République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de La Recherche Scientifique

Ecole Nationale Polytechnique

DEPARTEMENT D'ELECTRONIQUE

Projet de fin d'études
en vue de l'obtention du diplôme
d'ingénieur en Electronique

Thème

Watermarking des images

Encadré par :

Mme L. HAMAMI
Mr L. ABDELOUEL

Etudié par :

Mr. Mourad GUEHAM

Promotion : juin 2003

Remerciements

Je tiens à remercier vivement :

- Dieu tout puissant pour tout ce qu'il ma donné.
- Ma mère, mon père, mes frères et sœurs pour leurs encouragements et leurs patience .
- Mes promoteurs : Mme HAMAMI et Mr ABDELOUEL.
- Les membres du jury.
- Les enseignants, l'administration et le personnel de l'Ecole Nationale Polytechnique.

Watermarking des images

Résumé

Avec le développement des technologies de l'information et de la communication, la protection des droits d'auteurs est devenue plus importante : des outils très simples et largement disponibles peuvent copier et distribuer illégalement beaucoup de données numériques, et plus particulièrement les images. Le tatouage numérique, plus connu sous le nom de watermarking, est l'une des techniques proposées pour résoudre ce problème.

Après la présentation des différentes méthodes de tatouage d'images les plus utilisées et les attaques qu'elles peuvent subir, nous avons exposé deux méthodes de watermarking, l'une opère dans le domaine spatial et l'autre dans le domaine fréquentiel. Les deux méthodes utilisent le même principe : la technique multicouche.

Abstract

With the development of communication and information technologies, copyright protection became more significant: very simple and largely available tools can copy and distribute illegally many numerical data, and more particularly images. Watermarking is one of the techniques suggested to solve this problem.

After the presentation of the most used image watermarking methods and the attacks which they can undergo, we exposed two methods of watermarking, one operates in the space field and the other in the frequency field. The two methods use the same principle: multi-layer technique.

ملخص

مع تطور تكنولوجيات الإعلام و الاتصال، ازدادت أهمية حماية حقوق المؤلفين : فلقد ظهـــرت أدوات بسيطة واسعة الانتشار يمكنها نسخ و توزيع الكثير من المعطيات الرقمية، و خاصة الصور، بطرق غـــير شـــرعية و بسهولة تامة. من بين التقنيات التي اقترحت لمواجهة هذه الآفة، نجد مـــا يســـمى بتقنيـــة الوشـــم الرقمـــي (WATERMARKING).

بعد تقديم مختلف المناهج الأكثر استعمالا في الوشم الرقمي للصورة و الهجمات التي يمكن أن تستهدفها، قمنا بعرض طريقتين للوشم، إحداهما تعمل في الميدان الفضائي و الأخرى في الميدان الترددي. كلتـــا الطـــريقتين تستعملان نفس المبدأ: التقنية المتعددة الطبقات.

Mots clés:

Tatouage d'images, droits d'auteurs, domaine spatial, domaine fréquentiel, technique multicouche.

Keywords:
Image watermarking, copyright, spatial domain, frequency domain, multi-layer technique.

كلمات المفاتيح:

وشم الصور، حقوق المؤلفين، الميدان الفضائي، الميدان الترددي، التقنية المتعددة الطبقات.

SOMMAIRE

Introduction générale

Le développement des technologies de communication et de l'information a permis aux fraudes de se multiplier, provoquant le manque de méthodes concernant la protection des données numériques (images, son, vidéo...). Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité. Une image numérique, diffusée par exemple sur Internet, peut être aisément copiée puis rediffusée sur un réseau ou stockée sur CD-ROM sans prise en compte des droits d'auteurs. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le tatouage (watermarking).

L'objectif de ce Projet de Fin d'Etude est l'étude des algorithmes de tatouage d'images à la fois dans le domaine spatial et le domaine des transformées, ainsi que les différentes attaques que peut subir un système de marquage d'images. L'étude sera couronnée par l'implémentation de deux méthodes : l'une opérant dans le domaine spatiale et l'autre dans le domaine fréquentiel.

Dans le premier chapitre, on expose les principes et les propriétés générales des processus de tatouage d'images. Puis, on présente dans le chapitre 2 des généralités sur les images numériques en définissant les différentes notions de base. Les différentes techniques de tatouage, utilisées actuellement, seront présentées dans le chapitre 3. Le chapitre 4 sera consacré aux attaques contre les systèmes de tatouage d'images (traitement d'images, attaques géométriques, attaques cryptographiques etc..). Dans le chapitre 5, on va étudier deux méthodes en détaille : leur principe, description de la technique, implémentation (schéma d'insertion, schéma de détection ...). En fin, les résultats et les tests de robustesse seront donnés dans le chapitre 6. Le mémoire sera clôturé par la conclusion et les perspectives.

