit où a été insérée la marque.

Par analogie avec la cryptographie, on distingue deux types de schémas de tatouage :

**Le schéma symétrique** (aussi appelées " à clés privées ") repose sur le principe de la cryptographie symétrique (cf. 1.3.1). Le processus de détection utilise la même clé (privée) que le processus d'insertion [Kat02], c'est-à-dire la clé d'insertion correspond à la clé de détection $\left(K_I = K_D\right)$.

**Le schéma asymétrique** repose sur l'utilisation de deux clés: une clé $K_I$ d'insertion privée et une clé de détection publique $K_D$. Cette dernière permet donc à n'importe utilisateur de vérifier la présence du tatouage et de détecter la marque mais seule la connaissance de $K_I$ permet d'enlever ou détruire $w$.

## 1.5 Contraintes de conception d'un algorithme de tatouage

Quel que soit le schéma de tatouage, le concepteur doit faire un compromis entre L'imperceptibilité, la capacité et la robustesse aux attaques que le schéma va pouvoir supporter. Cela est illustré par la Figure 1.4.

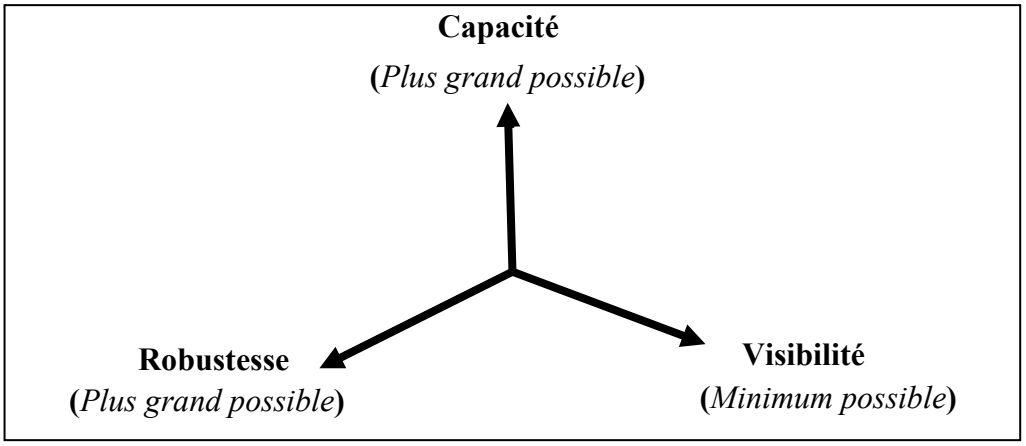



*Figure 1.4: Le compromis entre robustesse, capacité et visibilité*

**La capacité :**

On désigne par la capacité, la taille maximale de la marque qu'il est théoriquement possible d'insérer sans erreur. Plus que la capacité est grande plus la déformation est grande. En général, La taille de la marque est généralement fixée et elle est la même à la phase de l'insertion et l'extraction.

**L'imperceptibilité** :

Appelée aussi la distorsion d'insertion [Cox07], Il s'agit de faire en sorte que l'impact visuel du marquage soit le plus faible possible afin que l'image tatouée soit visuellement équivalente à l'image originale. Pour respecter cette contrainte d'imperceptibilité, l'algorithme de tatouage doit rendre l'énergie du watermark très inférieure à celle de l'image. Par exemple, insérer une marque de taille plus importante sans différencier le document tatoué de l'original induit que le schéma sera moins robuste.

**La robustesse :**

Il s'agit de la capacité à détecter la marque après des modifications dues à quelques attaques involontaires (des traitements qui ne visent pas forcément à retirer la marque) ou volontaires qui ont pour seul but de retirer le watermark (cf. la section 1.9).

En plus de classement présenté précédemment des schémas de tatouage, Il existe aussi trois types de schéma de tatouage en fonction de leur robustesse : le tatouage robuste, semi-fragile et fragile.

- **Tatouage robuste :** ils sont conçus dans le but de protéger des documents. Ils doivent résister au maximum d'attaques, voir même de leurs combinaisons, et permettre des attaques naturelles tout en préservant la signature. ce type de tatouage est utilisé surtout dans les applications de protection de copyright et le contrôle de copies que nous avons cité dans la section 1.2 ci-dessus.

- **Tatouage semi- fragile :** ce type de tatouage rend l'algorithme plus robuste face à certaines manipulations autorisées. Leurs applications sont surtout réservées à l'authentification d'images (par exemple les photos d'identité (cartes d'identité, passeport, permis de conduire), les images médicales (scanner, IRM, ...)). Divers méthodes d'authentification par le tatouage semi-fragile ont été proposées. Par exemple, une solution transparente à une compression JPEG a été proposée par Lin et Chang [Lin01b] en exploitant quelques propriétés d'invariance des coefficients de la DCT vis-à-vis de JPEG. une autre solution reposant sur la transformée en ondelettes est présentée dans [Lu03][Sun05]. Autres techniques reposent également sur l'insertion de données provenant elles-mêmes du document (self-authentification) [Boh09] [Rey00].

- **Tatouage fragile** : Il est néanmoins intéressant de remarquer qu'il peut être utile, dans certain cas, de favoriser une fragilité plutôt que une robustesse. Le principe de ce type d'algorithmes est d'exploitée la fragilité du tatouage afin d'authentifier (prouver l'intégralité) des images. De ce fait, si la marque est altérée, l'image n'est plus considérée comme authentifiée. Nous citons, par exemples, les techniques reposant sur la substitution de plan LSB[4] de l'image par la différence entre l'image et sa forme chaotique [Car11] ou par la carte des conteurs et les moments invariants [Kha06].

[4] Bit le plus moins significatif (LSB-least significant bit substitution)

En plus des contraintes précédentes, d'autres critères sont aussi à prendre en compte suivant l'application visé :

**La sécurité :**

Cette propriété est indépendante des trois premières mentionnées au-dessus. Il s'agit de protéger les informations insérées par des méthodes de cryptographie (cf.1.3) afin d'éviter qu'elles soient falsifiées ou manipulées. Le schéma de tatouage doit résister aux attaques visant à décrypter la clé $K_I$. La méthode du tatouage doit également respecter le principe de Kerckhoff : « *La sécurité d'un algorithme doit résider dans le secret de la clé. Les algorithmes utilisés doivent pouvoir être rendus publics*».

**La complexité algorithmique (Le coût):**

Dans certaines applications, comme le contrôle de diffusion et la sécurité des cartes d'accès, la rapidité est primordiale. La lecture doit être effectuée en temps réel. Généralement, en tatouage numérique, la complexité en écriture est moins cruciale que la complexité en lecture.

## 1.6 Le codage de la marque

Souvent, en tatouage numérique, la signature à insérer est un message binaire {0,1}, un logo (une image binaire ou de même nature que l'image originale). La marque est générée de façon pseudo aléatoire à partir de la signature. Le nombre utilisé dans cette génération constituera la première clé $K_I$ de l'algorithme du tatouage. Ce nombre permet par la suite de déterminer le message. Par exemple, Li et Cox dans [QLi07] brouillent (randomiser) l'information binaire à insérée de façon pseudo aléatoire afin d'améliorer la performance de la détection.

Les codes correcteurs d'erreur sont potentiellement utilisés en tatouage numérique pour coder et protéger la marque des erreurs de transmission ou de stockage (attaques), et ainsi augmenter les performances en termes de la robustesse des algorithmes de tatouage. Différents codes dérivés des codes correcteurs d'erreur sont alors proposés: dans [Che05], Chen et al proposent l'utilisation des codes cycliques dans l'authentification de visages

photographiques par tatouage d'images, ce sont des codes linéaires utilisés en raison de leurs bonne adaptation à la détection des erreurs indépendantes et à la détection possible par paquets ; Dans [Sch06], Schönfeld et Winkler propose l'insertion de watermark en utilisant le codage BCH.

## 1.7 Les méthodes d'insertion

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

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

### 1.7.1 Schéma additif

La Figure 1.5 présente le schéma aditif pour l'insertion du message. Le tatouage est ajouté aux composantes du document. D'où, la fonction $\varepsilon(I, m, K_I)$ est décrite par l'équation (1.2):

$$\varepsilon(I, m, K_I) = x + w \qquad (1.2)$$

Avec $w = g(m, K_I)$ et $x$ est le signal hôte extrait à partir de *I*.

Le signal hôte *x* peut cependant intervenir dans la génération de w, soit par l'emploi d'un masque perceptuel [Vin06][Ros06], soit dans une adaptation au tatouage: $w = g(m, K_I, x)$.

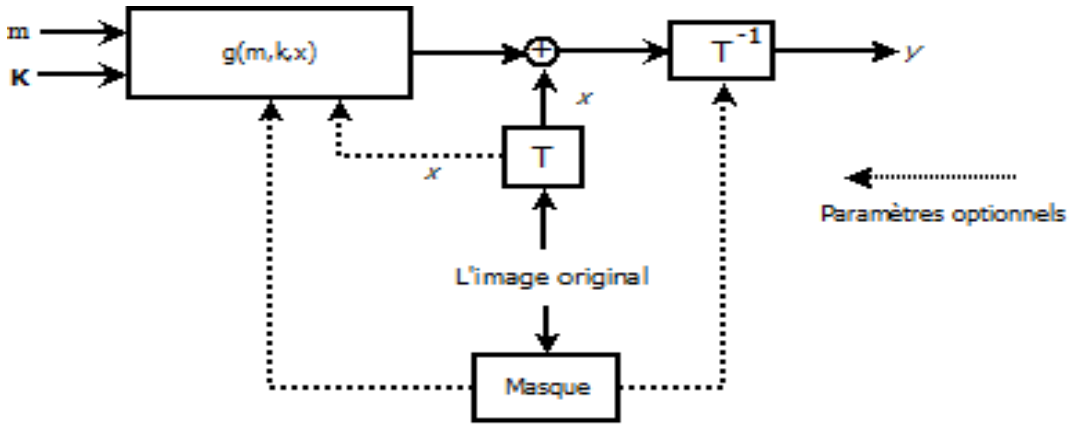



*Figure 1.5: L'insertion du message par tatouage additif*

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

La technique la plus populaire pour ce type de schéma est l'étalement de spectre. Cette technique a été utilisée pour la première fois en tatouage numérique d'image par Cox [Cox97]. Le principe consiste à coder les symboles de m séparément en utilisant une modulation par des séquences pseudo-aléatoire (appelées porteuses). Cette technique permet d'assurer un cryptage du message, de fait que la détection nécessite la connaissance de la porteuse utilisée qui dépend d'une clé secrète. La détection est effectuée par l'exploitation des caractéristiques statistiques de la marque insérée avec le document tatoué. Souvent un calcul de corrélation permet de détecter l'existence de la marque.

Formellement, le tatouage par étalement de spectre peut être modélisé comme suit : on cherche à insérer un message binaire de L bits $m \in \{0,1\}^L$ dans un vecteur $x \in \mathbb{R}^{N_v}$. Ce vecteur est censé capturer la plupart des informations perceptuelles sur le contenu à tatouer. Par exemple, *x* peut être issu d'une sélection de coefficients DCT par bloc, d'un ensemble de coefficients d'ondelettes, etc.

Le message $m$ est codé en utilisant *L* porteuses $u_i \in \mathbb{R}^{N_v}$ que l'on assimile à des mots de code. Ces porteuses sont issues d'un générateur pseudo-aléatoire initialisé avec une graine K qui fait office de clé secrète. Les porteuses $u_i$ sont des vecteurs gaussiens de loi $\mathcal{N}(0,1)$ et forment une base orthogonale, i.e. $\forall i \neq j, < u_i \mid u_j >= 0$ où $< . \mid . >$ désigne le produit scalaire. La construction du watermark (la marque de tatouage) *w* nécessite une modulation $s : 0,1 \to \mathbb{R}$ :

$$w = \sum_{i=0}^{L} u_i s\left(m(i)\right) \tag{1.3}$$

On ajoute ensuite *w* à *x* pour former *y* le vecteur tatoué :

$$y = x + w \tag{1.4}$$

Le décodage du message tatoué produit une estimation $\hat{m}$ :

$$\hat{m}(i) = signe\left(< y^* \mid y >\right) \qquad (1.5)$$

Où $y^*$ est le vecteur tatoué *y*, éventuellement attaqué.

L'étalement de spectre classique (SS) utilise une modulation simple. Le paramètre $\gamma$ permet de régler l'ampleur de la distorsion :

$$S_{SS}\left(m(i)\right) = \gamma(-1)^{m(i)} \qquad (1.6)$$

L'avantage de cette méthode de modulation est qu'elle a une grande robustesse aux déformations et bruit pouvant perturber l'image tatoué [Cox97]. Le principal inconvénient par contre, est la capacité de tatouage très réduite pour ce genre de méthode. En effet, le document hôte est considéré comme source d'interférences et une partie de la capacité est perdue pour résister à ces interférences. De plus, l'encodage se fait de manière indépendante de l'hôte (le vecteur *x*). Du point de vue visuel, le résultat est assez efficace, car la modulation par une séquence proche d'un bruit blanc passe bien inaperçue à peu près partout, sauf dans les sections uniformes. Pour cela, Malvar et Florêncio [Mal03] ont introduit l'étalement de spectre amélioré (ISS) qui permet de prendre en compte le vecteur $x$ dans le codage de message (l'information adjacente):

$$S_{ISS}\left(m(-1)\right) = \alpha(-1)^{m(i)} - \lambda\frac{< x \mid u_i >}{\|u_i\|^2} \qquad (1.7)$$

Où α et λ sont des paramètres ajustés pour contrôler le compromis entre l'invisibilité et la robustesse.

La probabilité d'erreur peut être calculée:

$$\rho = \mathrm{P}\left(\hat{m}(i) = 0 / m(i) = 1\right) \qquad (1.8)$$

Cette probabilité a été calculée dans [Bou08] par Bouchakour et *al*. On obtient :

$$\rho = \frac{1}{2} erfc\left( \sqrt{\frac{\frac{N\sigma_u^2}{\sigma_x^2} - \lambda^2}{2\left(\sigma_n^2 + 1\left(1-\lambda\right)^2 \sigma_x^2\right)}} \right) \qquad (1.9)$$

D'après [Bou08], La valeur optimale de λ peut calculée en utilisant le critère de Neyman-Pearson par l'équation (1.10) suivante:

$$\lambda_{opt} = \frac{1}{2}\left( \left(1 + \frac{\sigma_n^2}{\sigma_x^2} + N_v \frac{\sigma_u^2}{\sigma_x^2}\right) - \sqrt{\left(1 + \frac{\sigma_n^2}{\sigma_x^2} + N_v \frac{\sigma_u^2}{\sigma_x^2}\right)^2 - 4N_v \frac{\sigma_u^2}{\sigma_x^2}} \right) \qquad (1.10)$$

La variance $\sigma^2$ est définie comme suit:

$$\sigma^2 = \frac{1}{\left(MN\right)^2} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} Y_{i,j}^2 \qquad (1.11)$$

### 1.7.2 Schéma substitutif

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

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

#### 1.7.2.1 Le tatouage quantitatif

Appelé aussi tatouage substitutif avec dictionnaire [Vin06]. Le principe est de substituer le signal hôte par des états de quantification correspondant à différents messages à cacher. L'extraction se fait en prenant l'état le plus proche des données reçues z, et donc le message correspondant.

Contrairement à l'étalement de spectre vu au-dessus, l'avantage de schéma par quantification est qu'il est possible de définir un ensemble de quantificateurs tel qu'il n'y ait aucune erreur pour un niveau de bruit donné. Ainsi, si le bruit ajouté est inférieur à la distance minimale (Le pas de quantification) entre deux états de quantification ($\Delta$/2 dans le

cas présenté dans la Figure 1.6), l'extraction est sans erreur. De ce fait, il est possible de développer une résistance absolue à une attaque parfaitement (par exemple: JPEG).

Cependant, L'inconvénient majeur réside dans la résistance aux changements d'échelle du canal lors de l'attaque ( $y = \alpha \times x$ ) et à l'ajout de bruit non blanc. Les quantificateurs seront décalés et l'extraction sera mise en défaut.

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

La technique la plus populaire pour ce type de schéma est la quantification par la modulation d'index (QIM) de Chen et Wornell [Chen01]. En effet, les travaux de Chen et Wornell [Chen01] en 2001 marquent le début des recherches sur les fonctions d'insertion par quantification, qualifiés par la suite de codage informée. Le principe consiste à quantifier le vecteur *x* en utilisant un ensemble de quantificateurs indexés par le message à transmettre. Ainsi, à chaque symbole du message *m(i)* est associé un quantificateur différent, et le tatouage s'effectue par quantification du vecteur x avec le quantificateur correspondant au message à transmettre.

La Figure 1.6 illustre un exemple simple de quantification par QIM, considérons le cas où *m=0* ou *1*. Le vecteur *x* est divisé en deux ensembles de points disjoints A et B en utilisant d'une fonction de quantification *Q(x, m)* avec un pas de quantification $\Delta$. L'ensemble A correspond à *m=0* et B correspond à *m=1*. En suite, en fonction de bit à cacher, chaque élément de vecteur *x* est quantifié au plus proche point, c'est à dire *Q(x, 0)* ou *Q(x, 1)*.

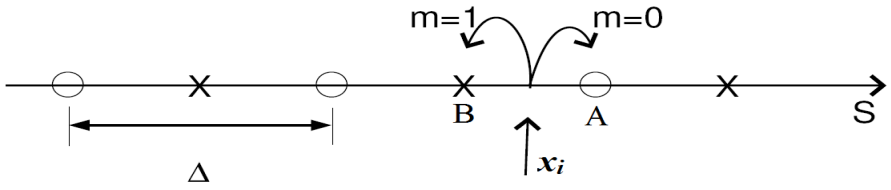



*Figure 1.6: un exemple simple de QIM, l'ensemble A et B sont représenté respectivement par un cercle et une croix*

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

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

Dither-modulation QIM (DM-QIM) [Chen01][Cox07] est l'implémentation de QIM la plus utilisée par le comité de tatouage numérique. Cela consiste à insérer avant quantification un signal permettant de réduire les artefacts visuels entre les données quantifiées puis reconstruites et les données originales. Il peut de plus servir de clef nécessaire à l'extraction (i.e. Appliquer un décalage aux quantificateurs). Les décalages sont représentés classiquement par des vecteurs pseudo-aléatoires appelés « *dither vectors* ». Il suffit de moduler le dither vector par le message à transmettre, c'est-à-dire faire correspondre à chaque symbole de message *m(i)* un unique dither vector *d(m(i))*. En plus, le dither vector peut être utilisé comme une clé afin d'améliorer la sécurité de la méthode. Cette clé doit être partagée entre le tatoueur et le décodeur.

En effet, l'opération consiste à quantifier chaque vecteur *x* par le dither vector qui le correspond en utilisant la fonction suivante :

$$y(n) = Q\left(x(n) + d\left(n, m(n)\right), \Delta\right) - d\left(n, m(n)\right);\ n = L \qquad (1.12)$$

Où

$$d(n,1)=\begin{cases} d(n,0)+\dfrac{\Delta}{2} & , d(n,0)>0 \\ d(n,0)-\dfrac{\Delta}{2} & , d(n,0)<0 \end{cases} \qquad (1.13)$$

$d(n,0)$ est une vecteur pseudo aléatoire à distribution uniforme choisit dans l'intervalle $\left[-\Delta/2, \Delta/2\right]$ généré par une clé sécrète **K**.

$Q(*,\Delta)$ est une fonction de quantification avec le pas $\Delta$, définie par :

$$Q(*,\Delta)=round\left(\frac{*}{\Delta}\right)\Delta \qquad (1.14)$$

La détection consiste à générer d'abord le *d(n,0)* par la clé sécrète *K* puis à calculer un vecteur Sz(n,0) correspondant à 0 et Sz(n,1) à 1. Ces deux vecteurs sont calculés de la même manière que l'insertion par l'équation (1.12), comme illustré dans l'équation suivante :

$$\begin{aligned} S_z(n,0)&=Q(z_n+d(n,0),\Delta)-d(n,0) \\ S_z(n,1)&=Q(z_n+d(n,0),\Delta)-d(n,1) \end{aligned} \qquad (1.15)$$

L'estimation de la marque consiste à déterminer lequel de ces deux vecteurs $S_z(n,1)$ et $S_z(n,0)$ minimise la distance euclidienne entre lui et le vecteur reçu z, selon l'équation suivante :

$$\hat{m}=\arg\min dist(z,S_z(n,l)) \qquad (1.16)$$

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

#### 1.7.2.2 Le tatouage par contrainte

Le principe est de substituer le watermark à des caractéristiques de l'image. Ces caractéristiques sont extraites en appliquant une contrainte ***c*** (une mesure de similarité, une propriété géométrique ou un critère d'ordre…) sur les composantes de l'image de telle sorte

que, à la détection, l'image est considérée comme tatouée si cette contrainte est vérifiée. La fonction d'insertion devient $\varepsilon(I, m, c, x, K_I)$.

Un exemple de méthode illustrant ce principe est celle proposée par Koch et Zhao [Koch98]. Cette méthode consiste à fixer une contrainte entre $m$ et une variable booléenne calculée à partir d'une comparaison entre les zones des coefficients DCT. L'extraction est effectuée en comparant les valeurs des coefficients DCT afin de déterminer si le bit concerné du message était un 0 ou un 1.

## 1.8 Les domaines d'insertion

Comme nous l'avons mentionné dans la section 1.4, l'insertion de la marque est effectuée dans un domaine d'une transformation inversible. Le choix du domaine d'insertion est une étape délicate dans la conception du système de tatouage. Différents critères régissent le choix d'un domaine adapté [Aws03][Cmb02]. Ce domaine peut :

- Permettre de décorréler le signal hôte (l'image) du signal de tatouage. Cette décorrélation tente de ramener le système de tatouage à avoir des performances optimales.
- Rendre la distorsion d'insertion moins faible. En effet, permettre une altération importante de certaines composantes de l'image sans modifier la perception de celui-ci peut faciliter la détection du tatouage.
- Etre invariant à certaines perturbations subies par l'image; ce critère est fréquemment utilisé lorsque les perturbations désynchronisantes sont considérées. Cette invariance facilite la conception de systèmes robustes aux perturbations.

La littérature propose les différents domaines respectant au moins l'un de ces critères (mais jamais les trois). Nous présentons dans les sous sections suivantes les domaines d'insertion les plus utilisés. Ainsi, nous présentons quelques exemples des méthodes de tatouage pour chaque domaine:

### 1.8.1 Le domaine spatial

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

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

La technique de substitution de plan LSB [Pan04] qui constitue l'une des premières méthodes proposées dans la littérature. En effet, les valeurs des pixels de l'image sont codées sur 8 bits. Ce qui permet de découper l'image en 8 plans comme illustré dans la Figure 1.7. La méthode de tatouage du LSB consiste donc à forcer le poids faible de chaque pixel à 0 ou 1, suivant la valeur du bit de la séquence contenue dans le watermark. Cette méthode est très simple, l'image marquée n'est pas visiblement dégradée parce que les données contenues dans les bits LSB sont visuellement insignifiantes. Cette simplicité se paye par une très faible robustesse : n'importe quel traitement, même peu important, suffit à modifier les LSB et donc à rendre l'extraction impossible. D'où elle peut être utilisée pour véhiculer des informations ou pour concevoir un schéma de tatouage fragile (cf. La section 1.4).

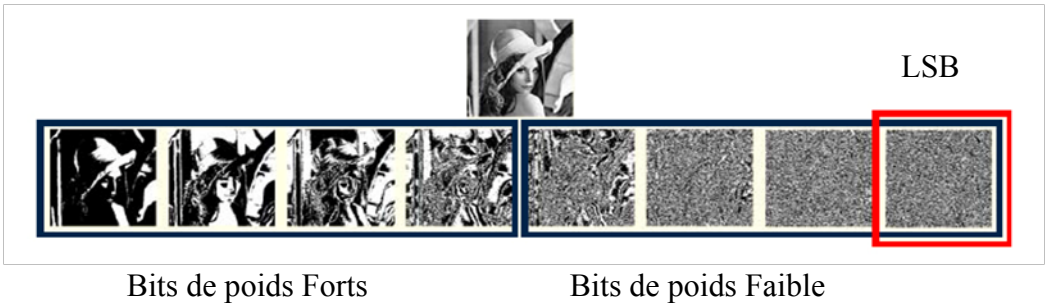



*Figure 1.7: Découpage de l'image lena en 8 plans*

Afin de gagner des performances au niveau de la robustesse, [Ben95] ont proposé une méthode renommée par Patchwork, qui repose sur la différence de luminance observée entre deux ensembles de pixels, déterminés à l'aide d'une clé. Ainsi, l'insertion consiste à modifier les pixels du premier ensemble d'une quantité $c$ et l'on diminue les pixels de

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

Une amélioration de la méthode précédente est présentée dans [Del00] et [Dar98]. Cette amélioration adapte la marque à l'image en utilisant sur critères visuels élémentaires. Il s'agit d'un tatouage par blocs de 8×8. La marque est incrustée dans ces blocs afin d'avoir une certaine résistance à la compression JPEG. En suite, chaque bloc est divisé en catégorie A ou B suivant une grille prédéfinie et choisie par le biais d'une clé secrète. L'insertion des bits dans les blocs est effectuée en utilisant un ensemble de règles basées sur l'analyse statistique de chaque bloc.

Récemment, des algorithmes robustes à quelques attaques géométriques sont proposés dans le domaine spatial. Nous citons par exemple celles publiés dans [Li09], [Wu07]. Néanmoins, les marquages dans le domaine spatial résistent très mal à tout type d'attaque, géométrique ou fréquentiel. Cet inconvénient a dirigé les chercheurs vers l'utilisation d'autres domaines robustes à ce type d'attaques comme DFT, DCT et DWT.

### 1.8.2 Le domaine de Fourier

La théorie de Fourier permet de décomposer une image en une série de sinusoïdes à différentes fréquences. L'équation (1.17) donne la décomposition d'une image $I_0$ de taille en $N1 \times N2$ utilisant la transformée de Fourier :

$$F(p,q) = \sum_{m=0}^{N_1-1} \sum_{n=0}^{N2-1} I_0(m,n) e^{-j(2\pi/N_1)pm} e^{-j(2\pi/N_2)qn} \tag{1.17}$$

Avec $j = \sqrt{-1}$, $p = 1,2,...,N_1$ et $q = 1,2,...,N_2$.

La décomposition de la transformée de Fourier inverse est donnée par :

$$I_0(m,n) = \frac{1}{N_1 N_2} \sum_{m=0}^{N_1-1} \sum_{n=0}^{N2-1} F(p,q) e^{j(2\pi/N_1)pm} e^{j(2\pi/N_2)qn} \tag{1.18}$$

L'équation (1.17) peut être représentée aussi sous la forme :

$$F(p,q) = \left|F(p,q)\right| e^{-j.\phi(p,q)} \qquad (1.19)$$

Où la fonction $\left|F(p,q)\right|$ représente le spectre de la transformée de Fourier de $I_0$ tandis que $\phi$ est sa phase. $\left|F(p,q)\right|^2$ est le spectre de puissance de $I_0$. La Figure 1.8 représente l'image Lena et le spectre de sa transformée de Fourier.

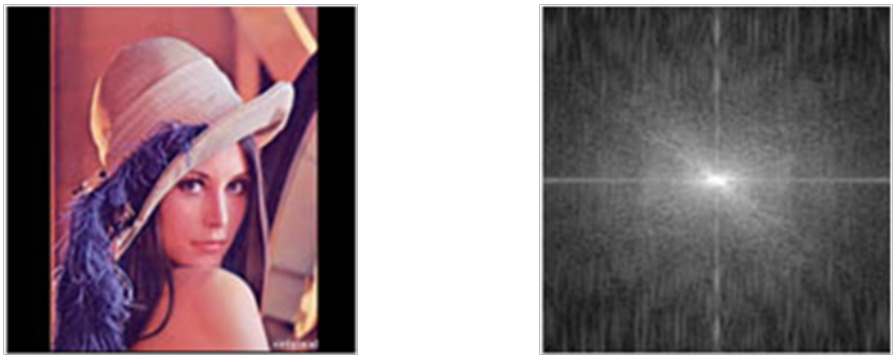


*Figure 1.8: Image Lena et son spectre de Fourier*

Cette transformation permet de contrôler les fréquences du signal. Elle permet de choisir adéquatement les zones adéquates à l'insertion de la marque, de telles sortes à obtenir un bon compromis robustesse-invisibilité. Aussi, le principal avantage de ce domaine est qu'il est invariant à la translation et au changement d'échelle.

