

11621.738

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de 8 Mai 1945 – Guelma -
Faculté des Sciences et de la Technologie
Département d'Electronique et Télécommunications



Mémoire de Fin d'études
pour l'obtention du diplôme de Master académique

Domaine : Sciences et Techniques

Filière : Télécommunications

Spécialité : Systèmes de Télécommunications

DIGITAL WATERMARKING et Biométrie

Présenté par :

- ❖ COULIBALY Diahara
- ❖ DIABY Tidiani

Sous la direction de :

- ❖ TABA Mohamed Tahar

Juin 2012



Remerciements

Louange à Allah Le Tout Miséricordieux Le Très Miséricordieux de nous avoir donné, volonté, courage et la chance d'accomplir ce modeste travail.

C'est un devoir bien agréable que de venir rendre hommage, au terme de ce travail, à ceux sans lesquels il n'aurait pas pu être réalisé. Nous tenons tout particulièrement à exprimer notre profonde gratitude au **Dr Taba Mohamed Tahar** notre encadreur, pour ses conseils providentiels, son encadrement inébranlable et sa patience inépuisable.

Aussi l'occasion nous est offerte de remercier ici, les personnes qui nous feront l'honneur de participer au jury chargé de juger ce travail, tout le corps enseignant du département Electronique et Télécommunications, en particulier ceux qui nous ont accompagné tout au long de cette formation.

Nous ne manquerions pas de saluer nos amis et camarades qui dans une ambiance familiale ont rendu des moments si acariâtres en des moments tellement savoureux

Enfin nous saluons tous ceux qui de près ou de loin ont participé à l'accomplissement de ce travail.



3.1.2. Insertion de la marque.....	20
3.1.3. Détection de la marque	21
3.2. Étalement de spectre	22
3.2.1. Principe de l'étalement et de dés-étalement	22
3.2.2. Insertion de la marque.....	27
3.2.3. Détection de la marque	28
3.3. Transformation en Ondelettes discrète (DWT)	29
3.3.1. Développements mathématiques	31
3.3.2. Insertion de la marque.....	36
3.3.3. Détection de la marque	36
4. Conclusion.....	37

Chapitre 3 : Biométrie et watermarking

1. Introduction	38
2. Caractéristiques des systèmes Biométriques.....	38
3. Survol des systèmes de reconnaissance biométrique	40
3.1. Reconnaissance des empreintes digitales	40
3.2. Reconnaissance faciale	41
3.3. Reconnaissance de l'iris	41
3.4. Reconnaissance des doigts et de la main	42
4. Comparaison des systèmes de reconnaissance biométrique	43
5. Limites techniques des systèmes de reconnaissance biométrique	45
5.1. Fiabilité	45
5.2. Vulnérabilité	46
6. Coût et mise en œuvre	47
7. Les applications de la biométrie.....	47
8. Conception du système de reconnaissance des empreintes digitales.....	49
8.1. Extraction des caractéristiques.....	50
8.2. Estimation d'orientation	51
8.3. Assortiment des empreintes digitales.....	53
8.3.1. Assortiment basé sur la corrélation	54
8.3.2. Assortiment basé sur rides.....	54

Liste des figures

<i>Figure 4.3 : Le PSNR en fonction du niveau de bruit.....</i>	<i>63</i>
<i>Figure 4.4 : L'authentification en fonction du niveau de bruit.....</i>	<i>65</i>

Liste des tableaux

Tableau 3. 1 : comparaison des différentes technologies de reconnaissance biométrique44

Liste des abréviations

ATM: Asynchronous Transfer Mode

BPSK: Binary Phase Shift Keying

CD: Compact Disc

CDMA: Code Division Multiplexing Access

CWT: Continuous Wavelet Transform

DCT: Discrete Consinus Transform

DS-CDMA: Direct Sequence- Code Division Multiplexing Access

DVD: Digital Versatile Disc

DWT: Discrete Wavelet Transform

FBI: Federal Bureau of Investigation

FMR: False Match Rate

FNMR: False Non Match Rate

HVS: Human Visual System

LSB: Least Significant Bit

LPD: Low Probability Detection

MAW: Multiresolution Analysis Wavelet

PDA: Personal Digital Assistant

PN: Pseudo-Noise

PSNR: Peak Signal to Noise Ratio

QMF : Quadrature Mirror Filters

R-D: Recherche et Développement

RGB: Red Green Blue

SNR: Signal to Noise Ratio

STFT: Short Time Fourier Transform

WD: Wigner Distribution

WT: Wavelet Transform

Introduction Générale

La protection de la propriété intellectuelle est devenue récemment un besoin pressant surtout avec l'évolution rapide des techniques de transmission numérique. De nos jours presque tous les types de médias (images, sons, vidéos, etc.) sont stockés sous forme de données numériques, et leur libre accès pose de nombreux problèmes de droits d'auteur. Cela vient principalement du fait de la banalisation des connexions internet haut débit, et des graveurs de CD/DVD qui représente un manque à gagner et des préjudices importants pour les grandes industries de médias. Le tatouage numérique en anglais « digital watermarking » consiste à insérer, à l'intérieur d'un document numérique, une signature, une marque plus ou moins visible, contenant un code, robuste face à toute attaque susceptible de modifier la donnée tatouée.

Par exemple, la marque ajoutée pourrait être alors un simple copyright ou un numéro de licence. L'avantage ici se situe dans le fait qu'il serait non seulement invisible pour l'observateur, mais de plus indélébile et robuste face aux traitements classiques appliqués aux images comme le fenêtrage, le lissage, les transformations géométriques ou la compression avec pertes.

Le tatouage d'images est une technique qui est en fait directement issue d'un art appelé la stéganographie. Cet art n'a que pour ainsi dire qu'un but précis, qui est de cacher au sein d'un message primaire, un message secondaire. Bien entendu, il faut que le message primaire soit lisible par tout un chacun, et qu'il reste visuellement inchangé par rapport à ce qu'il était avant l'introduction du message secondaire. Ce dernier se doit d'être parfaitement invisible, mais uniquement accessible par des personnes propriétaires d'une information secrète, une "clef" par exemple qui permettrait son extraction.

A la différence de la cryptographie, l'objectif n'est pas de dissimuler des informations dans d'autres, mais plus simplement de rendre l'information que l'on désire transmettre complètement illisible à toute personne ne possédant pas la « clef » nécessaire à son décodage. De plus en cryptographie si le message primaire est modifié, il devrait être impossible de le recouvrer, tandis qu'en stéganographie, le message secondaire est supposé rester accessible et ce même après de multiples recopies et manipulations diverses du message primaire.

Introduction Générale

Le watermarking apparait donc comme l'une des solutions les plus convoitées pour la protection des enregistrements numériques (image, vidéo et audio) et est certainement un moyen efficace de résoudre ces problèmes. C'est la raison pour laquelle beaucoup se tournent vers cette technologie récente et sophistiquée.

Les applications de la dite technique étant nombreuses, le sujet de notre projet touchera seulement le watermarking des images pour une application en biométrie.

Ainsi le premier chapitre abordera les généralités sur le watermarking dans un but de voir le sujet dans sa globalité et se familiariser avec la terminologie utilisée.

Le second chapitre s'attaque aux différentes techniques de watermarking partant des développements mathématiques à leurs applications et permet d'élaborer les différences majeures entre celles-ci ;

Le troisième chapitre parlera en un premier temps des techniques de base de la biométrie entre autres de la reconnaissance faciale et surtout des empreintes digitales qui font l'objet d'une attention particulière dans notre travail, ensuite nous aborderons en un second lieu la conception d'un système de reconnaissance d'empreintes digitales pour en connaître les caractéristiques afin de permettre une application du watermarking aux empreintes.

Et enfin un dernier chapitre où nous ferons une simulation sous MATLAB d'un système de digital watermarking: ceci nous permettra de consolider les concepts théoriques par la pratique.

Chapitre 1

Généralités sur Digital Watermarking

1. Introduction

Il existe plusieurs méthodes pour sécuriser un document. La cryptologie est la science qui permet de protéger des données. Elle regroupe les deux méthodes existantes de protection de l'information : la Cryptographie et la Stéganographie. Ces deux méthodes diffèrent dans les algorithmes, les effets et aussi dans la durée de protection.

La cryptographie permet de protéger une information pendant sa transmission. Elle a pour effet de rendre le document illisible entre le moment de son codage et celui de son décodage. Le contrôle de ces opérations est rendu possible grâce à l'utilisation de clés. Seul le (ou les) propriétaire(s) du (ou des) clé(s) aura (auront) accès à l'information. Cette méthode est adaptée pour protéger le document pendant sa transmission, entre utilisateurs autorisés.

La stéganographie se définit comme l'art de cacher une information dans un support. Deux types d'approches sont envisageables. La première consiste à cacher l'information à protéger à l'intérieur d'un autre document. Le principe ressemble à celui de la cryptographie, mais la présence de l'information n'est ainsi pas révélée. En effet, l'information est insérée ou extraite du support à l'aide de codes contrôlés par des clés. La seconde méthode d'utilisation de la stéganographie est d'intégrer une signature dans le document traité. Cette partie est appelée Tatouage. La stéganographie se distingue de la cryptographie dans la mesure où l'objectif principal en cryptographie est de rendre illisible le message primaire à toute personne ne possédant pas une information secrète.

C'est dans ce domaine que nous nous placerons tout au long de ce document. Contrairement à un stockage simple d'informations dans l'en-tête du fichier associé à une image, le tatouage est intimement lié aux données. L'information dissimulée dans l'image hôte a pour but de démontrer l'intégrité du document ou encore d'en protéger les droits d'auteur. Les attaques sur un document tatoué sont bien différentes des attaques sur un document stéganographié. En effet, le pirate ne cherche pas à lire les informations, mais simplement à laver le document du tatouage.

L'objectif du tatouage est le suivant :

- le propriétaire d'une image originale souhaite défendre ces droits de propriétés ;
- pour ce faire, il introduit une marque (un identifiant) dans l'image ;
- l'image ainsi modifiée est ensuite diffusée ;

– à tout moment, le propriétaire souhaite pouvoir extraire son identifiant de l'image face à une tierce personne, et ce même si l'image marquée a été modifiée entre-temps en une image "proche".

Nous illustrons cela sur la figure suivante :

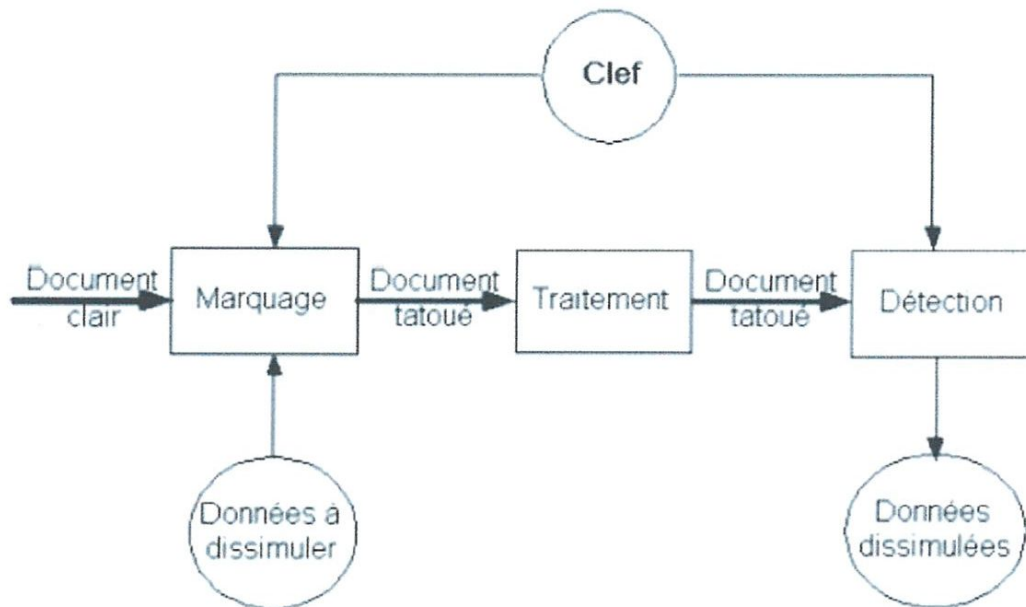


Figure 1.1: Objectif du tatouage

Le digital watermarking est considéré comme une solution efficace pour la protection de copyright des divers fichiers multimédias. Cette technique cache une certaine quantité d'information secrète dans la partie utile du fichier à protéger. Comparé avec la cryptographie, le tatouage numérique est capable de protéger les œuvres digitales après la phase de transmission et d'accès légal.

2. Définition

Le digital watermarking est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. Le message inclus dans le signal hôte, généralement appelé marque ou bien simplement message, est un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant du concepteur, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le signal hôte. Le nom de cette technique provient du marquage des documents papier et des billets.

3. Historique

Dans l'histoire de « Herodote » [2], D. Khan raconte que Histiaeus tatoua un message sur le crâne rasé d'un esclave et attendit que ses cheveux repoussent avant de l'envoyer à Aristagoras à Milet avec instruction de le raser une fois arrivé. Evidemment, les préoccupations n'étaient pas les mêmes que celles du Digital Watermarking mais les méthodes demeurent identiques par rapport à l'état de l'art.

Le digital watermarking est une discipline très récente, dont on fait remonter la naissance en 1990 avec l'article de Tanaka et al [10] sur une méthode pour cacher de l'information dans une image, ainsi qu'avec les articles de Caronni et Tirkel et al. en 1993[3].

Le terme digital watermark (tatouage numérique) fut pour la première fois employé en 1992 par Andrew Tirkel et Charles Osborne [3]. En fait, le terme utilisé par Tirkel et Osborne est originaire du Japon : « denshi sukashi » qui se traduit en anglais par electronic watermark.

4. Description et structure d'un système de Digital Watermarking

Chaque système de digital watermarking comprend au moins deux parties différentes: une unité d'intégration de watermark (filigrane) et une unité de détection et d'extraction de Watermark comme l'on peut constater sur la figure 1.2.

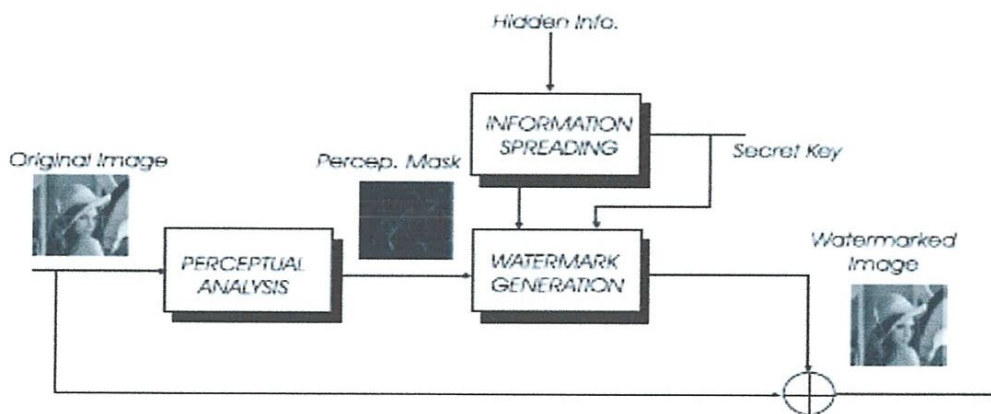


Figure 1.2 : Description d'un système de Digital Watermarking

L'image non marquée passe à travers un bloc d'analyse perceptuel qui détermine combien de pixels, peuvent être altéré afin que le résultat soit non-distinguable de l'image original. Il

prend en compte la sensibilité de l'œil humain à des changements dans les zones plates et sa tolérance relativement élevée à de petits changements aux bords.

5. Caractéristiques du digital watermarking

Plusieurs formes et degrés de watermarking existent. Ils sont généralement répertoriés par leurs degrés de priorités :

- visibles ou non visibles
- robustes ou fragiles
- Le ratio
- La complexité

5.1. Imperceptibilité

On exige normalement que l'image tatouée soit de façon perceptuelle semblable à l'image originale aussi que possible. Autrement, les déformations provoquées par le processus d'intégration du tatouage dégraderaient sa valeur esthétique. Cette propriété s'appelle l'imperceptibilité ou la transparence du système de watermarking. Un système de watermarking est très peu utile, s'il détruit l'image de couverture jusqu'au degré d'être inutile. Théoriquement, la marque devrait être invisible pour l'œil humain, même sur l'équipement de la plus haute qualité.

Pour maintenir l'imperceptibilité, des modèles soit de différences juste apparentes (JND), soit de système visuel humain (HVS : Human Visual System) sont appliqués pendant l'intégration de la marque. Le JND est la modification maximum admissible dans un signal tel que le signal modifié n'est pas distinguable par l'être humain. Le HVS spécifie que le système visuel des yeux humains a certaines caractéristiques. Les yeux sont moins sensibles aux changements faits à des régions en fortes textures comparées aux régions uniformes. Les régions texturisées ont des modèles complexes tandis qu'aux régions uniformes ils sont monotones. En utilisant HVS un plus grand poids de watermarking peut être employé dans une intégration additive pour les régions d'image qui ont des textures complexes comparées à ces régions aux textures simples.

Pour évaluer l'imperceptibilité, généralement, le rapport maximal de signal-bruit (PSNR) est employé.

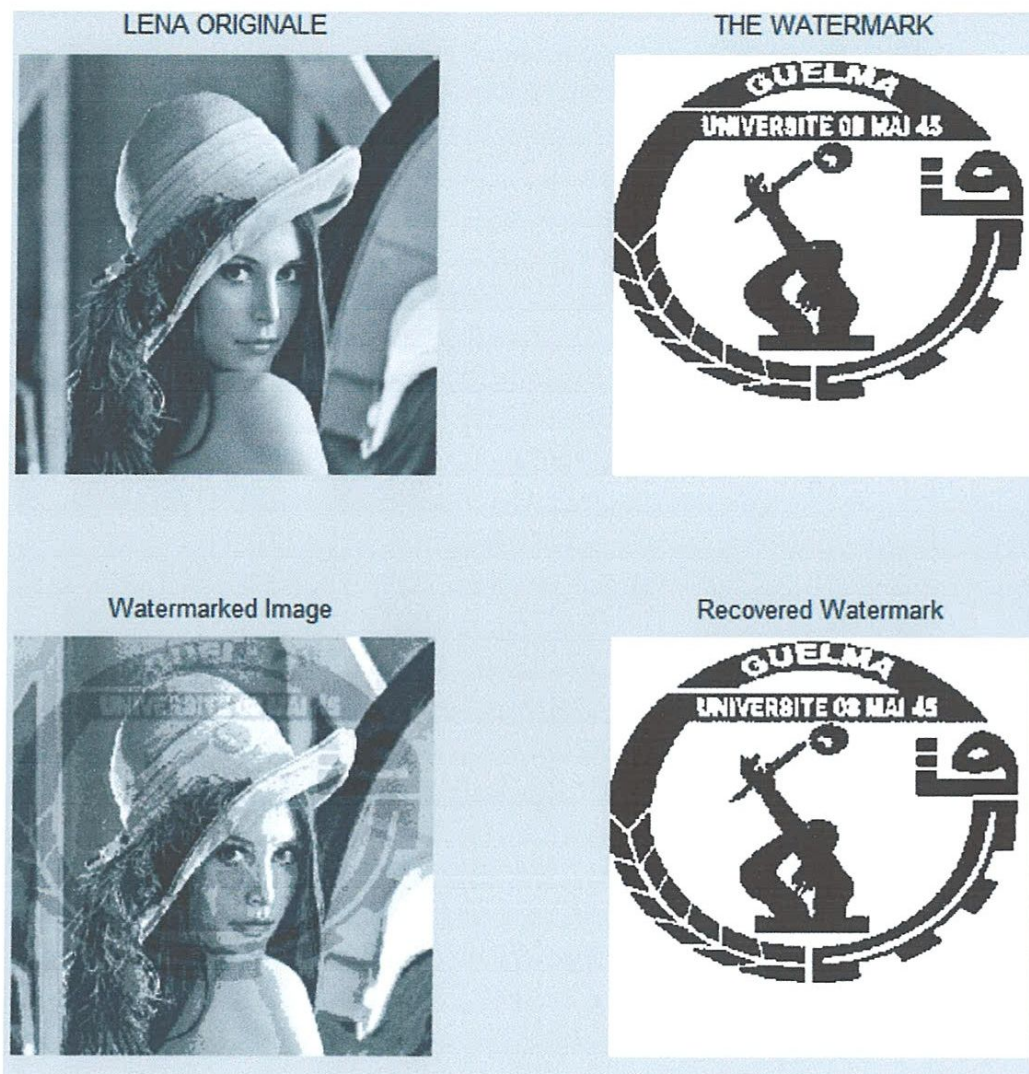


Figure 1.3 : Exemple de tatouage visible

5.2. Robustesse et fragilité

Le deuxième principal critère de qualité d'un algorithme de watermarking concerne sa robustesse face à des manipulations de l'image : celui-ci doit pouvoir conserver l'information stockée dans le marquage en dépit de diverses transformations.