Chapitre : I

Généralités sur le Watermarking des images

Généralités sur le Watermarking des images

I-1 Contexte :

Toute personne habituée à la navigation sur le Web, sait comme il est facile de récupérer des images, des photographies, des sons sans se douter que, dans la plupart des cas, il y ait violation des droits d'auteur. Des outils bon marché et facilement disponibles peuvent copier, manipuler et distribuer aisément des composants multimédias (images, photographies, vidéo, ou sons).
La plupart des temps,

- la duplication génère des copies parfaites.
- la manipulation et l'édition de ces copies trompent même les experts.
- la distribution en masse s'effectue en quelques secondes de manière électronique surtout grâce à Internet.

Le mécontentement vient surtout des propriétaires du fait que leurs créations sont mises à disposition sur Internet sans leur autorisation. Les artistes, les designers graphiques, les photographes et d'autres créateurs sont concernés par ce nouveau style de piratage. Beaucoup voient le **watermarking** comme une solution potentielle pour la protection des copyrights des œuvres numériques de valeur.

I-2 Définition : [1] [2]

Le watermarking (en français, le tatouage numérique) est une procédure qui vise à insérer de manière invisible une information numérique (watermark) à l'intérieur d'un document : image, son, vidéo... En dehors de l'informatique, les filigranes (nom français du watermark) existent dans les billets de banque, les timbres-poste.

Années	1992	1993	1994	1995	1996	1997	1998
Publications	02	02	04	13	29	64	103

Tableau 1.1 Nombre de publications traitant le tatouage numérique

watermarking robuste – watermarking fragile :

La procédure d'insertion d'une marque (typiquement quelques bits d'information) par tatouage numérique peut être conçue pour être soit très résistante soit très sensible aux manipulations. Dans le premier cas, on parle de watermarking robuste, utile aux problèmes liés à la protection des droits d'auteur, où le but est d'extraire la marque d'un détenteur de droit même si les données originales ont été plus ou moins fortement modifiées.

Dans le deuxième cas, on parle de watermarking fragile avec un but opposé : la marque doit disparaître après une manipulation visant à modifier le contenu du document. Le récepteur du document pourra ainsi savoir après vérification de l'existence de watermark, si ce dernier a été modifié ou pas.

I-3 Watermarking – Stéganographie – Cryptographie : [1]

La stéganographie est l'art de cacher un message secondaire dans un message primaire. Le message primaire reste lisible de tous, tandis que le message secondaire n'est lisible que par une ou plusieurs personnes propriétaires de l'information.

La stéganographie se distingue de la cryptographie dans la mesure où l'objectif principal en cryptographie est de rendre illisible un message primaire à toute personne ne possédant pas une information secrète adéquate.

Le watermarking est considéré comme une branche de la stéganographie, il permet de protéger les documents (images, sons, vidéos) tout en les laissant accessibles. Il se distingue par la condition de robustesse qui dépend de l'application et concerne en général la résistance du watermark aux différentes attaques.

I-4 Caractéristiques d'un bon watermark : [3]

Notons que les caractéristiques d'un bon watermark dépendent des domaines d'application. Dans le cas général, ces caractéristiques sont les suivantes :

1. **Imperceptibilité :** La marque doit être imperceptible pour tout être humain, c'est-à-dire qu'il est impossible au non-expert d'entendre ou de voir la marque. Dans le cas du tatouage d'images, on parle d'invisibilité plutôt que d'imperceptibilité. Ceci pose immédiatement le problème suivant : si on trouve un algorithme de compression du medium qui ne garde que les informations perceptibles de celui-ci, alors cette compression fait disparaître la marque. On peut, si l'on craint une telle compression, imposer une notion de déformation minimale du medium par la marque plutôt que celle d'imperceptibilité.

   Notons que certaines filigranes peuvent être visibles mais la plupart des techniques traitées dans la littérature concerne les filigranes invisibles car ils ont un champ d'application très vaste.