Piva et al. [Piva98] ont présenté une approche de tatouage d'images basée sur la transformée de Fourier discrète (DFT). Malgré sa faible robustesse, elle est intéressante pour la compréhension du tatouage d'image dans le domaine de Fourier. Cette méthode a été améliorée par Solachidis [Sol00] puis par F. Ros et al [Ros06]. La marque est générée d'une manière pseudo aléatoire à moyenne nulle. L'insertion se fait dans les bandes moyennes de fréquence. Comme illustré dans la Figure 1.9, les auteurs proposent d'insérer le même message deux fois dans deux sous bandes des fréquences moyennes. Un masque psychovisuels est utilisé pour remédier au problème de la difficulté de maîtriser le résultat au niveau local sur l'image finale.

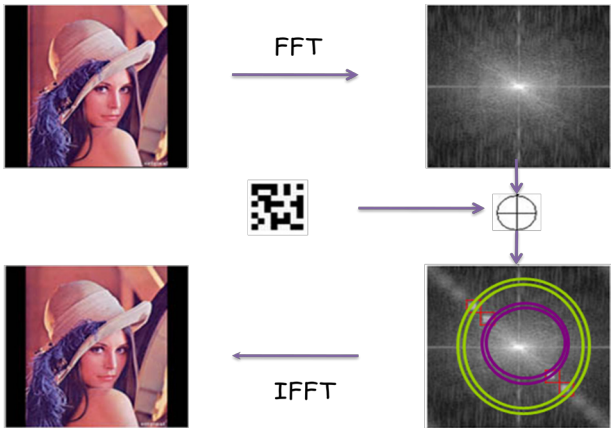



*Figure 1.9: Exemple d'insertion dans le domaine de Fourier*

Afin de pouvoir compenser une attaque basée sur des transformées géométriques, F. Ros et al [Ros06] ont ajouté des pics de référence aux amplitudes de DFT de l'image. Grâce à cette technique, il est possible de synchroniser le signal en détectant les pics insérés, la marque peut alors être extraite et décodée. La phase de détection consiste à calculer de la corrélation entre la marque générée et les coefficients de Fourier de l'image tatouée.

Une autre technique dans le domaine de Fourier est proposée par Perreira et al [Per99]. Cette méthode de tatouage est particulière dans le sens où elle fait intervenir deux techniques distinctes; l'une est destinée à réaliser le tatouage, l'autre utilise un gabarit particulier dont le but est de permettre la recherche de la transformation affine que l'image tatouée a subit afin de réaliser un recalage des informations à extraire.

L'invariance par translation est obtenue par la transformation de Fourier de l'image en utilisant que le module [Ros06]. Alors que les invariances par rotation et changement d'échelles peuvent être obtenues par la transformation de Fourier-Mellin du module [Rua97] [Lin01a]. En effet, 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 ; et d'autre part, par un changement de repère, de cartésien vers logarithmique-polaire. Ce changement de repère ramène les opérations de rotation et de changement d'échelle à une translation. Cependant, la difficulté de l'implémentation constitue un problème majeur de cette transformation [Qi04].

### 1.8.3 Le domaine de la transformée en Cosinus Discrète (DCT)

La transformée en cosinus discrète DCT afin d'anticiper et de rendre le watermark plus robuste à une compression JPEG, puisqu'elles utilisent le même espace qui sert au codage de l'image. Elle permet entre autres de réduire la corrélation spatiale entre les pixels d'une image. Un autre avantage en faveur de l'utilisation de DCT est la possibilité de bénéficier des études psychovisuelles déjà menées en codage de source (par exemple, les travaux de Watson [Wat97] et Lubin [Lub95]). En effet, elles se proposent de prendre en compte les phénomènes connus comme la représentation de la couleur, la sensibilité au contraste et les effets de masquage.

La transformée en cosinus discrète d'une image $I_0$ de taille $N_1 \times N_2$, notée par $F_{DCT}(I_0)$, est donnée par :

$$F(p,q) = \frac{2\Lambda(p)\Lambda(q)}{\sqrt{N_1 N_2}} \sum_{m=0}^{N_1-1} \sum_{n=0}^{N_2-1} I_0(m,n).\cos\left[\frac{\pi(2m+1)p}{2N_1}\right].\cos\left[\frac{\pi(2n+1)q}{2N_2}\right] \quad (1.20)$$

Avec :

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & si \quad \xi = 0 \\ 1 & \sin on \end{cases}$$

La transformée en cosinus discrète inverse, notée par $F_{DCT}^{-1}$, est donnée par

$$I(m,n) = \frac{2}{\sqrt{N_1 N_2}} \sum_{p=1}^{N_1} \sum_{q=1}^{N_2} F(p,q)\Lambda(p)\Lambda(q).\cos\left[\frac{\pi(2m+1)p}{2N_1}\right].\cos\left[\frac{\pi(2n+1)q}{2N_2}\right] \quad (1.21)$$

De nombreuses méthodes ont été développées dans ce domaine. Dans [Cox97], Cox et al présentent un schéma non aveugle de tatouage par l'étalement de spectre dans le domaine de DCT. La marque est insérée par une modification de 1000 coefficients DCT plus grandes amplitudes, de façon à ce que le watermark soit inséré dans les zones visuellement significatives.

Le calcul la DCT sur toute l'image prendrait un temps très long. Pour éviter cela, on applique la DCT sur des blocs de longueur fixe. Généralement, la taille des blocs DCT utilisée est de 8 x 8 pixels : ce choix donne un meilleur compromis entre la qualité et le temps de calcul. La Figure 1.10 présente une technique non-aveugle proche de la méthode de [Cox97] est présentée par Suhail [Suh03], mais ne travail pas sur l'image complète. L'image est préalablement découpée en blocs. Le message, constitué d'une séquence aléatoire, est inséré dans les fréquences moyennes de chaque bloc. Les résultats présentés par les auteurs montrent une nette amélioration de l'ensemble des caractéristiques comparées aux résultats de [Cox97].

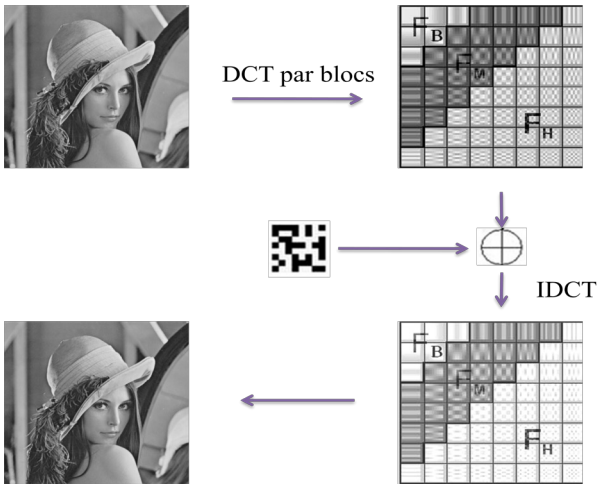



*Figure 1.10: Exemple d'insertion dans les fréquences moyennes de DCT.*

Dans [Koch98] une technique de tatouage d'image dans le domaine de DCT est proposée. Le principe consiste à insérer la marque dans un bloc de taille 8×8. Pour chaque bloc, les auteurs calculent la transformé DCT puis ils sélectionnent deux ou trois coefficient des moyennes fréquences. Ces coefficients sont ensuite quantifiés à l'aide de la table de quantification correspondant à la compression JPEG [Pen93]. La quantification des coefficients DCT par QIM est présentée dans [QLi07], [Che07] et [Wu11].

### 1.8.4 Domaine d'ondelettes

L'utilisation de la transformée en ondelette discrète DWT est intéressante pour le tatouage numérique grâce à son utilisation dans l'algorithme de la compression JPEG2000. De plus, cette transformée peut être interprétée comme une décomposition de l'image en sous bandes fréquentielles ce qui permet de développer facilement des masques psycho-visuels. En plus de la robustesse commune avec la DCT, le tatouage dans le domaine d'ondelettes est robuste à un changement d'échelle de facteur. De plus, les masques perceptuels sont plus fins et il y a moins d'effets de blocs.

Dans le chapitre suivant, nous détaillons le principe de cette transformation, ainsi que les différents algorithmes basant sur cette transformée comme domaine d'insertion.

### 1.8.5 Autres domaines

Outre les FFT, DCT et DWT précédemment cité, d'autres transformations inversibles classiques en traitement d'images ont été aussi envisagées, sans apporter en pratique une amélioration significative des performances ou des invariances géométriques. Nous citons par exemple, l'utilisation de la décomposition en valeurs singulières (SVD) [Hu11] [Qua04] et La transformation de Karhunen-Loève (KLT) [Sta03].

### 1.8.6 La combinaison des domaines

Nous trouvons aussi dans la littérature des méthodes qui reposent sur l'utilisation de la combinaison entre les domaines d'insertion (algorithmes hybrides). Nous citons l'exemple de la méthode présentée dans [Lef01]. Cette méthode de tatouage est particulière dans le sens où elle effectue un tatouage dans le domaine spatial et fréquentiel. Dans le domaine spatial, la marque est incrustée via l'algorithme du "2-D Cyclic Pattern". Dans le domaine fréquentiel, un gabarit est incrusté afin de permettre la détection des transformations géométriques de type rotation et changement d'échelle. Enfin, un masque psychovisuel est utilisé afin de garantir l'invisibilité de la marque dans l'image.

Dans [Gan04], [Yav07] et [He06], un schéma hybride basé sur DWT et la décomposition en valeurs singulières (SVD) est présenté. Après la décomposition de l'image en quatre

sous-bandes, Les auteurs appliquent la SVD à chaque bande, et insèrent les données de la marque en modifiant les valeurs singulières.

Le domaine DWT et celui de Fourier ont été combinés par Hu et al [Hu11]. DFT est utilisée pour palier au problème de désynchronisation liée aux attaques géométriques par l'insertion d'un gabarit dans les moyennes fréquences. Alors que, DWT est utilisé pour insérer la marque.

## 1.9 Attaques sur les images tatouées

Comme nous l'avons déjà mentionné dans le paragraphe 1.4 ci-dessus, dans le cas d'un tatouage robuste, la marque doit résistée à un grand nombre d'attaques volontaires (piratage) ou naturelles Les algorithmes de tatouage d'image sont généralement développés pour répondre à une ou plusieurs attaque(s) en particulier. Cela signifie qu'il est impossible de développer un algorithme général pour l'ensemble des attaques connues et inconnues. Dans cette section, nous allons présenter une liste non exhaustive des attaques les plus courantes que peut subir une image.

Dans la littérature, plusieurs classifications des attaques de tatouages ont été proposées. Par exemple, celles présentées par S. Voloshynovskiy et al. [Vol01a] et Cox et al [Cox07].

La classification proposée par Cox et al est basée sur la nature des transformations appliquées sur l'image et sur l'intention de l'utilisateur. En effet, cette classification distingue deux types d'attaques : les attaques à la robustesse et celles sur la sécurité. En outre, celle proposé par Voloshynovskiy comporte quatre catégories d'attaques : les attaques d'effacement, les attaques géométriques, les attaques de cryptographie et les attaques de protocoles.
En se basant sur [Vol01a] et [Cox07], nous proposons dans la Figure 1.11 une classification en trois catégories :

- Les attaques d'effacements.
- Les attaques géométriques.
- Les attaques de sécurités

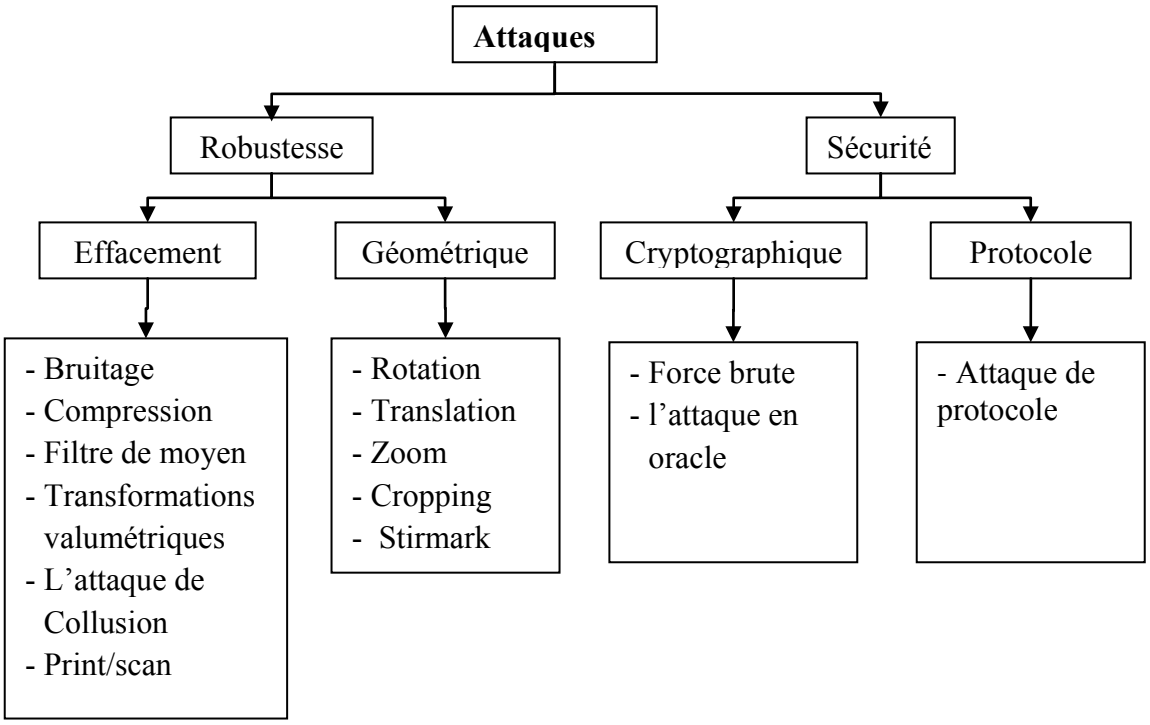



*Figure 1.11: La classification des attaques que peut subir un document tatoué*

## 1.9.1 Attaque d'effacement

Ce sont des attaques liées à l'image (ou au signal de watermark), dont le but est de faire disparaître le watermark masqué dans l'image. Cela se résume à des transformations plus ou moins violentes. Ces transformations ont pour but de rendre illisible le marquage. Il est intéressant de remarquer néanmoins que ces attaques ne sont pas forcément volontaires. En effet, sans le savoir, l'image peut être dégradée suffisamment pour que le tatouage soit effacé. Un algorithme de marquage robuste est sensé résister de manière efficace à ce type de transformations, ou du moins tant que l'image reste utilisable. Nous citons par exemple :

### 1.9.1.1 Attaques par filtrage

Le filtrage correspond à l'augmentation (resp. la diminution) des composantes hautes fréquences. En effet, L'ajout d'un bruit blanc gaussien ou un filtre moyen permet de désynchroniser la phase de l'insertion et la détection. Un exemple simple, si le marquage est effectué en modifiant la luminance de certains pixels. Il suffit alors d'effectuer un filtre

passe-bas sur l'image afin d'avoir alors la quasi certitude de détruire complètement le tatouage.

#### 1.9.1.2 Attaque par mosaïques.

Ce type d'attaque a comme principe de découper l'image en plusieurs morceaux, qui sont ensuite juxtaposés. On peut donc la regarder sans s'apercevoir de la manipulation, mais le tatouage est totalement désynchronisé si sa détection est automatisée. Cette attaque vise les moteurs de recherche automatique (crawlers) des marques dans les images sur Internet.

#### 1.9.1.3 Transformations valumétriques.

Le principe de ce type d'attaque est de changer la luminance de l'image par une fonction non-linéaire. Nous distinguons dans ce type d'attaques l'étalement d'histogramme, égalisation d'histogramme, transformation Gamma, etc.…

#### 1.9.1.4 Compression

La compression avec perte cherche à simplifier le codage du document, en supprimant l'information peu significative ; comme le tatouage est imperceptible, il est naturellement considéré comme peu significatif. En fait, les algorithmes dans le domaine spatial souffrent des attaques par compression. Dans le but d'augmenter la robustesse face à la compression, l'une des techniques de tatouage consiste à mettre en évidence la simulation d'un processus de compression dans la mise au point d'un algorithme de tatouage [Gm03], d'autres techniques consistent à concevoir des algorithmes de tatouage adaptés au contenue des images dans le domaine DCT ou DWT.

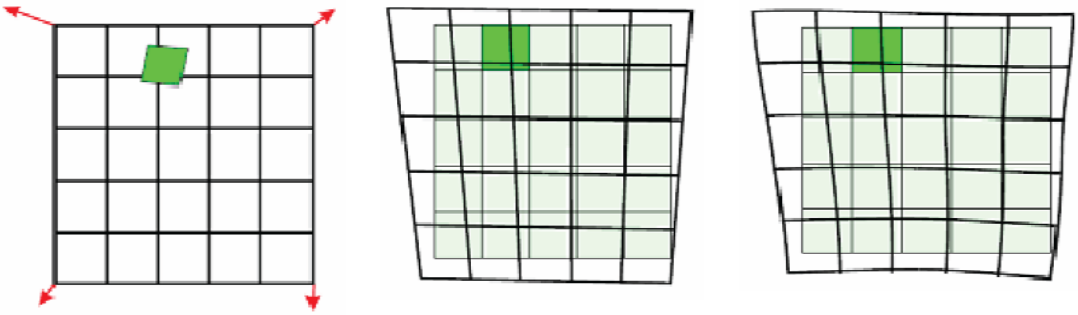
#### 1.9.1.5 Conversions analogique-numérique

La conversion analogique-numérique entraîne en général une désynchronisation du signal de tatouage, ainsi que de petites distorsions. Par exemple, le processus d'impression suivie d'un scan (Print/scan) d'une image, l'enregistrement d'un film à l'aide d'un caméscope dans une salle de cinéma ou le réenregistrement de la musique.

### 1.9.2 Attaques géométriques

Ce genre de transformation a pour effet de désynchroniser le signal de tatouage, ce qui empêche la détection de la marque, c'est-à-dire la difficulté de localiser la marque en empêchant ou diminuant l'exactitude de celle-ci. Il existe plusieurs transformations géométriques. Certaines sont utilisées couramment dans le traitement d'images, nous citons les plus usuelles:

- Rotation : des petites angles de rotation, n'ont pas l'habitude de changer la valeur commerciale de l'image, mais peuvent rendre le watermark non détectable.
- Scaling (modification des dimensions) : ce type d'opération est appliqué quand une image imprimée est scannée ou quand une image numérique de haute résolution est utilisée pour des applications électroniques, telles que la publication Web.
- Cropping (rognage) : Supprimer ou couper une partie d'une image qui s'étend au-delà d'une certaine limite, le bord de la fenêtre, par exemple. Certains programmes graphiques autorisent aussi le rognage comme moyen de tout masquer, sauf un objet donné, afin que les outils de dessin s'appliquent à l'objet seul.
- Stirmark : consiste à appliquer une succession de distorsions géométriques aléatoires appliquées globalement et localement à plusieurs endroits dans l'image [Pet98] (voir la Figure 1.12).



L'image originale

*Figure 1.12 la distorsion géométrique locale appliquée par Stirmark [Pet98].*

Bien que plusieurs méthodes de tatouage soient plus robustes à plusieurs attaques d'effacement, souvent elles ne sont pas robustes aux attaques géométriques. Une solution consiste à utiliser en parallèle des techniques de synchronisation spéciales pour résister à ces attaques. Ces techniques reposent souvent sur l'utilisation soit d'un domaine d'une transformation invariante (Fourier-Mellin), l'ajout d'un pattern de synchronisation (insertion d'un template) [Vol01b] [Ser02] ou des marques périodiques [Kes10]. Cependant, en exploitant la connaissance préalable du système de synchronisation utilisé, l'attaquant peut concevoir des attaques dédiées pour introduire une désynchronisation entre la phase d'insertion et celle de la détection.

### 1.9.3 Attaques sur la sécurité

La plupart des algorithmes de tatouage sont public, alors si on suppose qu'un pirate connaît l'algorithme mais il n'a aucune information le secret (comme par exemple des porteuses ou des clefs secrètes). Il lui suffit d'avoir plusieurs documents tatoués puis d'observer la réponse des documents modifiés à la zone de détection et de choisir celui qu'est proche d'un document tatoué sans modification mais en hors de la zone de détection. Parmi les attaques sur la sécurité nous citons:

**L'attaque de cryptographie :**

Le principe consiste à rendre un système de tatouage inutilisable en exploitant des failles dans la gestion des clés (déchiffrer la clé) et ensuite de faire disparaître de la marque de tatouage, d'accéder aux informations confidentielles, ou de tatouer un document en s'appropriant illégalement une identité. On distingue généralement deux types : L'attaque par force brute qui consiste à tester toutes les clés possibles. L'autre est l'attaque en oracle imaginée par Linnartz et al [Linn98]. Dans cette attaque le pirate insère des contenus en entrée au décodeur puis observe en sortie les messages décodés afin d'estimer la forme de la frontière entre les documents tatoués et les documents non tatoués [Ngu03].

**Attaques de protocoles :**

Cette attaque vise à trouver une faille dans le protocole de système de tatouage, puis d'accéder aux informations confidentielles, ou de tatouer un document avec une fausse marque.

**L'attaque de collusion :**

Dans ce type d'attaque suppose que le pirate dispose de plusieurs versions d'un document tatoué par différentes clés ; l'attaque consiste à construire un document sans tatouage. Une modélisation par la théorie des jeux [Boy05] consiste à formaliser la rivalité naturelle entre le tatoueur et l'attaquant et d'établir une stratégie optimale de tatouage.

## 1.10 Outils d'évaluation

### 1.10.1 Les mesures de distorsion

**Le MSE: Mean Square Error**

Le MSE représente l'erreur quadratique moyenne entre l'image tatouée et celle originale. Afin de permettre d'évaluer l'influence de la marque sur l'image cette mesure évalue l'influence de la marque sur l'image. Il est définit comme suit :

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{ij} - I_{ij}^{*}\right)^{2}}{MN} \qquad (1.22)$$

$I$ et $I^{*}$ sont respectivement l'image originale et l'image tatouée de tailles $N \times M$ où $I_{ij}$ et $I_{ij}^{*}$ sont leurs composantes.

**Le PSNR : Peak Signal Noise Ratio**

Le PSNR permet de déterminer l'imperceptibilité de la signature. En d'autre terme, il permet d'évaluer la dégradation en dB de l'image originale provoquée par l'insertion de la marque, et éventuellement par d'autres attaques. Lorsque le PSNR est élevé, la distorsion devient moins importante. On considère généralement en tatouage d'images qu'un tatouage est imperceptible quand le PSNR est supérieur à 36 dB [Cox07].

Le PSNR est définit comme suit :

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^2}{MSE}\right) \tag{1.23}$$

$$PSNR = 20\log_{10}\left(\frac{255}{MSE}\right) \tag{1.24}$$

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

Le Tableau 1.1 représente d'autres mesures de distorsion utilisées dans la littérature. Ces mesures sont basées aussi sur le calcul de la différence entre l'image originale et tatouée (attaquée ou non attaquée).

*Tableau 1.1: Métriques de distorsion basées sur la différence entre l'image originale et tatouée.*

| **Les Mesures** | **Les formules** |
|---|---|
| Maximum difference | $MD = \max_{m,n}\left\|I_{m,n} - I^*_{m,n}\right\|$ |
| Average Absolute Difference | $AD = \frac{1}{MN}\sum_{m,n}\left\|I_{m,n} - I^*_{m,n}\right\|$ |
| Norm. Average Absolute Difference | $NAD = \sum_{m,n}\left\|I_{m,n} - I^*_{m,n}\right\| \Big/ \sum_{m,n}\left\|I_{m,n}\right\|$ |
| $L^p$-Norm | $L^P = \left(\frac{1}{MN}\sum_{m,n}\left\|I_{m,n} - I^*_{m,n}\right\|^p\right)^{1/p}$ |
| Laplacian Mean Square Error | $LMSE = \sum_{m,n}\left(\nabla^2 I_{m,n} - \nabla^2 I^*_{m,n}\right)^2 \Big/ \sum_{m,n}\left(\nabla^2 I^*_{m,n}\right)^2$ |
| Image Fidelity | $IF = 1 - \sum_{m,n}\left(I_{m,n} - I^*_{m,n}\right)^2 \Big/ \sum_{m,n} {I_{m,n}}^2$ |
| Signal to Noise Ratio | $SNR = \sum_{m,n} {I_{m,n}}^2 \Big/ \sum_{m,n}\left(I_{m,n} - I^*_{m,n}\right)^2$ |

Une étude comparative entre ces mesures est présentée par Eskicioglu et Fisher [Esk95].

La corrélation normale (NC), entre la marque extraite $\hat{m}$ et l'originale $m$ , est aussi utilisée pour évaluer la qualité de l'extraction de la marque cachée. Cette corrélation est calculée par la formule (1.25) suivante :

$$NC = \frac{\sum_{i=1}^{N_m}\sum_{j=1}^{M_m} m(i,j) \times m^*(i,j)}{\sum_{i=1}^{N_m}\sum_{j=1}^{M_m} (m(i,j))^2} \qquad (1.25)$$

Où $N_m \times M_m$ est la taille du message binaire

## 1.10.2 Les logiciels d'évaluation

Les méthodes de tatouage sont de plus en plus nombreuses. Néanmoins, il est difficile de les comparer et de trouver celle adaptée à ses besoins dans la mesure où les tests présentés sont très souvent différents. En effet, tant les documents d'évaluation utilisés que les transformations qu'ils subissent changent d'une étude à l'autre. Face à toutes ces attaques, plusieurs outils logiciels ont été proposés pour aider à l'évaluation des algorithmes de tatouage numérique d'image, comme Checkmark ([PVM+01, VPP+01]), StirMark [Pet98], optiMark [Nik01], nous citons :

**Checkmark**

Ce programme, développé pour Matlab, prend mieux en compte la luminance et le contraste d'une image que le PSNR.

Les attaques possibles sont:

- Compression en ondelette JPEG2000
- Attaque de copie
- Débruitage
- Débruitage et modulation psychovisuelle
- Suppression de lignes

- Dithering, ré-échantillonnage
- Petites déformations géométriques

**StirMark**

Le logiciel StirMark est le premier banc de test apparu pour quantifier la résistance des schémas de tatouage. StirMark permet de faire subir à une image un jeu complet de tests. Les fonctionnalités que propose le logiciel peuvent se décomposer ainsi:

- Calcul du PSNR de l'image après insertion de la signature avec différentes forces de marquage
- Calcul du temps nécessaire à l'insertion de la signature
- Ajout de bruit dans l'image
- Génération d'image compressée avec l'algorithme JPEG
- Filtre médian
- Suppression aléatoire de ligne
- Découpage de l'image
- Changement d'échelle
- Rotation de l'image
- Rotation et découpage de l'image
- Rotation et changement d'échelle
- Transformations affines
- Génération de distorsion géométrique aléatoire sur l'image

## 1.11 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur le tatouage d'images numériques. Nous nous sommes intéressés aux terminologies et aux notions liées aux

techniques du tatouage numérique. Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle.

Nous avons aussi abordé les différentes phases de la conception d'une méthode de tatouage. Un schéma de tatouage permet d'insérer une information d'identification dans une image. Ce schéma se compose de deux phases : la phase d'insertion qui consiste à insérer (ou à cacher) une information d'identification et la phase de détection qui consiste à détecter ou à décoder la marque insérer. La phase d'insertion est souvent précédée par un codage de la marque.