Or très peu d'algorithmes résistent à une simple compression ou un changement de format, mais ils sont sensés résister tout de même à des attaques basiques telles que des translations ou des rotations de l'image (souvent utilisées pour la mise en page).

Il est néanmoins intéressant de remarquer qu'il peut être utile, dans certains cas, de favoriser une fragilité plutôt qu'une robustesse. Pour s'assurer par exemple de l'intégrité d'un document, le fait de le tatouer avec un algorithme fragile permettra, par la suite de vérifier si l'information marquée est toujours présente, ce qui sous-entend donc qu'elle n'a subi aucune

modification malveillante (par exemple, une modification brutale de certaine partie textuelle). Cela permet donc une certaine falsification de l'image.

A noter que :

- Pour le watermarking fragile : le message dépend du document donc toute modification de celui-ci implique une modification du dit message, il permet une vérification d'intégrité ;
- Pour le watermarking robuste : lequel doit résister à des attaques, il conserve l'origine du document, contrôle les copies...
 - Un cas intermédiaire : Les Semi-fragiles

Le watermarking semi-fragile combine à la fois les propriétés des marquages robuste et fragile. Comme les robustes, ils tolèrent certains changements de l'image, comme des rotations, translations ou addition de bruit. Et comme les watermarks fragiles, ils sont capables de déterminer les régions où l'image a été brutalement modifiée et celles où elle reste authentique. Par conséquent les watermarks semi-fragiles arrivent à différencier les changements "léger" comme l'ajout d'un bruit à des changements «destructeurs».

5.3. Le Ratio

Celui-ci constitue la quantité d'information que l'on peut rentrer dans une image. En pratique, de 16 à 64 bit suffisent pour assurer le système de copyright. Des données brutes volumineuses sont rarement cachées en tant que watermark (signifiant "filigrane" comme cité plus haut, donc quelque chose de relativement discret), mais plutôt des informations suffisamment détaillées pour permettre de récupérer une donnée via un autre moyen (tel des pointeurs vers une donnée extérieure à l'image). Il existe néanmoins certaines images qui s'auto-suffisent, ayant l'information brute stockée en tant que marquage. Ce genre de marquage s'applique surtout plus à une vidéo qu'à une image fixe.

5.4. Complexité

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

6. Les attaques

On distingue deux types d'attaques, celles passives et celles actives. Les premières visent simplement à déceler la présence d'un tatouage invisible caché dans l'image. Les secondes attaques cherchent à éliminer cette marque.

Ces deux attaques ont des buts différents. L'attaque passive s'applique davantage à la sténographie, on cherche à déterminer si une image contient un message ou pas.

L'attaque active est, en général, malveillante et vise à supprimer d'un média le tatouage (copyright, empreinte digitale) afin de pouvoir l'utiliser sans autorisation préalable de l'auteur par exemple.

Dans ce paragraphe, nous présentons différents types d'attaques classiques.

- Les traitements bienveillants ou innocents qui sont relatifs à de simples traitements de données.
- La compression : la compression provoque une perte de détails (composante haute fréquence de l'image). Dans ce cas, la marque doit posséder une composante basse fréquence conservée après le processus de compression.
- Le filtrage ou le lissage : les composantes hautes fréquences sont atténuées
- Transformations géométriques usuelles : le but est de pouvoir isoler une partie de l'image, de faire un agrandissement ou une réduction. Dans ces cas, nous observons une perte de synchronisation, c'est-à-dire de possibilité de localisation de la marque.
- Conversions numériques/analogiques
 - Les traitements malveillants qui peuvent avoir trois actions:
 - effacement de la signature,
 - désynchronisation de la signature,
 - utilisation des inconvénients liés à l'algorithme de marquage.

Nous résumons les différentes attaques sur la figure suivante :

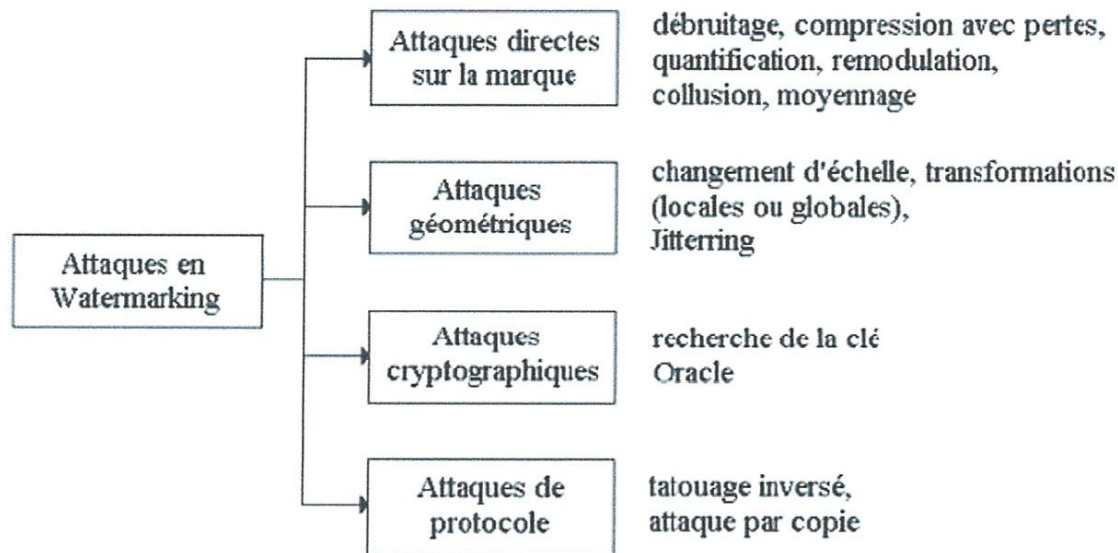


Figure 1.4 : Différents types d'attaque

7. Techniques de watermarking

Ces algorithmes se distinguent essentiellement par quatre points :

- La façon de sélectionner les différents points de l'image originale (ou blocs) qui contiendront les données du watermark.
- la manière de faire correspondre l'image hôte avec l'information à enfouir (relation binaire entre les bits par exemple). C'est ce que l'on appelle la modulation.
- Le prétraitement de l'information avant son enfouissement : pré-formatage ou encore redondance de l'information.
- Le choix du domaine de travail : spatial ou fréquentiel.

Concrètement, les algorithmes appartiennent à deux grandes familles : ceux opérant sur le domaine spatial, et ceux sur le domaine fréquentiel.

Nous analyseront d'une part des exemples de type d'algorithme travaillant sur le domaine spatial, en notant notamment leurs principaux avantages et défauts, puis nous parlerons des algorithmes opérant sur le domaine fréquentiel.

Les techniques purement spatiales résistent mal à certaines attaques comme le zoom et le recadrage, tandis que la plupart des techniques opérant dans le domaine des fréquences et le domaine mixte résistent bien à ce type d'attaques.

Les techniques purement spatiales résistent mal à certaines attaques comme le zoom et le recadrage, tandis que la plupart des techniques opérant dans le domaine des fréquences et le domaine mixte résistent bien à ce type d'attaques.

7.1. Domaine spatial

Le domaine spatial est le domaine classique où chaque valeur en (x,y) correspond à la valeur des pixels ; nous pouvons alors la visualiser dans un espace à 3 dimensions où les axes X et Y représentent les deux dimensions de l'image, et l'axe Z représente la valeur des pixels. Dans ce domaine on peut citer des techniques comme le bit de poids faible qui est la méthode la plus basique du "data embedding" et l'algorithme de Patch work ...

7.2. Domaine fréquentiel

Le domaine fréquentiel est un espace dans lequel l'image sera considérée comme une somme de fréquences de différentes amplitudes.

Les techniques utilisées dans ce domaine sont : La Discrete Cosine Transform (DCT), l'étalement de spectre et la Discrete Wavelet Transform (DWT).

8. Applications

Dans cette section nous discutons certains des scénarios là où le watermarking est déjà bien employé comme autres applications potentielles. La liste donnée ici est nullement complète et prévoit pour donner une perspective de la large gamme des possibilités d'affaire qu'offre le watermarking.

➤ Watermarking Vidéo

Dans ce cas-ci, la plupart des considérations faites dans les sections précédentes tiennent. Cependant, maintenant l'axe des temps peut être exploité pour augmenter la redondance de la marque. Comme dans le cas d'images immobiles, les watermarks peuvent être créés dans l'un ou l'autre des domaines spatial ou fréquentiel. Dans le dernier, les résultats peuvent être directement extrapolés aux séquences Mpeg-2.

➤ **Watermarking Audio**

Encore, les considérations précédentes sont valides. Dans ce cas-ci, les propriétés du marquage en temps et en fréquence de l'oreille humaine sont utilisées pour cacher le filigrane et le rendre inaudible.

La plus grande difficulté se situe dans la synchronisation de la marque et le fichier audio tatoué, mais des techniques qui surmontent ce problème ont été proposées.

➤ **Etiquetage**

Le message caché pourrait également contenir des étiquettes qui permettent par exemple d'annoter des images (ou audio). Naturellement, l'annotation peut également être incluse dans un fichier séparé, mais avec les résultats du watermarking, il est plus difficile de détruire ou de perdre cette étiquette, puisqu'elle devient étroitement liée à l'objet qui annote. Ceci est particulièrement utile dans les applications médicales puisqu'il empêche des erreurs dangereuses.

➤ **Empreinte digitale**

C'est semblable à la précédente application et permet l'acquisition d'appareils (comme les appareils-photo visuels, les enregistreurs audio, etc..) et d'insérer des informations sur l'appareil spécifique (par exemple, un numéro d'identification) et une date de création. Ceci peut également être fait avec des techniques numériques conventionnelles de signature mais avec le watermarking, il devient considérablement plus difficile d'enlever la signature. Quelques appareils-photo numériques utilisent déjà ce dispositif.

➤ **Authentification**

Dans le cadre d'application telle que l'authentification, le but est de détecter les modifications effectuées sur une donnée. Ce marquage est qualifié de "fragile". Il doit être résistant à des attaques classiques mais doit être détruit en cas de modification de la donnée. Dans ce cas, la marque peut être intégrée sur les objets principaux de la donnée. Si un de ces objets est modifié ou supprimé, la marque est alors détruite.

➤ **Contrôle de Copie et de playback**

Le message porté par la marque peut également contenir des informations concernant des permissions de copie et d'affichage. Puis, un module bloqué peut être ajouté dans la copie ou l'équipement de playback pour extraire automatiquement l'information de permission et une

transformation ultérieure de bloc s'il y a lieu. Afin d'être efficace, l'approche de cette protection exige des accords entre le contenu fournisseurs et fabricants d'électronique grand public pour introduire des détecteurs conformes de watermark dans leurs lecteurs et enregistreurs vidéo. Cette approche est utilisée pour le DVD (Digital Video Disc).

9. Conclusion

Ce chapitre nous a permis de mettre en évidence la composition de base d'un système de watermarking, il a aussi permis d'introduire le tatouage d'images à travers différentes notions associées à la problématique du tatouage. Nous avons analysé par exemple les notions d'invisibilité, de robustesse et de ratio qui sont des éléments fondamentaux pour la sécurisation de données multimédia. Plus généralement, les critères permettant de "quantifier" la qualité d'un tatouage sont précisés. Ensuite, nous décrivons quelques applications possibles de ce nouveau domaine de recherche.

Chapitre 2

Techniques de tatouage numérique

1. Introduction

Dans cette partie, nous cherchons tout d'abord à cerner chaque technique du côté mathématique pour par la suite faciliter la compréhension même de son utilisation en watermarking. Il s'agit à chaque fois de ressortir les problèmes, inconvénients et avantages de la technique en question.

La multiplicité des techniques est surtout liée à l'absence d'une technique efficace face toute forme d'attaque et ce en fonction de la donnée numérique à protéger. Cependant ces techniques sont en général répertoriées en deux catégories: les techniques opérant dans le domaine spatial et ceux opérant dans le domaine spectral ou fréquentiel.

2. Techniques dans le domaine spatial

2.1. Le bit de poids faible (LSB)

Il s'agit certainement de la méthode la plus basique du "data embedding". Par la définition de la valeur d'un pixel nous savons donc que pour les images en teinte de gris cette valeur varie de 1 à 255 correspondants à différents niveaux de gris (0 étant le Noir 255 le Blanc). Chaque pixel est donc codé sur 8 bits. Si nous considérons le fait qu'il est imperceptible pour l'œil humain, un changement, une variation d'une unité de gris, nous pouvons raisonnablement considérer que le dernier bit (bit de poids faible) n'est pas important, donc que nous pouvons le changer à notre guise.

C'est ce que nous faisons pour cacher par exemple une image binaire (noir et blanc) dans une image en nuance de gris, en ne reprenant simplement que le dernier bit de chaque pixel. Pour les images en couleurs, il suffit de travailler sur la luminance.

Cette méthode ne présente néanmoins aucun des critères abordés précédemment.

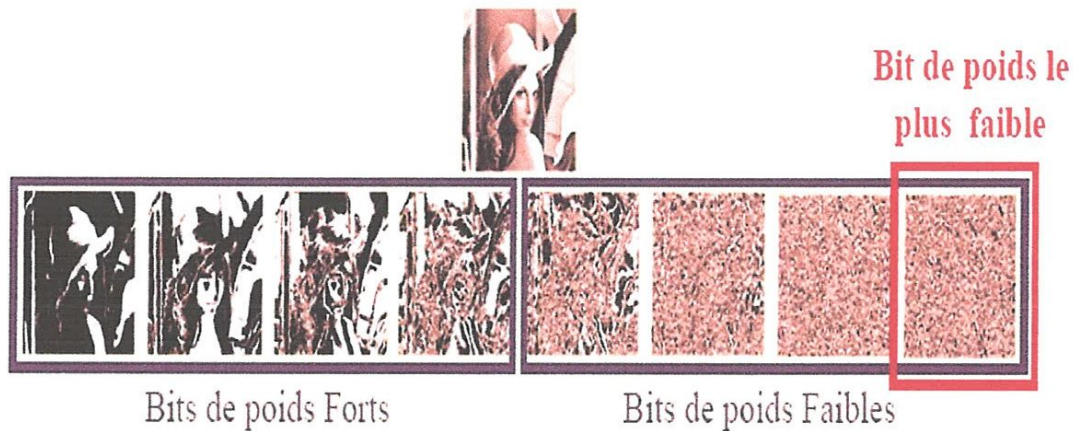
En général plusieurs méthodes sont proposées. L'une d'entre elles remplace d'abord le LSB de l'image par une séquence de bruit pseudo-aléatoire (PN), alors qu'une seconde ajoute une séquence de bruit pseudo-aléatoire (PN) au LSB des données. Et une autre méthode plus ancienne de watermarking obtient une somme des données d'image, puis inclut la somme dans

le LSB des Pixels aléatoirement choisis. Elles identifient la marque en employant la fonction spatiale d'auto-corrélation d'une séquence modifiée et la partie de l'image tatouée.

Il est très simple d'enlever ce marquage en mettant par exemple à 0 tous les bits de poids faible. De plus, tous les types de transformations fréquentielles, tels des filtres, sont radicaux pour ce marquage. Entre autres la compression JPEG ne lui laisse quasiment aucune chance.

Contrairement, à ce que l'on peut penser, l'œil humain est très sensible aux contrastes dans les gris de faibles intensités et beaucoup moins dans les teintes proche du blanc. Ainsi, certaines méthodes profitent de cela en adaptant le nombre de bits de poids faible à coder en fonction de la teinte en cours et de la teinte adjacente (tout en se référant à des données physiologiques sur les couleurs).

Avec cette technique il est possible d'enfuir tout un texte ou discours dans une image.



Exemple simplifié :

- Insérer un 'A' (en Binaire **01000001**, en Decimal 65)

Avant : 10000000, 00100100, 10110101, 00110101, 11110011, 10110111, 11100111, 10110011

Après : 10000000, 0010010**1**, 10110100, 00110100, 11110010, 10110110, 11100110, 10110011

Bit de poids
Le plus faible

Figure 2.1 : Technique du bit de poids

2.2. Algorithme de Patchwork

Pour renforcer un peu plus la robustesse de la méthode précédente, une idée basique, proposée par Bender & al en 1995 [19], consiste à répéter le même bit un grand nombre de fois pour qu'une étude statistique nous donne le bit marqué.

Toujours dans le domaine spatial, cette amélioration reste néanmoins relativement faible: il est très facile de vérifier qu'une image est marquée. En effet, bien que faisant partie des marquages "invisibles", une étude statistique des bits de poids faible nous renseigne sur l'existence du watermark.

3. Techniques dans le Domaine spectral

3.1. Transformée en Cosinus Discrète par Bloc 8x8 (DCT)

3.1.1. Développements mathématiques

Le passage par la DCT a été l'idée majeure pour la compression JPEG. En effet ce processus appartient à une classe d'opérations mathématiques, tout comme la Transformée de Fourier. Elle permet un changement de domaine d'étude, tout en gardant exactement la même fonction étudiée. Dans notre cas, on étudie une image, c'est à dire une fonction à 3 dimensions : X et Y, indiquant le pixel, et Z avec la valeur du pixel en ce point. Dans le cas d'une image couleur, il faut donc considérer indépendamment 3 fonctions, pour chacun des canaux RGB.

L'application de la DCT, ou d'une Transformée de Fourier fait passer l'information de l'image du domaine spatial en une représentation identique dans le domaine fréquentiel. Pourquoi ce changement de domaine est-il si intéressant? Justement parce qu'une image classique admet une grande continuité entre les valeurs des pixels. Les hautes fréquences étant réservées à des changements rapides d'intensité du pixel, ceux-ci sont en général minimales dans une image. Ainsi on parvient à représenter l'intégralité de l'information de l'image sur très peu de coefficients, correspondant à des fréquences plutôt basses. La composante continue (valeur moyenne de l'image traitée) ayant une grande importance pour l'œil.

La DCT s'applique à une matrice carrée. Le résultat fournit est représenté dans une matrice de même dimension. Les basses fréquences se trouvant en haut à gauche de la matrice, et les hautes fréquences en bas à droite.