2. **Spécificité :** Pour être clairement identifiable lors de son extraction, le watermark doit être suffisamment spécifique. Si les techniques de watermerking veulent conduire à l'élaboration de preuves légales, il faut que les filigranes soient assez spécifiques pour ne jamais condamner un innocent.

3. **robustesse :** L'image tatouée va subir des traitements de nature très variés, comme le filtrage, la compression avec perte, le ré échantillonnage (impression/ scannérisation) ... Il faut donc que le watermark soit assez robuste pour rester décelable tant que la dégradation de l'image par ces traitements reste peu signifiante.

4. **résistance aux attaques (sécurité) :** Plus que les traitements usuels, l'image tatouée va subir l'attaque de pirates voulant effacer le watermark. Ces pirates sont supposés connaître l'algorithme de marquage et donc être en mesure de développer des attaques spécifiques à cet algorithme. Là aussi, il faut que la destruction du watermark ne puisse se faire sans détérioration significative de l'image.

5. **Simplicité :** Les algorithmes d'insertion d'extraction du watermark doivent être de faible complexité et assez simples.

6. **Traitement dans le domaine compressé :**Puisque la plupart des images stockées ou échangées sont sous un format compressé, il doit être possible d'insérer le filigrane directement dans le domaine compressé(il est trop complexe de décompresser, insérer le filigrane puis recompresser l'image).
7. **Interopérabilité :**Il est souhaitable que les images non compressées puissent être tatouées sans avoir a les compresser d'abord, même si le watermarking se fait de plus en plus sur des médias compresses.
8. **Coût :**Le coût de mise en place du système du watermarking doit être raisonnable.

I-5 Les modèles de watermarking : [3]

La figure ci-dessous illustre une forme générique de procède du watermarking.