Nous avons présenté aussi une classification des techniques du tatouage selon différents critères : les champs d'application, les types d'algorithmes et les domaines d'insertion. Selon le dernier critère les techniques du tatouage peuvent utiliser le domaine spatial où l'insertion modifie directement les valeurs des pixels, mais la plupart des techniques de tatouage passent souvent par une transformée. Les plus populaires sont la transformée de Fourier, la DCT ou la transformée en ondelettes, et c'est cette dernière transformée qui sera présentée dans le chapitre suivant.

# Chapitre 2 Généralités sur les ondelettes

## 2.1 Introduction

La transformée d'ondelettes est un outil bien adaptée en traitement d'image. Spécialement, elle est utilisée dans tatouage numérique, le débruitage [Ben03], la compression [Elb06], la segmentation d'images, l'analyse de la texture, la détection de contours [Dou01a ] et dans l'extraction des informations manuscrite [Dou01b]. La transformée en ondelettes a eu et a toujours un grand avantage grâce à son avantage de palier à certaines carences de la transformée de Fourier essentiellement la localisation espace-fréquence. Les représentions à différentes résolutions permettent d'en extraire les tendances principales de l'image en un nombre restreint de coefficients, tout en localisant précisément les discontinuités. D'où la mise en valeur des zones les plus significatives de l'image.

Comme nous l'avons cité dans la section 1.8, en tatouage d'image numérique, il est commode de définir une transformée inversible et de manipuler l'image dans le domaine de cette transformée, plus tôt de la manipuler directement au niveau des pixels. Avec l'arriver de standard de compression JPEG 2000, l'utilisation des ondelettes est devenue assez courant en tatouage numérique pour assurer une certaine robustesse vis-à-vis de cette norme de compression et faciliter le développement des masques psycho-visuels.

Ce chapitre présente une synthèse sur la transformée en ondelettes. Nous aborderons le principe de cette transformée puis nous développerons la transformée rapide d'ondelette par lifting (FSDWT). Cette transformé sera utilisée comme domaine d'insertion pour les méthodes de tatouage développées dans le cadre de cette thèse. Enfin, nous présenterons aussi quelques techniques de tatouage basées sur la transformée en ondelettes.

## 2.2 Le principe de la transformée en ondelettes

La transformée de Fourier permet de connaître le comportement fréquentiel d'un signal mais perd toutes les informations relatives au temps, d'où est venu l'idée d'utiliser la transformée de Fourier à court terme, développée par GABOR en 1946. Cette transformée consiste à considérer le signal autour d'un temps t. Ce signal est analysé ensuite par une fenêtre glissante $g(u-t)$ centrée sur cette instant $t$ en appliquant sa transformée de Fourier définie par l'équation (2.1) suivante:

$$\int x(u)g(u-t)e^{-i2\pi vu}du \qquad (2.1)$$

Avec $x(u) \in L^2(\mathbb{R})$

Le glissement de cette fenêtre au long du signal permet de mesurer le continu spectral au cours de temps.

Cette manière d'analyse par la transformée de Fourier à court terme a quelques inconvénients :

- Si on considère une fenêtre large en temps, on constatera une bonne résolution fréquentielle contre une mauvaise résolution temporelle.
- Dans le cas contraire, si on considère une fenêtre étroite en temps, on constatera une résolution temporelle précise contre une mauvaise résolution fréquentielle.

Pour cela, Morlet a introduit la transformée en ondelettes qui est conçue pour être adaptative. Cette transformée permet de déterminer les différentes composantes fréquentielles d'un signal donné, ainsi que leur localisation spatiale ou temporelle.

Par définition, les ondelettes sont des fonctions gérées à partir d'une fonction appelée ondelette mère $\psi$ de moyenne nulle ( $\int_{-\infty}^{+\infty}\psi(t)dt = 0$ ) par dilatations et translations. Ainsi, la décomposition en ondelettes fait intervenir deux paramètres qui sont le facteur d'échelle $s$ et le facteur de translation $u$ :

$$\psi_{u,s} = \frac{1}{\sqrt{s}}\psi\left(\frac{t-u}{s}\right) \qquad (2.2)$$

L'ondelette $\psi_{u,s}$ ayant été déplacée pour être centrée sur $u$: c'est donc le point autour duquel l'analyse se fait. Le paramètre d'échelle $s$ permet d'obtenir des ondelettes à partir d'une ondelette mère, des ondelettes comprimées (support réduit) ainsi que des ondelettes dilatées (support étendu). Les ondelettes comprimées sont utilisées pour déterminer les composantes de haute fréquence tandis que les ondelettes dilatées permettent de déterminer les composantes de basse fréquence. Le paramètre $u$, quant à lui, permet d'analyser par translations successives le signal jusqu'à ce que celui-ci soit entièrement parcouru (cf. Figure 2.1).

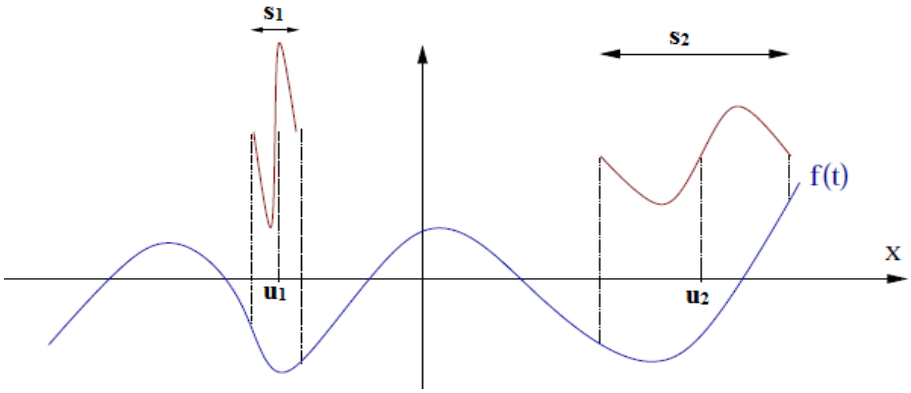



*Figure 2.1 : Exemples d'ondelettes:* $\psi_{u_1,s_1} = \frac{1}{\sqrt{s_1}}\psi\left(\frac{t-u_1}{s_1}\right)$, $\psi_{u_2,s_2} = \frac{1}{\sqrt{s_2}}\psi\left(\frac{t-u_2}{s_2}\right)$

La transformé continue d'ondelette d'un signal $x$ à l'échelle $s$ et à la position $u$ est donnée par :

$$Wx(u,s) = \int_{-\infty}^{+\infty} x(t)\frac{1}{\sqrt{s}}\psi^*\left(\frac{t-u}{s}\right)d\,t \qquad (2.3)$$

La transformation d'ondelette est inversible à condition que :

$C_\psi = \int_0^{+\infty} \frac{\left|\Psi(\omega)^2\right|}{\omega} d\omega < +\infty$ (Théorie Calderom, Grossmann, Morlet [Mal97]) avec $\Psi(\omega)$ est la transformée de Fourier de $\psi$.

L'inverse de la transformé en ondelettes est donnée par l'équation (2.4) suivante :

$$x(t) = \frac{1}{\sqrt{C_\psi}}\int\int Wx(u,s)\frac{1}{\sqrt{s}}\psi^*\left(\frac{t-u}{s}\right)d\,u\frac{ds}{s^2} \qquad (2.4)$$

La transformée discrète en ondelettes est dérivée de la version continue. Elle utilise un facteur d'échelle et une translation discrétisés. Nous parlons de la transformée en ondelettes discrète dyadique lorsque le facteur d'échelle est égal à $2^i$.

De nombreux types de la transformée en ondelettes ont été proposés dans la littérature [Dau92][Cha05]. On peut citer les plus utilisées, comme les ondelettes de : Morlet, Sombrero, Haar, Meyer, Daubechies, redgelette, countourlet et curvelettes…. Les deux premières sont des ondelettes continues tandis que les dernières sont des ondelettes discrètes.

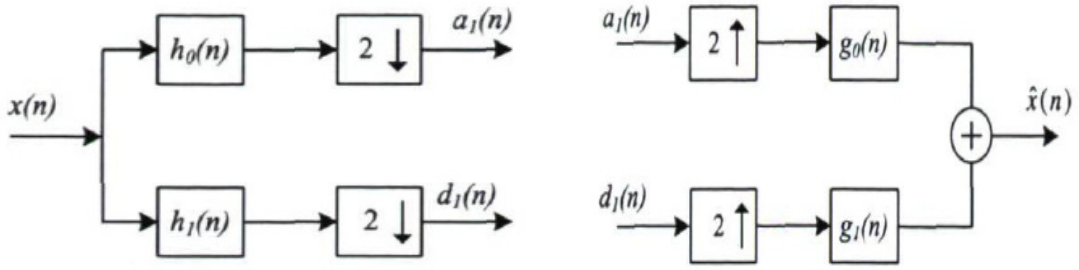
## 2.3 La transformée en ondelettes discrète

L'analyse multirésolution permet l'analyse d'un signal en différente bandes de fréquences, afin d'avoir une vue de la plus fine à la plus grossière. Le principe est d'analyser le signal à hautes fréquences, pour prélever les détails, ensuite analyser le signal à une résolution deux fois moins fine et réitérer l'opération en grossissant son échelle d'un facteur de deux, jusqu'à obtenir une description complète du signal. L'un des éléments fondamental de l'analyse multirésolution est l'introduction d'une matrice de dilatation D qui définit le "processus" de lissage lors d'un changement de résolution.

Nous présentons dans la Figure 2.2 et la Figure 2.3 l'algorithme de décomposition/synthèse rapide (DWT) d'un signal x(n) tel qu'il a été proposé par S. Mallat [Mal97]. Le calcul de l'approximation passe-bas et des coefficients d'ondelettes à l'échelle $l$ se résume à la convolution (filtrage) des coefficients de l'approximation passe-bas à l'échelle $l-1$ suivie d'une opération de décimation suivant D: $h_0(n)$ représente le filtre passe-bas, $h_1(n)$ est le filtre passe-haut, $2\downarrow$ représente l'opération de décimation d'un facteur 2 et $2\uparrow$ représente l'interpolation qui consiste à intercaler un zéro entre deux échantillons.

En suivant le même raisonnement que pour la décomposition, on obtient que la reconstruction de l'approximation passe-bas à l'échelle $l$ se résume à la convolution des coefficients de l'approximation passe-bas et des coefficients d'ondelettes à l'échelle $l+1$ précédée d'une opération d'interpolation suivant D. Comme pour l'analyse, ce processus

peut se réitérer permettant ainsi de reconstruire la séquence initiale à partir de tous les coefficients d'ondelettes et de la dernière approximation passe-bas.




*(a) Banc de filtres d'analyse* *(b) Banc de filtres de synthèse.*

*Figure 2.2 : Décomposition et reconstruction par la transformée en ondelettes (un seul niveau).*

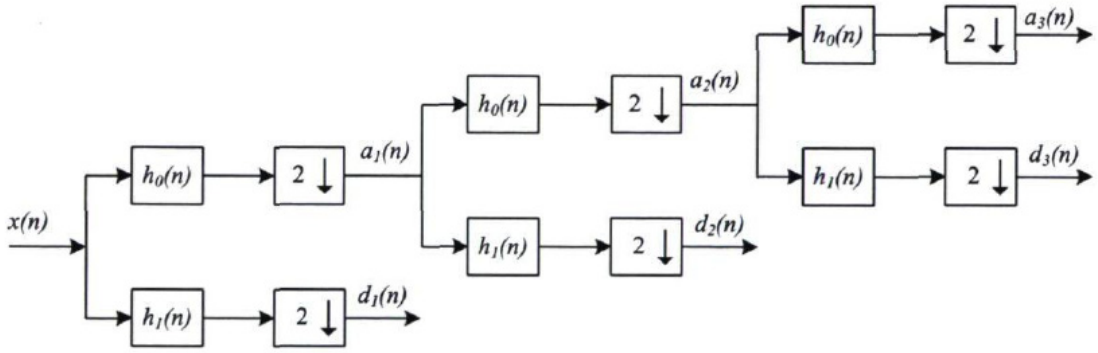



Figure 2.3 : *Décomposition en ondelettes sur trois de niveaux de résolution.*

Nous présentons sur la Figure 2.4 un exemple d'analyse de l'image Lina à partir d'un banc de filtres. La reconstruction d'une image à partir de ses coefficients en ondelettes prend une signification intuitive évidente : l'image, à sa résolution la plus grande, est égale à la somme d'une version floue, et des détails apparaissant à des échelles différentes, c'est à dire à des résolutions différentes.

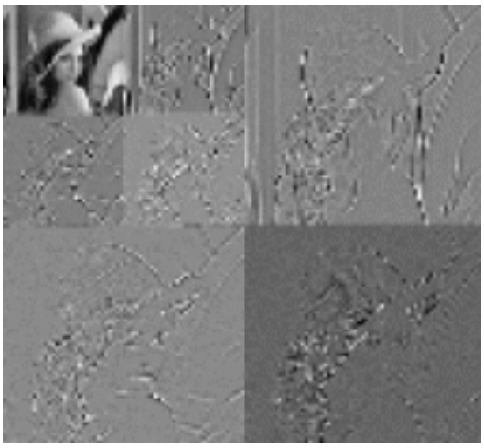


*Figure 2.4 : Décomposition par la transformée en ondelettes de l'image Lena.*

## 2.4 La transformée orthogonale en ondelettes basée sur le schéma lifting : algorithme 2D rapide de Faber-Schauder

La transformée en ondelettes discrète basée sur le schéma lifting a été proposé en 1995 par Sweldens [Swe95][Swe98] et dite ondelettes de deuxième génération, elle permet d'effectuer la transformée en ondelettes sans le banc de filtres.

Cette nouvelle décomposition a pour avantages :

- une implantation associée à un coût de stockage mémoire plus faible ;
- un schéma algorithmique plus "intuitif" (par exemple la reconstruction est un simple changement de signe dans les expressions) ;

En effet, le banc de filtres est remplacé par un certain nombre d'étapes comme illustré dans la Figure 2.5 : la décomposition, la prédiction et la mise à jour des coefficients. L'image qui résulte d'une telle transformation comporte une image d'approximation et trois images de détails. Le niveau suivant est réalisé en appliquant de nouveau la transformation sur l'image d'approximation.

Le signal (une image) est considéré comme une séquence $x^0 = \left(x^0_{m,n}\right)_{m,n\in\mathbb{Z}}$. L'algorithme de la transformée en ondelettes de Faber-Schauder (FSDWT) de $x^0$ est exprimée par une

décomposition non-orthogonales mais cette transformée est plus simple à exprimer par un schéma lifting [Dou01a]. FSDWT permet aussi la reconstruction parfaite du signal original $x^0$ ainsi que la réduction de la complexité de l'implantation comme la réduction de la quantité de mémoire ou le temps de calcul.

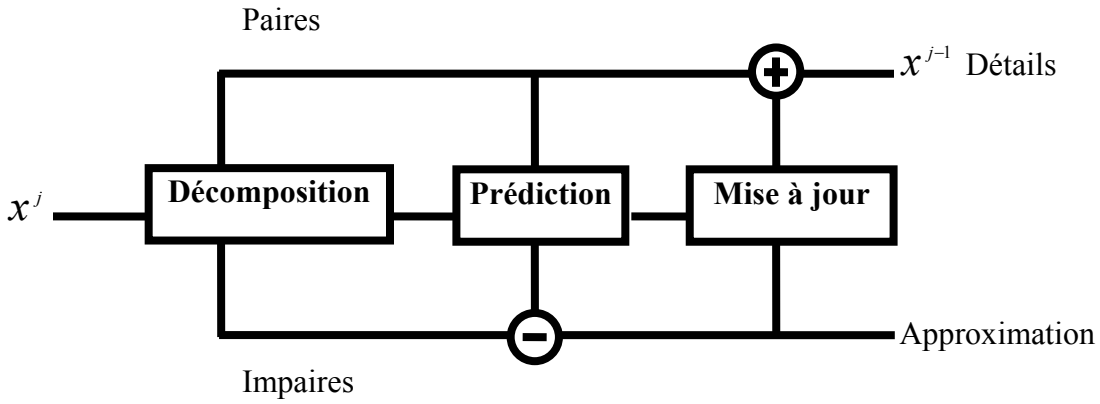



*Figure 2.5: la Transformation par lifting scheme*

La première étape est la **décomposition (Lazy wavelet transform)**. Elle consiste à décomposer le signal (l'image) d'entrée $x^0$ en quatre échantillons disjoints (cf. Figure 2.6) : échantillonnage pair et impair.

$$\begin{cases} g^{1,0} = x^0_{2m+1,2n} \\ g^{2,0} = x^0_{2m,2n+1} \\ g^{3,0} = x^0_{2m+1,2n+1} \\ x^{1,0} = x^0_{2m,2n} \end{cases} \qquad (2.5)$$

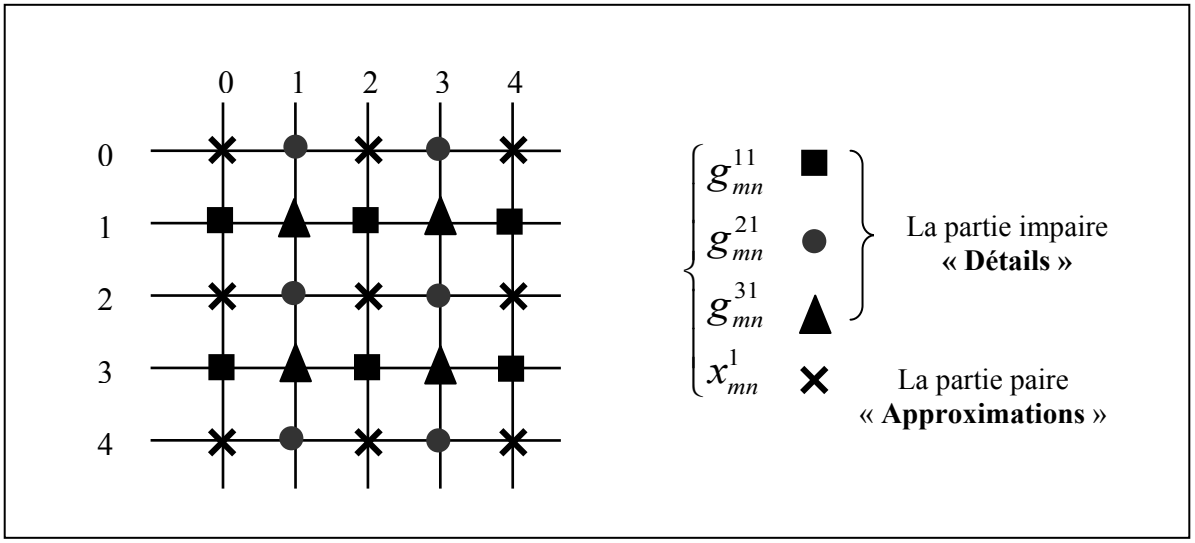



*Figure 2.6 : illustration de l'étape de la décomposition : la grille représente une image de taille* $5\times5$.

L'étape suivante est la **prédication.** Elle consiste à prédire les coefficients impairs à partir d'une combinaison linéaire des coefficients pairs voisins, pour assurer la corrélation existante entre les coefficients avec les indices pairs et les autres impaires :

$$\begin{cases} g_{mn}^{1,1} = g_{mn}^{1,0} - \dfrac{1}{2}(x_{m,n}^{1,0} + x_{m+1,n}^{1,0}) \\ g_{mn}^{2,1} = g_{mn}^{2,0} - \dfrac{1}{2}(x_{m,n}^{1,0} + x_{m,n+1}^{1,0}) \\ g_{mn}^{3,1} = g_{mn}^{3,0} - \dfrac{1}{4}(x_{m,n}^{1,0} + x_{m+1,n}^{1,0} + x_{m,n+1}^{1,0} + x_{m+1,n+1}^{1,0}) \end{cases} \qquad (2.6)$$

La dernière étape est la **mise à jour**. On cherche à préserver quelques propriétés du signal original dans la séquence $x^1$ par une pondération réalisée avec les séquences prédites précédemment, pour la FSDWT $x^1$ est simplement égal à $x^{1,0}$.

En résumé, la FSDWT est donné par l'algorithme suivant:

$$FSDWT:\begin{cases} x_{ij}^{0} = x_{ij} \qquad pour\ i,j \in \mathbb{Z} \\ pour\, 1 \le k \le N \ \ et\ \ i,j \in \mathbb{Z} \\ x_{ij}^{k} = x_{2i,2j}^{k-1} \\ g_{ij}^{k1} = (g_{ij}^{k1}, g_{ij}^{k2}, g_{ij}^{k3}) \\ g_{ij}^{k1} = x_{2i+1,2j}^{k-1} - \dfrac{1}{2}\left(x_{2i,2j}^{k-1} + x_{2i+2,2j}^{k-1}\right) \\ g_{ij}^{k2} = x_{2i,2j+1}^{k-1} - \dfrac{1}{2}\left(x_{2i,2j}^{k-1} + x_{2i+2,2j+2}^{k-1}\right) \\ g_{ij}^{k3} = x_{2i+1,2j+1}^{k-1} - \dfrac{1}{4}\left(x_{2i,2j}^{k-1} + x_{2i,2j+2}^{k-1} + x_{2i+2,2j}^{k-1} + x_{2i+2,2j+2}^{k-1}\right) \end{cases} \tag{2.7}$$

Cet algorithme est caractérisé par sa complexité qui est d'ordre $\mathcal{O}(N)$ où N est la taille de l'image. De plus, FSDWT est une transformation entière ce qui permet d'éviter le problème d'arrondis. Donc, elle est bien adaptée au traitement d'image numérique. Elle peut ainsi être utilisée dans des applications en temps réel comme le tatouage de portrait d'une carte biométrique. En effet, ces application ont recours plusieurs fois à transformée d'ondelette et sa transformée inverse.

La transformé inverse de cette transformation est donnée par l'algorithme (2.8):

$$IFSDWT:\begin{cases} \text{Pour} \quad 0 \le \mathrm{k} \le N-1 \quad et \quad i,j \in \mathbb{Z} \\ x_{2i,2j}^{k} = x_{i,j}^{k} \\ x_{2i+1,2j}^{k} = g_{i,j}^{k+1,1} + \dfrac{1}{2}\left(x_{i,j}^{k+1} + x_{i+1,j}^{k+1}\right) \\ x_{2i,2j+1}^{k} = g_{i,j}^{k+1,2} + \dfrac{1}{2}\left(x_{i,j}^{k+1} + x_{i,j+1}^{k+1}\right) \\ x_{2i+1,2j+1}^{k} = g_{i,j}^{k+1,3} + \dfrac{1}{4}\left(x_{ij}^{k+1} + x_{i+1,j}^{k+1} + x_{i,j+1}^{k+1} + x_{i+1,j+1}^{k+1}\right) \end{cases} \tag{2.8}$$

## 2.5 Représentation des coefficients d'ondelettes

La plupart des auteurs visualisent le résultat de la transformée en ondelettes par une séquence d'image pyramidal désignée par : "la représentation à échelles séparées". Dans cette représentation, la transformée en ondelettes discrète décompose une image en quatre sous-bandes, à savoir une sous-bande d'approximation LL et trois sous-bandes de détails : LH, HH et HL, correspondant, respectivement aux détails verticaux, diagonaux et horizontaux. La lettre H correspond au filtrage passe-haut et la lettre L à celui du passe-bas appliqués de façon séparable sur les lignes et les colonnes. La décomposition de la sous-bande d'approximation LL permet d'obtenir une représentation sous forme pyramidale. La Figure 2.7 montre la représentation à échelles séparées de la décomposition successive par la transformée en ondelettes discrète d'une image quelconque jusqu'à trois niveaux de résolution avec les sous-bandes correspondantes. De plus, la Figure 2.8 présente la décomposition par la transformée en ondelettes discrète de l'image Lena en 8 niveaux de résolution à l'échelle séparés.

Il existe une autre visualisation dite "**la représentions à échelles mixée**" qui consiste à affecter la valeur de chaque coefficient d'ondelette au pixel où la fonction de base associée atteint son maximum [Dou01a] (cf. Figure 2.9).

Les transformations par les schémas lifting, comme celle de Faber-Shauder, sont en fait des transformations linéaires. Donc, elles redistribuent différemment l'information contenue dans les valeurs des pixels des images originales. Ainsi, il est plus naturel de visualiser les coefficients issus de cette redistribution sur une seule image de la même manière que l'image originale.

Pour réaliser ceci, on utilise le même principe naturel qui est utilisé pour visualiser les images exprimées dans la base canonique. Ce principe consiste à effectuer la valeur de chaque coefficient d'ondelettes au pixel qui correspond au point où la fonction de base associée atteint son maximum.

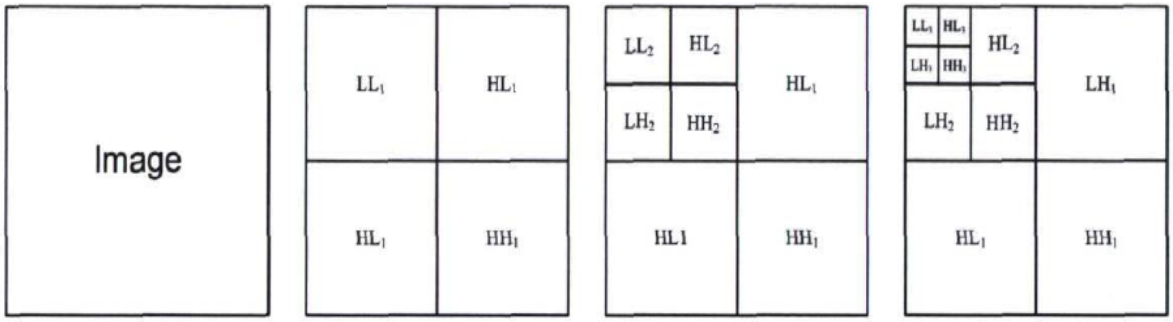



*Figure 2.7 : La représentation à échelles séparée d'une décomposition successive par la transformée en ondelettes discrète (jusqu'à trois niveaux).*

*Figure 2.8 : Décomposition par la transformée en ondelettes discrète de l'image Lena*

*Figure 2.9 : La représentation à échelles mixées de FSDWT de l'image Lena*

Cette représentation à échelles mixées des coefficients DWT d'une image permet de distinguer des régions très particulières autour des contours de l'image et les zones

texturées. Ces régions correspondent au zones où on a une grande densité de **coefficients significatifs** (ou dominants) d'ondelettes [Dou01b].

Dans les chapitres suivants, nous expliquerons comment peut-on utiliser cette représentation dans le tatouage d'image numérique.

## 2.6 Quelques algorithmes de tatouage utilisant la transformée en ondelettes

De nombreuses approches de tatouage d'image numérique dans les différents domaines d'insertion (cf. La section 1.8) ont été proposées, l'approche basée sur le domaine DWT reste l'un des plus efficaces et faciles pour mettre en œuvre des techniques de tatouage.

Le principe de tatouage numérique dans le domaine d'ondelettes est illustré dans la Figure 2.10. il consiste à décomposer l'image en utilisant la transformée en ondelettes DWT puis à insérer une marque dans une résolution donnée. L'enjeu le plus important dans le tatouage d'image basé sur DWT est de savoir comment choisir les coefficients à tatouer.

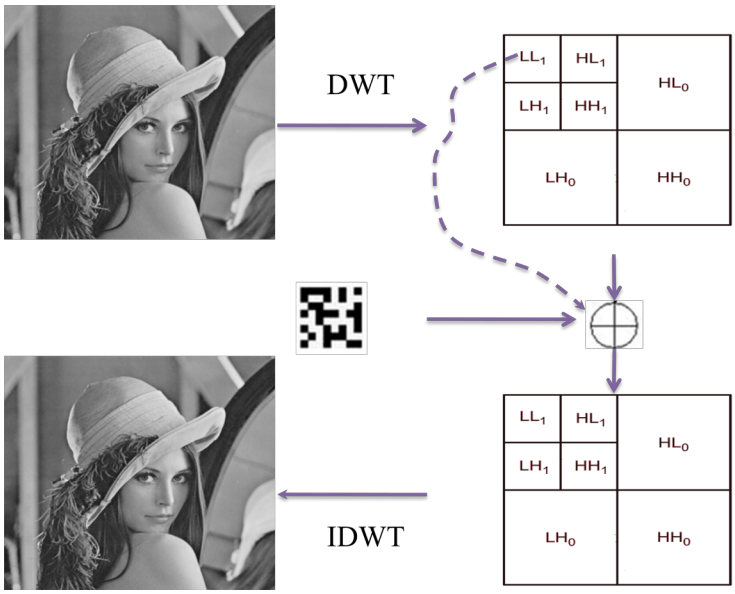



Figure 2.10 : *Exemple d'insertion dans le domaine d'ondelettes*

Certains travaux sont basés sur la modification des coefficients de toutes les sous-bandes [Kun97], d'autres s'appuient sur l'insertion dans HH ou LL [Dug98] [Che03]. Ces algorithmes permettent dans certains cas d'améliorer la robustesse vise à vis de quelques attaques telles que la compression, le filtrage et la mise à l'échelle (scaling). Dans Dugad et al. [Dug98], Kim et Moon [Kim99] ,Kwon et al [Kwo01], Wang et Huo [Wan97], Wang et al [Wan98] et Wang et al [Wan00], le marque est insérée dans les coefficients les plus significatifs.