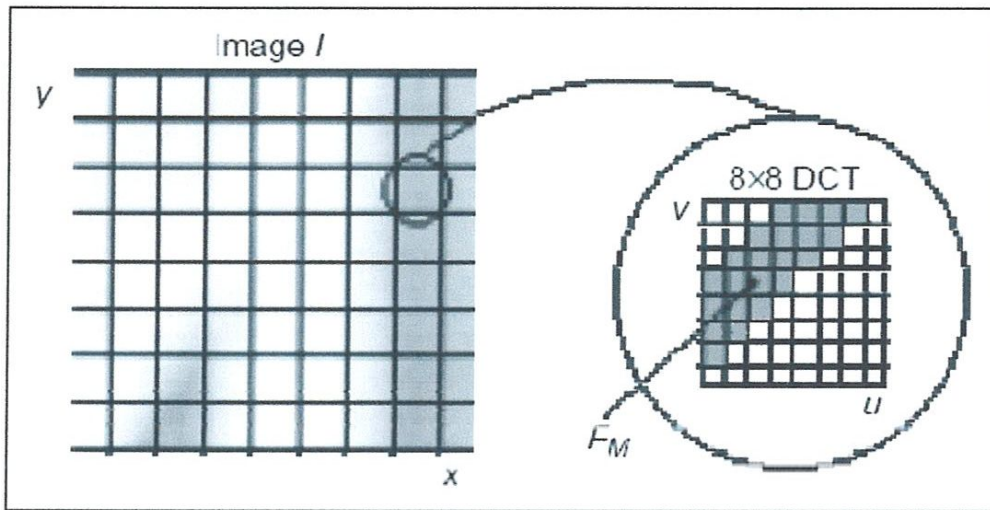


Figure 2.2 : Définition des bandes de fréquences moyennes dans un bloc de DCT.

La transformation matricielle DCT étant Orthogonale, elle s'accompagne d'une méthode d'inversion pour pouvoir revenir dans le domaine spatial. Ainsi après avoir fait des modifications dans le domaine fréquentiel, éliminer des variations de l'image quasiment invisibles par l'œil humain, on retourne à une représentation sous forme de pixels.

Formule pour calculer la DCT sur une matrice NxN

$$DCT(i,j) = \frac{1}{\sqrt{2}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel(x,y) \cos\left(\frac{(2x+1)i\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) \quad (2.1)$$

$$C(x) = \frac{1}{\sqrt{2}} \text{Si } x \text{ vaut } 0, \text{ et } 1 \text{ si } x > 0.$$

Formule pour calculer la IDCT sur une matrice NxN

$$pixel(x,y) = \frac{1}{\sqrt{2N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(i)C(j) DCT(i,j) \cos\left(\frac{(2x+1)i\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) \quad (2.2)$$

$$C(x) = \frac{1}{\sqrt{2}} \quad \text{Si } x \text{ vaut } 0, \text{ et } 1 \text{ si } x > 0.$$

➤ Avantage de la DCT

On a vu que la DCT était dans la même classe d'outils mathématiques que la Transformée de Fourier. Alors pourquoi les membres du groupe JPEG ont-ils fait le choix de la DCT? Ces deux méthodes permettent une décomposition de l'information dans une autre base : Une base de cosinus, ou la base de Fourier. Cependant, La décomposition dans la base de Fourier soulève plusieurs problèmes : si l'image présente des discontinuités, alors la décroissance des coefficients de la transformée de Fourier n'est qu'en $\frac{1}{K}$, K étant l'indice du coefficient.

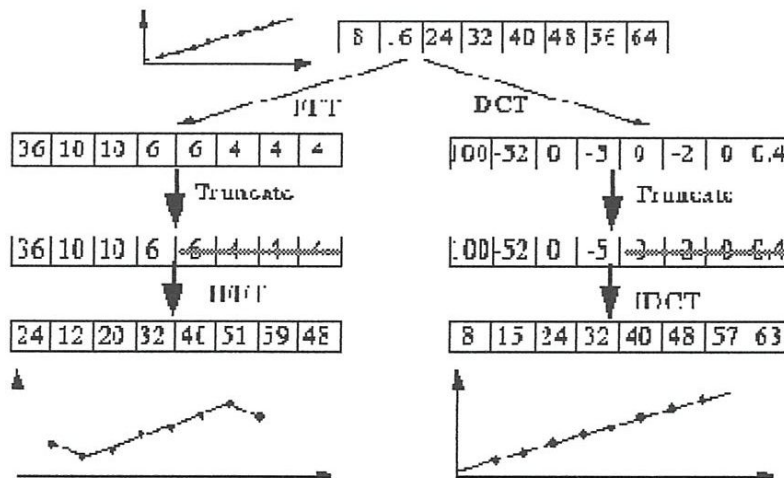


Figure 2.3: Décroissance des coefficients

Sur cette figure, on se rend compte que pour restituer convenablement l'information, on a besoin de beaucoup plus de coefficients que pour une DCT. La décroissance des coefficients n'étant pas suffisante pour pouvoir négliger rapidement les coefficients de grands indices. De plus en tronquant les derniers coefficients, on risque de voir se produire à la fin le phénomène de Gibbs, qui se traduit par une oscillation au niveau des discontinuités.

D'autre part, la fonction doit être périodique pour la transformée de Fourier, sinon on se retrouve avec une discontinuité au bord. Là encore se posera le phénomène de Gibbs qui risque fort de dégrader l'image.

Le fait de décomposer la fonction sur une base de cosinus fait que la fonction sera symétrique par rapport à $-\frac{1}{2}$. Cependant la DCT pose un problème d'optimisation. En effet le calcul d'un coefficient nécessite N^2 multiplications, or il y a N^2 coefficients à calculer. Le coût d'une telle décomposition devient alors démesuré si notre image est de taille 512x512. Ainsi, au lieu de traiter toute l'image, on découpe celle-ci en blocs 8x8. Ce choix représente un compromis performance qualité : en effet, en augmentant la taille de ces blocs, la compression serait meilleure, mais le coût en temps a été jugé trop grand. Sur chacun de ces blocs, on procède ensuite à une DCT.

Cela permet d'avoir un algorithme rapide. Cependant la DCT par blocs 8x8 est justement un des facteurs limitant de la compression JPEG : en effet lorsqu'on augmente la compression, on voit apparaître ces blocs.

3.1.2. Insertion de la marque

Soit $x[n] = x[n_1, n_2]$, $0 < n_1 < N_1$, $0 < n_2 < N_2$ une séquence bidirectionnelle discrète représentant la luminance d'une image échantillonnée de taille $N_1 \times N_2$ pixels. Dans la suite nous utiliserons toujours cette notation vectorielle pour représenter les séquences bidirectionnelles discrètes. Le watermark est généré comme un signal du domaine DCT $W[k]$ employant une technique similaire au système de modulation de l'étalement de spectre par séquence directe utilisé en communications. Ici nous supposons que la transformation DCT est appliquée en bloque de 8*8 pixels, comme dans l'algorithme de la compression jpeg. Nous permettrons au watermark de porter le message caché M avec une information qui pourrait être utilisée par exemple, pour identifier le destinataire prévu de l'image protégée. Ce message est généré par un encodeur dont le vecteur de codes est de dimension N , $b = (b_1, \dots, b_n)$. Donc une séquence bidirectionnelle $b[k]$ est générée dans ce que nous appelons un processus d'expansion, en répétant chaque élément b_i , $i \in \{1, \dots, N\}$ de mots de code dans un ensemble différent des points dans la grille du domaine DCT discret, de telle manière que toute l'image transformée soit totalement couverte.

Dans un but de sécurité, il est possible d'introduire une incertitude des coefficients DCT changés par chaque élément de mot de code en introduisant une étape d'imbrication, consistant en une clé dépendant d'une séquence aléatoire d'échantillons de $b[k]$.

Dans la suite nous dénoterons par S_i l'ensemble de coefficients de DCT liés aux coefficients b_i de mot code après l'étape d'intercalation. Le signal résultant est multiplié Pixel-par-Pixel

par le rendement $s[k]$ d'un générateur de séquences pseudo-aléatoire (P.R.S) avec un premier état qui dépend de la valeur de la clef secrète. En conclusion, le signal à spectre étalé est encore multiplié par ce que nous appelons un masque perceptuel $\alpha[k]$, qui est fondamentalement employé pour amplifier ou atténuer la marque à chaque coefficient de DCT de sorte que l'énergie de la marque est maximisée tandis que les changements subits par l'image sont maintenus invisibles. Le masque perceptuel $\alpha[k]$ est obtenu par une analyse perceptuelle de l'image originale $X[k]$, basé sur un modèle perceptuel dans lequel les propriétés du masquage de fréquence du HVS sont prises en considération. Le signal résultant est le watermark $W[k]$ et est ajouté à l'image originale $X[k]$ pour obtenir la version tatouée :

$$Y[k]=X[k] + W[k] \quad (2.3)$$

3.1.3. Détection de la marque

Maintenant analysons l'essai de détection du watermark, dans lequel nous devons décider si une image donnée contient une marque produite avec une certaine clef. Le problème de détection de la marque peut être mathématiquement formulé comme essai binaire d'hypothèse

$$H1 : Y[k]= X[k] + W[k]$$

$$H2 : Y[k]= X[k]$$

Où $X[k]$ est l'image originale, non disponible pendant l'essai,

$W[k]$ est un watermark produit de la clef secrète K qui est examinée. L'hypothèse $H1$ se résume à dire que l'image examinée en dessous contient une marque produite avec la clé K , et $H2$ se résume à dire qu'une marque produite avec K n'est pas présente dans $Y[k]$ (elle pourrait contenir, cependant, un tatouage produit avec une autre clef). Noter que ce n'est pas le but de la détection de marque d'examiner le message dans le watermark (s'il y a un tel message) et donc cette tâche est laissée à l'étape de décodage. Par conséquent, pendant la conception du détecteur nous devons prendre en compte l'incertitude de la valeur des mots de code du vecteur b . La règle de décision pour l'essai formulé ci-dessus est :

$$\Lambda(Y) > \eta \text{ pour } H1$$

$$\Lambda(Y) < \eta \text{ pour } H2$$

Où η est un seuil de décision et $\Lambda(Y)$ est la probabilité fonctionnelle

$$\Lambda(Y) = \frac{1}{L} \sum_{l=1}^L \frac{f(\frac{Y}{H1}, bl)}{f(\frac{Y}{H2})} \quad (2.4)$$

Dans la section suivante, nous dériverons l'expression pour ceci fonction de probabilité quand l'image originale est modélisé près une distribution gaussienne généralisée.

3.2.Étalement de spectre

L'étalement de spectre est un moyen de transmission dans lequel le signal occupe une largeur de bande au-dessus du minimum nécessaire pour envoyer l'information : la bande étalée est accomplie au moyen d'un code qui est indépendant de la donnée, et la réception synchronisée avec le code à la réception est employée pour le dé-étalement et donc de retrouver la donnée originale."

➤ Avantages

- Anti-interférence
- Camouflage de l'information
 - Interception délicate : Faible probabilité de l'interception
 - Décodage difficile si code inconnu
- Bonne résistance aux brouilleurs

Cette technique diminue le risque d'interférences avec d'autres signaux reçus tout en garantissant une certaine confidentialité. L'étalement de spectre utilise généralement une séquence ressemblant à du bruit pour étaler le signal de bande étroite en un signal large bande. Le récepteur régénère le signal original en corrélant le signal reçu avec une réplique de cette séquence. Deux motivations sont à l'origine de cette technique : en premier lieu, résister aux efforts ennemis pour brouiller le signal, puis cacher la communication elle-même.

Par ailleurs, l'étalement de spectre facilite les transmissions numériques dans les cas d'interférences par trajets multiples.

3.2.1. Principe de l'étalement et de dés-étalement

L'étalement de spectre (en anglais *Spread Spectrum*) est une technique par laquelle plusieurs utilisateurs peuvent être présents simultanément sur une même bande de fréquence.

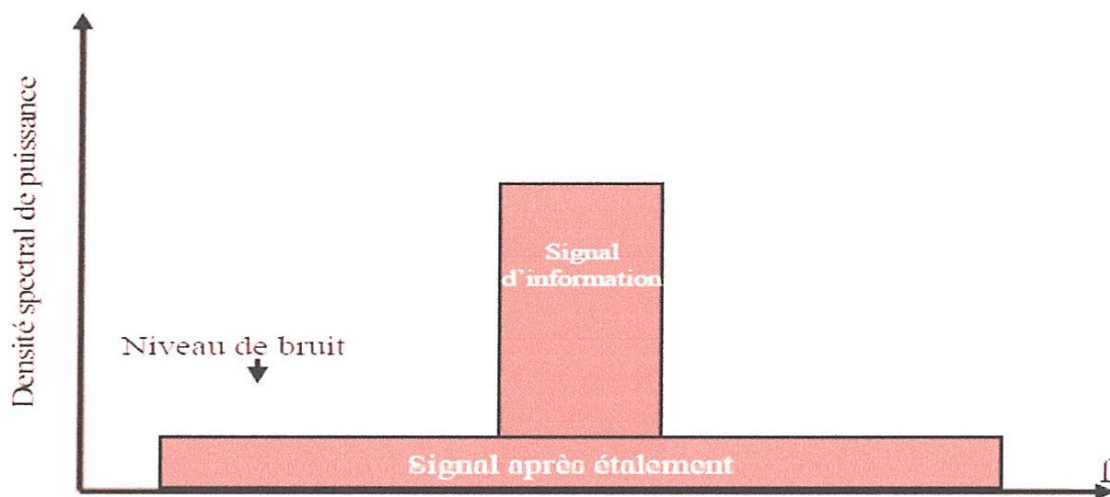


Figure 2.4 : Principe conceptuel de l'étalement de spectre

L'étalement de spectre peut être défini de la façon suivante : « L'étalement de spectre est une technique qui permet de transmettre un signal d'information sur une largeur de bande plusieurs fois supérieure à la largeur de bande minimale que le signal demande ». Pour cette raison, l'étalement de spectre est aussi considéré comme une forme de modulation. Dans un système à étalement de spectre, le signal transmis est « étalé » à partir d'un code indépendant du message d'information. Après s'être synchronisé avec l'émetteur, le récepteur doit utiliser ce même code pour « dé-étaler » le signal et pouvoir par la suite récupérer le message d'information.

Pour comprendre pourquoi l'étalement de spectre a eu tant de succès, il faut relire les travaux de Claude Shannon, qui a le premier formalisé ce concept.

Commençant par la célèbre expression qui détermine la capacité d'un canal :

$$C = B \log_2 (1 + (S/N)) \quad (2.5)$$

Où C est la capacité du canal en bits par seconde, B la largeur de bande du signal transmis en hertz, S la puissance du signal en watt, N la puissance du bruit en watt et \log_2 la fonction logarithme en base 2.

On voit sur l'expression précédente qu'il existe un rapport inverse entre la largeur de bande B (la bande occupée par le signal de transmission) et le rapport S/B (signal sur bruit) que l'on mesure à la réception. Plus précisément, on observe qu'un rapport signal sur bruit moins important est nécessaire pour conserver la même capacité de canal C si B augmente. C'est ainsi que l'on démontre les vertus de l'étalement de spectre : la largeur spectrale est accrue

afin d'obtenir de bonnes performances à la réception, le rapport signal à bruit étant réduit au minimum.

Le paramètre clé dans tout système d'accès radio à étalement de spectre est le gain de traitement. Ce dernier (que l'on notera G_p « *Processing Gain* ») est défini comme le rapport entre la largeur de bande occupée par un bit d'information après et avant étalement. Si l'on note « B_{inf} » la largeur de bande occupée par un bit d'information avant étalement et « B_{spr} » la largeur de bande du signal étalé, le gain de traitement satisfait :

$$G_p = \frac{B_{spr}}{B_{inf}} \quad (2.6)$$

La valeur de ce paramètre représente la capacité des systèmes d'accès radio à étalement de spectre à rejeter l'interférence. C'est-à-dire que plus « G_p » est grand plus le système résiste au bruit.

Dans la figure 2.4, on a volontairement inclus un signal de bruit présent sur une bande de fréquence assez large. Ce signal de bruit représente toutes les sources d'interférence et le bruit thermique. On observe sur la même figure que le signal étalé peut se retrouver noyé dans l'interférence au point qu'il donne l'illusion d'en faire partie. Un facteur essentiel qui explique le succès de l'étalement de spectre dans le domaine militaire est que sans la connaissance du code d'étalement, il est quasiment impossible de détecter le signal transmis et de récupérer le message d'information qu'on convoie. Cette propriété est appelée « faible probabilité de détection » (*LPD, Low Probability of Detection*).

De plus, le signal étalé résiste fort bien aux interférences qui occupent une largeur spectrale beaucoup plus étroite. Il faut préciser que l'on parle ici d'une source ponctuelle d'interférence qui ne serait présente que sur une bande étroite.

Cette robustesse provient tout simplement du fait que l'information est étalée sur une bande de fréquence assez importante et profite d'une certaine forme de diversité en fréquence : seule une partie du spectre du signal utile étalé est perturbée.

De plus dans ce système, la propriété de traiter des trajets multiples augmente le gain de traitement.

En effet, dans un canal à trajets multiples, plusieurs copies du signal transmis arrivent au récepteur à des instants différents. Un système à étalement de spectre présente une robustesse naturelle vis-à-vis des effets négatifs causés par les trajets multiples sur le signal.

La Figure 2.5 décrit le fonctionnement de base de l'étalement et du dés-étalement d'un système DS-CDMA.

On a pris pour exemple, un signal initial BPSK (Binary Phase Shift Keying) de fréquence R . Ce signal est donc composé d'une séquence de bits pouvant prendre les deux valeurs suivantes : «+1» et «-1 ». La méthode d'étalement consiste, dans cet exemple, à multiplier chaque bit du signal initial par une séquence de huit bits, chacun de ces huit bits étant appelé chip. Dans ce cas on a utilisé un facteur d'étalement de 8. On remarque que le signal final à l'apparence d'un signal aléatoire tout comme le code d'étalement utilisé. Ce signal large bande sera ensuite transmis sur l'interface air.

En ce qui concerne la procédure inverse, le dés-étalement, nous multiplions, bit par bit, le signal étalé par la même séquence de codes que nous avons utilisée précédemment pour l'étalement. Comme le montre la Figure 2.4, on a retrouvé exactement le signal initial et cette opération n'introduit aucun déphasage entre le signal initial et le signal final. La multiplication de la fréquence du signal par facteur 8 engendre un étalement similaire du spectre occupé par le signal résultant. Le dés-étalement permet de restaurer la bande passante initiale, proportionnelle à la fréquence R du signal.

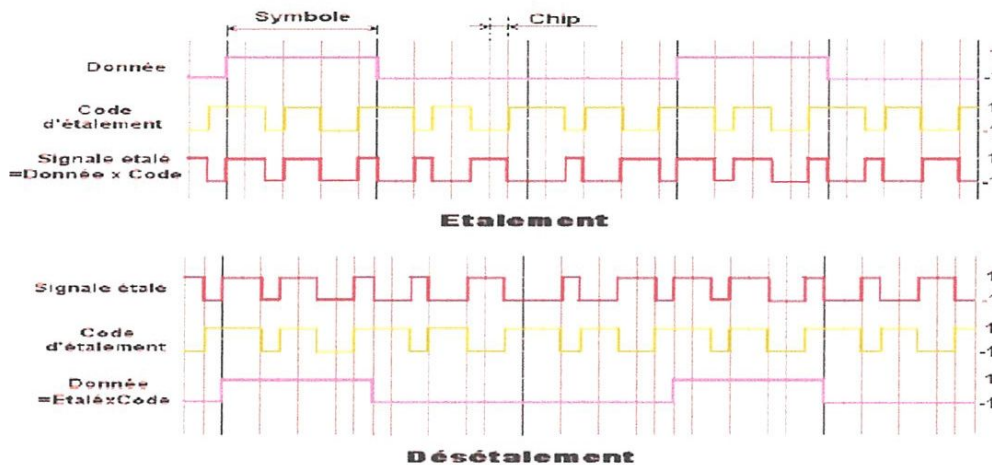


Figure 2.5: Etalement et dés étalement en DS-SS-SSS

Le fonctionnement de base d'un récepteur à corrélation en CDMA est présenté dans la Figure 2.5.

La partie supérieure de la figure montre la réception du signal attendu, c'est-à-dire le signal qui correspond au code d'étalement utilisé. Comme précédemment dans la Figure 4 nous remarquons l'étalement parfaitement synchronisé réalisé par le code. Ensuite, le récepteur intègre ou plus précisément somme le produit des bits du signal reçu par ceux du code d'étalement, cela par symbole.