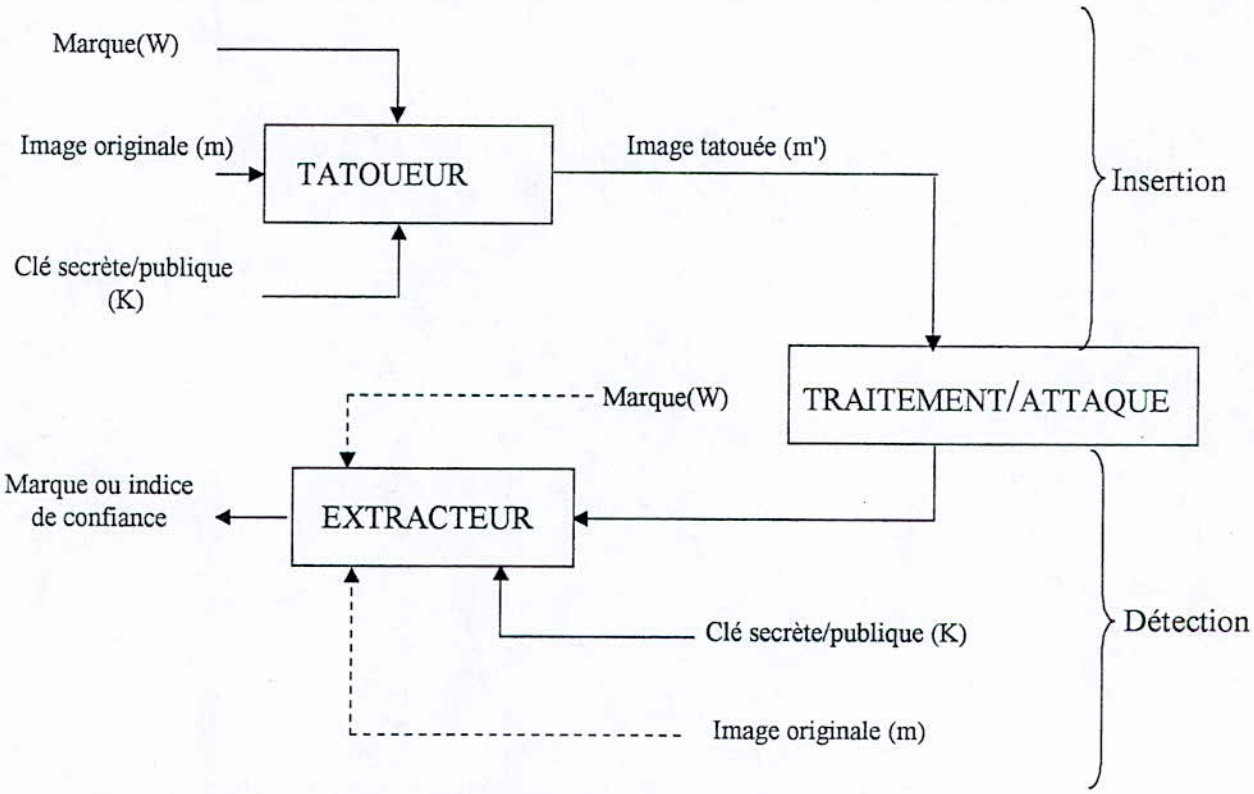


Schéma d'insertion /extraction d'un watermark

Par convention, on désigne par algorithme de tatouage (ou tatoueur) l'algorithme qui insère la marque dans l'image et par algorithme d'extraction (ou extracteur) l'algorithme qui retrouve cette marque. Quand on parlera d'algorithme de marquage,ce sera pour désigner la conjonction d'un tatoueur et d'un extracteur associé

On distingue d'abord deux types d'algorithme de marquage :

Algorithme de type I : si on ne passe pas à l'extracteur la marque w qu'on suppose avoir marqué l'image, charge à lui de déterminer la ou les marques éventuelles tatouées sur l'image, on dit que l'algorithme de marquage est de ***type I.***

Algorithme de type II : un autre cas serait celui ou on passe la marque supposée à l'extracteur, la réponse de celui-ci sera par oui ou par non (ou par un indice de confiance compris entre 0 et 1 dans le cas d'une extraction souple). Les algorithmes répondant à cette spécification sont dits de ***type II.***

D'autres caractéristiques tels le besoin ou non de fournir une marque à l'extracteur entre en jeu. C'est ainsi qu'on distingue les algorithmes de marquage suivants :

Le marquage privé : C'est celui ou l'image originale est donnée à l'extracteur. Dans ce type de marquage, on compare l'image originale à celle récupérée pour extraire la marque.

le marquage privé peut être de type I ou II. Il représente, historiquement, les premières solutions proposées dans le domaine de watermarking, il reste très lourd puisque on doit posséder l'originale de tous les image marquées. La base de données peut alors être gigantesque et peu pratique pour une utilisation sécurisée. Le marquage privé n'est pas donc très satisfaisant.

Le marquage aveugle : C'est celui ou l'extracteur n'a pas besoin de connaître l'image originale m. Seule une clé secrète lui est nécessaire pour extraire la marque.

Dans le marquage aveugle la même clé peut servir au marquage d'un grand nombre d'image (à condition que l'algorithme de marquage soit solide cryptologiquement). De plus la taille de la clé est beaucoup plus petite que celle de l'image qu'elle marque. C'est donc une solution plus satisfaisante que celle du marquage privé qui n'a que peu de chance de trouver des applications viables économiquement.

Le marquage semi-privé :c'est un marquage aveugle de *type II.*

Le marquage publique : c'est un marquage aveugle de *type I.*

Le marquage asymétrique : est celui où l'extraction de la marque ne nécessite pas la connaissance d'un secret. Ceci implique que tout le monde est capable de lire la ou les marques de l'image sans pouvoir les effacer. Cela pourrait se faire par un marquage sans clé ou alors par un tatouage avec clé secrète et une extraction avec clé publique

I-6 Applications :

Les applications du tatouage numérique sont nombreuses ; leur diversité fait que les contraintes qu'elles imposent varient selon l'application envisagée. Les contradictions existant entre ces contraintes rendent impossible la création d'un algorithme universel adaptable à toutes les applications. Il paraît donc nécessaire que la première étape de la conception d'un système de tatouage comprenne la définition des applications auxquelles la méthode sera destinée. On distingue généralement le contrôle du copyright, le fingerprinting, le contrôle de copies, l'insertion d'informations utiles etc.

1- Contrôle du copyright :

Le watermark peut indiquer qui est propriétaire du document. Ainsi, toute personne qui s'en réclamera propriétaire illégalement pourra être condamnée légalement, la marque sera une preuve devant le tribunal.

2- Permissions attachées aux documents (Le contrôle de copies) :

Dans ce cas le watermark contient des informations sur les permissions attachées aux document. Prenons l'exemple d'un film vidéo : il pourrait être marqué en copie illimitée, copie interdite (dans le cas où il est acheté dans le commerce), copie une fois seulement (film diffusé à la télé) charge au matériel de copie de transformer cette marque en une marque de copie interdite.