Kundur et Hatzinakos [Kun97] ont proposé l'un des premiers approche basées sur la transformée en ondelettes. Il s'agit d'un algorithme informé. La marque utilisée est une image binaire de taille 16 x 16 pixels. L'image originale et la marque ont été décomposées en utilisant la DWT jusqu'au niveau de résolution n. Les coefficients des sous-bandes LH, HH et HL de tous les niveaux de résolution ont été divisés en blocs de taille 8x8 pixels. Ils sont ensuite modifiés par l'insertion des coefficients DWT de la marque. Un seuil adaptatif est utilisé afin de savoir dans quel endroit exactement le watermark sera ajouté. Les résultats expérimentaux montrent la robustesse du schéma contre la compression JPEG, l'ajout de bruit et le filtrage.

Dans [Dug98], Dugad et al ont présenté un algorithme aditif de tatouage numérique basé sur la DWT et l'étalement du spectre. L'image originale est décomposée en utilisant la DWT à trois niveaux de résolution. La marque est insérée dans certains coefficients de la DWT ayant une énergie importante. Les résultats expérimentaux montrent la robustesse de l'algorithme contre la compression JPEG avec un facteur de qualité de 50%, le recadrage, le filtrage médian, l'ajout de bruit et la mise à l'échelle (scaling).

Une amélioration de la méthode précédente [KH97], en utilisant une technique de quantification, est présentée par Chen et Lin [Che03]. Dans cette méthode, chaque bit du tatouage est inséré par la modulation d'un ensemble de coefficients de l'ondelette. Deux watermarks identiques sont insérés dans la composante de basse fréquence et haute fréquence, pour augmenter la robustesse contre les différents types d'attaque. Un modèle visuel humain est utilisé pour déterminer la quantité du signal tatoué qui peut être inséré à chaque localisation sans affecter la qualité visuelle de l'image.

D'autre chercheurs divisent l'image en blocs puis applique DWT sur chaque bloc puis insèrent la marque dans ces blocs. Huang et Yang [Hua04] a proposé un algorithme de tatouage basée sur DWT. L'image originale est divisée en m blocs de taille n*n, puis chaque bloc est décomposé par DWT. Le watermark est inséré dans les coefficients d'ondelettes de sous-bandes moyennes de chaque bloc. Khelifi et al [Khe05] ont proposé une technique aveugle et adaptative. L'image originale est divisée en blocs qui non chevauchés et classés en blocs uniforme ou non uniforme en utilisant un classifieur basé sur JND. Puis chaque bloc est transformé par DWT. Le watermark est insérer dans la sous-bande haute de chaque bloc, en fonction sa classification.

Des méthodes basées sur les caractéristiques statistiques des coefficients d'ondelettes ont été aussi proposées. Zhang et al [Zha04] divisent l'image originale en $n \times n$ blocs puis chaque bloc est transformé par DWT. La moyenne et la variance des sous-bands sont utilisées pour sélectionner les coefficients à modifier. Hsieh [Hsi01] ont proposé une méthode basée sur le tatouage de l'arbre des coefficients significatifs (QSWT). Wang et Lin [Wan04] ont proposé une méthode aveugle où chaque bit de watermark est inséré à l'aide de deux arbres. L'un de ces deux arbres est quantifié par rapport à un indice d'une quantification. Les deux arbres (quantifiées et non quantifiée) présentent une grande différence statistique. Cette différence est utilisée ensuite pour extraire de la marque. Li Liang, et Niu [Li06] ont amélioré la méthode [Wan04], en exploitant le système visuel humain afin de résister efficacement à l'attaque géométrique. Wu et Huang [Wu07] ont amélioré la méthode de Wang et Lin [Wan04] en utilisant la moyenne minimum pour extraire la watermark.

L'inconvénient majeur de ces méthodes ([Hsi01], [Wan04], [Li06], [Wan04] et [Wan04]) est la sélection des coefficients significatives qui est très long du point de vie de temps de calcul. Ainsi de ne pas résister efficacement aux attaques géométriques et au filtrage passe-bas comme le filtrage médian ou filtrage gaussien.

La transformée en ondelettes a été utilisée aussi pour l'authentification d'image par le tatouage fragile. Par exemple, celle proposé par Lin et Chang [Lin98]. Il s'agit de choisir, tout d'abord, un bruit pseudo-aléatoire et une ondelette de base, qui constituent le secret du

système d'authentification. Puis de décomposer l'image en 4 sous-bandes (LL, LH, HL et HH) en fonction de l'ondelette de base choisie au départ. La différence est que l'insertion consiste à substituer la sous-bande HH par le bruit pseudo-aléatoire et à effectuer ensuite la transformation en ondelettes inverse afin d'obtenir l'image tatouée. Le processus d'authentification consiste alors à effectuer la même décomposition que lors de la phase d'insertion, puis à corréler la sous-bande HH obtenue avec le bruit pseudo-aléatoire. Si l'image n'a subi aucune manipulation, le résultat du test ressemblera à une matrice de points uniformément répartis. Dans le cas contraire, la distribution perdra son caractère uniforme dans les régions où l'image a été manipulée. Par contre, les auteurs ne démontrent pas la robustesse de leur méthode face à des attaques spécifiques visant par exemple à substituer la sous-bande HH ou au contraire à la préserver (i.e. modifier l'image, puis réinsérer la sous-bande HH de l'image originale protégée).

## 2.7 Conclusion

Dans ce chapitre, nous avons traité la transformation d'ondelettes et leur importance aujourd'hui dans le domaine du traitement d'images. Plus précisément, ce chapitre a décrit la transformation d'ondelettes non orthogonales de Faber-Schauder (FSDWT) qui va servir dans les méthodes de tatouage développées dans le cadre de cette mémoire de thèse. Cette méthode se distingue par sa simplicité (Algorithme lifting Scheme, opérations arithmétiques, sans traitement aux bords), sa grande capacité à détecter les contours (qui représentent les régions les plus intéressants pour l'insertion des tatouages numériques). En plus, les coefficients d'ondelettes sont représentés par une distribution à échelles mixées. Cette représentation a l'avantage de faire coïncider chaque coefficient d'ondelettes avec la localisation de sa fonction d'ondelette ce qui permet notamment, dans les méthodes proposées, de bien sélectionner les régions d'insertion des tatouages. Nous avons présenté aussi quelques algorithmes utilisant la transformée en ondelettes comme domaine d'insertion.

Dans les chapitres suivants, nous présenterons des méthodes de tatouage dans le domaine d'ondelettes en utilisant la FSDWT à échelles mixées comme domaine d'insertion.

# Partie 2

# Chapitre 3 Tatouage d'image robuste des coefficients d'ondelettes à échelles mixées

## 3.1 Introduction

Dans le chapitre 1, nous avons présenté les différentes étapes de la conception d'une méthode de tatouage. Nous avons aussi présenté les différentes approches du tatouage d'image en faisant la distinction entre les méthodes qui opèrent dans le domaine spatiale et celles qui opèrent dans le domaine fréquentiel et la transformé en ondelettes. Egalement, nous avons présenté les techniques d'insertion par étalement de spectre et celle utilisant la quantification par QIM.

Nous avons présenté aussi, dans le chapitre 2, la transformé FSDWT et la représentation à échelles mixés. Nous avons présenté les différentes approches utilisées pour sélectionner les zones optimales pour marquer une image dans le domaine d'ondelettes. Cette sélection est importante, puisque dans un contexte de qualité, nous voulons trouver des solutions pour minimiser les effets dégradants l'image tatouée et augmenter la robustesse.

Dans ce chapitre, nous présentons deux méthodes robustes de tatouage d'images, à niveaux de gris, basées sur la transformée FSDWT et la représentée à échelles mixées. La détection est qualifiée aveugle, i.e. seule l'image tatouée et les clés sécrètes sont utilisées pour extraire la marque.

Le choix de FSDWT est motivé par sa capacité à bien détecter les régions autour de contours et les zones texturées. En effet, une des caractéristiques du système visuel humain est que l'œil est plus sensible aux modifications touchant les basses fréquences (i.e. zones uniformes) plutôt que les hautes fréquences qui correspondent aux zones autour des contours et aux zones texturées [Cox07]. L'idée est donc de privilégier ces zones lors de l'insertion de la marque. Pour cela, nous allons insérer la marque dans des blocs à forte

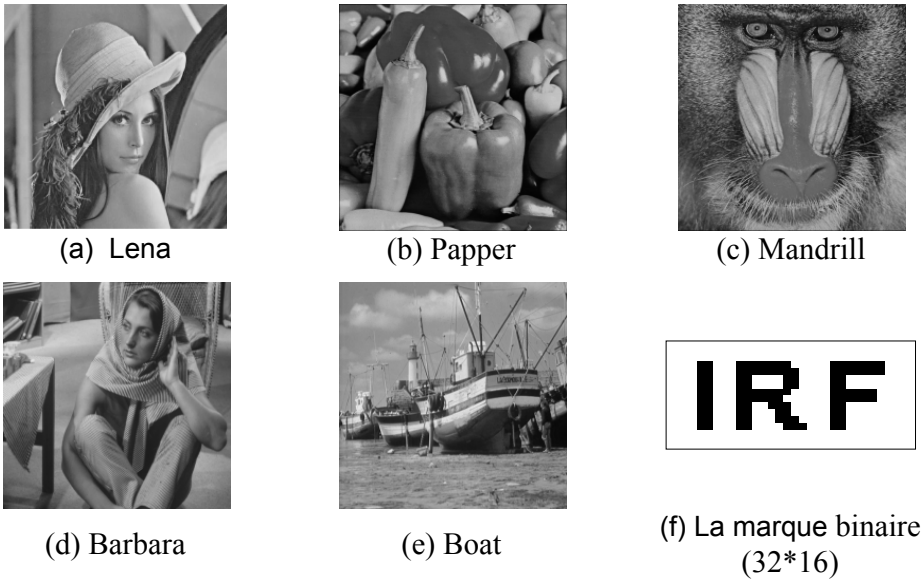
densité des coefficients significatifs d'ondelettes, qualifiés par «blocs dominants». Ces blocs correspondent aux zones autours des contours et des zones texturées.

La première méthode se base sur une insertion additive par l'étalement de spectre amélioré. En outre, la deuxième méthode se base sur une insertion substitutive par la méthode de la quantification QIM.

Des expérimentations ont été menées afin de valider les performances de deux approches proposées en termes d'invisibilité et de robustesse face à des manipulations usuelles d'images. Aussi, une comparaison entre ces deux méthodes de tatouage est effectuée afin de déterminer la méthode la plus adapté à FSDWT. Enfin, Nous effectuons une comparaison entre ces deux algorithmes proposés et une méthode de référence de base [Wan04].

## 3.2 Exemple d'application de l'algorithme d'insertion

La Figure 3.1: Images de test de taille 512×512 suivante montre quelques exemples d'images, de taille 512×512, que nous avons traité par les deux méthodes proposées.




(a) Lena (b) Papper (c) Mandrill

(d) Barbara (e) Boat (f) La marque binaire (32*16)

*Figure 3.1: Images de test de taille 512×512*

Les documents d'identité, tels que cartes d'identité, passeports et permis de conduire, contiennent des informations textuelles, un image d'identité, et éventuellement quelques autres caractéristiques biométriques comme les empreintes digitales ou une signature manuscrite. Aujourd'hui, avec le développement des nouvelles technologies, un contrefacteur peut aisément remplacer une photo ou modifier les informations sur un document d'identité dans la mesure où il est très difficile à le différencier de l'original.

Dans le but renforcer la sécurité de documents papiers tels qu'un passeport ou un badge d'accès, nous pouvons marquer la photo d'identité par des informations liées au document (les empreintes digitales, la signature manuscrite, …) de manière à lier l'image aux autres composantes du document. Dans ce contexte, nous avons traité ce type d'images. La Figure 3.2 montre quelques exemples d'images d'identité, de taille 256×256,  extraites de la base d'images que nous avons utilisée  pour évaluer ces  deux algorithmes robustes.

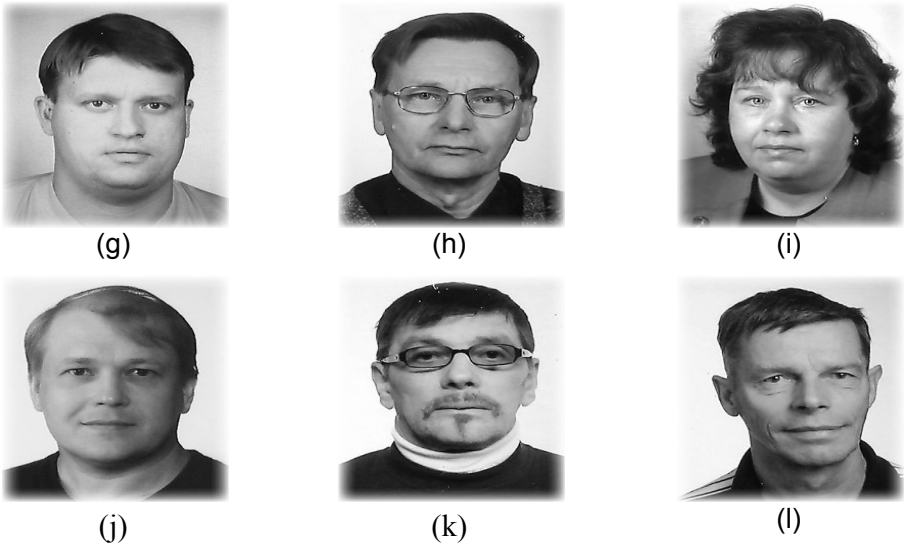



*Figure 3.2: Exemple d'images d'identité tatouées*

## 3.3 Localisation de  zones optimales pour insérer la marque

Nous avons cité dans la section 2.4 que FSDWT à échelles mixées a le pouvoir de décorréler les pixels des images originales et de concentrer l'information dans un nombre

réduit de coefficients d'ondelettes : **les coefficients significatifs** (ou dominants). En effet, ces coefficients correspondent essentiellement aux régions autour des contours et aux zones texturées [Dou01b].

En exploitant les caractéristiques statistiques de ces coefficients, on peut sélectionner ces coefficients significatifs en blocs dominants.

Dans cette section nous proposons deux méthodes de sélection de ces coefficients significatifs. Dans la première méthode, nous utilisons la densité des coefficients significatifs d'un bloc de taille 8×8. La deuxième méthode est basée sur l'histogramme des coefficients.

Nous obtenons dans les deux méthodes un masque, noté par $X$. Où, $X(i,j)$ vaut 0 si le coefficient $(i,j)$ n'appartient pas à un bloc dominant, sinon, $X(i,j)$ prend la valeur de ce coefficient $(i,j)$.

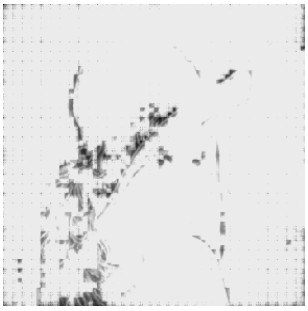
### 3.3.1 La sélection des blocs dominants basée sur la densité des coefficients significatifs

Cette méthode à été utilisée par Douzi et al [Dou01b] pour extraire la signature manuscrite du fond d'un chèque. Elle consiste à séparer les coefficients dominants (significatifs) de ceux non-dominants. Cette technique est décomposée en deux étapes. La première consiste à calculer la densité des coefficients significatifs, en considérant qu'un coefficient est significatif si sa valeur absolue dépasse un seuil *Sc*. La seconde étape consiste alors à sélectionner les blocs les plus denses en coefficients significatifs en se basant sur un seuil *Sd*. La Figure 3.3 montre les blocs dominants sélectionnés pour l'image Lena. Nous remarquons que les blocs sélectionnés sont ceux qui correspondent aux régions autour de contours et aux zones texturées (la figure 3.3-b). Aussi, nous distinguons que le nombre de blocs dominants dépend des seuils Sc et Sd.

(a) Les blocs dominants (bloc 8x8, SC=10, SD=20%).

(b) Les zones sélectionnées sur l'image (Sc=10, Sd=20%)

(c) Les blocs dominants (bloc 8, SC=10, SD=30%).



(d) Les zones sélectionnées sur l'image (Sc=10, Sd=30%)

*Figure 3.3: Les blocs dominants à grande densité de coefficients significatifs.*

### 3.3.2 La sélection des blocs dominants basée sur l'histogramme de coefficients d'ondelettes

La technique de seuillage présentée dans la section précédente, permet de sélectionner les blocs dominants. Cependant, cette technique utilise deux paramètres qu'il faut ajuster d'une manière manuelle. Nous présentons ici une technique de seuillage automatique des blocs dominants en se basant sur l'écart-type des blocs de coefficients.

Afin de choisir judicieusement ces blocs dominants, nous étudions l'histogramme des coefficients obtenus par la transformé FSDWT de l'image. La Figure 3.4 montre l'histogramme de ces coefficients. On peut s'apercevoir que l'histogramme est piqué au voisinage de zéro. Donc, les coefficients significatifs sont ceux éloignés de zéro [Mal97]. En se basant sur cette propriété, nous pouvons sélectionner les coefficients significatifs en

utilisant l'écart-type de chaque bloc de taille 8×8. En effet, Dès qu'un bloc contient un nombre plus grand de coefficients qui sont éloignés de zéro, son écart-type devient supérieur à l'écart-type global de l'image transformée.

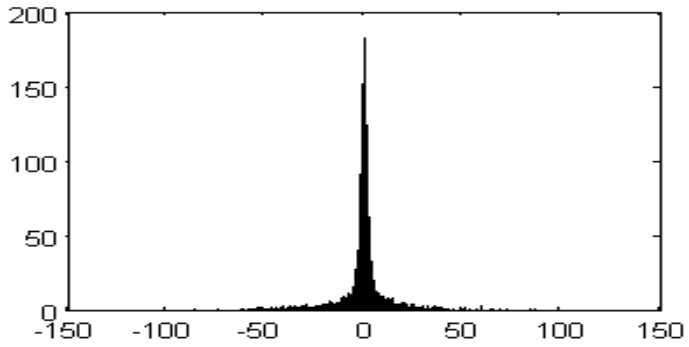


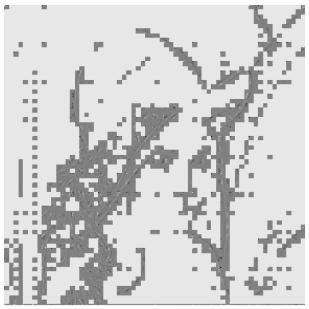

*Figure 3.4: L'histogramme des coefficients d'ondelettes de l'image Lena.*

Cette technique est décomposée aussi en deux étapes. La première consiste à calculer la l'écart-type globale $\sigma$ de la transformée de l'image. La seconde étape consiste alors à sélectionner les blocs les plus denses en coefficients significatifs selon le critère suivant :

Un bloc est dominant si $|\sigma'| > T\sigma$ .

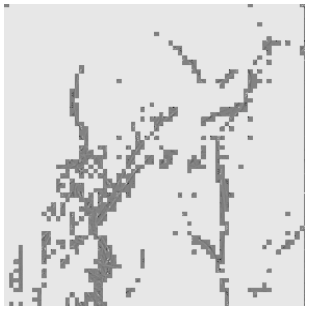
Où $\sigma'$ est l'écart type local de chaque bloc de taille 8×8 et $T$ ($T > 0$) est un paramètre qui permet de contrôler l'opération de seuillage et ainsi de contrôler la densité des coefficients significatifs.

La Figure 3.5 montre les blocs sélectionnés pour $T = 1$ et $T = 1.5$ . On peut remarquer que lorsque $T = 1$ (i.e. $|\sigma'| > \sigma$ ), nous arrivons à sélectionner la plupart des régions autour des contours et les zones texturées.



Les blocs dominants (T=1)

(b) Les zones sélectionnées sur l'image (T=1)



(c) Les blocs dominants (T=1.5)

(d) Les zones sélectionnées sur l'image (T=1.5)

*Figure 3.5: Les blocs dominants sélectionnés par la deuxième méthode.*

La Figure 3.6 montre que dans le cas d'une image d'identité, les coefficients non-dominants correspondent à l'arrière plan du portrait, où l'insertion de la marque introduit une forte dégradation de l'image tatouée. D'où, cette méthode permet de sélectionner d'une manière efficace et automatique les régions optimales pour tatouée une image.

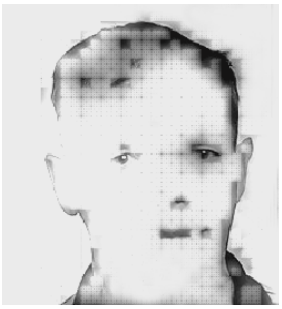
### 3.3.3 La capacité d'un algorithme opérant sur les blocs dominants

La Figure 3.7 montre le nombre des blocs dominants sélectionnés pour les images de test (cf. la Figure 3.1 et la Figure 3.2).  On remarque que, dans le cas d'insertion d'un bit par bloc, la capacité est supérieure à 512 bits pour toutes les images. On peut donc insérer une marque de taille inférieure à 512 bits, par exemple un logo binaire de taille 32×16.

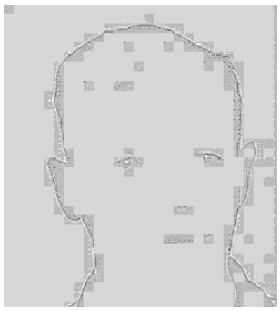
De plus, avec une telle capacité, on peut mettre en œuvre des codes correcteurs d'erreurs qui consistent à introduire une redondance dans l'information à transmettre. Ceci permet de détecter et éventuellement de corriger les cas où la transmission a modifié le message.

Cependant, Dans le cas où le nombre de bloc est inférieur à la taille de la marque, la solution est d'insérer deux bits (ou plus) par blocs.

Une image d'identité



Les zones sélectionnées sur l'image (T=1.5)



Les blocs dominants sélectionnés

*Figure 3.6 : Les blocs dominants d'une image d'identité.*

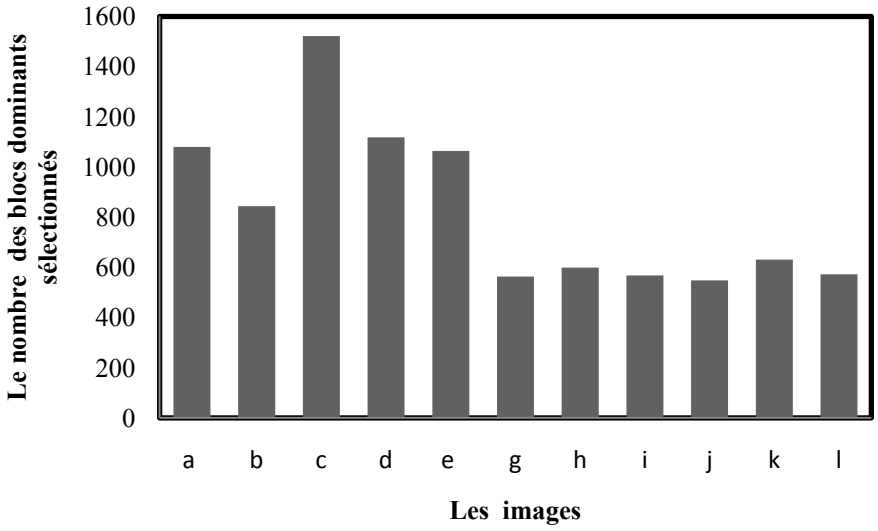



*Figure 3.7 : Capacité d'insertion de chaque image (cf. Figure 3.1 et Figure 3.2) :*

## 3.4 Algorithmes de tatouage robuste proposés

Les méthodes que nous allons décrire ici sont des méthodes de tatouage d'images numérique à niveaux de gris. Cependant, ces méthodes peuvent être aussi appliquées aux images couleurs. En effet, la composante bleue de la couleur est choisie pour l'insertion de la marque parce que le système visuel humain est moins sensible aux changements de la composante bleue que celle des composantes rouge et vert.

Ces méthodes sont basées sur le marquage des blocs dominants de la transformée FSDWT représentée à échelles mixées. Comme nous avons pu le voir dans l'état de l'art, il n'existe pas à ce jour des algorithmes utilisant la même approche. Nous allons maintenant étudier en détails ces méthodes robustes que nous avons développées.

### 3.4.1 Algorithme de tatouage numérique proposé basé sur ISS et FSDWT

Nous avons cité dans le chapitre 1 qu'on peut considérer le tatouage comme la transmission d'un signal (la marque) dans un canal bruité (l'image). La principale différence avec les télécommunications réside dans l'inversion du rapport Signal/Bruit : ici, l'image représente le bruit qu'a une puissance beaucoup plus grande que celle de la marque qui représente le signal (w). Cette analogie avec les télécommunications est à la base de

techniques de tatouage par étalement de spectre. Le tatouage devient alors une mise en forme du message, suivie d'une modulation.

Dans cette section, nous présentons un algorithme de tatouage numérique des images en niveaux de gris. Ledit algorithme est basé sur l'étalement de spectre amélioré (cf.la section 1.7.1) et la transformée en ondelettes FSDWT représentée à échelles mixées. L'algorithme proposé peut être décrit par les deux étapes : d'insertion et d'extraction de la marque.

#### 3.4.1.1 Processus d'insertion de la marque

En se basant sur le modèle générique présenté dans la section 1.4, le principe du processus d'insertion est représenté par le schéma Figure 3.8. L'algorithme d'insertion comprend en entrée une marque binaire m, une image $I_0$ et deux clés secrètes ***K1*** et ***K2*** spécifique au tatoueur. Cette phase d'insertion génère en sortie une image tatouée *Iw*.

La phase d'insertion est modélisée par la fonction suivante :

$$I_w = \varepsilon(I_0, K1, K2) \qquad (3.1)$$

Le processus d'insertion se résume par les étapes suivantes :

D'abord, nous transformons l'image originale par la transformée en ondelettes FSDWT représentée à échelles mixées. Puis nous sélectionnons les blocs dominants ***X***, en se basant sur l'algorithme présenté dans la section 3.3.2.

Afin de gagner une certaine robustesse face aux attaques de filtrage et d'autres attaques visant la localisation spatiale (cropping, changement d'échelle…), la séquence entière des blocs dominants est randomisée. Cette randomisation permet d'insérer chaque bit du message dans 64 coefficients aléatoires (***x***). Ainsi, les coefficients tatoués seront répartis sur toutes les échelles de FSDWT et donc seront répartis spatialement dans toute l'image. La clé **K1** utilisée pour randomiser les blocs dominants constitue en plus la première clé de sécurité de notre algorithme.

L'étape suivante consiste à générer, en utilisant une clé sécrète **K2**, une séquence pseudo-aléatoire ***u*** (la porteuse) à moyenne nulle, de langueur L (Taille des blocs dominants) et

dont les éléments sont égaux à $-\sigma_u$ ou $+\sigma_u$ indépendant de ***x***. Puis générer le watermark ***w*** à partir de ***m*** et de la porteuse *u* par un opérateur de génération (3.2) suivant :

$$w_x = (\alpha b - \lambda \hat{x}) u_i \qquad (3.2)$$

Où $\hat{x} = \dfrac{< x, u_i >}{\|u_i\|^2}$ et $b = \begin{cases} -1 & si \quad m_i = 0 \\ 1 & si \quad m_i = 1 \end{cases}$

α, λ contrôle la qualité visuelle de l'image tatouée et la robustesse de l'algorithme.