La partie inférieure de la figure 2.4 montre l'effet du dés-étalement quand il est appliqué au signal d'un autre utilisateur pour lequel l'étalement a été effectué avec une autre séquence d'étalement. Le résultat de la multiplication du mauvais signal par le code d'étalement puis son intégration par le récepteur donne une suite des valeurs proches de 0.

Comme nous pouvons le remarquer, l'amplitude du signal attendu est augmentée en moyenne par facteur 8 par rapport aux autres signaux qui interfèrent. Cette méthode de détection par corrélation permet donc d'amplifier le signal attendu d'un coefficient égal au facteur d'étalement, ici 8. Cet effet est appelé gain de traitement (*processing gain*). C'est un des aspects fondamentaux de tous les systèmes CDMA et des autres systèmes à étalement de spectre. Ce gain de traitement donne une certaine robustesse aux systèmes CDMA face aux interférences qui sont générées par la réutilisation des mêmes porteuses sur des stations de base proches les unes des autres.

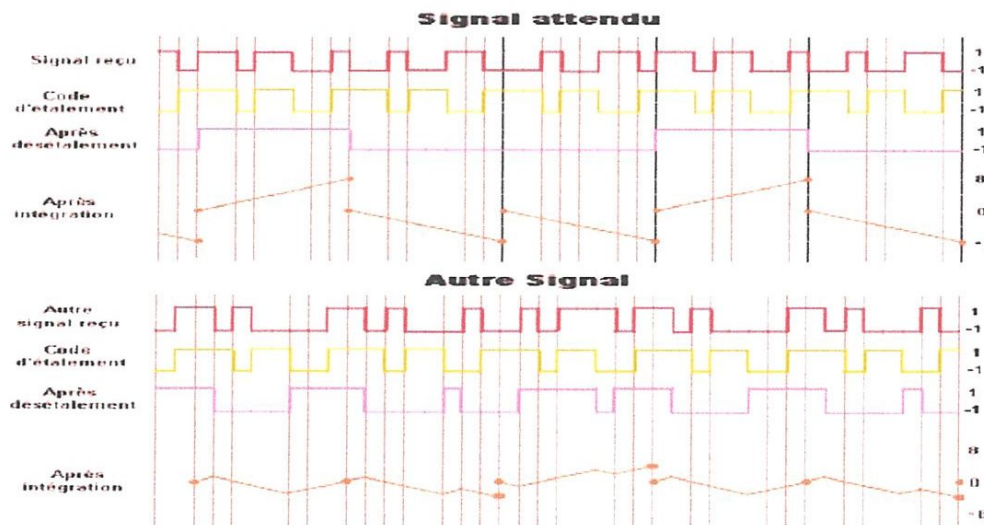


Figure 2.6 : Principe de corrélation du récepteur en CDMA

Remarque

Parmi les propriétés de l'étalement de spectre citées ci-dessus, une en particulier (le camouflage de l'information) va nous amener à l'utiliser dans notre étude (watermarking).

3.2.2. Insertion de la marque

Notre but est d'insérer une signature binaire $B = \{b_0, \dots, b_N\}$ d'une longueur de N bits dans une image I . Pour le moment nous ne considérons que les images comportant 256 niveaux de

gris différents. Le tatouage w est défini par une superposition linéaire de N fonctions bidimensionnelles $p_i(x,y)$, chacune représentant un bit :

$$w(x,y) = \sum_{i=1}^N p_i(x,y) \quad (2.7)$$

L'image tatouée I' est générée en ajoutant le tatouage w à l'image :

$$I'(x,y) = I(x,y) + w(x,y) \quad (2.8)$$

Les fonctions bidimensionnelles p_i sont définies par :

$$p_i(x,y) = b_i \alpha(x,y) \phi_i(x,y) \quad (2.9)$$

Où b_i définit la valeur du bit i projetée de $\{0,1\}$ à $\{-1,1\}$, et $\phi_i(x,y)$ est une fonction de modulation bidimensionnelle pseudo-aléatoire. $\alpha(x,y)$ est une fonction de pondération ayant pour but d'adapter le tatouage numérique à l'image de telle sorte que l'énergie du tatouage soit maximisée sous la contrainte que la qualité de l'image tatouée ne soit pas inférieure à un certain seuil.

Les fonctions de modulation ϕ_i sont orthogonales, c'est-à-dire :

$$\langle \phi_i, \phi_j \rangle = \delta_{ij} \|\phi_i\|^2 \quad (2.10)$$

Où $\langle ., . \rangle$ est le produit scalaire, δ_{ij} la fonction Delta de Kronecker, et $\|\cdot\|^2$ représente l'énergie de la fonction de modulation.

Il y a plusieurs moyens de générer ces fonctions de modulation. Dans les applications de tatouages numériques, il est important d'avoir un contrôle maximal sur les artefacts. En principe, les fonctions de modulation sont définies de sorte que l'intersection des ensembles de positions (x,y) ayant une valeur $\phi_i(x,y) \neq 0$ soit vide. Cette technique nous assure que chaque valeur de l'image originale est modifiée par une fonction seulement. Les fonctions sont générées en utilisant des ensembles de positions S_i dépendant d'une clé k . Comme mentionné précédemment, l'intersection des ensembles doit être nulle, c'est-à-dire $S_i \cap S_j = \emptyset$, $\forall i \neq j$. Les fonctions de modulation peuvent donc être définies ainsi :

$$\phi_i(x,y) = \begin{cases} s_i(x,y) & \text{si } (x,y) \in S_i \\ 0 & \text{ailleurs.} \end{cases} \quad (2.11)$$

Dans notre cas, les fonctions S_i sont des fonctions pseudo-aléatoires avec une distribution bimodale de $\{-1,1\}$, mais d'autres distributions sont aussi possibles.

Pour avoir un contrôle maximal sur les artefacts, nous introduisons la densité D qui définit la fraction des pixels de l'image qui sont modifiés par le processus de tatouage numérique. Cette densité D est donnée par :

$$D = \frac{|\{U_{i=1}^N S_i\}|}{|\{S\}|} \quad (2.12)$$

Où $|\{.\}|$ est le cardinal de l'ensemble et $\{S\}$ l'ensemble universel. La probabilité de distribution des positions dans l'image est uniforme, ce qui veut dire que la probabilité d'une position de faire partie de l'ensemble S_i est $\frac{D}{N}$

Comme déjà remarqué par plusieurs auteurs, cette méthode de tatouage numérique peut être considérée comme une modulation par étalement de spectre [14].

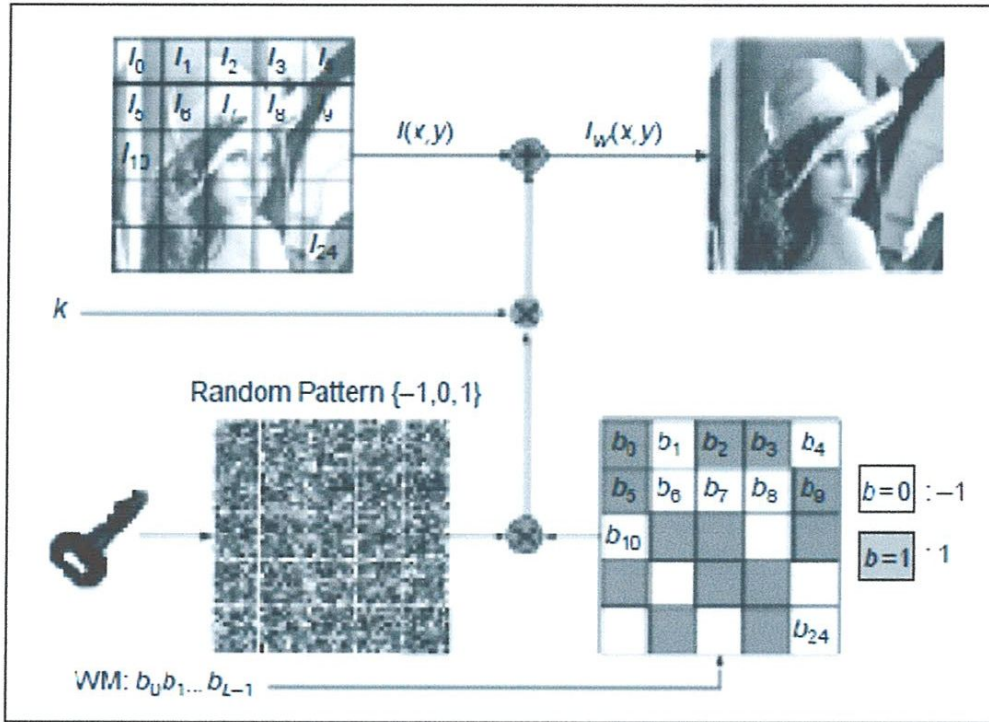


Figure 2.7 : Procédure d'insertion du watermark (technique de l'étalement de spectre)

3.2.3. Détection de la marque

Pour démoduler l'information insérée dans l'image, on utilise un corrélateur linéaire qui calcule la corrélation entre l'image tatouée et la fonction de modulation. Suite au fait que les propriétés statistiques de l'image ne sont pas stationnaires, et que l'espérance n'est pas égale à zéro, nous proposons un processus de traitement préalable de l'image. Ce processus a pour but de diminuer la variance de l'image, résultant en une augmentation de la performance du système. La statistique du détecteur est donnée par :

$$r_i = \langle \epsilon(I'), \phi_i \rangle \quad (2.13)$$

Où ϵ est la fonction de traitement préalable de l'image, et I' l'image tatouée. Dans notre cas, le processus de traitement préalable est une convolution avec un filtre non-adaptatif qui calcule une prédiction du tatouage inséré. Le filtre H_+^w d'une taille de w est définie par :

$$H_+^w : h_+(x,y) = \begin{cases} -\frac{1}{2w-2} & \text{si } x = 0 \text{ et } 0 < |y| \leq \frac{w-1}{2} \\ -\frac{1}{2w-2} & \text{si } y = 0 \text{ et } 0 < |x| \leq \frac{w-1}{2} \\ 1 & \text{si } x = 0 \text{ et } y = 0 \\ 0 & \text{ailleurs} \end{cases} \quad (2.14)$$

En utilisant ce filtre, qui a la forme d'une croix, la statistique de détection peut être exprimée ainsi :

$$\begin{aligned} r_i &= \langle I' * H_+^w, \phi_i \rangle \\ &= \langle (I + w) * H_+^w, \phi_i \rangle \\ &= \langle w * H_+^w, \phi_i \rangle + \langle I * H_+^w, \phi_i \rangle \end{aligned} \quad (2.15)$$

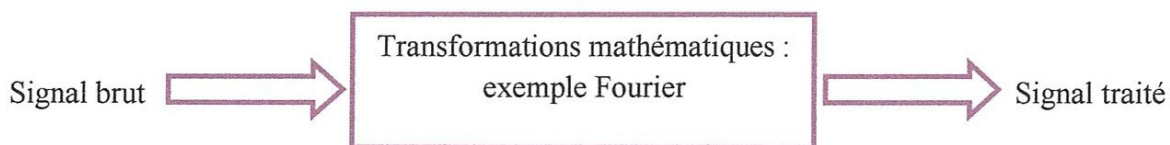
La valeur d'un bit caché est maintenant trouvée en observant le signe de la statistique de détection :

$$\tilde{b}_i = \begin{cases} 1 & \text{si } r_i \geq 0 \\ 0 & \text{si } r_i < 0 \end{cases} \quad (2.16)$$

Cette approche, basée sur le filtre de prédiction présente ci-dessus, peut être améliorée en utilisant des filtres plus performants et adaptatifs, tels les filtres de Wiener.

3.3. Transformation en Ondelettes discrète (DWT)

Les transformations mathématiques sont appliquées aux signaux bruts pour obtenir davantage d'informations qui sont disponibles dans ces signaux.



En pratique, la plupart des signaux, sous leur format brut, sont représentés dans le domaine temporel. La représentation du signal est une représentation temps - amplitude.

Cette représentation n'est pas toujours la meilleure pour toutes les applications en traitement du signal. Dans beaucoup de cas, l'information la plus pertinente est cachée dans la

composante de fréquence du signal. Souvent, l'information qui ne peut pas être distinguée dans le domaine temporel pourrait être facilement visible dans le domaine fréquentiel.

Le spectre de fréquence d'un signal est constitué par les composantes de fréquence de ce signal.

C'est la transformation de Fourier qui nous permet de mesurer la fréquence, de trouver le contenu en fréquences du signal.

Si on effectue la TF d'un signal représenté dans le domaine temporel, on obtient la représentation fréquence– amplitude de ce signal.

La transformation de Fourier est une transformation réversible entre le signal brut et le signal traité (transformé). Cependant, seulement l'un des deux est disponible à un instant donné. Aucune information de fréquence n'est disponible dans le domaine temporel et aucune information temporelle n'est disponible fréquentiel du signal. Ceci n'est pas un inconvénient pour analyser des signaux dont la structure n'évolue pas ou peu (statistiquement stationnaires), mais devient un problème pour l'étude de signaux non stationnaires.

De tels signaux nécessitent la mise en place d'une analyse temps-fréquence qui permettra une localisation des périodicités dans le temps et indiquera donc si la période varie d'une façon continue, si elle disparaît puis réapparaît par la suite, etc.

Pour une telle analyse, nous avons le choix parmi les méthodes suivantes :

- la Transformée de Fourier fenêtrée (Short Time Fourier Transform (STFT)),
- la Distribution de Wigner (Wigner Distribution(WD)),
- la Transformée en Ondelettes (Wavelet Transform(WT)).

Dans le cas de la Transformée de Fourier fenêtrée, le choix de la fonction de fenêtre est malheureusement liée à l'application et trouver une bonne fonction de fenêtre pourrait être bien difficile !

Ceci a pour conséquence une perte de résolution.

Une fenêtre étroite donne une bonne résolution temporelle, mauvaise résolution fréquentielle

Une fenêtre large donne une bonne résolution fréquentielle, mauvaise résolution temporelle.

Et donc pour pallier à cet inconvénient (Éliminer, dans une certaine mesure, le dilemme de la résolution) la solution est l'utilisation des ondelettes.

Une ondelette est une petite onde (ou vague) qui a un début et une fin. On utilise les ondelettes pour représenter une fonction (ou un signal) comme une somme pondérée de ces petites ondes translatées ou dilatées.

3.3.1. Développements mathématiques

L'analyse des ondelettes décrite dans l'introduction est connue comme la transformation en ondelettes continue ou cwt.

Plus formellement on lui écrit comme :

$$\gamma(s, \tau) = \int f(t) \Psi_{s,\tau}^*(t) dt \quad (2.18)$$

Où * dénote la conjugaison complexe. Cette équation montre comment une fonction $f(t)$ est décomposée en un ensemble de fonctions de base $\Psi_{s,\tau}(t)$, appelées ondelettes. Les variables s et t sont les nouvelles dimensions, la fréquence et le temps, après la transformation en ondelette. Pour compléter l'équation (2.19) de Sake donne la transformation inverse.

$$f(t) = \iint \gamma(s, \tau) \Psi_{s,\tau}(t) d\tau ds \quad (2.19)$$

Les ondelettes sont produites d'une ondelette de base simple $\Psi_{s,\tau}(t)$, le prétendu ondelette mère, par dilatation et la translation :

$$\Psi_{s,\tau}(t) = \frac{1}{\sqrt{s}} \Psi\left(\frac{t-\tau}{s}\right) \quad (2.20)$$

Dans (2.20) s est le facteur de dilation, τ est le facteur de translation et le facteur $s^{-1/2}$ est pour la normalisation d'énergie à travers les différentes dilatations.

Il est important de noter qu'en (2.18), (2.19) et (2.20) les fonctions d'ondelette mère ne sont pas spécifiées. C'est la différence entre la transformation en ondelette et la transformée de Fourier, ou toute autre transformation. La théorie de la transformation en ondelette opère avec les propriétés générales des ondelettes et de la transformation en ondelette seulement. Il définit un encadrement dont l'un peut concevoir des ondelettes au goût et aux souhaits.

- Il existe de nombreuses ondelettes mères possibles.

Ainsi définie c'est une transformation continue à rapprocher de la transformation de Fourier continue.

La transformation en ondelette est une transformation linéaire.

Il existe trois sortes de transformée en ondelettes : la CWT, la DWT et les transformations en ondelettes basées sur l'analyse multi- résolution (MAW).

La différence principale entre les deux (DWT et CWT) est que la CWT fonctionne sur toutes les valeurs continues de la fréquence et du temps tandis que la DWT fonctionne sur un sous-ensemble spécifique défini sur l'ensemble de toutes les valeurs discrètes de la fréquence et du

temps. La DWT permet d'adapter cette transformation dans le domaine des ondelettes au monde des ordinateurs (valeurs discrètes).

Bien que la transformée en ondelettes continues discrétisées permette le calcul de la CWT par des ordinateurs, elle n'est pas une vraie transformée discrète.

En fait, la série d'ondelette est simplement une version échantillonnée de la CWT, et les informations qu'elle fournit sont fortement redondantes en ce qui concerne la reconstruction du signal. Cette redondance, d'autre part, exige une quantité significative de temps et de ressources de calcul. D'où le besoin de la DWT.

➤ Calcul de la DWT

La DWT analyse le signal à différentes bandes de fréquence avec différentes résolutions en décomposant le signal par une approximation grossière et une information détaillée. La DWT utilise deux ensembles de fonctions, appelés fonctions d'étalement (scaling functions) et des fonctions d'ondelette (wavelet functions), qui sont associées à des filtres passe bas et passe haut, respectivement. La décomposition du signal en différentes bandes de fréquence est simplement obtenue par les filtrages successifs passe haut et passe bas d'un signal définie dans le domaine temporel. Le signal original $x[n]$ est d'abord passé par un filtre passe haut demi-bande $g[n]$ et un filtre passe bas $h[n]$.

Après le filtrage, on peut éliminer la moitié des échantillons selon la règle du Nyquist, puisque le signal a maintenant la fréquence la plus élevée de $\pi/2$ radian au lieu de π . Le signal peut donc être sous échantillonné par 2, en enlevant simplement un échantillon sur deux.

Ceci constitue un niveau de décomposition et peut être exprimé comme suit :

$$y_{haut}[k] = \sum x[n] \cdot g[2k - n] \quad (2.21)$$

$$y_{bas}[k] = \sum x[n] \cdot h[2k - n] \quad (2.22)$$

Cette décomposition divise en deux la résolution de temps puisque seulement la moitié du nombre d'échantillons caractérise maintenant le signal entier. Cependant, cette opération double la résolution de fréquence, puisque la bande de fréquence du signal enjambe maintenant seulement la moitié de la bande de fréquence précédente, réduisant effectivement l'incertitude dans la fréquence par moitié. Le procédé ci-dessus, qui est également connu comme codage de sous bande (subband coding), peut être répété pour davantage de décomposition. À chaque niveau, le filtrage et le sous-échantillonnage auront comme conséquence d'obtenir la moitié du nombre d'échantillons (et par conséquent la moitié de la

résolution temporelle) et la moitié de la bande de fréquence enjambée (et par conséquent la double la résolution fréquentielle).