On ajoute ensuite *w* à chaque bloc dominant ***x*** pour former y le vecteur tatoué :

$$y = x + w_x \qquad (3.3)$$

En effet, La séquence u est ajoutée ou soustraite de coefficients x en fonction de la variable selon le bit (ou bits) à transmettre. Le bit est ainsi réparti dans l'ensemble de la gamme de fréquence où est choisie la porteuse. Cette technique permet également d'assurer un cryptage du message. En effet, la démodulation du signal nécessite la connaissance de la porteuse qui a été utilisée pour porter le signal or celle-ci dépend de clé secrète ***K2***.

L'étape finale consiste à calculer l'image tatouée ***Iw*** en appliquant la transformée en ondelettes inverse IFSDWT.

### 3.4.1.2 Processus d'extraction de la marque

Cet algorithme est du type aveugle, c'est-à-dire, pour extraire la marque nous avons besoin que l'image tatouée, la clé ***K2*** utilisée pour générer la porteuse pseudo-aléatoire u et ***K1*** utilisée pour randomiser les blocs dominants. Le schéma du processus d'extraction est illustré à la Figure 3.9, et est décrit par les étapes suivantes :

La première étape consiste à transformer l'image tatouée (reçu) $I_w^*$ par la transformée FSDWT représentée à échelles mixées. Puis à sélectionner les blocs dominants sélectionnés en utilisant l'algorithme de la section 3.3.2 de la même manière que la phase d'insertion.

Ensuite, nous générons la séquence pseudo-aléatoire ***u*** en utilisant la clé ***K2*** et puis nous estimons la $w_c^*$ représentant la marque cryptée à partir des blocs dominants sélectionnés de la manière suivante :

1- On calcule le coefficient de corrélation entre chaque bloc de 64 coefficients et la séquence ***u***, comme suit :

$$r = \frac{< x \mid u >}{< u \mid u >} \tag{3.4}$$

2- On décode la marque crypté $m_c^*$ par :

$$m_c^* = signe(r) \tag{3.5}$$

L'étape suivante consiste à appliquer sur $m_c^*$ l'opération inverse de randomisation qui a été appliquée sur les dominants dominant dans la phase d'insertion. On obtient donc une image marque estimée décryptée $m^*$. En fin, nous calculons la mesure objective NC (ou RBE) entre la marque m et la marque extraite $m^*$.

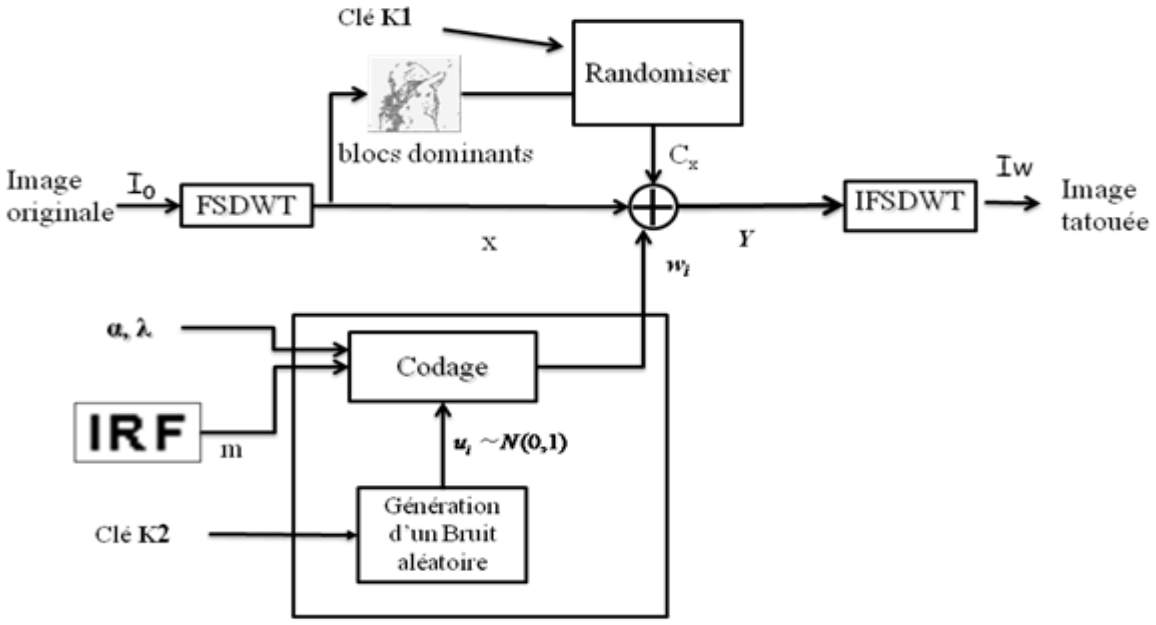



*Figure 3.8: Schéma du processus d'insertion ISS de la marque.*

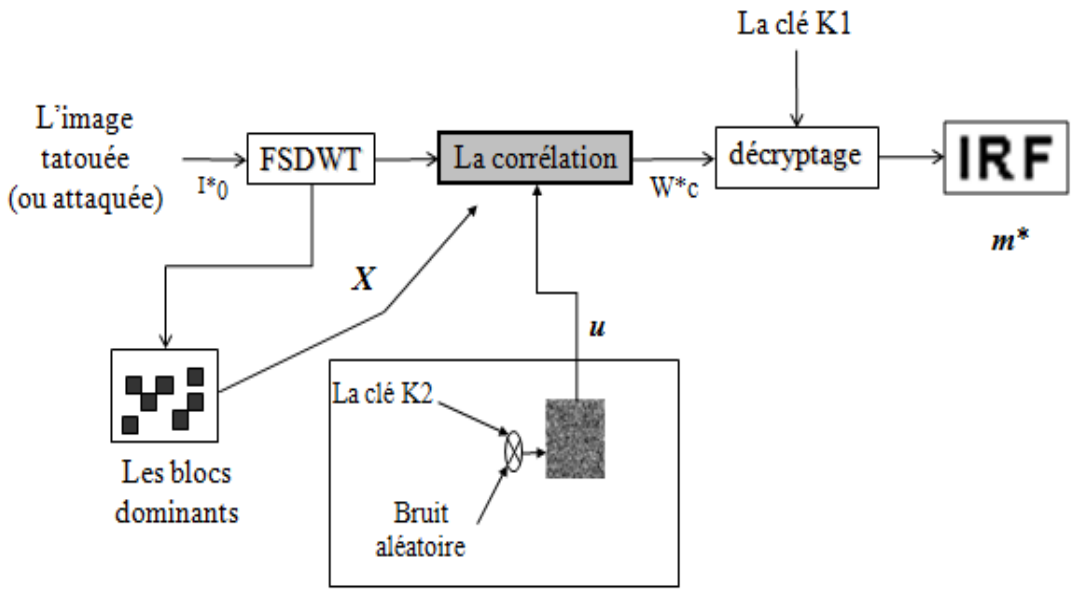



*Figure 3.9 : Schéma du processus d'extraction de la marque de l'algorithme ISS*

### 3.4.1.3 Simulations et résultats expérimentaux

Dans cette section, nous évaluons les performances de cette méthode en termes d'imperceptibilité et robustesse. Pour ce faire, on utilise différentes images à niveaux de gris de taille 512 x 512 pixels (cf. Figure 3.1 et Figure 3.2). Un message binaire de taille 32×16 bits, identifiée par "IRF" (cf. Figure 3.1(f)), est tatoué dans chaque image. Les résultats expérimentaux sont séparés en deux parties : la première est consacrée au teste de la propriété d'imperceptibilité alors que la deuxième est consacrée à l'analyse de la robustesse contre quelques types d'attaques.

Nous avons utilisé le PSNR pour estimer la distorsion des images tatouées. Aussi, après l'extraction de la marque, le coefficient de corrélation est calculé en utilisant la marque originale et celle extraite. Ce coefficient permet de juger l'existence et l'exactitude de la marque extraite. Ces deux métriques ont été présentées dans la Section 1.9.1.

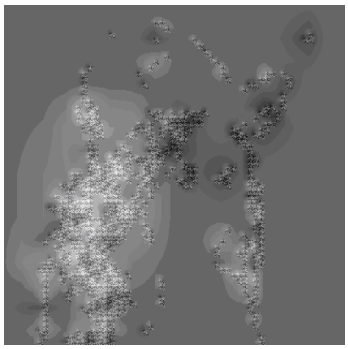
**Dégradations visuelles**

La Figure 3.10 montre l'image originale $I_0$ et l'image tatouée $Iw$ et leur différence absolue amplifiée. D'après la valeur du PSNR, on remarque que la mesure objective calculée entre l'image originale $I_0$ et l'image tatouée $Iw$ est élevée. De plus, l'algorithme

proposé extrait la marque insérée de façon parfaite. Aussi, d'après l'image de différences, montrée à la Figure 3.10(c), on remarque que la marque a été bien insérer dans les régions autour des conteurs et les régions texturées où ils sont invisibles.

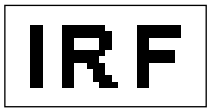
(a) L' image originale

(b) L'image tatouée
PNSR= 34.14 dB



(c) Image de la différence


(d) La marque




(e) La marque extraite
NC=1

*Figure 3.10: Comparaison entre l'image originale et l'image tatouée pour une insertion par ISS*

**Fiabilité de détection et unicité de la marque**

Un algorithme de tatouage d'images doit pouvoir détecter la marque insérée dans l'image, mais il doit aussi pouvoir la différencier vis-à-vis d'autres marques différentes appelées couramment fausses alarmes. Cette distinction doit être la plus évidente possible, dans le but d'éviter tout conflit.

La Figure 3.11 présente la réponse du détecteur à 1000 porteuses générées aléatoirement (générées à partir des clés différentes). Notre porteuse, utilisée pour générer la marque qui est implantée dans l'image, apparaît en position 100. Aucune attaque n'a été portée à l'image. Les courbes montrent que l'on peut détecter parfaitement la marque dans les

images tatouées sans équivoque, suggérant que l'algorithme a des taux de réponse de fausses alarmes.

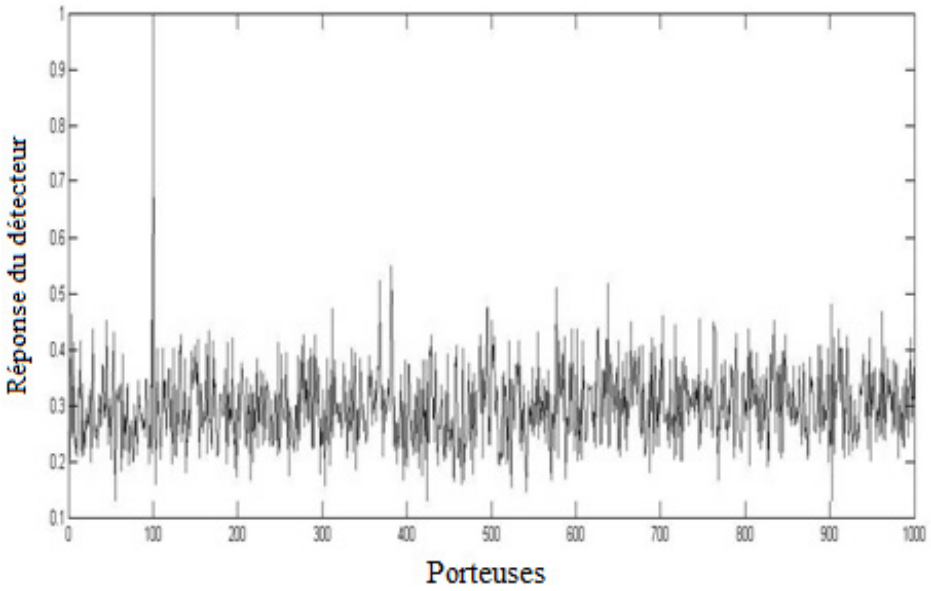



*Figure 3.11 : La réponse du détecteur aux différentes porteuses générées aléatoirement*

**Robustesse**

Afin de vérifier la robustesse de cet algorithme proposé, on a testé l'algorithme face à différents types d'attaques, y compris la compression JPEG, bruit blanc gaussien additif, le bruit Sal & Pepper, le filtre médian et ainsi que d'autres attaques.

Les premiers tests ont été effectués sur l'image de test Lena. L'image est tatouée de manière à fixer le PNSR sur 35dB. La Figure 3.12 représente les différentes images tatouées et attaquées alors que la Figure 3.13 représente les marques extraites. D'après les valeurs de la corrélation normalisée (NC), on peut déduire que les premiers tests de robustesse sont encourageants. Néanmoins, ces valeurs sont parfois un peu loin de la valeur idéale de 1 pour la corrélation normalisée.

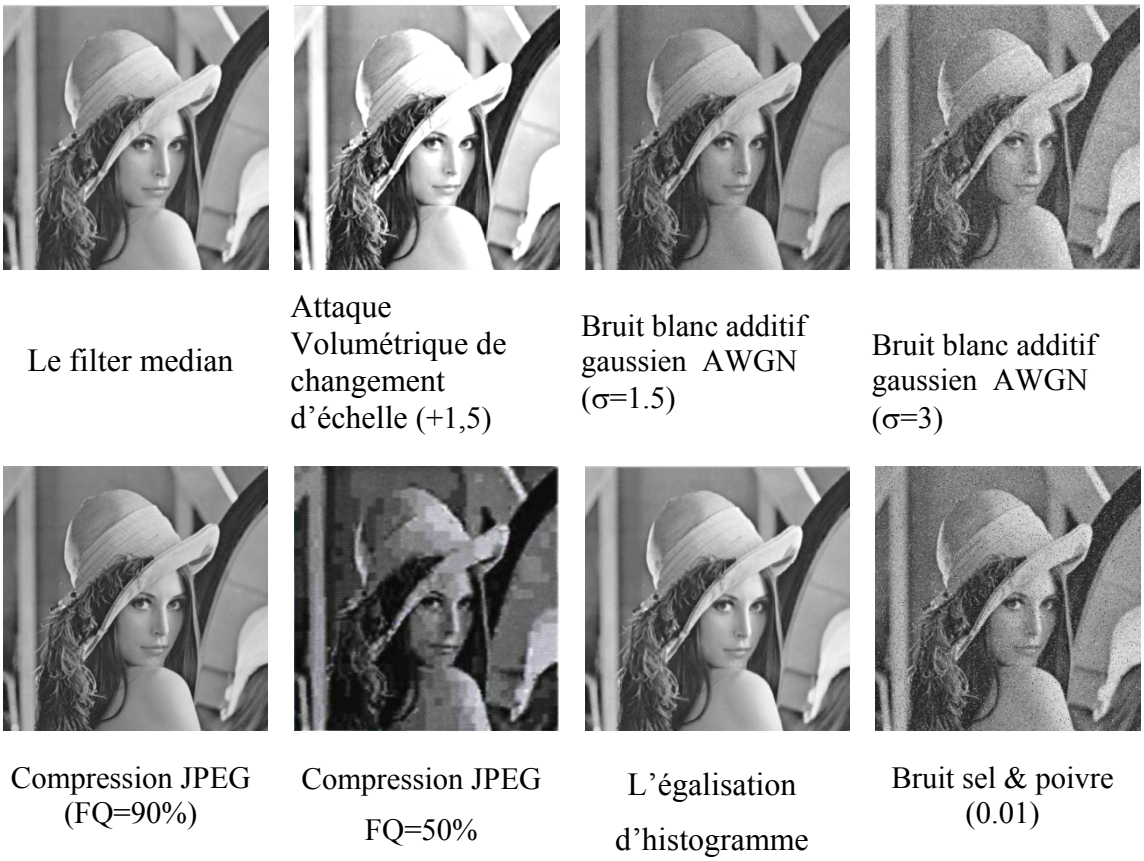



*Figure 3.12: Image tatouée et attaquée par différentes attaques.*

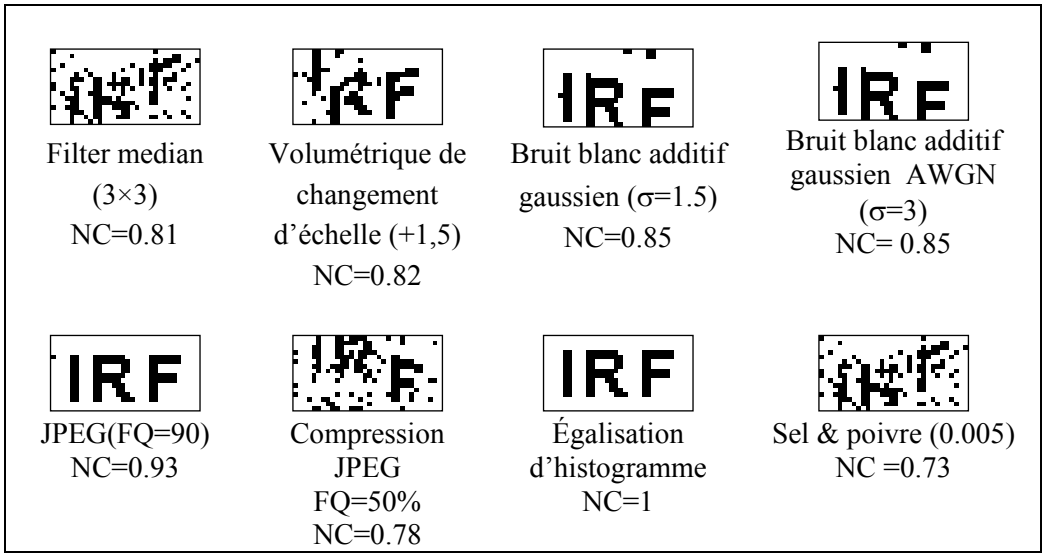



*Figure 3.13: Les marques extraites après quelques attaques sur l'image Lena*

Nous avons aussi appliqué cet algorithme sur les images présentées dans la Figure 3.1. Les images sont tatouées de telle sorte à obtenir PNSR=35dB. Le Tableau 3.1 et le Tableau 3.2 montrent la mesure objective entre la marque extraite $m^*$ et la marque $m$ après l'application des attaques sur l'image tatouée. D'après les valeurs de la corrélation normalisée (0<NC < 0.52), on peut en déduire que cet algorithme résiste aux attaques présentés dans les tableaux 3.1 et 3.2.

*Tableau 3.1: Les marques extraites après une compression JPEG*

| Facteur de qualité | 100 | 90 | 70 | 60 | 50 |
|---|---|---|---|---|---|
| Lena |  |  |  |  |  |
| NC | 1 | 0.93 | 0.84 | 0.82 | 0.78 |
| Barbara |  |  |  |  |  |
| NC | 1 | 0.88 | 0.78 | 0.74 | 0.66 |
| Papper |  |  |  |  |  |
| NC | 1 | 0.81 | 0.86 | 0.84 | 0.79 |
| Boat |  |  |  |  |  |
| NC | 1 | 0.89 | 0.80 | 0.79 | 0.82 |
| Mandrill |  |  |  |  |  |
| NC | 1 | 0.91 | 0.88 | 0.84 | 0.84 |

Les expériences réalisées sur les images de tests ont permis d'évaluer les performances de cette méthode et d'apprécier sa robustesse face à la compression JPEG et à l'ajout de bruit. La figure 3.14 montre que les attaques géométriques (rotation, changement d'échelle, fenêtrage et translation …) font tomber les scores de manière très significative. En effet toute désynchronisation spatiale change l'ordre des blocs. Ainsi il suffit par exemple de tourner avec 4° pour rendre la méthode inefficace.

*Tableau 3.2 : Mesure objective entre la marque extraite $m^*$ et la marque $m$ après l'application d'un ensemble d'attaques sur l'image tatouée*

| | Non attaquée | Filtre médiane | *Bruit blanc Gaussien additif (AWGN)* | | | l'ajout une valeur constante | | | Attaque volumétrique de changement d'échelle (+1.5) | | | Egalisation d'histogramme |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 3×3 | 1.5 | 3 | 5 | 10 | 20 | 30 | 1.5 | 2 | 3 | |
| Lena (NC) | 1 | 0.81 | 0.97 | 0.85 | 0.76 | 1 | 1 | 1 | 0.82 | 0.67 | 0.54 | 1 |
| La marque extraite |  |  |  |  |  |  |  |  |  |  |  |  |
| Barbara (NC) | 1 | 0.61 | 0.96 | 0.91 | 0.89 | 0.93 | 0.93 | 0.93 | 0.82 | 0.62 | 0.52 | 0.89 |
| La marque extraite |  |  |  |  |  |  |  |  |  |  |  |  |
| Papper (NC) | 1 | 0.63 | 1 | 0.89 | 0.83 | 1 | 1 | 1 | 0.83 | 0.67 | 0.52 | 1 |
| La marque extraite |  |  |  |  |  |  |  |  |  |  |  |  |
| Boat (NC) | 1 | 0.68 | 1 | 0.99 | 0.93 | 1 | 1 | 1 | 0.81 | 0.64 | 0.62 | 1 |
| La marque extraite |  |  |  |  |  |  |  |  |  |  |  |  |
| Mandrill (NC) | 1 | 0.64 | 1 | 0.96 | 0.92 | 1 | 1 | 1 | 0.91 | 0.85 | 0.71 | 0.97 |
| La marque extraite |  |  |  |  |  |  |  |  |  |  |  |  |

Attaque par Rotation (2°) :: ISS : NC= 0.68 | Attaque par Rotation (4°) : NC= 0.54 | attaque par Stirmark: NC= 0.46 | Attaque par cropping: NC= 0.47

*Figure 3.14: Exemples d'attaques géométriques*

## 3.5 Algorithme de tatouage numérique proposé basé sur QIM et FSDWT

Dans cette section, nous présenterons le deuxième algorithme de tatouage d'images numérique. Cet algorithme opère dans le domaine de la transformé FSDWT à échelles mixées. L'insertion est effectuée par la quantification par QIM (cf.1.7.2.1) des blocs dominats. L'algorithme proposé peut être décrit, de la même manière que le précédent algorithme, par les deux étapes : d'insertion et d'extraction de la marque.

### 3.5.1 Processus d'insertion de la marque

Considérons l'image originale $I_0$ en niveau de gris de taille N x N pixels, et la marque ***m*** binaire de taille 32 x 16 pixels. Le schéma du processus d'insertion est représenté à la Figure 3.15 et se résume par les étapes suivantes :

1. Transformer l'image originale par la transformée en ondelettes basée sur le schéma de lifting (FSDWT) à échelles mixées en n niveaux de résolution.
2. Sélectionner les blocs dominants ***X*** en se basant sur l'algorithme de la section 3.4.1.
3. Encrypter ensuite la marque ***m*** par une permutation pseudo-aléatoire en utilisant une clé ***K1***. On obtient donc une image marque cryptée ***Wc***.

4. Insérer les bits de la marque cryptée en utilisant la technique DM-QIM, présentée dans la section 1.7.2.1, en utilisant la fonction suivante :

$$y(n) = Q\left(x(n) + d\left(n, m(n), \Delta\right)\right) - d\left(n, m(n)\right) \qquad (3.6)$$

Où

$$d(n,1) = \begin{cases} d(n,0) + \dfrac{\Delta}{2} & , d(n,0) > 0 \\ d(n,0) - \dfrac{\Delta}{2} & , d(n,0) < 0 \end{cases} \qquad (3.7)$$

n =1.. taille de message m et *d(n,0)* est un vecteur pseudo aléatoire à distribution uniforme choisit dans l'intervalle [-Δ/2, Δ/2] généré par une clé ***K2***.

$Q(*, \Delta)$ est une fonction de quantification avec pas Δ, définie par :

$$Q(x, \Delta) = round\left(\frac{x}{\Delta}\right)\Delta$$

Les clés ***K1*** et ***K2*** permettent de sécuriser notre schéma de tatouage.

5. Finalement, reconstruire l'image tatouée ***Iw*** à partir des coefficients tatoués $y_n$ en appliquant la transformée en ondelettes inverse IFSDWT.

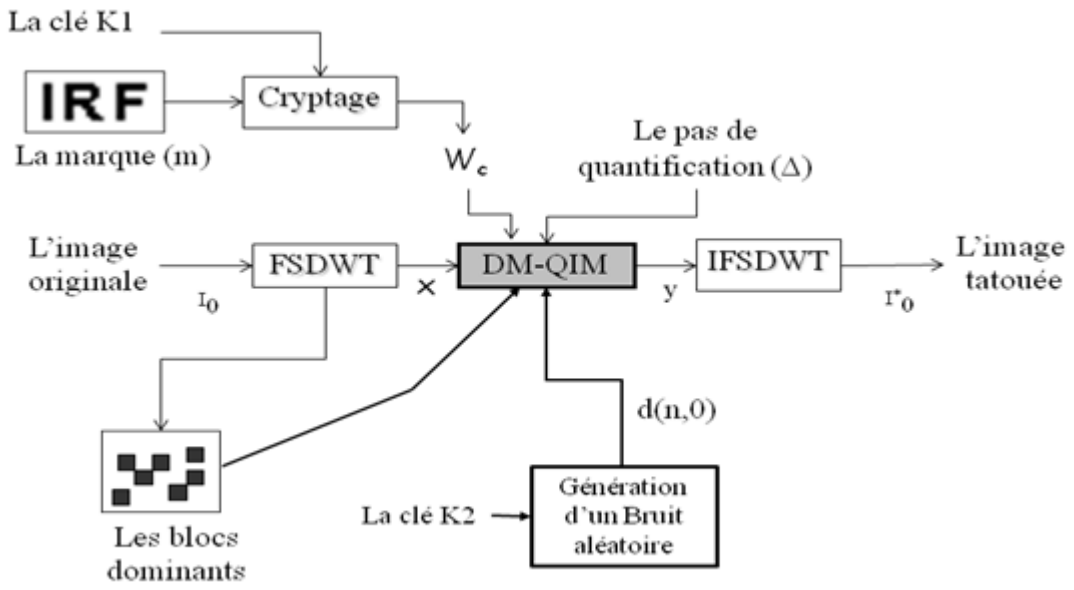



*Figure 3.15: Schéma du processus d'insertion de la marque.*

### 3.5.2 Processus d'extraction de la marque

Cet algorithme est du type aveugle, c'est-à-dire que l'image originale $I_0$ n'est pas nécessaire pour le processus d'extraction. Le schéma du processus d'extraction est illustré à la Figure 3.16, et est décrit par les étapes suivantes :

D'abord, on décompose l'image $I_0^*$ par la transformée en ondelettes basée sur le schéma lifting (FSDWT) en *n* niveaux de résolution.

Ensuite, on sélectionne les blocs dominants choisis de la même manière que la phase d'insertion.

Puis, on estime ensuite la marque obtenue $W_c^*$ à partir des blocs dominants sélectionnés. Cette estimation est effectuée en utilisant la méthode de détection décrite dans la section 1.6.2.1. elle consiste à générer d'abord le la séquence aléatoire *d(n,0)* par la clé *K2* puis à calculer un vecteur Sz(n,0) correspondant à 0 et un autre Sz(n,1) correspondant à 1. Ces deux vecteurs sont calculés en utilisant l'équation suivante :

$$S_z(n,0) = Q(z_n + d(n,0), \Delta) - d(n,0)$$
$$S_z(n,1) = Q(z_n + d(n,0), \Delta) - d(n,1) \qquad (3.8)$$

L'estimation de la marque consiste à déterminer lequel de ces deux vecteurs $S_z(n,0)$ ou $S_z(n,1)$ qui minimise la distance euclidienne avec le vecteur reçu z, selon l'équation suivante :

$$W_c^* = \arg\min dist\left(z, S_z(n,l)\right) \qquad (3.9)$$

La marque $W_c^*$ obtenue est une marque cryptée.

Puis, on décrypte la marque cryptée estimée $W_c^*$ en utilisant la clé ***K1***. On utilisera l'algorithme de décryptage qui consiste à inverser la permutation pseudo-aléatoire utilisée dans la phase de cryptage. On obtient donc une image marque estimée décryptée $m^*$.