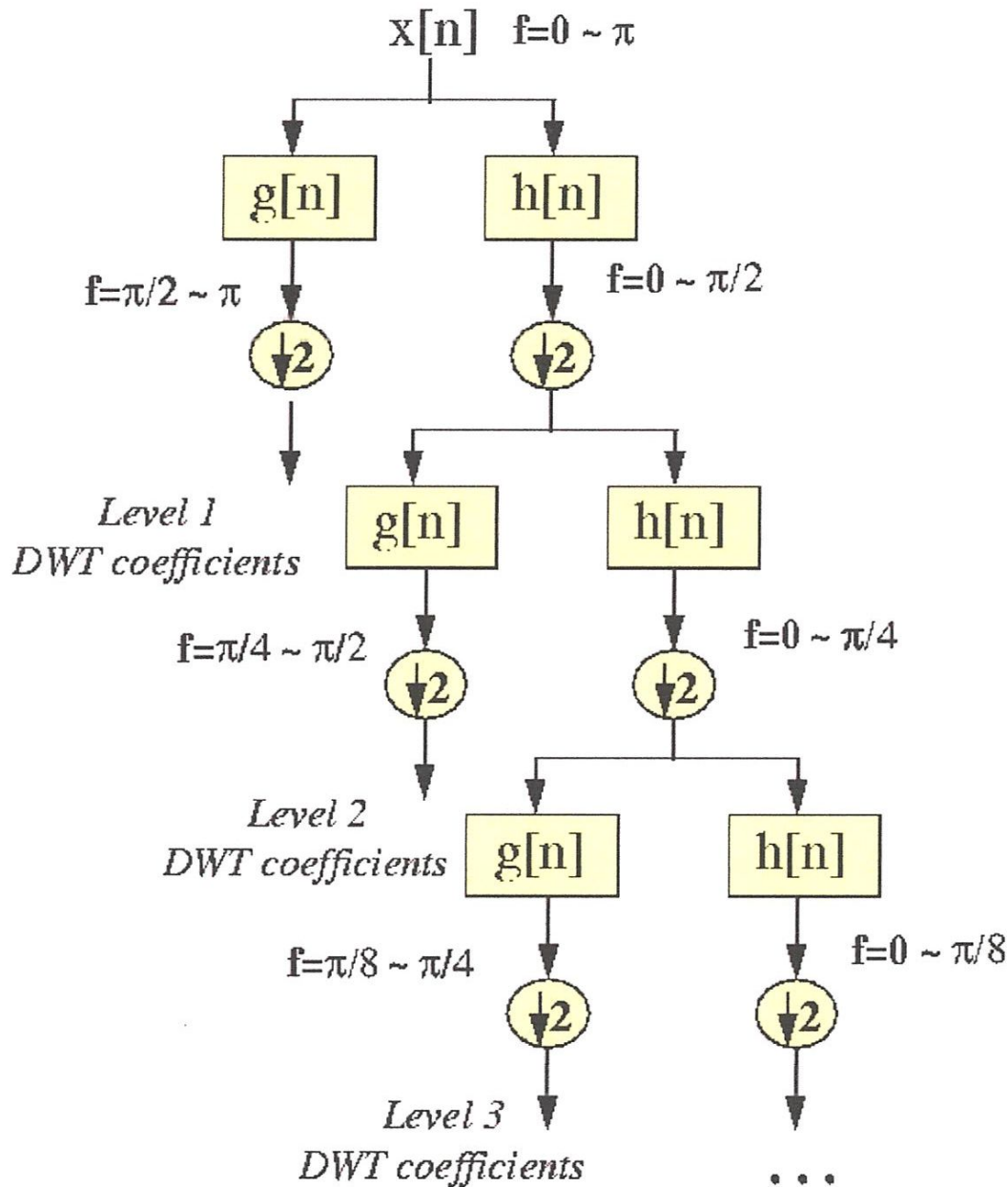


Figure 2.8 : Décomposition du signal par filtrages successifs

La figure ci-dessus illustre ce procédé, où $x[n]$ est le signal original à être décomposé, $h[n]$ et $g[n]$ sont les filtres passe bas et passe haut, respectivement. La largeur de la bande du signal à chaque niveau est marquée sur la figure en tant que "f".

Notez que dû au sous-échantillonnage successifs par 2, la longueur de signal doit être une puissance de 2, ou au moins un multiple de la puissance de 2, pour que cette procédure soit

efficace. La longueur du signal détermine le nombre de niveaux en lesquels on peut décomposer le signal. Pour cet exemple spécifique il y aurait 8 niveaux de décomposition. Chaque niveau de décomposition ayant la moitié du nombre d'échantillons du niveau précédent.

Le processus de décomposition continue jusqu'à ce que deux échantillons soient laissés. La DWT du signal original est alors obtenu en concaténant tous les coefficients à partir du dernier niveau de la décomposition (deux échantillons restants, dans ce cas-ci). La DWT aura alors le même nombre de coefficients que le signal original.

Les fréquences qui sont les plus importantes dans le signal d'origine apparaîtront en tant qu'amplitudes élevées dans la région du signal de la DWT qui inclut ces fréquences particulières. La différence de cette transformée avec la transformée de Fourier est que la localisation dans le temps de ces fréquences ne sera pas perdue. Cependant, la localisation dans le temps aura une résolution qui dépend de quel niveau elle apparaît. Si l'information principale du signal se situe dans les hautes fréquences, c'est qui est le cas le plus fréquent, la localisation dans le temps de ces fréquences sera plus précise, puisqu'elles sont caractérisées par plus de nombre d'échantillons.

Si l'information principale se trouve seulement aux fréquences très basses, la localisation dans le temps ne sera pas très précise, puisque peu d'échantillons sont employés pour exprimer le signal à ces fréquences. Cette procédure offre en effet une bonne résolution dans le temps aux hautes fréquences, et une bonne résolution de fréquence aux basses fréquences. Beaucoup de signaux produits en pratiques sont de ce type.

Les bandes de fréquence qui ne sont pas très importantes dans le signal d'origine auront des amplitudes très basses, et ainsi ses parties dans le signal DWT peuvent être négligées sans subir une perte importante d'information. Ceci permet ainsi la réduction de données.

Une propriété importante de la DWT est le rapport entre les réponses impulsionnelles des filtres passe haut et passe bas. Ces filtres ne sont pas indépendants l'un de l'autre, et ils sont liés par :

$$g[L-1-n] = (-1)^n h[n] \quad (2.24)$$

où $g[n]$ est le filtre passe haut, le $h[n]$ est le filtre passe bas, et L est la longueur de filtre (en nombre des points). Notons que les deux filtres sont d'indice impair de versions en alternance inversée les unes des autres.

La conversion de passe bas au passe haut est fourni par le terme $(-1)^n$.

Des filtres satisfaisant cette condition sont généralement utilisés dans le traitement des signaux, et ils sont connus comme filtre miroir en quadrature « Quadrature Mirror Filters (QMF) ». Les deux opérations de filtrage et de sous-échantillonnage peuvent être exprimées en (2.21) et (2.22).

La reconstruction dans ce cas est très facile puisque les filtres de demi-band forment des bases orthonormées. La procédure précédente est suivie dans un ordre renversé pour la reconstruction.

Les signaux à chaque niveau sont sur-échantillonné par deux, passés par les filtres $g'[n]$, et $h'[n]$ (passe haut et passe bas respectivement) et ensuite additionnés. Le point intéressant ici est que les filtres d'analyse et de synthèse sont identiques, sauf pour une inversion dans le temps. Par conséquent, la formule de reconstruction devient (pour chaque niveau) :

$$x[n] = \sum (y_{haut}[k] \cdot g[-n+2k]) + (y_{bas}[k] \cdot h[-n+2k]) \quad (2.25)$$

Cependant, si les filtres ne sont pas demi-band parfaits, alors une reconstruction parfaite ne peut pas être réalisée. Bien qu'il ne soit pas possible de réaliser des filtres parfaits, dans certaines conditions il est possible de trouver des filtres qui fournissent la reconstruction parfaite. Les plus célèbres sont ceux développés par Ingrid Daubechie appelés ondelettes de Daubechies (Daubechie's wavelets).

3.3.2. Insertion de la marque

La représentation des ondelettes de l'image transformée en 4 niveaux est montrée dans la figure 2.9.

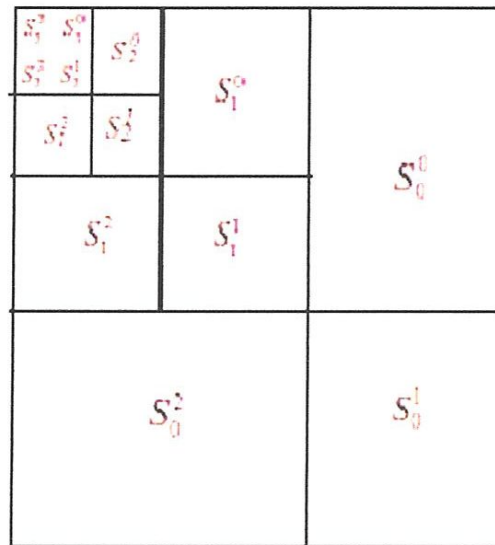


Figure 2.9 : Décomposition de 4 niveaux d'une image en ondelette

Représentons chaque sous-bande avec $S_l^\theta(i, j)$ où $\theta \in \{LL, LH, HL, HH\}$ représente l'orientation et $l \in \{0, 1, 2, 3\}$ donne le niveau de résolution de la sous-bande de l'image de la taille $I \times J$. Soit $x(m, n)$ représentant le watermark de taille $M \times N$. L'algorithme pour inclure le logo (watermark) en niveau de gris est formulé comme suit :

Étape 1 : Décomposer l'image hôte en L niveaux et l'image de logo en l niveaux en utilisant la DWT. Trouver les facteurs de poids $w_l^\theta(i, j)$ pour des coefficients d'ondelette.

Étape 2 : Des coefficients significatifs dans chaque bande sont trouvés dehors basés sur leurs facteurs de poids. Des facteurs de poids de chaque sous-bande sont assortis dans l'ordre décroissant, pour trouver le poids de seuil comme donné au-dessous :

$$T_l^\theta = S(p \times G_{Sl}) \quad (2.26)$$

Où $S(\cdot)$ sont les facteurs assortis de poids de la sous-bande, p est le pourcentage des coefficients d'ondelette dans lesquels le watermark est enfoncé et G_{Sl} est la taille de la sous-bande. Les coefficients, qui ont des facteurs de poids davantage que la valeur seuil T_l^θ , sont considérés en tant que coefficients significatifs et sont employés pour enfoncer le watermark.

Étape 3 : Ajouter les bits du watermark aux coefficients significatifs de toutes les sous-bandes en utilisant l'équation suivante :

$$\hat{S}_l(i, j) = S_l(i, j) + \alpha w_l(i, j) x(m, n) \quad (2.27)$$

Ici la constante α , donne la force de watermark.

Étape 4 : Après avoir intégré les bits du watermark, la transformation inverse en ondelette de niveau L de l'image est effectuée pour obtenir l'image tatouée.

3.3.3. Détection de la marque

Pour l'extraction de la marque de l'image tatouée, on a besoin des images originale et tatouée. Bien qu'en considérant l'acceptabilité de l'image originale, il peut ne pas être possible dans certaines applications pratiques d'effectuer cette opération, on considère que les applications où la robustesse est importante et a accès à l'image originale. Les étapes pour l'extraction du watermark sont les suivantes :

Étape 1 : L'image originale et l'image tatouée sont décomposées en ondelette de 4 niveaux.

Les facteurs de poids sont trouvés en considérant l'image originale (décomposée en ondelette)

Étape 2 : Chaque répétition de bits du watermark est extraite de l'image tatouée comme donné ci-dessous :

$$x'(m,n) = [\hat{S}_l^\theta(i,j) - S_l^\theta(i,j)] / w_l^\theta(i,j) \quad (2.28)$$

Où $\hat{S}_l^\theta(i,j)$ est la sous bande de l'image suspectée.

Étape 3 : Les bits extraits correspondants du watermark sont combinés en multipliant par le poids de distorsion comme donné ci-dessous :

$$\hat{x}(m,n) = \hat{x}(m,n) + x'(m,n) \times [w_l^\theta(i,j) * 2^l / \sqrt{D_l^\theta(i,j)}]^2 \quad (2.29)$$

Où $w_l^\theta(i,j)$ est le facteur de poids du pixel correspondant et $D_l^\theta(i,j)$ est la distorsion calculée dans la fenêtre de voisinage $N_x \times N_y$, comme suit :

$$D_l^\theta(i,j) = \frac{\sum_{x=i-N_x/2}^{i+N_x/2} \sum_{y=j-N_y/2}^{j+N_y/2}}{N_x \times N_y} \times [\hat{S}_l^\theta(i,j) - S_l^\theta(i,j)]^2 \quad (2.30)$$

Les poids w_l^θ calculés pour des coefficients de sous-bande de plus basse fréquence sont très petits par rapport aux coefficients de sous-bande de fréquence plus élevée. Pendant la combinaison des répétitions du watermark ces poids donnent plus de force aux coefficients extraits de sous-bandes à haute fréquence.

Par conséquent, pour donner des poids égaux aux coefficients extraits de toutes les sous-bandes, le facteur 2^l de multiplication est employé.

Étape 4 : Les poids correspondants de distorsion se résument comme suit :

$$sum(m,n)=sum(m,n) + [w_i^0(i,j)*2^l/\sqrt{D_i^0(i,j)}]^2 \quad (2.31)$$

Étape 5 : Après avoir extrait tout les bits du watermark et en combinant avec l'équation (2.29), ils sont normalisés comme donné ci-dessous :

$$\hat{x}(m, n) = \frac{\hat{x}(m,n)}{sum(m,n)} \quad (2.32)$$

Étape 6 : Pour former le logo extrait, prendre la transformation en ondelette inverse de niveau l $\hat{x}(m, n)$ et la mesure entre 0 et 255. Pour découvrir si le logo est présent ou pas, le logo extrait est visuellement vérifié et comparé au logo original.

4. Conclusion

La technique du bit de poids faible est la toute première utilisée pour le watermarking, elle reste très fragile face aux attaques les plus utilisées comme les attaques géométriques, l'ajout de bruit ou encore la compression JPEG.

Pour améliorer la robustesse, d'autres techniques ont vu le jour : la DCT, elle résiste très bien à la compression jpeg et aux bruits, aussi nous avons parlé de la DWT et de l'étalement de spectre qui ont une plus grande robustesse que la première technique (LSB).

Le choix d'une technique se fait en fonction de la donnée à tatouée, du type de tatouage souhaité, c'est-à-dire que la marque doit être adaptée à la donnée et la robustesse, la visibilité d'un tatouage est fonction des objectifs du concepteur.

Chapitre 3

Introduction à la biométrie

1. Introduction

La biométrie ou plus précisément la reconnaissance biométrique est l'exploitation automatisée ou semi-automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité d'un individu. Elle suscite une attention accrue depuis les attaques terroristes du 11 Septembre 2001. Les gouvernements de nombreux pays comptent de plus en plus sur la biométrie pour accroître la sécurité dans les aéroports et aux postes frontaliers et pour produire des pièces d'identité encore plus sûres. Des technologies qui font appel à la biométrie sont aussi utilisées ou mises à l'épreuve dans une foule d'applications commerciales.

Ce chapitre donne un aperçu comparatif des principales technologies biométriques qui sont disponibles ou le seront sous peu et examine les préoccupations soulevées au sujet de la sécurité et de la protection de la vie privée dans le contexte de la biométrie. Il décrit également de façon technique la reconnaissance des empreintes digitales.

2. Caractéristiques des systèmes biométriques

Pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle répond aux critères suivants :

- Universalité : chaque personne doit présenter cette caractéristique.
- Caractère distinctif : la caractéristique doit être suffisamment différente chez deux personnes.
- Permanence : la caractéristique doit être suffisamment immuable pendant une période donnée.
- Perceptibilité : la caractéristique doit pouvoir être mesurée quantitativement.

Il faut prendre en compte plusieurs autres facteurs pour savoir si l'on doit utiliser un système de reconnaissance biométrique des personnes, notamment :

- La performance : fiabilité et rapidité de reconnaissance du système ; ressources requises pour obtenir la fiabilité et la rapidité de reconnaissance voulues ; facteurs opérationnels et environnementaux qui influent sur la fiabilité et la rapidité du système.
- L'acceptabilité : mesure dans laquelle les gens sont disposés à accepter l'utilisation d'une technologie de reconnaissance biométrique à des fins d'identification.
- La facilité de contournement : facilité avec laquelle le système peut être induit en erreur par des méthodes frauduleuses.

Dans un système de reconnaissance biométrique, un appareil saisit et enregistre les caractéristiques en question, et un logiciel interprète les données et détermine l'acceptabilité de la personne (selon le système employé, un préposé peut intervenir dans la détermination de l'acceptabilité). Les systèmes de reconnaissance biométriques fonctionnent à trois niveaux : (i) un capteur prend une observation de la caractéristique biométrique ; (ii) le système traduit l'observation en termes mathématiques et produit une signature ou un gabarit biométrique ; (iii) l'ordinateur introduit la signature biométrique dans un algorithme et la compare à une ou plusieurs autres signatures biométriques entreposées dans la base de données du système.

Un système de reconnaissance biométrique peut fonctionner en mode vérification ou en mode identification. En mode vérification (comparaison individuelle), le système vérifie l'identité de la personne. Il valide son identité en comparant les données biométriques saisies aux gabarits biométriques de la personne entreposés dans la base de données du système (ou sur une carte à puce portée par la personne). La vérification de l'identité est habituellement utilisée pour l'identification catégorique, lorsqu'on veut éviter que plusieurs personnes utilisent la même identité. En mode vérification, l'enrôlement est une étape cruciale de l'établissement d'un système de reconnaissance biométrique efficace. A cette étape, chaque utilisateur fournit un échantillon de la caractéristique biométrique visée (en interagissant avec l'appareil de saisie). Le système prélève de l'information caractéristique de cet échantillon et entrepose les données produites sous forme de gabarit. L'utilisateur interagit avec le système une autre fois pour vérifier que les données correspondent au gabarit. En cas de non concordance, le processus est répété jusqu'à ce qu'une concordance soit enregistrée et que l'enrôlement soit terminé.

En mode identification (comparaison collective), le système reconnaît une personne en examinant tous les gabarits dans le système à la recherche d'un appariement.

Etant donné que de nombreuses comparaisons doivent être effectuées en mode identification, un appariement accidentel ou des appariements multiples sont possibles. L'identification est un élément crucial pour des applications comme les listes de surveillance, pour lesquelles le système détermine si le gabarit biométrique d'une personne se trouve dans sa base de données.

3. Survol des systèmes de reconnaissance biométrique

Il existe une variété de technologies de reconnaissance biométrique, soit sur le marché, soit à l'étape de la recherche et du développement (R-D). Les technologies les plus courantes servent à la reconnaissance des empreintes digitales, du visage, de l'iris et de la main ou des doigts. Les technologies moins fréquemment utilisées s'appuient sur la reconnaissance des images rétinienne et de la démarche et sur la vérification dynamique de la signature. Nous effectuerons ci-après un survol des quatre systèmes de reconnaissance biométrique les plus couramment utilisés et une comparaison de 15 techniques de reconnaissance biométrique déjà disponibles sur le marché ou en voie de développement.

3.1. Reconnaissance des empreintes digitales

Les services de police ont recours à la comparaison manuelle des empreintes digitales pour identifier des personnes depuis la fin des années 1800. A la fin des années 1960 et au début des années 1970, le Federal Bureau of Investigation (FBI) américain a commencé à financer des recherches sur des technologies utiles en la matière ; ces recherches ont mené à la mise au point de systèmes semi-automatisés de reconnaissance des empreintes digitales. Les progrès technologiques ont conduit à l'élaboration et à la mise en marche de systèmes entièrement automatisés et rapides de vérification des empreintes digitales. Les systèmes employés pour les opérations d'identification sur une grande échelle (comparaison collective) exigent l'information provenant des 10 doigts (plutôt que d'un seul), et les examinateurs humains doivent parfois intervenir pour la comparaison finale des empreintes. Le capteur employé pour saisir l'image numérique de la surface d'une empreinte digitale peut être le balayage optique (le plus courant), capacitif, ultrasonique ou thermique.

La reconnaissance par les empreintes digitales est très fiable, difficile à contourner (dans le cas des systèmes évolués) et généralement peu coûteuse. La technologie n'est toutefois pas discrète et la prise d'empreintes digitales évoque le système pénal.

3.2. Reconnaissance faciale

Les premiers algorithmes de reconnaissance faciale utilisaient des modèles géométriques simples. Le premier système semi-automatisé de reconnaissance faciale a été élaboré au cours des années 1960. L'opérateur devait situer les caractéristiques (yeux, oreilles, nez et bouche) sur la photographie pour que le système puisse mesurer les distances et les proportions par rapport à un point de référence commun puis les comparer aux données de référence. Les technologies actuelles de reconnaissance faciale utilisent des représentations mathématiques complexes et des procédés d'appariement évolués.

Le rendement des systèmes de reconnaissance faciale existant sur le marché dépend de la manière dont les images faciales sont obtenues. Ces systèmes réussissent mal à reconnaître un visage à partir d'images saisies de deux points de vue très différents sous des éclairages différents. Certains analystes se demandent si le visage, en l'absence de toute information contextuelle, constitue une base suffisante pour reconnaître une personne avec un degré de confiance très élevé en le comparant à un grand nombre d'identités.

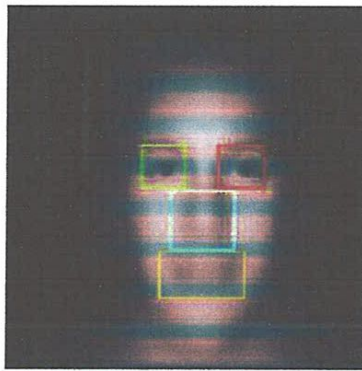


Figure 3.1 : Reconnaissance du visage

3.3. Reconnaissance de l'iris

L'iris est un muscle à l'intérieur de l'œil qui règle la taille de la pupille et détermine ainsi la quantité de la lumière qui y pénètre. Chaque iris présente une texture très détaillée et unique dont la striation, les creux et les sillons permettent de reconnaître une personne. Les systèmes automatisés de reconnaissance de l'iris sont relativement récents : le premier brevet pour l'algorithme a été délivré en 1994 et les premiers produits commerciaux ont été mis en marché en 1995. Ces systèmes illuminent l'iris avec une lumière proche de l'infrarouge (inoffensive pour l'œil) et en prennent une photo au moyen d'un appareil photo numérique de grande qualité. Les motifs aléatoires de l'iris sont alors encodés en termes mathématiques et les codes ainsi produits sont comparés de manière statistique à un ou à plusieurs gabarits.

Etant donné qu'il est difficile de modifier chirurgicalement l'iris et que les iris artificiels (par exemple lentilles de contact) sont faciles à reconnaître, il est relativement difficile de tromper un système de reconnaissance de l'iris. Ces systèmes sont très fiables (dans la mesure où l'enrôlement est réussi) et rapides, puisqu'ils donnent des résultats en quelques secondes. Un de leurs inconvénients tient à ce qu'ils ne sont pas largement acceptés par le public comme outil de reconnaissance, surtout en raison de craintes (non fondées) que la lumière infrarouge endommage l'œil.

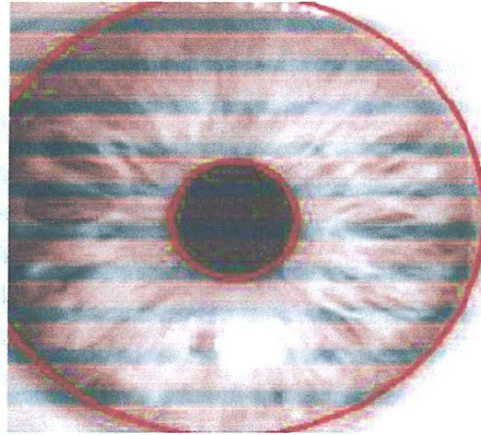


Figure 3.2: Image d'Iris

3.4. Reconnaissance des doigts et de la main

Les systèmes de reconnaissance biométrique de la géométrie de la main sont sur le marché depuis les années 1980 et sont utilisés dans des centaines d'endroits partout dans le monde. Ces systèmes mesurent et enregistrent la longueur, la largeur, l'épaisseur et la surface de la main d'une personne. Un appareil photo placé au-dessus de la main prend une image de celle-ci et des miroirs disposés à certains angles permettent la prise d'une image latérale ; on crée ainsi un gabarit de vérification qui est comparé au gabarit créé lors de l'enrôlement.

Les systèmes de reconnaissance de la géométrie de la main sont très répandus, parce qu'ils sont faciles à utiliser, largement acceptés par le public et relativement peu coûteux. L'inconvénient, c'est que ces systèmes ne peuvent servir qu'à la vérification et non à l'identification, car la géométrie de la main n'est pas incomparable.

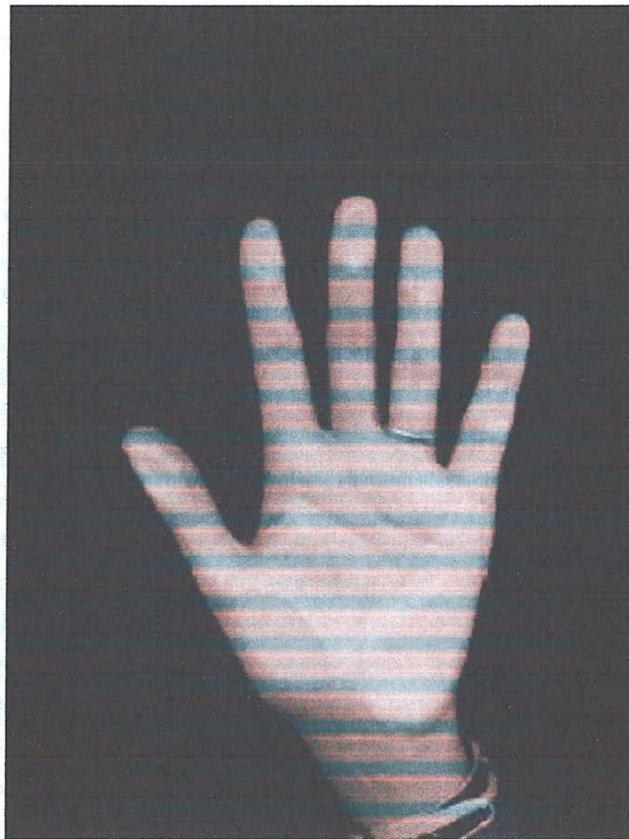


Figure 3.3: Reconnaissance de la main

4. Comparaison des systèmes de reconnaissance biométrique

Il existe un certain nombre d'autres techniques de reconnaissance biométrique sur le marché ou à l'étape de la R-D. Le tableau 1 présente une comparaison entre 15 identifiants biométriques en fonction de sept facteurs. (On trouvera la description de ces facteurs dans la partie précédente du présent chapitre).

Tableau 3. 1 : comparaison des différentes technologies de reconnaissance biométrique (E= Elevé ; M= Moyen ; F= Faible)

Identifiant biométrique	Universalité	Caractère distinct	Permanence	Facilité de saisie	Performance	Acceptabilité	Facilité de contournement
ADN	E	E	E	F	E	F	F
Oreille	M	M	E	M	M	E	M
Visage	E	F	M	E	F	E	E
Thermogramme facial	E	E	F	E	M	E	F
Empreintes digitales	M	E	E	M	E	M	M
Démarche	M	F	F	E	F	E	M
Géométrie de la main	M	M	M	E	M	M	M
Veine de la main	M	M	M	M	M	M	F
Iris	E	E	E	M	E	F	F
Dynamique de la frappe	F	F	F	M	F	M	M
Odeur	E	E	E	F	F	M	F
Empreinte palmaire	M	E	E	M	E	M	M
Rétine	E	E	M	F	E	F	F
Signature	F	F	F	E	F	E	E
Voix	M	F	F	M	F	E	E



Figure 3.4: Comparaison des différents systèmes

5. Limites techniques des systèmes de reconnaissance biométrique

5.1. Fiabilité

La fiabilité d'un système de reconnaissance biométrique est caractérisée par deux statistiques sur l'erreur :

- (i) Le taux de faux rejets, c'est-à-dire l'attribution par le système à une même personne de mesures biométriques provenant de deux personnes.
- (ii) Le taux de fausses acceptations, c'est-à-dire l'attribution par le système à deux personnes distinctes de deux mesures biométriques d'une même personne ;

Ces deux mesures d'erreur sont reliées, et il existe un point d'équilibre entre les deux pour chaque système biométrique. Chacune est fonction du seuil de décision du système, une valeur établie par le concepteur ou l'opérateur du système, qui définit le point auquel un appariement est effectué. Les résultats supérieurs au seuil sont des équivalences et les résultats inférieurs au seuil, des non-équivalences. Si le seuil est abaissé pour rendre le système plus tolérant aux variations des données saisies et au bruit, le taux de fausses acceptations augmente. Inversement, si on rehausse le seuil pour que le système soit plus sûr, le taux de faux rejets augmente. Le point auquel les deux taux sont égaux est le point d'équivalence des erreurs. Plus cette valeur est faible, plus le système est fiable, car il y a alors un bon équilibre de la sensibilité. Outre ces taux d'erreur, le taux d'échec à la saisie et le taux d'erreur à l'enrôlement sont également employés pour établir la fiabilité d'un système biométrique.

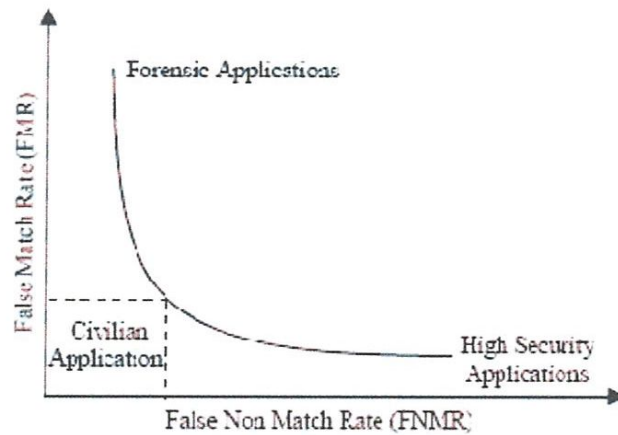


Figure 3.5: Relation entre taux de faux rejets et taux de fausses acceptations

$$FMR = \frac{\text{Nombre de Fausses acceptations (FA)}}{\text{Nombre d'imposteurs}} \quad (3.1)$$

$$FNMR = \frac{\text{Nombre de Faux rejets (FR)}}{\text{Nombre de clients}} \quad (3.2)$$

FMR: Le taux de fausses acceptations

FNMR : Le taux de faux rejets

$$TER = \frac{\text{Nombre de FA} + \text{Nombre de FR}}{\text{Nombre total de clients}} \quad (3.3)$$

Il convient d'étudier attentivement les affirmations faites par les fournisseurs au sujet de la fiabilité de leurs produits, car :

- (i) Il se peut que le fournisseur ne mentionne qu'une des statistiques décrites ci-dessus, pour soutenir ses prétentions ;
- (ii) Les taux de fiabilité présentés par les fournisseurs sont habituellement établis au moyen de tests ou de l'utilisation de systèmes de reconnaissance de petite envergure dans des conditions contrôlées ;
- (iii) Les impératifs de fiabilités d'un système biométrique dépendent de l'utilisation à laquelle on le destine : vérification ou identification.

5.2. Vulnérabilité

Un système de reconnaissance biométrique risque d'être « dupé » à dessein ou accidentellement. Les systèmes sont exposés à des dommages ou à des attaques, d'une part, au niveau de l'appareil ou de l'équipement connexe à l'interface utilisateur et, d'autre part, au niveau du système. Les appareils peuvent être vulnérables à la duperie (contournement par un imposteur), à la détérioration par l'environnement ou à des attaques matérielles, et à des dommages aux câbles, fils et autres conduits de communications. Pour ce qui est du système, les algorithmes et les gabarits prêtent flanc aux attaques de pirates informatiques ; les données sont susceptibles d'être effacées, modifiées ou volées au niveau de l'administrateur ou du compte ; et les éléments logiciels (par exemple les pilotes) ne sont pas à l'abri des attaques. L'emploi de systèmes de reconnaissance biométrique multimodaux faisant appel à plusieurs technologies et aux données de plusieurs caractéristiques biométriques est un moyen de repousser les limites de fiabilité et de vulnérabilité évoquées ci-dessus.

Il faut également souligner que, pour ce qui est de la vérification de l'identité, la biométrie peut uniquement confirmer que la personne contrôlée est celle qui s'est inscrite dans le système ; si cette personne a utilisé des documents de base (par exemple un acte de naissance) falsifiés pour s'enrôler, le système ne pourra pas confirmer la véritable identité de la personne.

6. Coût et mise en œuvre

Les coûts de mise en œuvre et d'exploitation sont un autre aspect préoccupant des systèmes de reconnaissance biométrique. Certains systèmes de reconnaissance biométrique utilisés en entreprise, sur une petite échelle, sont relativement peu chers à installer et à entretenir ; cependant, le coût global du cycle de vie d'autres systèmes plus complexes destinés à des exploitations sur une grande échelle peut être prohibitif pour certaines entités (y compris des gouvernements). Il faut inclure dans le coût total de ces systèmes non seulement les immobilisations initiales en matériels et logiciels, mais aussi les coûts de la production de pièces d'identité (dans certains cas), la formation et l'embauche de personnel, l'entretien du matériel et la gestion des bases de données.

7. Applications de la biométrie

Les techniques biométriques sont appliquées dans plusieurs domaines et les applications sont divisées en trois groupes principaux :

- Applications commerciales: telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'Internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicale, etc...
- Applications de gouvernement: telles que la carte nationale d'identification, le permis du conducteur, la sécurité sociale, la contrôle de passeport, etc...
- Applications juridique: telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc...

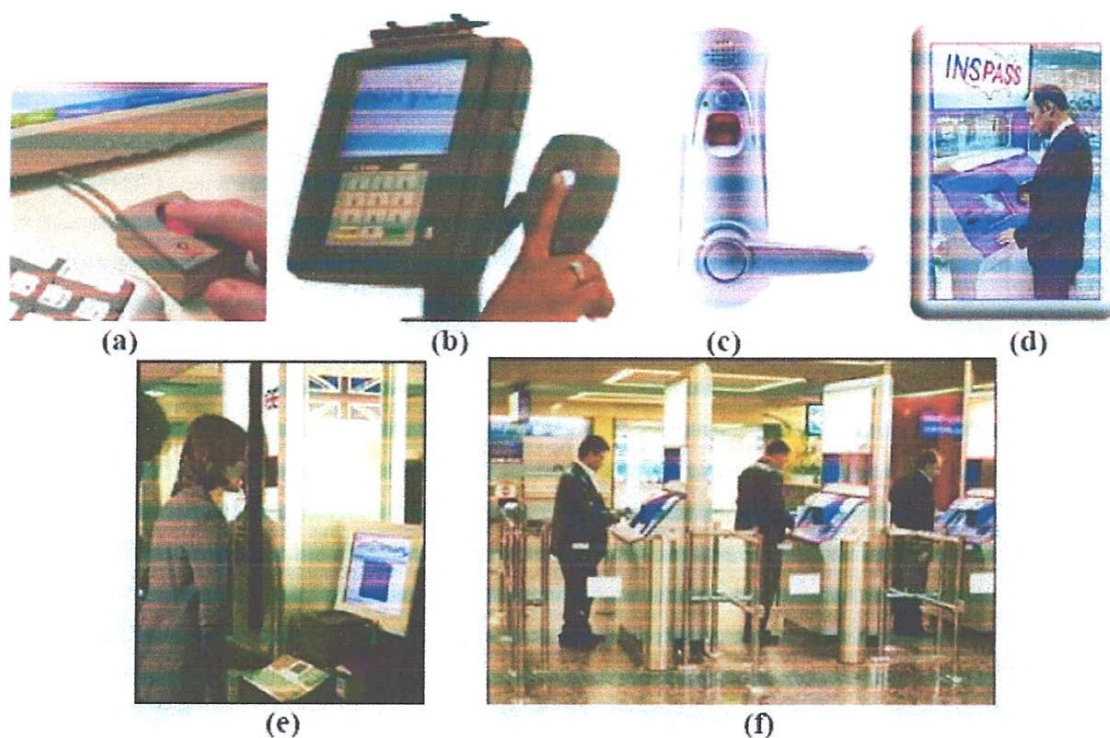


Figure 3.6: Applications biométriques

8. Conception du système de reconnaissance des empreintes digitales

Un système de reconnaissance des empreintes digitales est un système automatique de reconnaissance de formes qui se compose de trois étapes principales :

- **Acquisition** : Les empreintes digitales sont capturées et stockées sous forme d'image.
- **Extraction des caractéristiques**: les caractéristiques essentielles sont extraites à partir des images.

- **Prise de décision** : Les caractéristiques acquises sont comparées avec les caractéristiques stockées dans une base de données et à partir du résultat de cette comparaison une décision est prise.

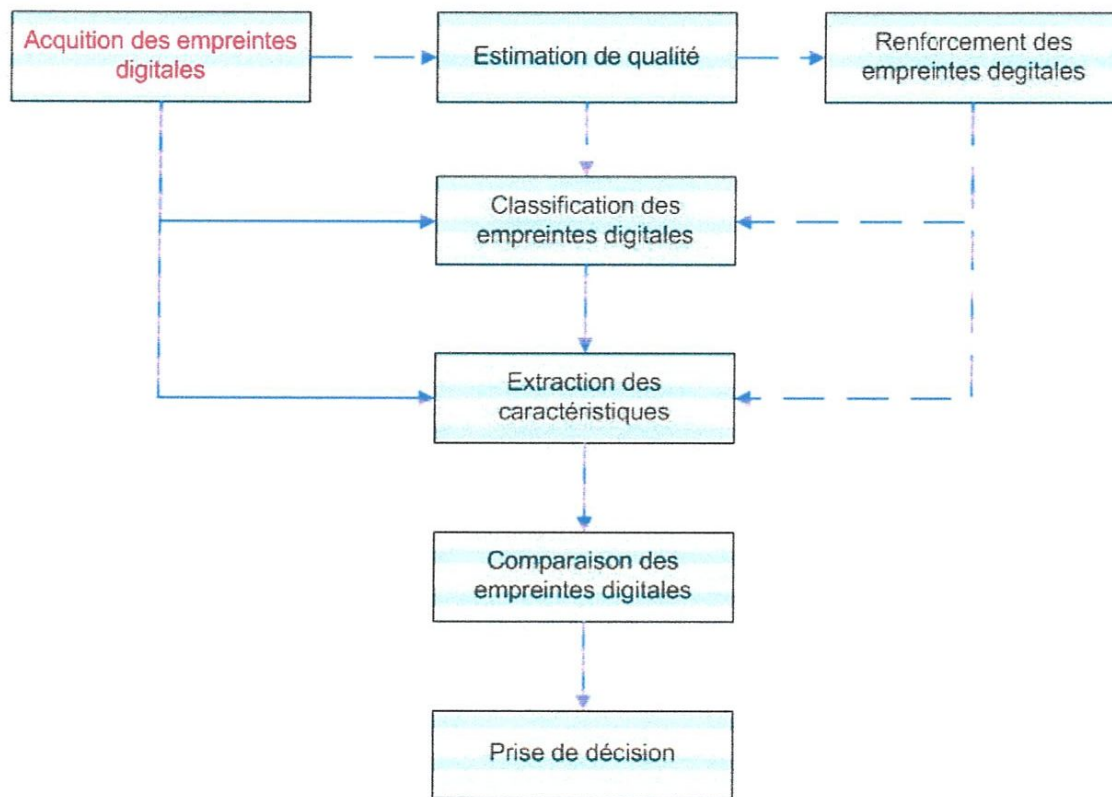


Figure 3.7: Conception d'un système biométrique basé sur les empreintes digitales

8.1. Extraction des caractéristiques

La plupart des systèmes de reconnaissance des empreintes digitales emploient des minuties comme caractéristiques des empreintes digitales. Alors cette partie présentera les méthodes pour extraire des minuties à partir des empreintes digitales.