En fin, on calcule la mesure objective NC (ou RBE) entre la marque ***m*** et la marque extraite $m^*$.

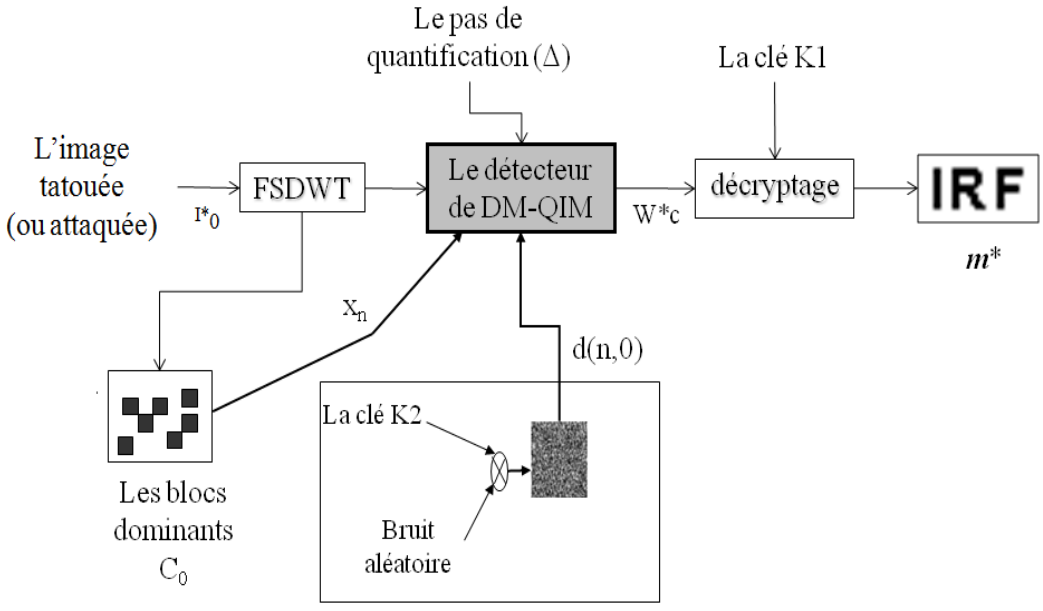



*Figure 3.16 : Schéma du processus d'extraction de la marque*

### 3.5.3 Simulations et résultats expérimentaux

Nous présentons dans cette section les résultats de notre algorithme de tatouage numérique basé sur QIM et la transformée FSDWT.

Tout comme l'algorithme de tatouage numérique utilisant ISS, on utilise la mesure objective: le PSNR pour mesurer la qualité de l'image tatouée $I_w$ par rapport à l'image originale $I_0$. La similarité entre la marque estimée $m^*$ et la marque originale $m$ est mesurée, cette fois encore, par la corrélation normalisée (NC) et le rapport des bits erronés (RBE).

Le pas de quantification Δ est empiriquement ajusté pour contrôler la force d'insertion. En effet, ce pas Δ permet de contrôler les dégradations visuelles et la robustesse. La Figure 3.17 montre le rapport des bits erronés (RBE) en fonction de Δ, nous remarquons que plus le pas de quantification Δ est grande, plus nous arriverons à détecter la marque sans erreurs. L'efficacité de la détection se réduit considérablement pour les petites valeurs de Δ. Cela est due au fait que le bruit ajouté par la séquence aléatoire d dépasse $\frac{\Delta}{4}$ [Chen01].

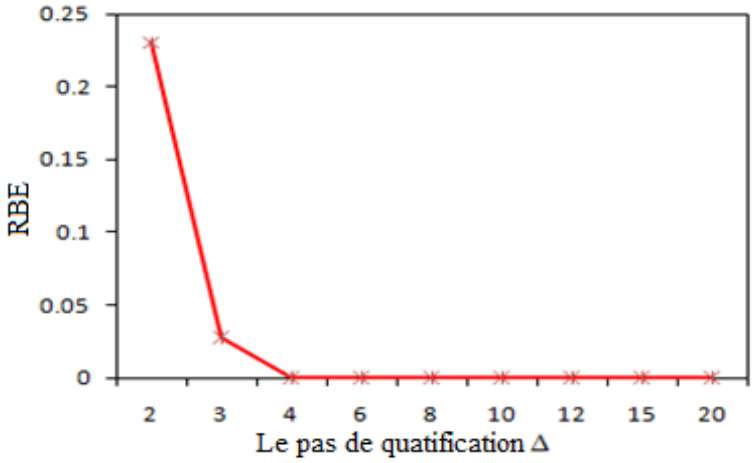



*Figure 3.17: RBE en fonction de pas de quantification Δ*

La Figure 3.18 présente le PSNR en fonction de pas de quantification Δ utilisé pour tatouer toutes les images d'identité de la base de test. Les valeurs de Δ sont rangé de 2 à 30. Pour une taille large de pas Δ, l'algorithme devient plus robuste mais la distorsion augmente aussi.

A partir de l'expérience, si nous fixons Δ = 20, le PSNR moyen de la base d'images est environ 35 dB.

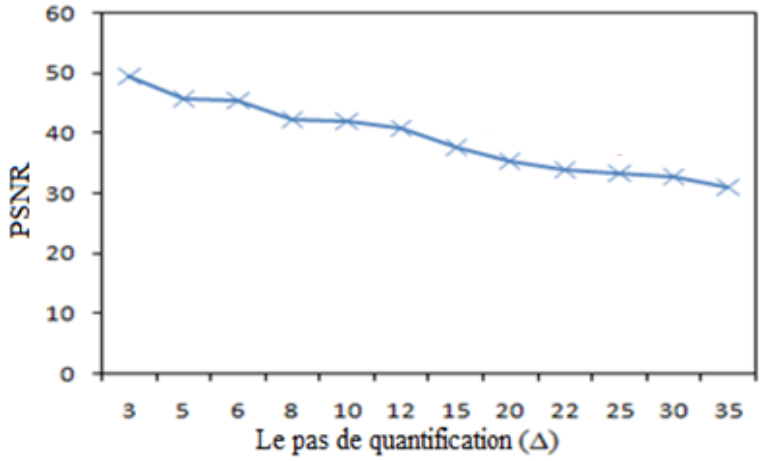
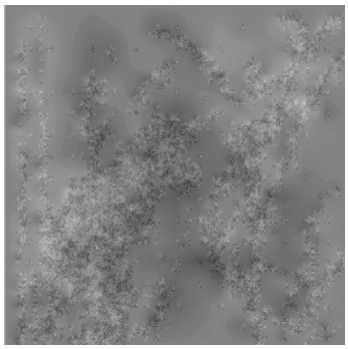



*Figure 3.18: La relation entre le pas de quantification et PSNR*

Les Figure 3.19 et Figure 3.20 montrent une image originale $I_0$ et l'image tatouée $I_w$ et leur différence absolue amplifiée par un facteur égal à 30. D'après les valeurs du PSNR, on remarque que les mesures objectives calculées entre l'image originale $I_0$ et l'image tatouée $I_w$ sont élevées. De plus, l'algorithme proposé extrait la marque insérée de façon parfaite. Dans tous les cas, la valeur du rapport des bits erronés RBE est minimale. Aussi, d'après les images de différences (la Figure 3.19(c) et la Figure 3.20(c)), il est évident de remarquer que la marque est ajoutée sur les régions autour des conteurs et les régions texturées où ils ne sont pas perceptibles.

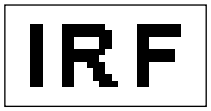
(a) L' image originale

(b) L'image tatouée



(c) Image de la différence


(d) La marque

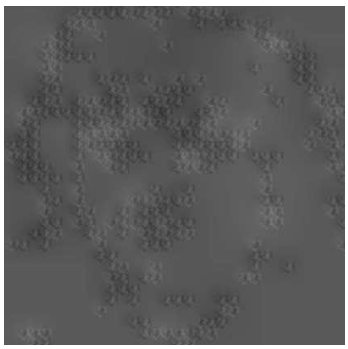



(e) La marque extraite
RBE= 0

*Figure 3.19: Comparaison entre l'image originale et l'image tatouée (PNSR= 38.64 dB, T=1, Δ=15).*

(a) L'image originale

(b) L'image tatouée :
PNSR= 37.79dB



(c) Image de la différence

*Figure 3.20: Comparaison entre l'image originale et l'image tatouée (PSNR = 37.79 dB).*

Afin de vérifier la robustesse de cet algorithme, on l'a testé face à différents types d'attaques, y compris la compression JPEG, bruit blanc gaussien additif, le bruit Sal & Pepper, le filtre médian et ainsi que d'autres.

Nous avons effectué les premiers tests sur l'image Lena. Nous avons tatoué l'image de test d'une manière à fixer le PNSR sur 35 dB. La Figure 3.21 représente les marques extraites.

D'après les valeurs du rapport des bits erronés (RBE), on peut déduire que cet algorithme résiste aussi à ce type d'attaques.

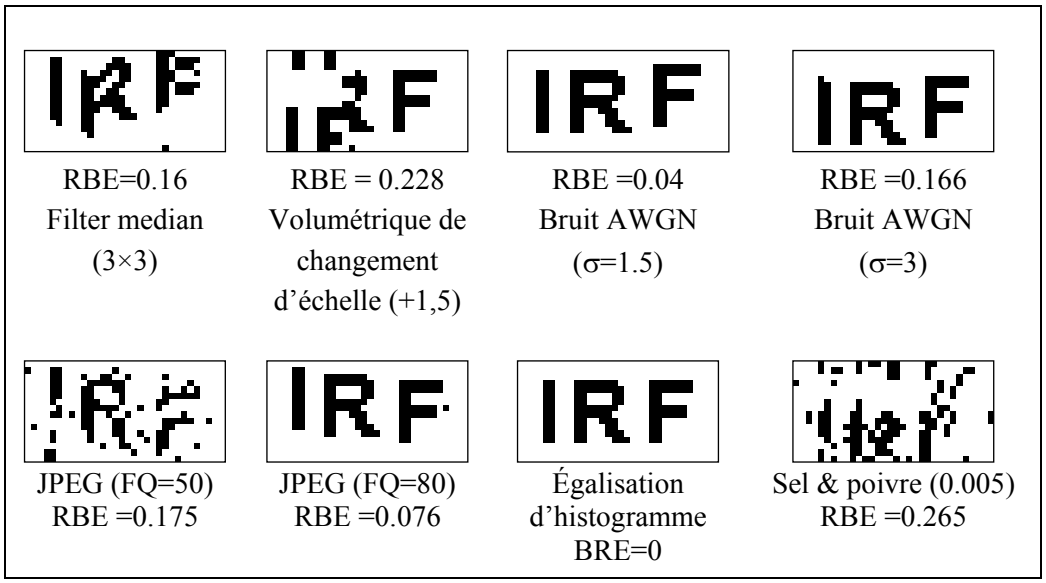



*Figure 3.21: Les marques extraites après quelques attaques sur l'image Lena*

## 3.6 La comparaison entre les deux méthodes proposées

Dans cette section, nous présentons une comparaison des méthodes proposées en termes de critère robustesse. Cette comparaison est réalisée en marquant une base d'images d'identité. Cette base comporte 200 images de taille 256×256. Pour fins de comparaison, Nous avons tatoué les images d'une manière à fixer le PNSR à environ 35 dB pour toutes images tatouées. Aussi, on utilise le rapport de bits erronés (RBE) entre la marque $m$ et la marque extraite $m^*$.

Le tableau 3.4 présente les valeurs moyennes du rapport des bits erronés (RBE) entre la marque originale la marque extraite $m^*$ à partir des images tatouées. D'après les valeurs du RBE ($0 < RBE < 0.356$) on peut déduire que les deux algorithmes sont performants. En effet, l'insertion dans les blocs dominants offre un bon compromis entre l'invisibilité et la robustesse. Néanmoins, ces valeurs sont parfois un peu loin de la valeur idéale de 0 pour le

rapport des bits erronés. Ces résultats peuvent être améliorés en utilisant des codes correcteurs d'erreurs.

On remarque aussi que les performances obtenues par les deux algorithmes proposés dans ce chapitre sont très proche. Cependant, l'algorithme utilisant QIM donne des résultats légèrement meilleurs pour une attaque compression JPEG. Par contre, L'algorithme basé sur ISS est performant lorsqu'il s'agit d'attaques par filtrage.

D'après les tests de robustesses, le tableau 3.2 et la figure 3.20 illustrant les marques extraites. On peut conclure que ces deux méthodes proposées résistent aux attaques suivantes : bruit, filtrage gaussien, recadrage, compression JPEG, volumétrique de changement d'échelle, égalisation d'histogramme.

*Tableau 3.3: Résultats des tests de robustesse pour les images d'identité*

| **Les attaques** | **RBE (FSDWT-ISS)** | **RBE (FSDWT-QIM)** |
|---|---|---|
| Non attaqué | 0 | 0 |
| Filtre médian 3×3 | 0.19 | 0.203 |
| Filtre médian 5×5 | 0.198 | 0.21 |
| Bruit sel & poivre 0.01 | 0.191 | 0.2082 |
| Bruit sel & poivre 0.02 | 0.28 | 0.356 |
| Bruit blanc Gaussien additif AWGN (σ=1) | 0 | 0 |
| Bruit blanc Gaussien additif AWGN (σ=2) | 0.12 | 0.18 |
| Bruit blanc Gaussien additif AWGN (σ=2.5) | 0.181 | 0.22 |
| Bruit blanc Gaussien additif AWGN (σ=3) | 0.189 | 0.226 |
| Recadrage (10% supprimé) | 1 | 0.02 |
| Recadrage (20% supprimé) | 0.16 | 0.16 |
| JPEG (FQ=50) | 0.22 | 0.203 |
| JPEG (FQ=60) | 0.18 | 0.181 |
| JPEG (FQ=70) | 0.174 | 0.168 |
| JPEG (FQ=80) | 0.161 | 0.159 |
| JPEG (FQ=90) | 0.10 | 0.095 |
| JPEG (FQ=100) | 0 | 0 |

*Tableau 3.4: Comparaison en terme d'imperceptibilité entre l'image marque W et l'image marque extraite W* avec la méthode de Wang et Lin.*

| Attaques | NC FSDWT-ISS | NC FSDWT-QIM (38.64 dB) | NC Wang and Lin (PNSR=38.2 dB) |
|---|---|---|---|
| Non attaquée | 1.00 | 1.00 | 1.00 |
| Le filtre médian 3×3 | 0 .81 | 0.59 | 0.51 |
| Le filtre médian 4×4 | 0.67 | 0.36 | 0.23 |
| Bruit gaussien | 0.83 | 0.69 | 0.64 |
| JPEG (FQ=50) | 0.73 | 0.78 | 0.28 |
| JPEG (FQ=70) | 0.79 | 0.84 | 0.28 |
| JPEG (FQ=80) | 0.86 | 0.91 | 0.57 |
| JPEG (FQ=90) | 0.93 | 1 | 1 |

## 3.7 Conclusion

La transformée FSDWT exprimé par lifting à échelles mixées représente un domaine d'insertion efficace pour tatouer les images et essentiellement les images d'identité, en offrant des zones optimales pour insérer une marque. Ces zones ont été qualifiées par « blocs dominants ».

Dans ce chapitre, nous avons sélectionné ces blocs dominants d'une manière automatique, en exploitant les caractéristiques statistiques des coefficients de la transformée FSDWT à échelles mixées. Nous avons montré que ces blocs correspondent aux régions autour des contours et aux zones texturées.

Nous avons également proposé deux méthodes de tatouages robustes basées sur FSDWT à échelles mixées en prenant en compte: la détection aveugle de la marque et le bon compromis entre la qualité visuelle d'images tatouées et la robustesse contre les attaques. La première méthode est basée sur une insertion additive par l'étalement de spectre, et la

deuxième méthode est basée sur une règle substitutive en quantifiant les coefficients des blocs dominants de FSDWT par QIM.

Les résultats expérimentaux d'imperceptibilité et de robustesse montrent que les méthodes proposées maintiennent une haute qualité d'images tatouées et très robustes contre plusieurs attaques conventionnels. Les performances obtenues sont très proches. Cependant, l'algorithme utilisant QIM donne des résultats légèrement meilleurs contre une compression JPEG. Par contre, L'algorithme basé sur ISS est performant contre les attaques par filtrage. Ces méthodes ont été aussi comparées à une méthode de référence de base en tatouage d'images dans le domaine d'ondelettes. Nos algorithmes résistent mieux contre la compression et l'ajout de bruit. Nous avons aussi implémenté ces deux en développant un prototype logiciel basé sur le langage de programmation C++ et un outil Matlab (Cf. Annexe A).

Dans le chapitre suivant, nous présenterons une méthode hybride d'authentification d'image basée sur les blocs dominants et les moments invariants de l'image à tatouée.

# Chapitre 4 Authentification d'images basée sur les descripteurs de forme et les coefficients dominants d'ondelettes

## 4.1 Introduction

La technologie numérique rend la transmission, le stockage et la modification de documents multimédia beaucoup plus aisées qu'auparavant. Ce qui a posé le problème de la sécurité de ces données. Le tatouage fragile constitue une technique qui permet d'authentifier et de vérifier l'intégrité du document tatoué. Il est fragile aux modifications, et permet de vérifier que le document n'a pas été retouché et donc de l'authentifier.

Dans ce contexte un nouveau schéma de tatouage fragile d'images est présenté. Le principe de ce schéma est basé sur l'utilisation des descripteurs statistiques de l'image et les blocs dominants de la transformée FSDWT à échelles mixées. A la réception, une mesure de similarité, entre le vecteur descripteur reçu et celui de l'image reçue, est calculée pour décider si l'image tatouée a subit des modifications lors de la transmission. En effet, les descripteurs utilisés sont très sensibles aux déformations et au bruit. Aussi, comme nous l'avons cité au paravent, la représentation à échelles mixées des coefficients de la transformée en ondelettes a le pouvoir de concentrer l'information dans un nombre réduit de coefficients les plus significatifs. Ces coefficients peuvent être sélectionnés par blocs en utilisant leurs caractéristiques statistiques.

Ce chapitre présente une vue détaillée sur les techniques utilisées dans ce schéma. Nous abordons plus précisément trois étapes. Dans la première étape, nous verrons la technique utilisée pour extraire les descripteurs de l'image à tatouer. Puis, la manière de construire de la marque à partir de ces descripteurs et les blocs dominants de la transformée en ondelettes FSDWT. Dans la deuxième étape nous expliquons la phase d'insertion qui consiste à

substituer le plan LSB des pixels par la marque crée. Dans la troisième étape, nous verrons la manière de détecter, à la réception, si l'image tatouée a subi des modifications. Si le vecteur de caractéristiques reçu coïncide avec celui extrait à partir de l'image tatouée, alors l'image est authentique à l'image originale, sinon elle n'est pas.

Enfin, nous présentons les résultats expérimentaux effectués afin de pouvoir évaluer notre schéma de tatouage fragile.

## 4.2 Les descripteurs

### 4.2.1 Principe

Un descripteur est définit comme l'information utilisée pour caractériser le contenu d'une image [Ngu09]. Des nombreux descripteurs sont utilisés pour décrire les images, principalement en en terme de formes, de couleurs et textures. Les descripteurs de forme sont largement utilisés dans la recherche d'image par similarité [Flu09Flu09Flu09]. Ils sont utilisés aussi en tatouage fragile [Li03][kha06].

La forme est une caractéristique visuelle importante. Elle présente un descripteur de base pour décrire le contenu et la structure d'une image.

Nous distinguons généralement deux catégories de descripteurs de forme ; les descripteurs basés sur les régions et les descripteurs basés les contours. Les premiers utilisent les moments géométriques qui permettent de caractériser l'intégralité des formes d'une image. La seconde catégorie référence au descripteur de Fourier, ils sont introduits par F. P. Kuhl et C. R. Giardina [Kuh82] pour décrire les formes des contours.

Les moments géométriques sont utilisés en tatouage fragile pour leur sensibilité aux déformations et au bruit (i.e. aux attaques). Un changement dans l'image entrainera une modification de ces moments, ce que permet de vérifier si une image tatouée a subi des modifications lors de transfert vers le récepteur. Nous détaillons dans ce qui suit les moments géométriques :

### 4.2.2 Les moments géométriques

Les moments géométriques [Son99] permettent de décrire une image à l'aide de propriétés statistiques. Ils représentent les propriétés spatiales de la distribution des pixels dans l'image.

Les moments $M_{pq}$ d'une image à taille M×N, d'ordre (p+q) de la fonction de la densité $f(x,y)$ sont définis par la formule suivante :

$$M_{pq} = \sum_{x=0}^{m} \sum_{y=0}^{n} x^p y^p f(x,y) \qquad (4.1)$$

Le moment d'ordre 0 $M_{0,0}$ représente l'aire de la forme de l'objet. Les deux moments d'ordre 1 $M_{1,0}$ et $M_{0,1}$ associé au moment d'ordre 0 permettent de calculer le centre de gravité de l'objet. Les coordonnées $(x_g, y_g)$ de ce centre sont présentées par l'équation (4.2):

$$x_g = \frac{m_{1,0}}{m_{0,0}} \text{ et } y_g = \frac{m_{0,1}}{m_{0,0}} \qquad (4.2)$$

### 4.2.3 Les moments invariants de HU

Les moments géométriques sont utilités limitée puisqu'ils varient à chaque changement d'échelle et à l'orientation de l'objet. Un ensemble de moments invariants serait plus utile. Hu [Hu62] a proposé un ensemble de sept moments invariants aux translations, rotations et changement d'échelle. Ils sont avantageux au tatouage fragile pour lors grande sensibilité au bruit et aux attaques.

Ces moments invariants peuvent être extraites d'une image binaire ou une image en niveau de gris.

Ceci peut être dérivé en calculant d'abord les moments centrés par l'équation suivante :

$$\mu_{pq} = \sum \sum (i - x_g)^p (i - y_g)^q f(i,j) \qquad (4.3)$$

Les moments centrés sont utilisés pour calculer les moments centrés normalisés : Ils sont calculés par l'expression suivante :

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\left(\frac{p+q}{2}+1\right)}} \quad pour\ p+q \geq 2 \tag{4.4}$$

A partir des moments centrés normalisés, nous pouvons calculer un ensemble de sept paramètres invariants. Ces sept moments invariants sont :

$$\phi_1 = \eta_{20} + \eta_{02} \tag{4.5}$$

$$\phi_2 = (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^{\ 2} \tag{4.6}$$

$$\phi_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \tag{4.7}$$

$$\phi_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \tag{4.8}$$

$$\begin{aligned}\phi_5 = {} & (\eta_{30} - 3\eta_{12})(\eta_{21} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2\right] \\ & + (3\eta_{21} + \eta_{03})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]\end{aligned} \tag{4.9}$$

$$\phi_6 = (\eta_{20} - \eta_{02})\left[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{30})^2\right] + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}) \tag{4.10}$$

$$\begin{aligned}\phi_7 = {} & (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})\left[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} - \eta_{03})^2\right] \\ & + (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})\left[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2\right]\end{aligned} \tag{4.11}$$

Dans notre travail, le vecteur $V = (\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7)$ constitue un vecteur descripteur de l'image originale qui sera inséré dans le plan LSB de l'image elle-même.

À la détection, Nous calculons la distance entre le vecteur descripteur $V_d$ de l'image reçue et celui extrait $V_d^*$ afin de vérifier l'authenticité de l'image reçue.

$$Dist(V_d, V_d^*) = \left( \sum_{i=0}^{7} \left| V_d(i) - V_d^*(i) \right|^2 \right)^{1/2} \qquad (4.12)$$

Dans la littérature, on distingue d'autres descripteurs de forme telle que les moments Legendre, les moments de Zernike.

## 4.3 Algorithme de tatouage fragile proposé

Dans cette section, nous présentons l'algorithme de tatouage numérique fragile des images. Cet algorithme est basé sur les descripteurs de forme et les coefficients d'ondelettes de la transformée en ondelettes FSDWT représentée à échelles mixées. L'algorithme proposé peut être décrit par les deux étapes : l'insertion et la détection.

### 4.3.1 Processus d'insertion

Considérons l'image originale $\boldsymbol{I_0}$, une image à niveau de gris de taille N x N pixels, et une information d'identification $\boldsymbol{m}$. Le schéma du processus d'insertion est représenté à la Figure 4.2 et se résume par les phases suivantes :

La première phase consiste à sélectionner les blocs dominants de l'image originale. La Figure 4.1 montre les étapes de sélection des blocs dominants. D'abord, nous appliquons la transformée FSDWT sur l'image originale sans le plan LSB. Nous éliminons ensuite la 1ère échelle afin d'augmenter la capacité d'intégration, puis nous représentons le reste des coefficients à échelles mixées. Nous sélectionnons ensuite les blocs dominants en se basant sur l'algorithme présenté dans la section 3.3.2. Puis nous randomisons ces blocs en utilisant une clé ***k1***, afin de rendre difficile leur reconstruction par un utilisateur non autorisé.

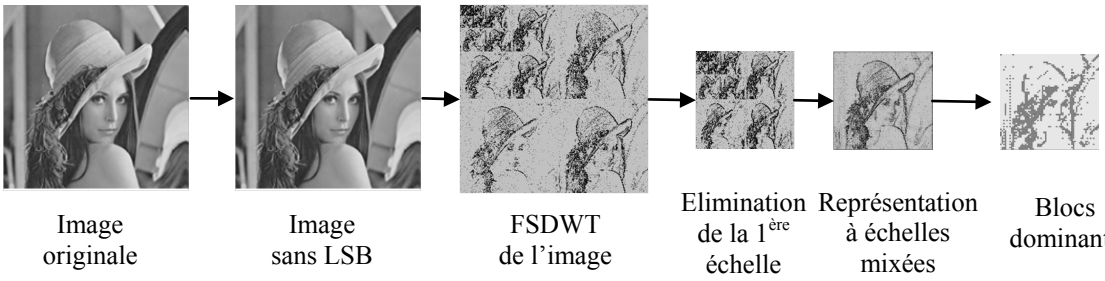



*Figure 4.1: La sélection des blocs dominats.*

La phase suivante consiste à extraire le vecteur descripteur $V = (\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7)$ à partir des moments Hu de l'image originale sans le plan LSB.

Le plan de bits LSB de l'image est ensuite substitué par les données cryptées $\boldsymbol{W}$ qui sont composées de :

- L'information d'identification ***m*** ;
- Le vecteur descripteur de l'image ***V***.
- Les blocs dominants l'image originale ***X***.

### 4.3.2 Processus d'extraction de l'information et vérification de l'authenticité

Cet algorithme est du type aveugle, c'est-à-dire que l'image originale $I_0$ n'est pas nécessaire pour le processus d'extraction. Le schéma du processus d'extraction est illustré à Figure 4.3 qui est décrit par les étapes suivantes :

La première étape consiste à extraire d'abord les informations d'identifications et le vecteur descripteur $V_d^*$ qui ont été insérés dans plan LSB de l'image reçue. Ensuite, nous calculons le vecteur descripteur $V_d$ à partir de l'image reçue sans le plan LSB. Si l'image reçue est intacte, cela signifie que le vecteur descripteur reste inchangé. Dans le cas contraire, nous procédons à l'identification des régions altérées :

D'abord, nous extrayions les blocs dominants du plan LSB de l'image reçue et à inverser la randomisation appliquée sur ces blocs lors de l'insertion en utilisant la clé ***k1***. Puis, nous

décomposons l'image $I_w^*$ par la transformée en ondelettes basée sur le schéma lifting (FSDWT). Puis, Nous sélectionnons les blocs dominants choisis de la même manière que la phase d'insertion. Une simple comparaison des ces deux séquences de blocs dominants permet de localiser les zones altérées.