Un extracteur de minuties cherche des arêtes de ride et des bifurcations dans les empreintes digitales. Si les rides sont bien déterminées, alors l'extraction de minuties est une tâche relativement simple. Cependant, dans la pratique, il n'est pas toujours possible d'obtenir une carte parfaite de rides. Donc la performance des algorithmes actuellement disponibles d'extraction de minuties dépend fortement de la qualité des images des empreintes digitales d'entrée.

Typiquement, un algorithme d'extraction de minuties se compose de 4 étapes principales : Estimation d'orientation, segmentation, détection de rides, détection de minuties et le processus entier d'un algorithme d'extraction de minuties est montré dans la figure 3.8

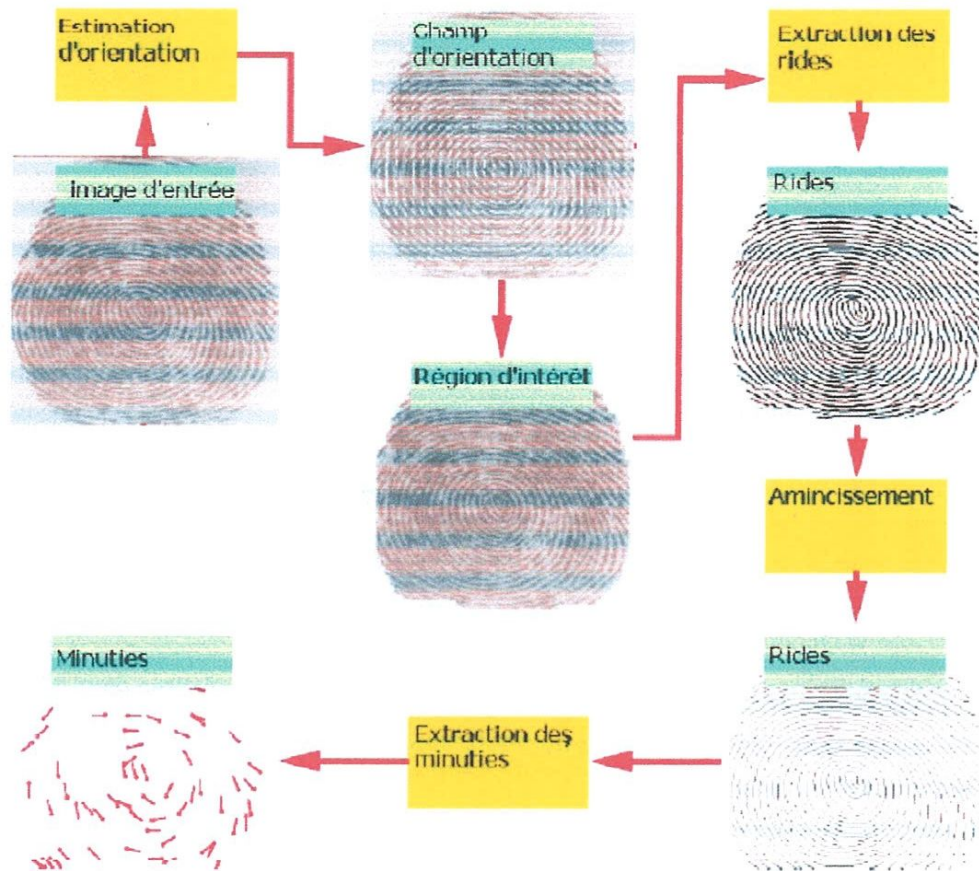


Figure 3.8: Processus d'extraction des minuties

8.2. Estimation d'orientation

Le champ d'orientation d'une image d'empreinte digitale représente la nature intrinsèque de l'empreinte digitale. C'est un étage essentiel pour déterminer les rides d'empreinte digitale et pour trouver la région d'intérêt d'image d'empreinte digitale, Il existe plusieurs méthodes pour estimer le champ d'orientation des images d'empreinte digitale.

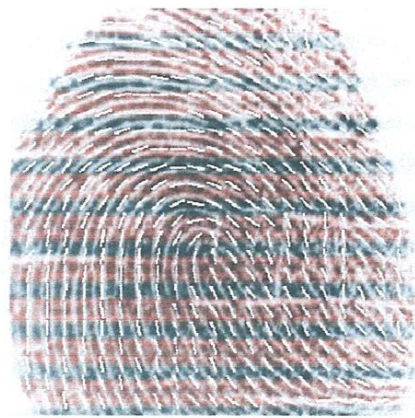


Figure 3.9: Le champ d'orientation d'une image d'empreinte digitale

L'idée principale de cette méthode est que l'image d'empreinte digitale se divise en plusieurs fenêtres de taille $W \times W$, pour tout pixel dans chaque fenêtre on calcule les gradients G_x et G_y et puis on calcule l'orientation locale de ce pixel en utilisant la formule :

$$V_x(i,j) = \sum_{u=i-W/2}^{i+W/2} \sum_{v=j-W/2}^{j+W/2} (2G_x(u,v)G_y(u,v)) \quad (3.4)$$

$$V_y(i,j) = \sum_{u=i-W/2}^{i+W/2} \sum_{v=j-W/2}^{j+W/2} (G_x^2(u,v) - G_y^2(u,v)) \quad (3.5)$$

$$\theta(i,j) = \frac{1}{2} \tan^{-1} \left(\frac{V_x(i,j)}{V_y(i,j)} \right) \quad (3.6)$$

+ W est la taille de la fenêtre locale;

+ G_x et G_y sont les grandeurs de gradient dans les directions x et y

➤ Segmentation

Après avoir estimé le champ d'orientation d'une image d'empreinte digitale, un algorithme de segmentation qui est basé sur le niveau de certitude du champ d'orientation est employé pour localiser la région d'intérêt dans l'image d'empreinte digitale. Le niveau de certitude du champ d'orientation au pixel (i,j) est défini comme suit:

$$CL(i,j) = \sqrt{\frac{1}{W^2} \frac{V_x^2(i,j) + V_y^2(i,j)}{V_e(i,j)}} \quad (3.7)$$

$$V_e(i,j) = \sum_{u=i-W/2}^{i+W/2} \sum_{v=j-W/2}^{j+W/2} (G_x^2(u,v) + G_y^2(u,v)) \quad (3.8)$$

+ $CL(i,j)$ est l'orientation locale du pixel (i,j)

Pour chaque pixel, si son niveau de certitude du champ d'orientation est inférieur d'un certain seuil T , le pixel est marqué comme pixel de fond. Sinon il est marqué comme un pixel de la région d'intérêt.

➤ Détection de rides

L'objectif de l'algorithme de détection de rides est de séparer des rides des vallées dans une image d'empreinte digitale. Il existe plusieurs d'approches :

+ *Seuil Fixe/adaptatif*: les pixels plus sombres qu'un seuil constant/variable sont déterminés pour être des pixels de rides dans l'empreinte digitale. Ces approches généralement ne fonctionnent pas bien pour les parties bruyantes et l'image avec un contraste bas.

+ *Minimum Local* : cette l'approche emploie une propriété de rides c'est que les valeurs de niveau gris sur des rides atteignent leurs minimum local tout le long de la direction normale de l'orientation locale des rides.

Normalement le résultat obtenu est une image binaire dans laquelle les pixels noirs sont les pixels des rides et les pixels blancs sont des pixels des vallées ou du fond.

Généralement les rides détectées sont épaisses, puis un algorithme amincissant est employé pour obtenir des rides. Ces rides sont utiles pour détecter des minuties.

➤ *Détection de minuties*

Lorsque les rides sont bien déterminées les minuties seront facilement détectées:

+ Les pixels avec trois pixels voisins sont identifiés comme bifurcations.

+ Les pixels avec un pixel voisin sont identifiés comme arêtes de ride

Cependant, Ce n'est pas le fait que toutes les minuties détectées sont des bonnes minuties à cause du bruit.

➤ *Post-traitement*

Dans cette étape, les vraies minuties sont extraites en utilisant un certain nombre d'heuristiques. Par exemple, trop de minuties dans une petite région peuvent indiquer que la présence du bruit et elles pourrait être jetée. Deux arêtes de rides sont trop proches indiquent des fausses minuties produites par une coupure dans le ride etc...

8.3. Assortiment des empreintes digitales

Il est très difficile pour assortir sûrement deux empreintes digitales. La cause principale c'est la variabilité dans différentes impressions du même doigt (c.-à-d., grandes variations d'intra-classe). Les facteurs principaux responsables des variations d'intra-classe sont:

- Le déplacement,
- La rotation,
- La déformation non-linéaire,
- La variation des pressions,
- Le changement d'état de peau,
- bruit, et erreurs d'extraction des caractéristiques
- etc...

Par conséquent, les empreintes digitales du même doigt peuvent être différentes tandis que les empreintes digitales de différents doigts peuvent être ressemblantes.

Pour résoudre ce problème, il existe plusieurs approches et elles sont classées en 3 catégories principales :

8.3.1. Assortiment basé sur la corrélation

Cette approche est basée sur la corrélation des pixels de deux empreintes digitales. Deux images d'empreinte digitale sont superposées et la corrélation (au niveau d'intensité) entre les pixels correspondants est calculée pour différents alignements (par exemple déplacements et rotations). Cette approche est assez facile à réaliser mais son résultat est sensible à la variation comme la rotation, le déplacement, etc...

8.3.2. Assortiment basé sur rides

Dans cette approche, on utilise des caractéristiques extraites des rides (orientation, texture, forme de ride, etc...) pour comparer des empreintes digitales.

L'avantage de cette approche c'est que les caractéristiques des rides peuvent être extraites plus sûrement, cependant les distinctions de ces caractéristiques sont faibles

8.3.3. Assortiment basé sur minuties

C'est l'approche la plus utilisée dans la littérature, des minuties sont extraites à partir des deux empreintes digitales et stockées sous forme d'un ensemble de points dans le plan de deux dimensions. L'assortiment basé sur les minuties, essentiellement, se compose de trouver l'alignement entre les minuties du motif et les minuties d'entrée. Le résultat est le nombre maximum des paires de minuties. Il existe 3 méthodes différentes pour assortir des minuties

- Assortiment des minuties basé sur la transformation de Hough.
- Assortiment des minuties basé sur la minimisation d'énergie.
- Assortiment des minuties basé sur l'alignement.

9. Conclusion

Etant donné l'omniprésence des préoccupations en matière de sécurité dans le monde d'aujourd'hui, il est peu probable que les systèmes de reconnaissance biométrique disparaissent. Ils deviendront sans doute monnaie courante aux frontières, dans les aéroports et dans les autres établissements où la sécurité est un enjeu. L'organisation de l'aviation civile internationale a établi des normes pour les documents de voyage lisibles à la machine, y compris l'inclusion d'identificateurs biométriques ; ainsi, le passeport électronique

biométrique deviendra probablement un jour le seul document acceptable pour les voyages internationaux.

Les systèmes de reconnaissance biométrique sont des dispositifs de sécurité intrusifs. Certaines personnes s'opposent donc carrément à leur utilisation, alors que d'autres sont d'avis qu'ils peuvent être nécessaires dans certains cas, mais seulement si des mesures de sécurité et des mesures juridiques appropriées sont en place pour protéger les renseignements personnels de nature délicate recueillis. Au nombre des préoccupations particulières que soulève l'utilisation de ces systèmes figurent, entre autres, les limites sur le plan technique (fiabilité et vulnérabilité), la surveillance accrue et dans certains cas inutile des activités quotidiennes des citoyens, le vol ou la manipulation de données biométriques et d'autres renseignements personnels conservés dans des banques de données centralisées, le détournement de l'utilisation et le coût élevé de la mise en place et de l'exploitation de bon nombre de ces systèmes.

Les systèmes de reconnaissance biométrique peuvent être des outils importants pour améliorer la sécurité dans certaines situations. Cependant, avant de prendre une décision quant à la mise en place de ces systèmes, les Etats envisageront peut être d'effectuer des analyses détaillées pour s'assurer que le recours à ces systèmes est vraiment nécessaire et qu'il n'existe aucun autre moyen moins intrusif d'obtenir le même résultat. De plus, les technologies de reconnaissance biométrique employées devraient être à la fois efficaces et utilisées de manière à réduire au minimum toute ingérence dans la vie privée.

Chapitre 4

Résultats de simulations

1. Introduction

Ce dernier chapitre présente les résultats de simulations permettant de valider les concepts théoriques, les phénomènes décrits dans les chapitres précédents pour enfin tester les performances de chaque technique de watermarking, selon les critères suivants :

- La robustesse
- L'imperceptibilité
- Le ratio

L'étude introductive sur la biométrie a eu pour intérêt d'abord de connaître le fonctionnement d'un système de reconnaissances d'empreintes digitales, ensuite de connaître les caractéristiques sur lesquelles la décision est prise.

Terminons par une analyse des effets d'une marque incorporée à une image d'empreinte digitale. Celle-ci gardera-t-elle ses caractéristiques pour le système de reconnaissance d'empreintes digitales ?

2. Présentation de Matlab

MatLab est un système interactif de programmation scientifique, pour le calcul numérique et la visualisation graphique. Développé à l'origine pour le calcul matriciel (le nom MatLab est dérivée de cette représentation $\text{MatLab} = \text{Matrix Laboratory}$), il offre aujourd'hui bien d'autres possibilités. Il contient des bibliothèques spécialisées (toolbox) qui répondent à des besoins spécifiques : analyse numérique, traitement du signal, traitement de l'image, etc. MatLab est un logiciel qui permet de faire des calculs mathématiques et numérique, et non un logiciel de calcul formel et symbolique comme Maple. Matlab connaît un grand nombre d'opérations ou de fonctions mathématiques : fonctions usuelles, calcul matriciel, fonctions plus spécifiques du signal (FFT, etc).

Pour la validation de notre système de watermarking :

L'image hôte utilisée est en nuance de gris (Lena ou l'image d'empreinte digitale), chaque pixel est codé sur 8 bits. Les watermarks (le logo 'CS' et copyright) sont en format binaire, chaque pixel est codé sur un bit.

Retrouver la marque enfouie en dessous d'une image revient à comparer la marque après recouvrement à l'originale, après que l'image tatouée ait été soumise à la compression JPEG ou à l'ajout de bruit. Le cas souhaité serait d'avoir ces deux marques identiques quelque soit la qualité de compression ou le pourcentage de bruit ajouté.

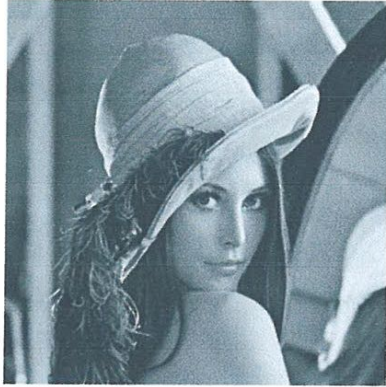
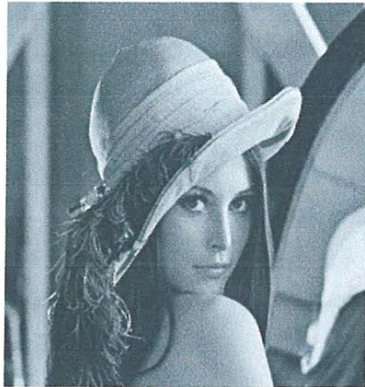




$$PSNR(I_r, I_m) = 10 \log_{10} \left(\frac{D^2}{EQM} \right) \tag{4.1}$$

$$EQM(I_r, I_m) = \frac{1}{M \times N} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (I_r(x,y) - I_m(x,y))^2 \tag{4.2}$$

D est la dynamique du signal (255 pour des pixels codés sur un octet).

M, N est la taille de l'image en pixel.

Technique de LSB

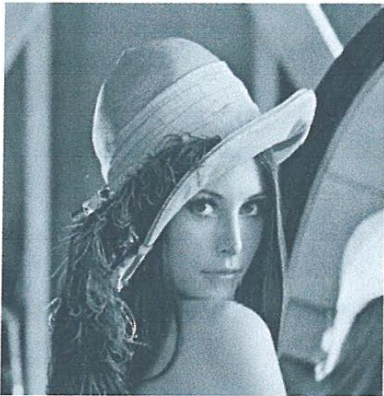





Lena sans compression	Lena après compression Q = 100	Lena après compression Q = 90
		
PSNR= 50.3523dB	PSNR=50.3279 dB	PSNR=41.3621dB
<p>Watermark extrait</p> 	<p>Watermark extrait</p> 	<p>Watermark extrait</p> 

Par simulation nous confirmons qu'aux bits de poids faibles les modifications sont imperceptibles pour l'œil humain. Plus on avance vers les bits de poids élevés l'intensité de perception augmente donc on peut voir de mieux en mieux la marque en dessous de l'image hôte.







Technique de CDMA

Lena sans compression	Lena après compression Q = 100	Lena après compression Q = 90
		
PSNR= 37.3325 dB	PSNR=37.2618dB	PSNR=36.5387dB
Watermark extrait 	Watermark extrait 	Watermark extrait 

Technique de DCT

Lena sans compression	Lena après compression Q = 30	Lena après compression Q = 20
		
PSNR= 34.0888 dB	PSNR=30.1566 dB	PSNR=30.2441
watermark extrait 	watermark extrait 	watermark extrait 

Technique de DWT

Lena sans compression	Lena après compression Q = 30	Lena après compression Q = 20
		
PSNR= 35.3256 dB	PSNR=dB	PSNR=33.3924dB
Watermark extrait 	Watermark extrait 	Watermark extrait 

Utilisons des courbes pour mieux illustrer le phénomène de dégradation des images face aux attaques. Commençons par tracer les courbes de PSNR par rapport à la qualité de compression Q pour voir la différence de luminance. Un PSNR plus élevé signifie que les images tatouée et originale s'apparentent plus.

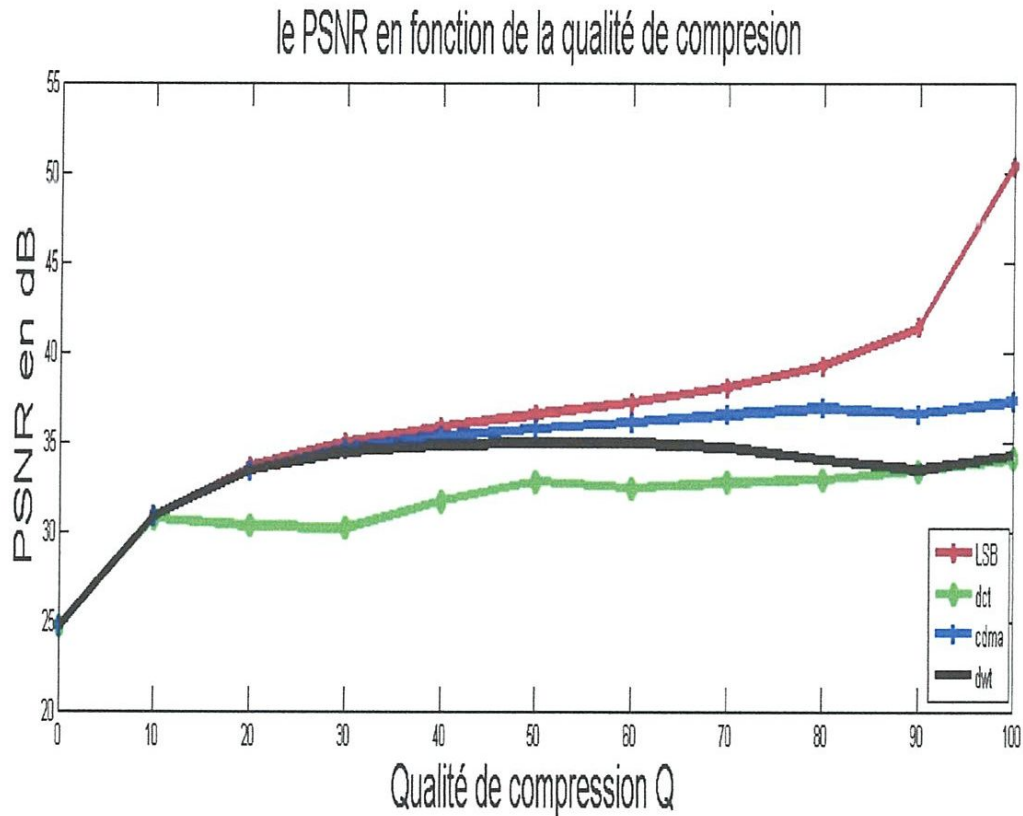


Figure 4.1 : Le PSNR en fonction de la compression.