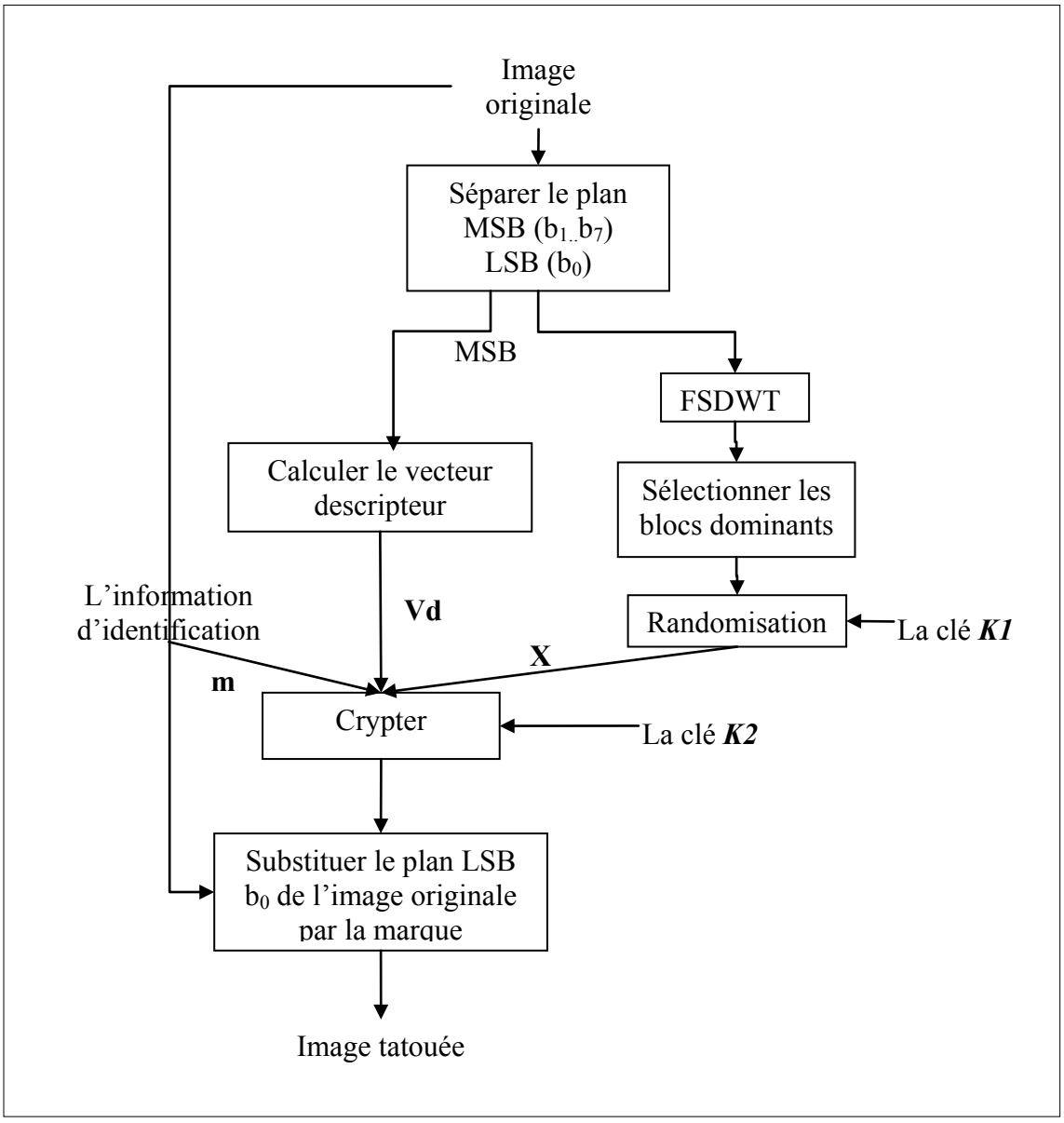



*Figure 4.2: Schéma du processus d'insertion de la marque.*

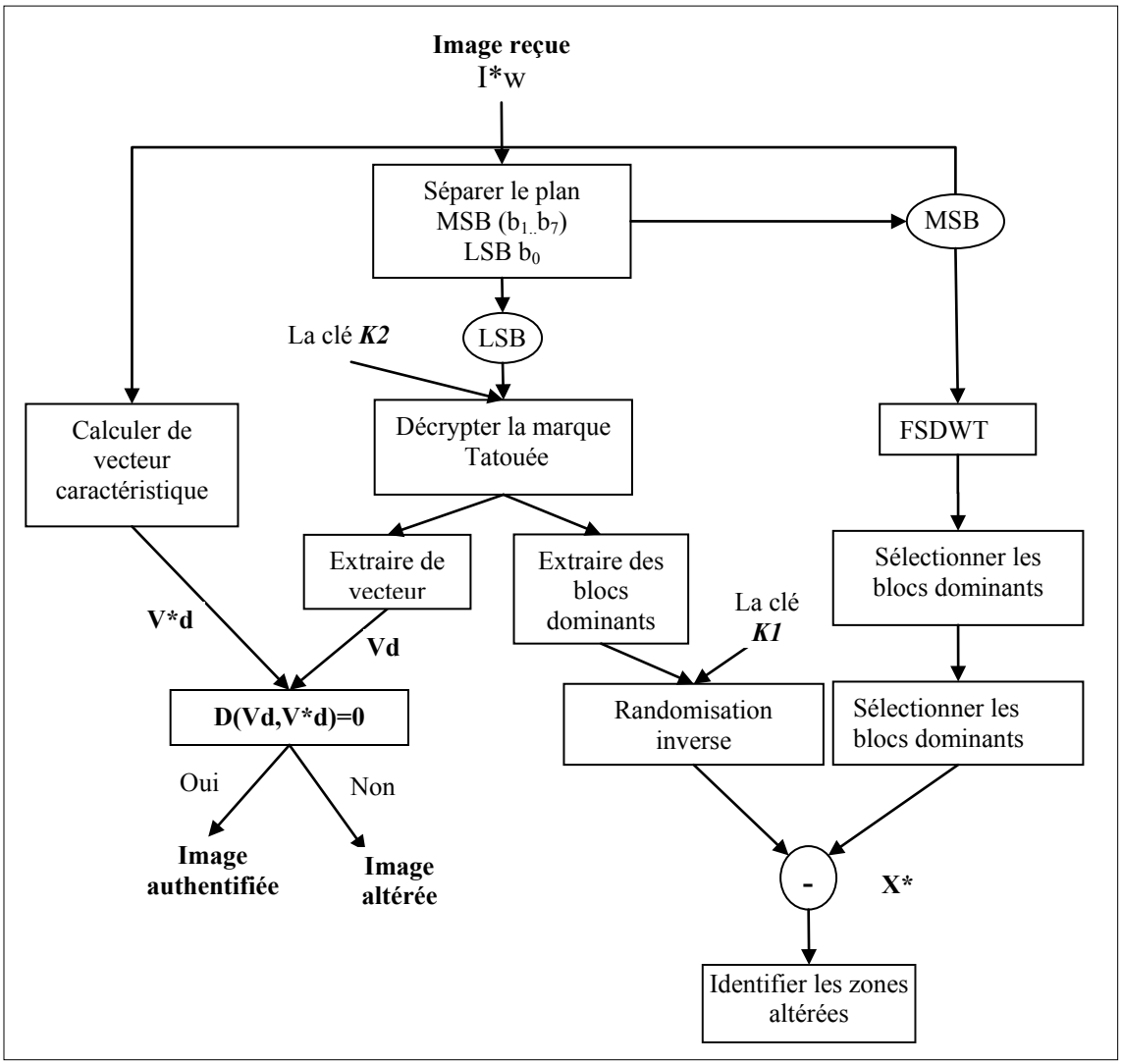


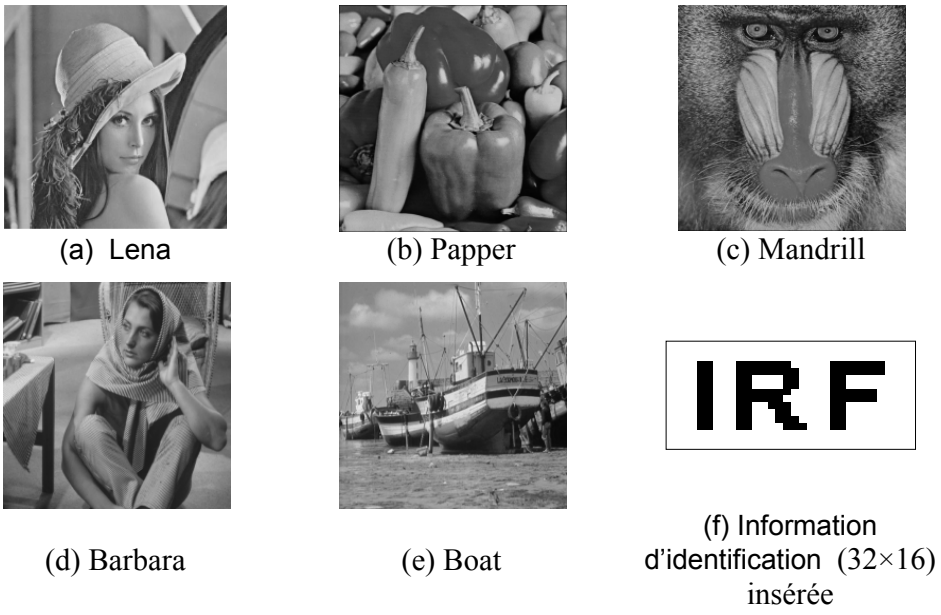

*Figure 4.3: Schéma du processus de détection et d'authentification.*

## 4.4 Simulations et résultats expérimentaux

Dans cette section, nous évaluons l'efficacité de notre méthode en termes de degré de dégradation de l'image tatouée et de la sensibilité et l'aptitude de détecter toute manipulation dans l'image. Pour ceci, nous séparons les tests en deux parties : la première est d'analyser la propriété d'imperceptibilité et la deuxième est l'évaluation de la propriété de fragilité par rapport aux attaques.

### 4.4.1 Propriété d'imperceptibilité

Afin de s'assurer des résultats obtenus, nous appliquons notre méthode aux mêmes images que nous avons utilisées pour tester l'imperceptibilité de notre algorithme aveugle (Figure 3.1) et leurs images tatouées sont illustrées dans la Figure 4.4.




(a) Lena (b) Papper (c) Mandrill

(d) Barbara (e) Boat (f) Information d'identification (32×16) insérée

*Figure 4.4: Images tatouées $I_w$.*

A partir de ces figures, on peut voir que la dégradation des images tatouées est imperceptible par l'observateur.

Nous avons jugé utile de présenter aussi le PSNR des images tatouées afin de déterminer le degré de dégradation de l'image tatouée. Le tableau 4.1 présente les valeurs de PSNR. D'après ce tableau il est claire que les valeurs de PSNR sont très bonnes, ce qui signifie que notre méthode de tatouage maintien une haute qualité d'images tatouées.

*Tableau 4.1 : Qualité des images tatouées.*

| Image tatouée | PNSR |
|---|---|
| (a) | 47.99 |
| (b) | 48.44 |
| (c) | 48.87 |
| (d) | 48.23 |
| (e) | 49.81 |

### 4.4.2 Localisation des régions attaquées

La Figure 4.5 montre un exemple sur l'image Lena avec une attaque visible. L'image de test de la Figure 4.5(a) est tatouée par les informations d'identification de la Figure 4.5(f)). La marque insérée w est composée du vecteur descripteur $V_d$ et les blocs dominants sélectionnés de la transformé FSDWT de l'image sans pan LSB. Le plan LSB est substitué par **w**.

Afin de localiser les régions attaquées, nous sélectionnons les blocs dominants de la transformée FSDWT de l'image reçue. Puis ces blocs dominats sont comparés à ceux extraits du plan LSB. Cette comparaison permet d'identifier la région altérée. En cas d'absence d'une attaque, nous obtenons un plan gris (Figure 4.5(e)).

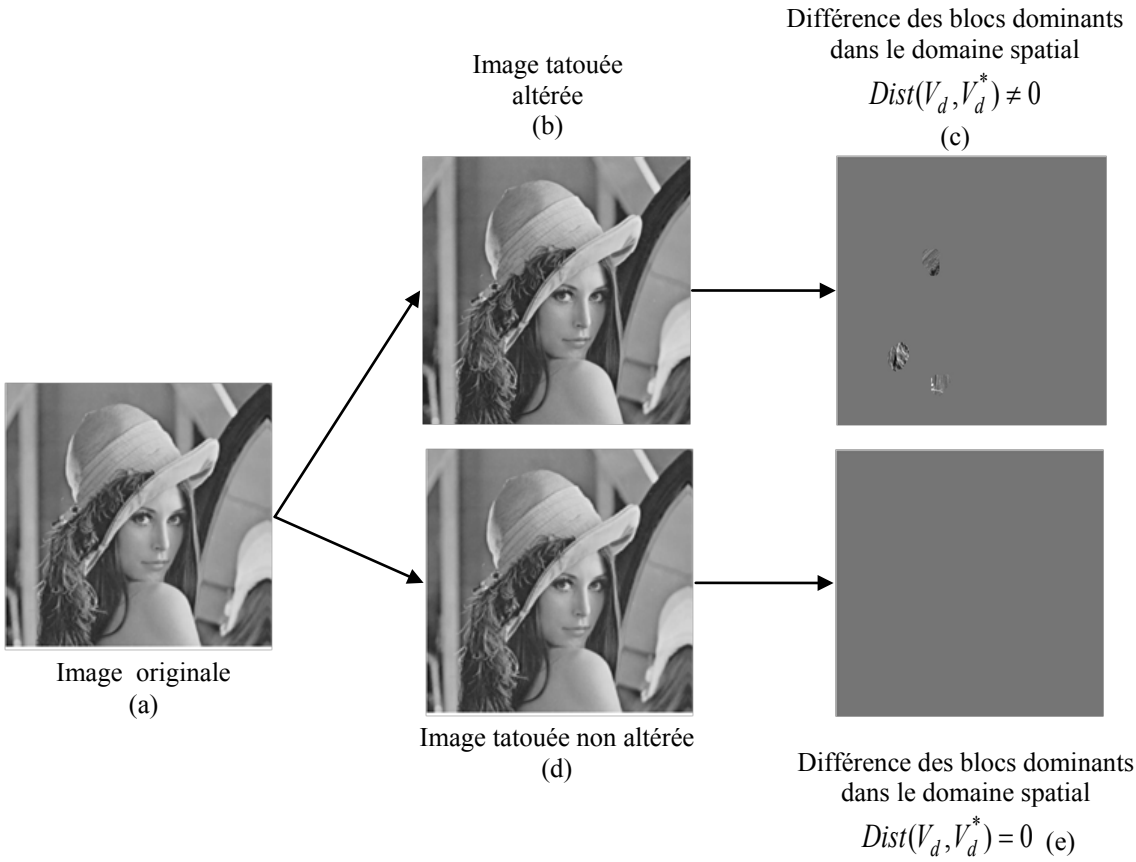



*Figure 4.5: Résultat obtenu en utilisant notre méthode de tatouage fragile*

## 4.5 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle méthode hybride de tatouage fragile d'images pour la vérification d'intégrité. Cette méthode est basée sur l'utilisation des moments invariants de l'image et les blocs dominants de la transformée FSDWT à échelle mixée. L'originalité de notre méthode réside dans l'utilisation des blocs dominants de la transformée en ondelettes à échelles mixées pour détecter les zone altérée d'une image attaquée. Le vecteur descripteur, calculé à partir des moments invariants, est utilisé pour détecter si l'image a été altérée durant sa transmission. Les blocs dominants ont été obtenus par le seuillage sur les coefficients de la transformée FSDWT de l'image sans le plan LSB. Cette nouvelle méthode est efficace en termes d'imperceptibilité et de détection des zones altérées après une attaque.

Le schéma proposé peut être intégrée dans une application d'authentification de documents. Où n'importe quel utilisateur peut vérifier si un document issu de la base est authentique ou non. Finalement, nous souhaitons à terme étendre cette méthode afin de gérer d'autres sources de Documents tels que des vidéos.

# Conclusion générale

À cause des utilisations illicites des documents numériques, le tatouage numérique a été introduit comme une technique alternative à la cryptographie et efficace pour la protection des images et la vérification de l'intégrité des données. Pour une application dédiée à la protection des images des documents d'identité, le tatouage numérique doit trouver le meilleur compromis entre deux critères contradictoires : la robustesse et l'imperceptibilité. En outre, pour une application de la vérification de l'intégrité et l'authenticité des images, le tatouage numérique doit être moins robuste (fragile) et une bonne imperceptibilité.

Au cours de cette thèse nous avons étudié la problématique liée au tatouage numérique des images. Après avoir étudié un panel assez diversifié des techniques de tatouage, nous avons élaboré trois approches du tatouage numérique. Aussi, nous avons abordé le principe de la transformée en ondelettes. Nous avons développé l'algorithme rapide de transformé en ondelette FSDWT exprimé par un schéma lifting. La représentation à échelles mixées des coefficients d'ondelettes a été aussi présentée. Cette transformée FSDWT, représentée à échelles mixées, représente un domaine d'insertion efficace pour tatouer les images et essentiellement les images d'identité, en offrant des zones optimales pour insérer une marque.

Notre première contribution a porté sur la sélection automatique des blocs dominants d'une manière automatique, en exploitant les caractéristiques statistiques des coefficients de la transformée FSDWT. Nous avons montré que ces blocs correspondent aux régions autour des contours et aux zones texturées où l'insertion permet de développer des algorithmes de tatouage robuste.

La deuxième et la troisième contribution sont le développement de deux méthodes de tatouages robustes basées sur FSDWT à échelles mixées en prenant en compte: la détection aveugle de la marque et le bon compromis entre la qualité visuelle d'images tatouées et la robustesse contre les attaques. La première méthode est basée sur une insertion additive par

l'étalement de spectre amélioré ISS, et la deuxième méthode est basée sur une règle substitutive en quantifiant les coefficients des blocs dominants de FSDWT par QIM. Les résultats expérimentaux d'imperceptibilité et de robustesse montrent que les méthodes proposées maintiennent une haute qualité d'images tatouées et très robustes contre plusieurs attaques conventionnels. Les performances obtenues sont très proches. Cependant, l'algorithme utilisant QIM donne des résultats légèrement meilleurs contre une compression JPEG. Par contre, l'algorithme basé sur ISS est performant contre les attaques par filtrage. Ces méthodes ont été aussi comparées à une méthode de référence de base en tatouage d'images dans le domaine d'ondelettes. Nos algorithmes résistent mieux contre la compression et l'ajout de bruit.

La première version de la méthode basée sur l'étalement de spectre classique fut présentée à *la conférence internationale(ICISP08)* à Cherbourg-Octeville, Normandy, France en juin 2008 [Hajji08]. La version détaillée de cette méthode basée sur ISS et DWT à échelles mixées a été présentée et acceptée au journal *International Journal of Engineering and Industries (IJEI)*. Il est publié dans le numéro 3 du volume 2 en 2011 [Hajji11a].

La méthode basée sur QIM et DWT à échelles mixées fut présentée à l'*International Conference on Multimedia Computing and Systems (ICMCS)- IEEE*, à Ouarzazte, Maroc en avril 2011[Hajji11c]. La version détaillée de cette méthode a été présentée et acceptée au *Journal of Electronic Imaging*. Elle sera publiée dans le numéro 1 du volume 21 en mars 2012.

Dans la quatrième contribution nous avons proposé une nouvelle méthode hybride de tatouage fragile d'images pour la vérification d'intégrité. Cette méthode est basée sur l'utilisation des moments invariants de l'image et les blocs dominants de la transformée FSDWT à échelle mixée. Le vecteur descripteur, obtenu à partir des moments invariants, est utilisé pour détecter si l'image a été altérée durant sa transmission. L'originalité de notre méthode réside dans l'utilisation des blocs dominants de la transformée en ondelettes à échelles mixées pour détecter les zones altérées d'une image attaquée. Le plan de bits LSB a été utilisé pour insérer la marque. Cette marque est a été construite à partir de l'information d'identification de l'image, des blocs dominants de l'image à tatouée et du

vecteur descripteur. Ce travail a été présenté et accepté à l'*International Journal of Computer Applications(IJCA)*. Il est publié dans le numéro 6 du volume 28 en juillet 2011 [Hajji11b].

## Suggestions de travaux futurs

Les méthodes de tatouages présentées dans ce mémoire de thèse peuvent être améliorées. Des travaux futurs sont envisageables concernant la proposition d'autres solutions pour améliorer les performances des algorithmes proposés dans cette thèse. Ces solutions peuvent être des solutions propres à chaque algorithme.

Concernant les deux algorithmes de tatouage robuste d'image, présentés dans le chapitre 3, d'autres modifications peuvent être aussi apportées à ces algorithmes pour les rendre plus efficace en utilisant l'histogramme des coefficients dominants pour insérer la marque sans altérer l'ordre de la densité de ces coefficients dominats. De plus, une étude approfondie sur les méthodes de synchronisation pourrait améliorer la robustesse contre les attaques géométriques.

Pour l'algorithme de tatouage fragile d'images proposé dans le chapitre 4, une combinaison entre la quantification QIM et le vecteur descripteur pourrait susceptible de conduire à une plus grande imperceptibilité et plus grande efficacité de l'algorithme proposé. Parmi les pistes d'améliorations possibles, nous pensons que cet axe de recherche est le plus prometteur. C'est dans cette direction que nous orienterons nos prochains travaux.

# Annexe A Les prototypes logiciels développés

## A) Le prototype logiciel développé en C++

Nous avons essayé, au cours de ce travail, de développer un prototype logiciel basé sur le langage de programmation C++. Ce prototype permettra de tatouer une image numérique en utilisant les deux algorithmes robustes que nous avons proposé dans le chapitre 3. Nous avons basé sur le noyau d'un logiciel développé par l'équipe PRISE, Polytech, Orléans en France. La Figure 5.1 présente le diagramme de classe des principales classes que nous avons utilisé pour développée ce logiciel (cf. Figure 5.2) :

**La classe CWaterImage :**

Cette classe est chargée de réaliser le stockage des paramètres d'une image à tatouer ou tatoué avec l'aide de CBmp.

**La classe CBmp :**

La classe CBmp permet entre autre de lire et sauvegarder une image au format Bmp. Elle permet aussi d'accéder aux différents plans de l'image (RVB).

**La classe CWatermarking**

La classe CWatermarking est la classe mère des différents algorithmes de tatouage d'image. Les images sont ici traité et comme étant des plan. L'algorithme tatoue un message sur le plan transmis. Il est à la charge de l'utilisateur de cette classe de transmettre le plan de couleur qui lui convient (Red, Green Blue ou Gray).

**La Classe CISSHAJJI**

Cette classe contient les données membres et les méthodes relatives à la gestion de l'algorithme basé sur l'étalement de spectre. Cet algorithme réalise le tatouage d'une image dans le domaine de la transformée FSDWT à échelle mixées. Le principe consiste à ajouter aux blocs dominants une séquence aléatoire suivant le bit de la marque à cacher. La

détection est effectuée par un calcul de la corrélation entre les blocs dominants de l'image reçue et la séquence utilisée lors de la phase d'insertion.

**La classe CQIMHAJJI**

Cette classe contient les données membres et les méthodes relatives à la gestion de l'algorithme basé sur modulation d'index (QIM). Le principe consiste à quantifier les coefficients des blocs dominants. La détection repose sur le calcul de la distance minimale entre les blocs dominants les quantificateurs.

**La classe Indexblock**

Cette classe contient les données membres et les méthodes relatives à localiser les zones optimale pour l'insertion (Les blocs dominants).

## B) L'outil Matlab développé

Nous avons aussi développé un outil Matlab (Toolbox). Ce toolbox permettra de tatouer les images numériques en utilisant les algorithmes robustes. L'avantage de cet outil est qu'il permet d'intégrer facilement et d'évaluer rapidement une méthode de tatouage. Comme le montre la Figure 5.3, l'interface permet de tatouer une image en parcourant les différentes étapes : La transformée DWT, la localisation des blocs dominants, l'insertion et aussi la détection.

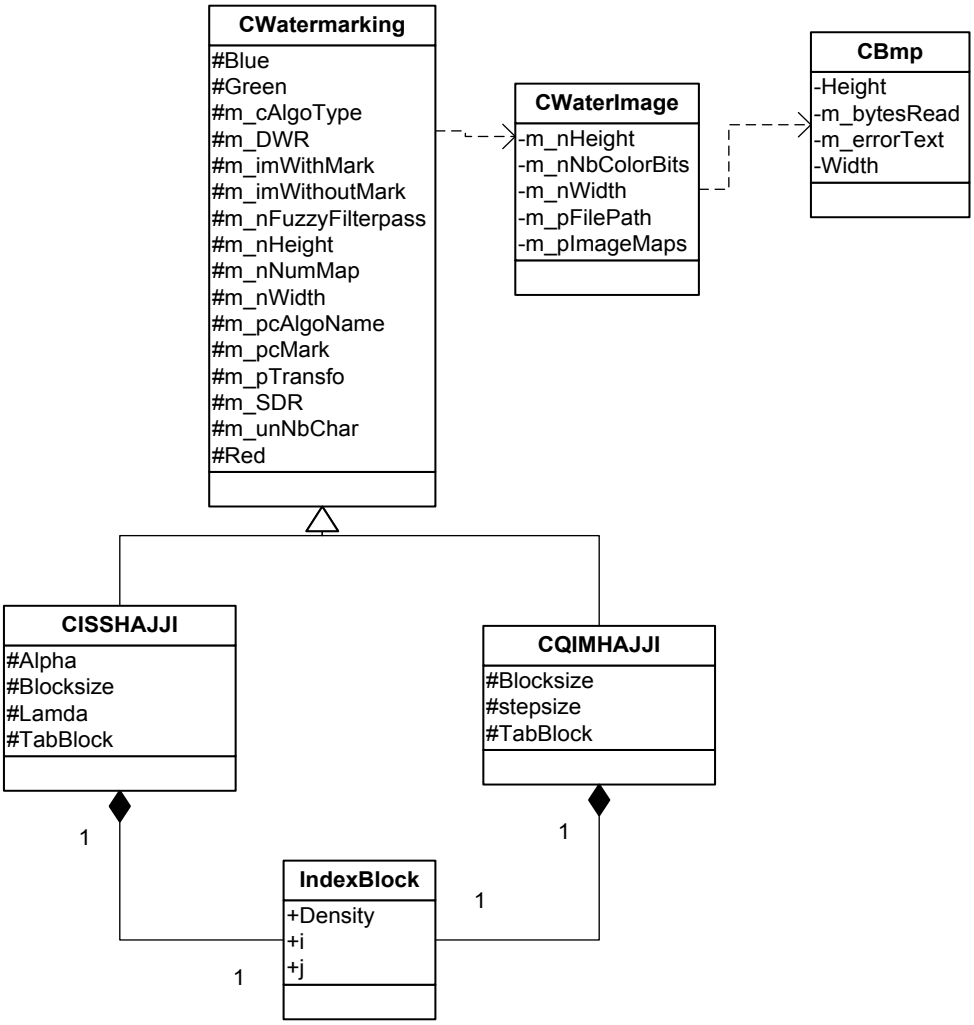



*Figure 5.1: Le diagramme de classe des principales classes.*

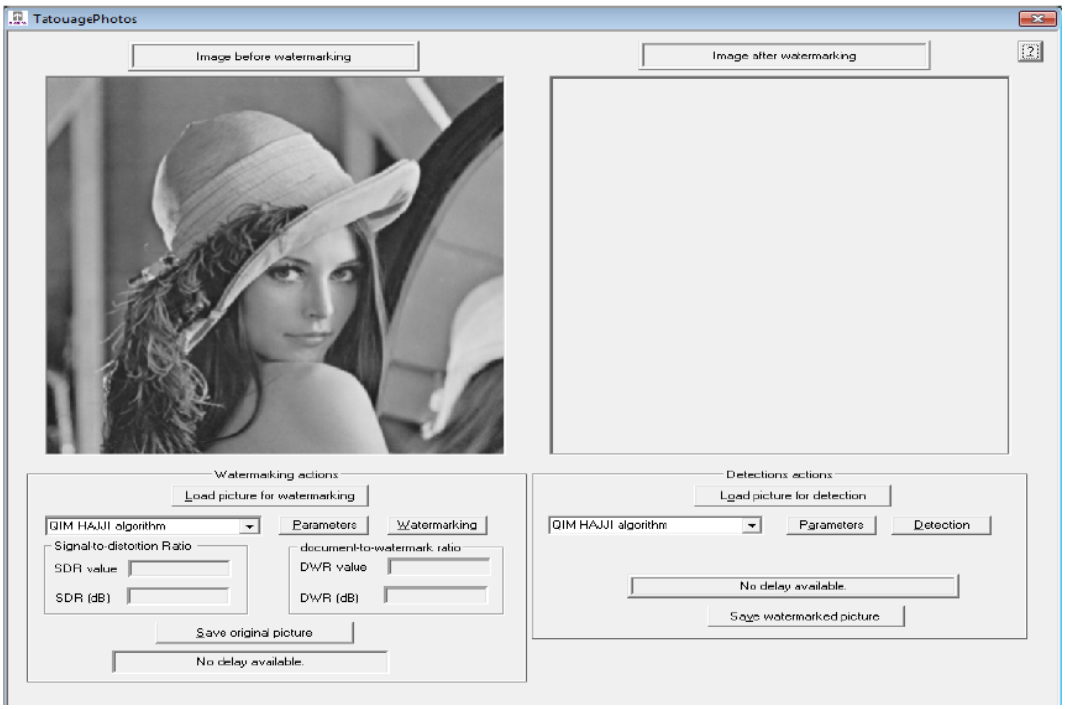



*Figure 5.2: L'interface de l'outil développé en C++.*

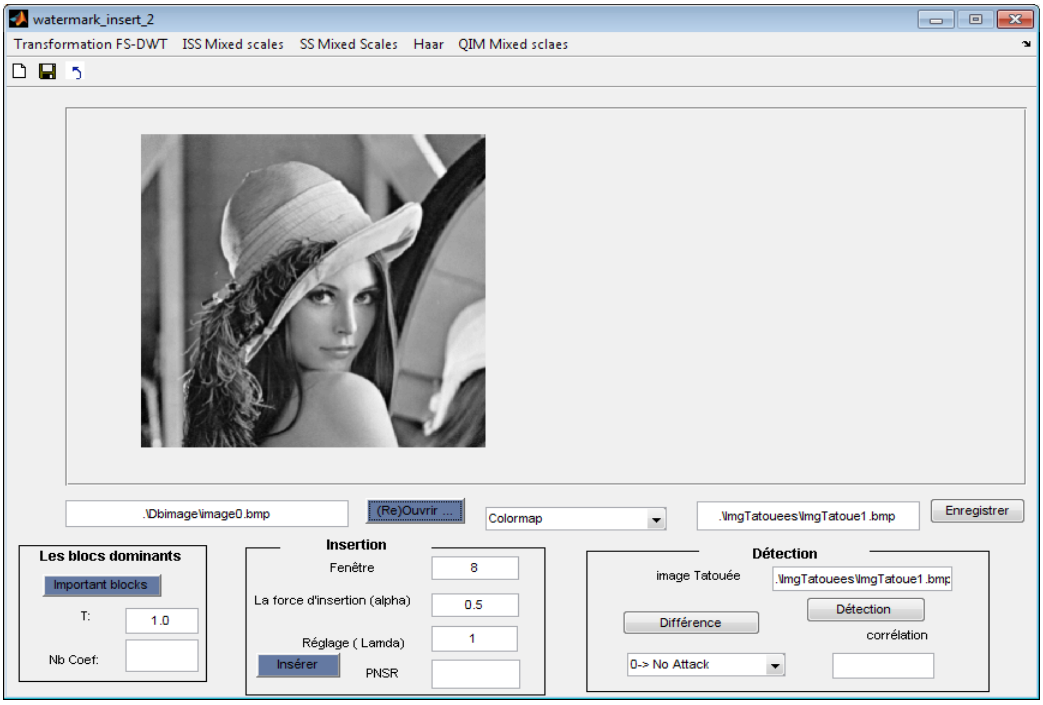



*Figure 5.3 : L'interface de l'outil développé en Matlab.*

# Bibliographie

[Bel94] M. Bellare, P. Rogaway: Optimal Asymetric Encryption – How to Encrypt with RSA, *Eurocryptn LNCS,* 94.