Cette courbe montre que pour la technique du LSB la différence entre les images originale et tatouée est minimale, ensuite le cdma, le dwt et enfin la dct. Ce qui fait qu'une image tatouée par la technique de substitution de bits de poids faible est moins bruyante (plus nette) que celle tatouée par les autres techniques étudiées ici. Cela veut dire que pour le LSB l'imperceptibilité est grande que pour les autres techniques. Cependant toutes ces techniques sont d'une imperceptibilité acceptable.

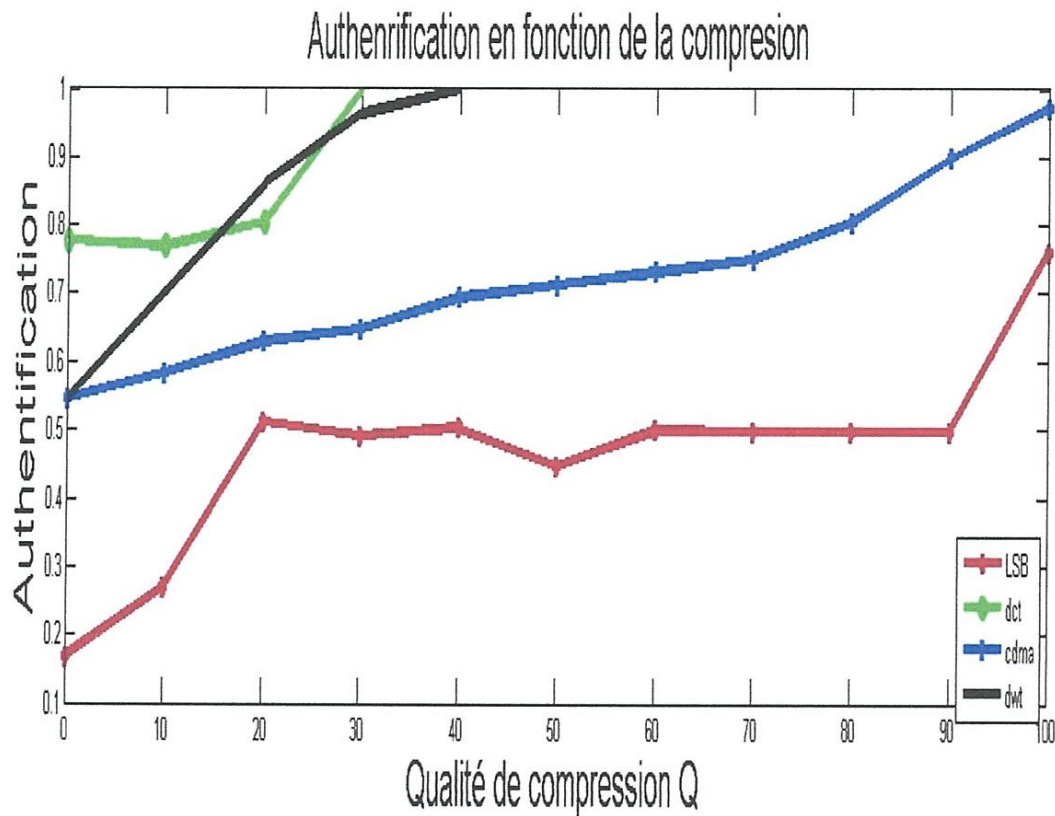











Figure 4.2 : L'authentification en fonction de la compression.

Sur la figure 4.2, on peut remarquer que la technique de LSB résiste très mal à la compression JPEG, ce qui se manifeste sur la courbe par une très faible authentification entre les watermarks original et extrait comparée aux autres techniques. Pour la DCT l'authentification est maximale entre une qualité de compression variant de 30% à 100%, le watermark extrait est donc identique à celui inséré. Pour la DWT les images sont identiques entre $Q=40\%$ et 100%. Plus l'authentification s'affaiblit et s'écarte de sa valeur maximale, plus le watermark extrait sera de moins bonne qualité et en un certain niveau il sera irrécupérable.

La technique de l'étalement de spectre (CDMA) résiste mieux à la compression que celle du LSB mais moins que les deux autres techniques. Cependant il est à remarquer que les résultats de notre simulation (cas du cdma) n'atteignent pas les performances des documents consultés qui prétendent qu'une extraction correcte du watermark est possible pour $Q=90$.

Etudions maintenant l'efficacité des techniques de tatouage soumises au bruit. Dans le tableau ci-dessous, comparons les watermarks extraits pour différents rapport signal sur bruit (SNR).

CDMA SNR=10 dB 	CDMA SNR= 25 dB 	CDMA SNR= 60 dB 
DCT SNR= 10 dB 	DCT SNR= 15 dB 	DCT SNR= 20 dB 
DWT SNR=10 dB 	DWT SNR=15 dB 	DWT SNR=20 dB 

Ce tableau montre que la technique de DWT est la plus robuste face au bruit, plus robuste que la technique DCT. Les résultats pour la technique de LSB ne figurent pas dans le tableau parce que tout simplement quelque soit la quantité ajoutée la marque n'est pas perceptible (elle est confondue à du bruit ou simplement du blanc).

Maintenant, analysons cette comparaison sur des courbes.

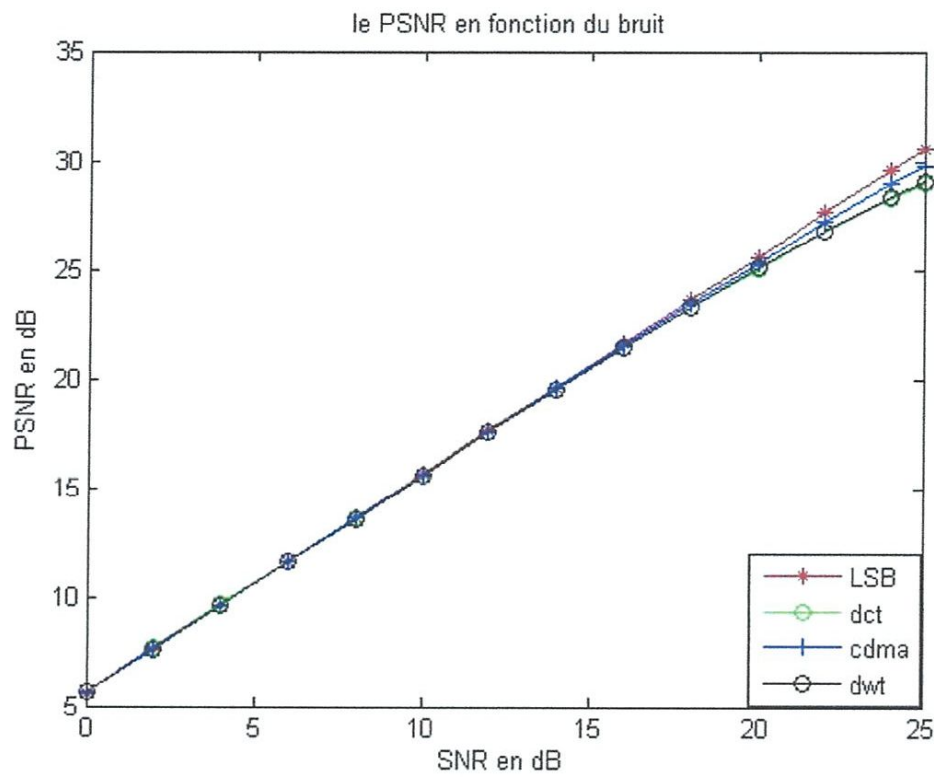


Figure 4.3 : Le PSNR en fonction du niveau de bruit

Cette figure montre que face au bruit les quatre techniques ont des PSNR très proches ce qui veut dire que la perceptibilité de la marque est au même degré d'une technique à l'autre (face au bruit).

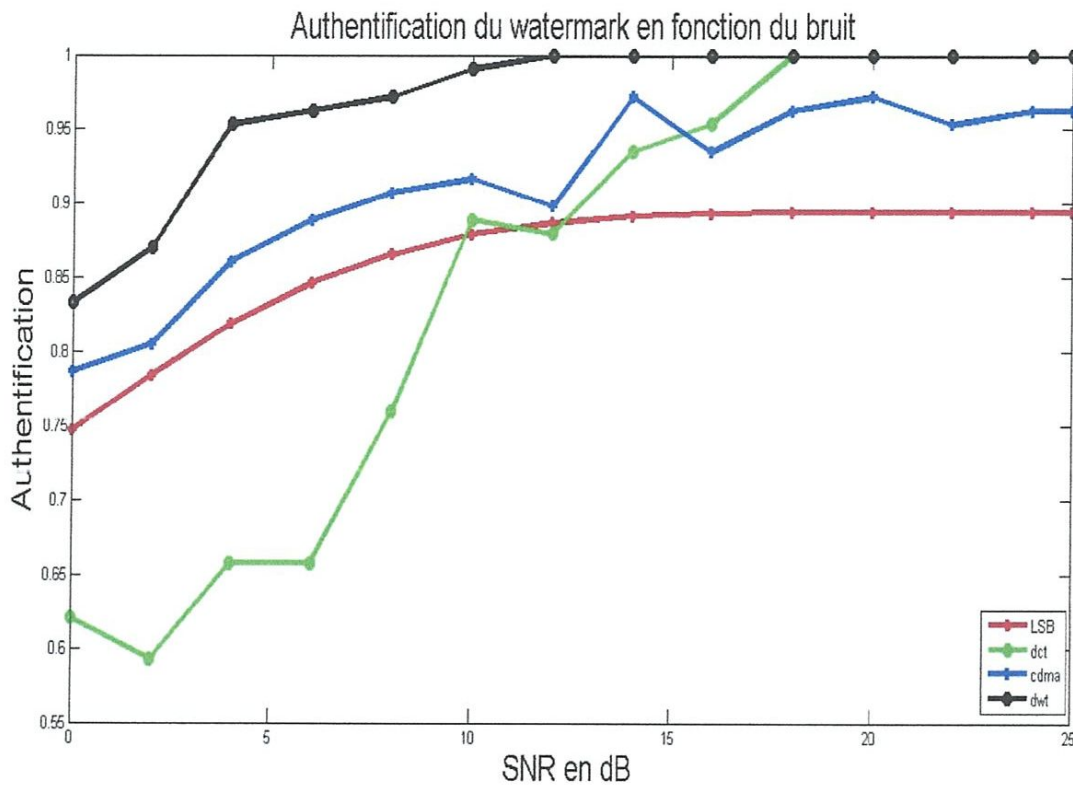








Figure 4.4 : L'authentification en fonction du niveau de bruit

La courbe d'authentification du LSB que nous percevons en rouge est stationnaire à partir d'un SNR=18 dB jusqu'à 100 dB. Pour dire que cette technique ne permet pas une extraction de la marque quelque soit le niveau de bruit qui attaque l'image tatouée (on n'extrait que du bruit). Avec la technique du CDMA à partir de 20 dB on pourrait extraire la marque sans que celle-ci ne soit identique à l'originale. Il y'a un minimal nombre de bits erronés entre la marque originale et la marque extraite. Cependant même avec un SNR=100 dB cette extraction n'est pas meilleure. Les seules techniques qui permettent donc de retrouver la marque de façon identique à l'originale sont la DWT et la DCT respectivement à partir seulement d'un SNR= 12 dB et un SNR=18 dB.

Pour l'empreinte digitale toutes les expériences déjà effectuées restent valables. Vérifions donc par la technique de DCT l'acceptabilité de la dégradation provoquée par l'intégration d'une marque.

Empreinte sans compression	Empreinte avec compression Q=30	Empreinte sans compression Q=20
		
PSNR= 34,3344 dB	PSNR= 30,6717 dB	PSNR= 29,9578 dB
		

Ce qui surtout sur le tableau ci-dessus est intéressant, c'est que l'image hôte (l'empreinte digitale) après intégration de la marque garde une certaine ressemblance à l'originale (il y'a une petite dégradation).

4. Conclusion

Dans cette étude nous avons présenté un certain nombre de techniques pour le watermarking des images numériques, aussi bien en touchant les limitations que les possibilités de chacune. Ce qui est suffisant pour tirer plusieurs conclusions au sujet du digital watermarking.

La technique de substitution du LSB n'est pas un très bon candidat pour le tatouage numérique dû à un défaut d'un niveau minimal de robustesse. Des marques incorporées par LSB peuvent facilement être enlevées en utilisant des techniques qui ne dégradent pas visuellement l'image au point d'être apparentes. En outre si l'un des algorithmes de tatouage

visuellement l'image au point d'être apparentes. En outre si l'un des algorithmes de tatouage moins robuste est employé, le message codé peut être facilement récupéré et même changé par un tiers. Il s'avérerait que le LSB restera dans le domaine de la stéganographie dû à sa capacité énorme de stockage d'information.

Une autre observation est que les techniques dans le domaine fréquentiel sont des candidats meilleurs pour le watermarking que les techniques dans le domaine spatial, pour les deux raisons de la robustesse et de l'impact visuel. Tatouer dans le domaine DCT s'est avéré fortement résistant à la compression de JPEG aussi bien qu'à des quantités significatives de bruit aléatoire.

Le domaine des ondelettes DWT aussi s'est avéré fortement résistant à la compression et au bruit, avec des quantités minimales de dégradation visuelle. La technique des ondelettes est à noter la technique la plus robuste face au bruit.

La technique d'étalement de spectre (CDMA) n'a pas une bonne robustesse que ça soit face au bruit ou face à la compression JPEG. Cependant elle a la particularité d'être la plus sécurisée par sa propriété de LPD (Low Probability Detection).

Les domaines des ondelettes et DCT sont des domaines les plus prometteurs pour le tatouage numérique.

Les empreintes digitales pourraient être tatouées sans pour autant perdre leurs caractéristiques de reconnaissance.

Conclusion générale

Le problème de protection de la propriété intellectuelle est surtout lié aux développements des techniques de transmission numérique. Pour lutter contre ce phénomène une solution serait de mettre un terme à cette évolution rapide mais une autre solution bien plus raisonnable en ce 21^{ème} siècle serait l'usage du tatouage numérique.

Le tatouage est un domaine très prometteur pour la protection des médias numériques. Parmi les techniques étudiées dans ce mémoire, les deux techniques DCT et DWT sont les plus performantes en termes de robustesse et d'imperceptibilité. La technique de CDMA malgré une moins bonne robustesse que ces deux techniques, est aussi une technique très sécurisée (un autre critère important) d'où la popularité de la dite technique dans le domaine du tatouage numérique.

La technique du LSB avec une grande capacité de charge utile (ratio) est un candidat maître pour la stéganographie.

Des améliorations de ces techniques ou la mise au point de nouvelles techniques plus efficaces pourrait pallier aux limitations de performance et être une source d'émergence pour cette nouvelle discipline si on peut l'appeler de la sorte qui est le watermarking. Un autre point à souligner qui pourrait être un réel handicap pour le développement du domaine est la difficulté d'application au grand public.

Hormis les problèmes judiciaires et d'acceptation du public des techniques de reconnaissance biométrique, l'utilisation du tatouage en biométrie pourrait combler ses inefficacités c'est-à-dire réduire considérablement les problèmes de contournement des imposteurs.

Cette étude ne prétend point que le watermarking puisse éradiquer le piratage mais il pourrait réduire considérablement le fléau. Le tatouage est de ce fait appliqué dans un certain nombre domaines et de façon satisfaisante en l'occurrence son application pour l'authentification des billets d'argent.

Un grand pas vers l'avènement du digital watermarking serait la vulgarisation du matériel de tatouage numérique par les quelques sociétés fabricants.

Bibliographie

- [1] DANG Hoang Vu Promotion X - IFI, Hanoi, Vietnam, rapport final du tipe Sujet Biométrie pour l'Identification, Juillet 2005.
- [2] D. Kahn, *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, December 1996.
- [3] Fernando Perez-Gonzalez And Juan R. Hernandez, *A Tutorial on Digital Watermarking*, <http://liris.cnrs.fr/Documents/Liris-1452.pdf>.
- [4] Inconnu, *A Really Friendly Guide to Wavelets*, C. Valens, 1999
- [5] Ingemar J. Cox, Matthew L. Miller, Jeffrey A Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, ed. Morgan Kaufmann second edition.
- [6] Jonathan K. Sui, Frank Hartung and Bernd Girod, digital watermarking of text, image, and video documents, *Comput. & Graphics*, Vol. 22, No. 6, pp. 687±695, Elsevier Science Ltd. All rights reserved Printed in Great Britain, 1999.
- [7] J. R. Hernandez, F. Perez-Gonzalez, J. M. Rodriguez, and G. Nieto, "Performance analysis of a 2d-multipulse amplitude modulation scheme for data hiding and watermarking of still images," *IEEE J. Select. Areas Commun*, vol. 16, pp. 510–524, May 1998.
- [8] J. R. Hernandez , F. Perez-Gonzalez and M. Amado, *DCT-Domain Image watermarking And Generalized Gaussian Models* Dept. Tecnologias de las Comunicaciones, ETSI Telecom., Universidad de Vigo, 36200 Vigo, Spain.
- [9] Julien Pugliesi – Cedric Piovano, *Le tatouage d'images ou "Watermarking"*, Université de Nice - Sophia Antipolis Licence d'Informatique, Travail d'études, Juin 2004.
- [10] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. 1990IEEE Military Communications Conference*, pp. 216–220, 1990.
- [11] Keith G Boyer, *The Fast Wavelet Transform (FWT)*, a thesis submitted to the University of Colorado at Denver in partial fulfillment of the requirements for the degree of master of science applied mathematics, 1995.
- [12] Lalita Acharya, Tomasz Kasprzycki, *La biométrie et son usage par l'Etat*, Etude générale, Bibliothèque du parlement, Publication no 06-30-F, Révisé le 16 Avril 2010.
- [13] Mark A. Sturza, *Spread Spectrum Techniques and Technology*, 3C Systems Company.
- [14] Mazen Youssef, *Modélisation, simulation et optimisation des architectures de récepteur pour les techniques d'accès W-CDMA*, these de doctorat présentée pour obtenir le grade de docteur de l'université Paul Verlaine – Metz.

Bibliographie

- [15] Raymond L. Pickholtz, Fellow, IEEE, Donald L. Schilling, Fellow, IEEE, And Laurence B. Milstein, Senior Member, IEEE, Theory Of Spread-Spectrum Communications-A Tutorial, IEEE Transactions On Communications, Vol/Com -30, No-5, May 1982.
- [16] Rene Alt, La Transformation En Ondelettes Université Pierre Et Marie Curie.
- [17] Teddy Furon, Thèse présentée pour obtenir le grade de docteur de l'Ecole Nationale Supérieure des Télécommunications Spécialité : Signal et Images, Application du tatouage numérique à la protection de copie, mars 2002.
- [18] Shoemaker Chris, Independent Study, EER-290 Prof Rudko, Spring 2002.
- [19] W.Bender, D. Gruhl, N. Morimoto "Technique for data hiding", in Proc.SPIE, 1995, vol. 2420.
- [20] W.Bender, D. Gruhl, N. Morimoto, and A. Lu, "Technique for data hiding", IBM systems journal, 35(3), pp 313-336,1996.
- [21] Stephane Mallat, A Wavelet Tour of Signal Processing,
- [22] Stefan Winkler, Martin Kutter, vers un tatouage à étalement de spectre optimal utilisant le système visuel humain, Sophia Antipolis, France.