[Ben03] M. Benabdellah , S. Rerbal, N. Habibes, A. Meziane Tani, A. Nemmiche : Traitement numérique du signal physiologique :Application au débruitage et à l'analyse de l'ECG par Ondelettes, *CISTEMA*, 2003

[Ben95] W. Bender, D. Gruhl, N. Morimoto: Techniques for data hiding, *Dans Proceedings of the SPIE*, 1995.

[Boh09] A. Bohra, O. Farooq: Blind self-authentication of images for robust watermarking using integer wavelet transform. *AEU-International Journal of Electronics and Communication*, Vol. 63(8): pp. 703-707, 2009.

[Bou08] M. Bouchakour, G. Jeannic, and F. Autrusseau: JND mask adaptation for wavelet domain watermarking, *in Proceedings ICME*, pp. 201-204, 2008.

[Boy05] J P Boyer, P Duhamel, J Blanc-Talon : Tatouage Semi-Fragile et Théorie des Jeux : Etude d'un Système Basé sur le SCS, Compression et représentation des signaux Audiovisuels, *CORESA*, Renne, 2005.

[Bug98] S. Burgett, E. Koch, and J. Zhao: Copyright labelling of digitized image data. *IEEE Commun. Mag*, Vol. 36: pp 94–100, 1998.

[Bur97] C. S. BURRUS, R. A. GOPINATH et H. Guo : Introduction to Wavelets and Wavelet Transforms : *A Primer, Prentice Hall*, 1997.

[Car11] D. Caragata, A. L. Radu, S. El Assad: Fragile Watermarking using Chaotic Sequences, *International Journal for Information Security Research (IJISR)*, Vol. 1(1), March 2011

[Cha05] V. Chappelier : Codage progressif d'images par ondelettes orientées, *thèse de doctorant,* Université de Rennes 1, 2005.

[Che03] L. Chen and J. Lin. Mean Quantization Based Image Watermarking. Image Vision and Computing,Vol. 21(8) : pp. 717–727, 2003.

[Che05] V. Chen, M. Lounici et S. Ruan, Authentification de visages photographiques par tatouage d'images, *Colloque National de la Recherche Universitaire dans les IUT (CNRIUT'05)*, Rouen, France, mai 2005.

[Che07] C. Chen, X. Wu: An Angle QIM Watermarking Algorithm Based on Watson Perceptual Model, *Fourth International Conference on Image and Graphics (ICIG 2007)*, pp. 324-328, 2007.

[Chen01] B. Chen and G. W. Wornell: Quantization index modulation methods: A class of provably good methods for digital watermarking and information embedding, *IEEE Trans. Information Theory*, vol. 47(4): pp. 1423-1443, May 2001.

[Can05] C. Chang, A. Maleki, and B. Girod,: Adaptive Wavelet Transform for Image Compression via Directional Quincunx Lifting, " Proc. IEEE International Workshop on Multimedia Signal Processing, MMSP-05, Shanghai, China, November 2005

[Cox07] I J. Cox and M L. Miller and J. Bloom and J. Fridrich and Ton Kalker: Digital watermarking and steganography (second edition), M*organ Kaufmann*, 2007.

[Cox97] I.J. Cox, J. Killian, F.T. Leighton, T. Shamoon: Secure spread spectrum watermarking for multimedia. *IEEE Trans. Im. Proc.*, Vol. 6(12: pp. 1673–1687, 1997.

[Cox98] I. J. Cox, M.L. Miller, A. L. McKellips: Watermarking as communications with side information, *IEEE J. Selected Areas Communi*, Vol. 16(4): pp. 587-593, May 1998.

[Dar98] V. Darmstaedter, J.-F. Delaigle, J.J. Quistquater, B. Macq: Low Cost Spatial Watermarking, *Computer & Graphiccs*, vol. 22(4), pp. 417 – 424, 1998.

[Dau92] I. Daubechies: Ten Lectures on Wavelet, *Capital city press,* États-Unis, 1992.

[Del00] J. F Delaigle: Protection of Intellectual Property of Images by Perceptual Watermarking, *thèse de doctorant*, spécialité Sciences Appliquées, université catholique de Louvain, septembre 2000, p 233.

[Dif76] W. Diffie et M.E Hellman : New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol.22(6) : pp. 644-654, 1976.

[Dig10] Digimarc. Site internet de la société. 2010. *http://www.digimarc.com*, 2010.

[Dou01a] H. Douzi : Base d'ondelettes de Faber_Schauder et applications au traitement d'images, *thèse du doctorat*, 2001.

[Dou01b] H. Douzi, D.Mammass and F. Nouboud: Faber-Schauder Wavelet Transform, Application to Edge Detection and Image Characterization, *Journal of Mathematical Imaging and Vision*, Vol. 14(2): pp. 91-101, 2001.

[Dug98] R. Dugad, K. Ratakonda, N. Ahuja: A new wavelet-based scheme for watermarking images, *In IEEE ICIP*, Chicago, pp. 419–423.1998.

[DWA10] Site internet de Digital Watermarking Alliance 2010, *http://www.digital-watermarkingalliance.org/*.

[Egg03] J. J. Eggers, R. Bäuml, R. Tzschoppe, et B. Girod: Scalar costa scheme for information embeddin, *IEEE Transaction on Signal Processing*, Vol. 51(4): pp. 1003– 1019, Janvier 2003.

[Elb06] E. Elbasi and A. M. Eskicioglu: A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands, *EI*, 2006-6072-2.

[Esk95] A. Eskicioglu and P. Fisher: Image Quality Measures and their Performance, *IEEE Transaction on communication*, Vol. 43(12): pp.2959–2965, 1995.

[Fou01] W. Fourati, M.S. Bouhlel, L.Kamoun: Etude de la norme JPEG 2000 en vue de son implémentation, *1éres Journées Scientifiques des Jeunes Chercheurs*

*en Génie Electrique et Informatique (GEI'200l).* Sousse Nord, Tunisie, 2001.

[Fei73] H. FEISTEL: Cryptography and Computer Privacy, *Scientific American*, Vol. 228(5): pp. 15-23, 1973.

[FIPS10] SHA-1, Secure Hash Standard (SHS), *spécification, (FIPS 180-1)*, http://www.itl.nist.gov/fipspubs/fip180-1.htm, 2010.

[FIPS99] FIPS PUB 46-3, Data Encryption Standard (DES), *NIST* (1999).

[Flu09] J. Flusser, T. Suk ,B. Zitová: Moments and Moment Invariants in Pattern Recognition, *Wiley & Sons Ltd*., 2009.

[Fur05] B, Furht, E. Muharemagic, D. Socek: Multimedia Encryption and Watermarkin, *Springer*, 2005.

[Gan04] Emir Ganic and Ahmet M. Eskicioglu: Robust DWT-SVD domain image watermarking: embedding data in all frequencies, *ACM Special Interest Group on Multimedia,* pp.166-174, Magdeburg, Germany, 2004.

[Goa07] T.-G Gao, Q.-L Gu: Reversible watermarking algorithm based on wavelet lifting scheme, *International Conference on Wavelet Analysis and Pattern Recognition*, pp.1771-1775. 2007.

[Gol01] O. Goldreich: Foundations of Cryptography. *Cambridge University Press,* Weizmann Institute of Science, 2001.

[Gro03] David Gross-Amblard: Query-preserving watermarking of relational databases and XML documents, *In Proceedings of the Nineteenth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS)*, pp. 191-201, 2003.

[Hajji08] M. El hajji H. Douzi and R. Harba: Watermarking Based on the Density Coefficients of Faber-Schauder Wavelets, *In Proceedings of ICISP08, Lecture Notes in Computer Science (LNCS)*, Vol. 5099: pp455-462, 2008.

[Hajji11a] M. El Hajji, H. Douzi, R. Harba, F. Ros: Improved Spread Spectrum Watermarking Based on Wavelet Dominant Coefficients, *International Journal of Engineering and Industries (IJEI)*, Vol. 2(3): pp. 131-140, 2011.

[Hajji11b] M. El Hajji, H Ouaha, K Afdel, H.Douzi. Multiple Watermark for Authentication and Tamper Detection using Mixed scales DWT. *International Journal of Computer Applications (IJCA)*, Vol. 28(6): pp:34-38, August 2011.

[Hajji11c] M. El Hajji, D. Douzi, D. Mammass, R. Harba, A robust wavelet-based watermarking algorithm using mixed scales, p 1 - 5 , 7-9 April 2011 Print ISBN: 978-1-61284-730-6, International Conference on Multimedia Computing and Systems, (ICMCS), IEEE, 2011.

[He06] Ke-feng he, et al: Watermarking for images using the HVS and SVD in the wavelet domain, *Dans Proceedings of IEEE International Conference on Mechatronics and Automation*, pp.2352- 2356,2006.

[Hsi01] M. Hsieh, D. Tseng, Y. Huang: Hiding digital watermarks using multiresolution wavelet transform. *IEEE Transactions on Industrial Electronics*, Vol. 48(5): pp.875–882. 2001.

[Hu11] Y. Hu, Z. Wang, H. Liu, G. Guo: A Geometric Distortion Resilient Image Watermark Algorithm Based on DWT-DFT. *Journal Of Software*, Vol. 6(9): pp. 1805-1812. 2011.

[Hu62] M.K. Hu: Visual Pattern Recognition by moment invariants. *IRE Transaction on Information Theory*, Vol. 8(2) : pp. 179–187, 1962.

[Hua04] J. Huang, C. Yang: Image digital watermarking algorithm using multiresolution wavelet transform, *dans Proceedings of the IEEE International Conference on System*s, Man and Cybernetics, pp. 2977–2982, 2004.

[Kal99] T. KALKER, G. DEPOVERE, J. HAITSMA, M. MAES: A video Watermarking system for broadcast monitoring, *Proc. of SPIE, Security and Watermarking of Multimedia content*, vol. 3657: pp. 103-112, 1999.

[Kun97] D. KUNDUR, D. HATZINAKOS: A Robust Digital Image Watermarking Method using Wavelet-Based Fusion. *In IEEE International Conference on Image Processing*, vol. 1: pp. 544-547, Santa Barbara, États-Unis, 1997.

[Kat02] S. Katzenbeisser, H. Veith: Securing Symmetric Watermarking Schemes Against Protocol Attacks, *Proceedings of the SPIE*, Security and Watermarking of Multimedia Contents, vol. 4675(4): pp. 260-268, 2002.

[Kes10] A. Keskinarkaus, A. Pramila, T. Seppanen: Image watermarking with a directed periodic pattern to embed multibit messages resilient to print-scan and compound attacks, *Journal of Systems and Software,* Vol. 83(10): pp. 1715-1725, 2010.

[Kha06] Y. I. Khamlichi, M. Machkour, K. Afdel, A. Moudden: Multiple watermark for tamper detection in mammography image, *WSEAS Trans. on Computers*, Vol. 5(6): pp. 1222-1226, 2006.

[Khe05] F. Khelifi, A. Bouridane, F. Kurugollu et al: An improved wavelet-based image watermarking technique, *Dans Proceedings of the IEEE AVSS*, pp. 588–592. 2005.

[Kim99] R. J. Kim, Y. S. Moon: A robust wavelet-based digital watermarking using level-adaptive thresholding, *Dans Proceedings of the IEEE ICIP*, pp. 226–230. 1999.

[Koch98] E. Koch, S. Burgett, and J. Zhao: Copyright labeling of digitized image data, *IEEE Commun. Mag.*, pp. 94-100, Mar. 1998.

[Kuh82] F. P. Kuhl, C. R. Giardina: Elliptic fourier feature of a closed contour. In Computer Vision, *Graphics and Image Processing*, Vol. 18: pp. 236–258, 1982.

[Kut99] M. Kutter and F. Petitcolas: A Fair Benchmark For Image Watermarking Systems, *dans Electronic Imaging'99: Security and Watermarking of Multimedia Contents*, Vol. 3657: pp.226-239, 1999.

[Kwo01] S. G. Kwon, S. W. Ban, I.-S. Ha et al: Highly reliable digital watermarking using successive subband quantization and human visual system, *dans Proceedings of IEEE ISIE, Pusan*, pp. 205–209. 2001.

[Lef01] F. Lefèvre, D. Guéluy, D. Delannay, B. Macq: A Print and Scan Optimized Watermarking Scheme, *IEEE Multimedia Signal processing*, 2001.

[Li03] c. T. Li, D.C. Lou, J.L. Liu: Image integrity and Verification via Content-Based Watermarks and a Public Key Cryptosysytem, *Journal of Chinese Institue of Electrical enregineering*, Vol. 10: pp 99-106, 2003.

[Li06] E. Li, H. Liang, X. Niu: An integer wavelet based multiple logo watermarking scheme. *Dans Proceedings of the IEEE WCICA*, pp. 10256–10260. 2006.

[Li09] Lei-Da Li, Bao-Long Guo: Localized image watermarking in spatial domain resistant to geometric attacks, *AEU - IJE*, Vol. 63(2): pp. 123-131, 2009.

[Lin01a] C.-Y. Lin, M.Wu, J. Bloom, M. Miller, I. Cox, and Y.- M. Lui: Rotation, scale, and translation resilient public watermarking for images, *IEEE Transactions on Image Processing*, vol. 10(5): pp. 767–782, 2001.

[Lin01b] C Y. Lin, S. F. Chang: A robust image authentication method distinguishing JPEG compression from malicious manipulations. *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 11(2): pp. 153-168, 2001.

[Lin98] C. Y. Lin, S. F. Chang: A Watermark-Based Robust Image Authentication Using Wavelets, *ADVENT Project Report*, Columbia University, 1998.

[Linn98] J.P. Linnartz, M.V. Dijk: Analysis of the Sensitivity attack against Electronic Watermarks in Images, *Proceedings of 2nd Workshop on Information Hiding*, Portland, *Springer Verlag – LNCS*, avril 1998.

[Lu03] C. S. Lun, H. Y. M. Liao: Structural digital signature for image authentication: an incidental distortion resistant scheme, *IEEE Transactions on Multimedia*, Vol. 5(2): pp. 161-173, 2003.

[Lub95] J. Lubin: A visual discrimination model for imaging system design and evaluation, *Dans Vision Models for Target Detection and Recognition, ed. E. Peli, 245–283*, World Scientific Publishing, 1995.

[Mal03] H. Malvar and D. Florêncio: Improved spread spectrum: a new modulation technique for robust watermarking, *IEEE Transactions on Image Processing*, vol. 51: pp. 898–905, 2003.

[Mal97] S.G. Mallat: A wavelet tour of signal processing, *Academie Press,* 1997

[Man01] A. Manoury: Tatouage d'Images Numériques par Paquets d'Ondelettes, *thèse du doctorat*, 2001.

[Ngu03] P. Nguyen et S. Baudry : Le tatouage de données audiovisuelles, *Les Cahiers du numérique*, Vol. 4 : pp. 135-165, 2003.

[Ngu09] T. O. Nguyen: Localisation de symboles dans les documents graphiques. *Thèse de Doctorat, Université Nancy 2*, Décembre 2009.

[Nik01] N. Nikolaidis, S. Tsekeridou, A. Tefas, V. Solachidis, A. Nikolaidis, I. Pitas: A benchmarking protocol for watermarking methods, *Dans ICIP (3)*, pp. 1023-1026, 2001.

[Pan04] S. Pan, H.-C. Huang, and L. C. Jain: *Intelligent Watermarking Techniques, World Scientific Publishing Company*, Singapore, ISBN: 981-238-757-9, 2004.

[Pen93] W.B. Pennebakker, J.L. Mitchell: The JPEG Still Image Data Compression Standard. New York: Van Nostrand, 1993.

[Per99] S. Perreira, J. J. K. O Ruanaidh, F. Deguillaume, G. Csurka, T. Pun: Template Based Recovery of Fourier-Based Watermarks Using Log-polar

and Log-log Maps, *IEEE int. Conf on Multimedia Computing and Systems (ICSMS'99)*, Florence, Italy, June 1999.

[Pet98] F.Petitcolas, R. anderson, M. Kuhn: Attacks on copyritht Marking Systems, *Lecture Notes in computer Sciences (LNCS)*, Vol. 1525: pp. 219-239, 1998.

[Piv99] A. Piva, M. Barni, F. Bartoini, V. Cappellini, A. Lippi: A DWT-based technique for spatio-frequency masking of digital signatures, *Proc. IS&T/SPIE, conf. on security and watermarking of multimedia contents*, pp. 31-39, January 1999.

[Piva98] A. Piva, M. Barni, F. Bartolini: Copyright Protection of Digital Images by Means of Frequency Domain Watermarking, *in Mathematics of Data/Image Coding, Compression, and Encryption*, *Proceedings of SPIE*, Vol. 3456, pp. 25-35, San Diego, California, 1998.

[QLi07] Q Li, I J. Cox: Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking, *IEEE transactions on information forensics and security*, vol. 2 (2), june 2007.

[Qi04] X. Qi and J. Qi: Improved affine resistant watermarking by using robust templates, *Proceedings of the IEEE International Conference on Acoustics*, *Speech, and Signal Processing (ICASSP)*, vol. 3: pp. 405-408, 2004.

[Qua04] Liu Quan, AI Qingsong: A combination of DCT based and SVD based watermarking, *ICSP proceedings of IEEE International conference on signal processing*, pp. 873-876, 2004.

[Ras06] Rashmi Agarwal, M.S. Santhanam: Digital watermarking in the singular vector domain, arXiv:cs.MM/0603130 v1, 2006.

[Rey00] C. Rey, J.-L. Dugelay: Blind Detection of Malicious Alterations On Still Images Using Robust Watermarks, *IEEE Secure Images and Image Authentication colloquium*, London, UK, 2000.

[Rey01] C. Rey and J. Dugelay: Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images, *Traitement du Signal*, Vol. 18(4): pp. 283–295, 2001.

[Ros06] F. Ros, J. Borla, F. Leclerc, R. Harba, N. Launay : Watermarking for Plastic Card Supports, *9ème Conference Maghrébine sur Les Technologies de L'Information*, *MCSEAI*, Agadir 2006.

[Rua97] J. Ruanaidh, T. Pun: Rotation, scale and translation invariant digital image watermarking, *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, 1997.

[Sch06] D Schönfeld, A Winkler: Embedding with syndrome coding based on BCH codes, *Poceedings of the 8th ACM Workshop on Multimedia and Security*, pp. 214–223, 2006.

[Ser02] C. Serdean, M. Ambroze, M. Tomlinson G. Wade: Dwt based video watermarking for copyright protection invariant to geometrical attacks, *International Symposium on Communication Systems, Networks and Digital Signal Processing*, (Staffordshire University, UK), July 15-17 2002.

[Son99] M. Sonka, V. Hlavac, R. Boyle: Image Processing, Analysis and Machine Vision. *PWS Publishing, seconde edition*, 1999.

[Sol00] V. Solachidis, I Pitas: Self-similar ring shaped watermark embedding in 2-D DFT domain, *EUSIPCO 2000*, 5-8 September 2000.

[Sta03] T Stathaki,P Dafas: Digital Image Watermarking Using Block-Based Karhunen-Loeve Transform. *Proceedings of the 3rd International Symposium (ISPA),* Rome, Italy, pp. 1072–1075, September 18-20, 2003.

[Sti10] http://www.petitcolas.net/fabien/watermarking/stirmark, 2010.

[Suh03] Mohamed A. Suhail: Digital Watermarking-Based DCT and JPEG Model, *IEEE Transactions on Instrument and Measurements*, vol. 52(5), pp. 1640-1647, October 2003.

[Sun05] S.-F. Sun, Q. nad Chang: A secure and robust digital signature scheme for PEG2000 image authentication, *IEEE Transactions on Multimedia*, Vol. 7(3): pp. 480-494, 2005.

[Swe95] W. Sweldens: The Lifting Scheme: A new philosophy in orthogonal wavelet constructions, *in A. F. Laine and M. Unser, editors, Wavelet Applications in Signal and Image Processing III, Proc. SPIE*, vol. 2569: pp. 68-79, 1995.

[Swe98] W. Sweldens: The lifting scheme: A construction of second generation wavelets, *SIAM Journal on Mathematical Analysis*, vol. 29(2): pp. 511–546, 1998.

[Tea80] M.R. Teague: Image analysis via the General Theory of moments, *Applied optics*, vol. 19(8): pp. 1353-1356, 1980.

[Vin06] M. Vincent: Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique, *thèse de doctorat*, Toulouse, 2006.

[Vol01a] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun: Attack modelling: Towards a second generation watermarking benchmark. *Proc. Signal Processing*, vol.81: pp.1177–1214, 2001.

[Vol01b] S. Voloshynovskiy, F. Deguillaume, T. Pun: Multibit digital watermarking robust against local nonlinear geometrical distortions, *Proceedings of the IEEE International Conference on Image Processing (ICIP),* IEEE Computer Society Press, Los Alamitos, CA, pp. 999-1002, 2001.

[Wan00] Y. P. Wang, M. J. Chen, P. Y. Cheng: Robust image watermark with wavelet transform and spread spectrum techniques, *In Thirty-Fourth Asilomar Conference on Signals Systems and Computers*, pp. 1846–1850, Pacific Grove, 2000.

[Wan04] S. H. Wang, Y.P. Lin: Wavelet tree quantization for copyright protection watermarking, *IEEE Transactions on Image Processing*, Vol. 13(2), 154–165. 2004.

[Wan97] H. J. Wang, C. C. J. Huo: A multi-threshold wavelet coder (MTWC) for high fidelity image compression, *Proceedings of the IEEE ICIP*, Santa Barbara, pp. 652–655. 1997.

[Wan98] H. J. Wang, P. C. Su, C. C. J Kuo: Wavelet-based digital image watermarking. *Optics Express*, Vol. 3(12): pp. 491–496. 1998.

[Wat97] A. B. Watson and J. Solomon: Model of visual constrast gain control and pattern masking, *Journal of the Optical Society of America*, vol. 14, pp. 2379–2391, Sept. 1997.

[Wu07] X. Wu, Z-H. Guan, Z. Wu: A Chaos Based Robust Spatial Domain Watermarking, *Algorithm Advances in Neural Networks – ISNN 2007*, *Lecture Notes in Computer Science*, Vol. 4492: pp.113-119, 2007.

[Wil05] Wilfred Ng, Ho-Lam Lau: Effectives approaches for watermarking XML data, *Proceedings of the 10th International Conference on Database Systems for Advanced Applications, DASFAA'05*, *Lecture Notes in Computer Science*, vol. 3453: pp. 68–80, 2005.

[Wol96] R.B. Wolfgang, E. J. Delp: A watermark for digital images, *Proceedings of the 1996 International Conference on Image Processing*, Vol. 3, pp. 219-222, Lausanne, Switzerland, Sept. 1996.

[Wol97] M. Wolkenstein, H. Hutter, S. G. Nikolov: M. Grasserbauer: Improvement of signification by means of wavelet, denoising. *Fresenius Journal of Analytical Chemistry*, Vol. 357(7): pp.783-788, 1997.

[Wu07] G.D. Wu, P.H Huang: Image watermarking using structure based wavelet tree quantization. *In Proceedings ICIS*, Melbourne, Australia, pp. 315–319. 2007

[Wu11] C.H. Wu, Y. Zheng, W.H. Ip, C.Y. Chan, K.L. Yung, Z.M. Lu: A flexible H.264/AVC compressed video watermarking scheme using particle swarm optimization based dither modulation, *International Journal of Electronics and Communications*, Vol. 65(1): pp.27-36, 2011.

[Yav07] E. Yavuz, Z Telatar: Improved SVD-DWT based digital image watermarking against watermark ambiguity. *In Proceedings of the 2007 ACM symposium on Applied computing (SAC '07),* ACM, New York, NY, USA, pp. 1051-1055, 2007.

[You11] Youtube : Site web internet de la société. 2011, *http://www.youtube.com/t/contentid*.

[Zha04] G. Zhang, S. Wang,Q. Wen: An adaptive block-based blind watermarking algorithm, *In Proceedings of the IEEE ICSP*, pp. 2294–2297, 2004.

[Zha06] Z. Zhang, W. Huang, J. Zhang, H. Yu, and Y. Lu: Digital image watermark algorithm in the curvelet domain, *In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06)*, pp. 105–108, 2006.