3- Le fingerprinting :

On peut également marquer l'ayant droit du document, c'est-à-dire la personne à qui le propriétaire a donné une copie. Ainsi, chaque copie du document contient une marque différente (qu'on appelle empreinte) permettant d'identifier son utilisateur. Cette technique est appelée le "fingerprinting".

4- Autres applications :

Le watermarking peut être également utilisé pour un grand nombre d'applications non liées à la sécurité, telle que l'insertion d'informations utiles (meta-données) comme par exemple le nom de la personne se trouvant dans une image, ou un pointeur pour avoir plus d'information sur une image (titre, date, auteur, adresse électronique etc.)

Avant de présenter l'état de l'art des systèmes de tatouage d'images, le chapitre suivant sera consacré à l'étude des images numériques.

Chapitre : II

Généralités sur les images numériques

Généralités sur les images numériques

II-1 Qu'est-ce qu'une image ? [4] [5]

Parmi les nombreuses définitions du mot image, on peut retenir celle qui la définit Comme la représentation exacte, ou la représentation analogique d'une scène réelle, d'un être ou d'une chose par la peinture, la sculpture, le dessin, la photographie, le film,.... Etc. l'image est une représentation bidimensionnelle représentée par une matrice de points, où chacun est susceptible d'être porteur d'une information différente au autres. Mathématiquement, l'image est décrite par une fonction continue F(x,y) de brillance définie dans un domaine borné ; tel que x et y sont les Coordonnées spatiales d'un point de l'image et F est une fonction d'intensité lumineuse(appelée aussi luminance ou brillance). Sous cet aspect, l'image est inexploitable par l'ordinateur, ce qui nécessite sa numérisation. L'opération de numérisation se décompose en deux étapes :

- **L'échantillonnage :** qui consiste à transformer le signal continu en une suite d'échantillons ou de points élémentaires, souvent appelés pixels (*Picture elements).*
- **La quantification :** qui consiste à mesurer les échantillons selon un choix limité de valeurs appelées niveaux de quantification.

II-2- L'image numérique : [6]

L'image numérique est une collection de points (pixels) réparties en lignes et en colonnes, ayant chacun comme caractéristique un niveau de gris ou de couleur prélevé à l'emplacement correspondant dans l'image réelle. L'image numérique est représentée comme une matrice bidimensionnelle de valeurs numérique $F(x,y)$ où :

x et y : coordonnées cartésiennes d'un point de l'image.
$F(x,y)$: Niveau de gris ou de couleurs en ce point.

L'image numérique est la base de traitement d'images.

II-3 Caractéristiques d'une image numérique :

II-3-1 Pixel : [7]

Contraction de l'expression anglaises « *Picture elements* : éléments d'image » le pixel est le plus petit point de l'image. Si le bit est la plus petite unité d'information que peut traiter un ordinateur, le pixel est le plus petit élément que peuvent manipuler les matériels et logiciel d'affichage et d'impression.

En général, dans le cas d'une image à niveau de gris;chaque pixel est codé sur un octet ce qui donne 256 niveaux de gris différents. Dans une image couleur (R,B,V), un pixel peut être représenté sur trois octets. Un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B) ; ce qui donne 16,7 millions de couleurs différentes.

II-3-2 Résolution : [8]

La résolution d'une image est définie par un nombre de pixels par unité de longueur de la structure à numériser (classiquement en dpi (dots per inches) ou ppp (points par pouce)). Ce paramètre est défini lors de la numérisation et dépend principalement des caractéristiques du matériel utilisé lors de processus de numérisation. Plus le nombre de pixels est élevé par unité de longueur de la structure à numériser, plus la quantité d'information qui décrit cette structure est importante et plus la résolution est élevée. La résolution d'une image numérique définit le degré de détail qui va être représenté sur cette image.

A noter que certains matériels de numérisation permettent de faire varier la résolution d'acquisition.

NB : Cette notion est distincte de *la résolution du format de l'image* qui correspond au nombre de pixels qui compose l'image en hauteur et en largeur c.a.d : la taille de l'image en pixels (512 pixels par 512 pixels par exemple)).

Les phénomènes de numérisation dépendent des 2 équations suivantes :
(X * résolution) = x pixels
(Y * résolution) = y pixels

où X et Y représente la ***taille (en pouces ou mètres)*** de la structure à numériser,
où 'résolution' représente la résolution de numérisation,
et où x et y représente la ***taille (en pixels)*** de l'image.

Exemple théorique :

Une image de 1*1 pouce scannée a 100 dpi aura une taille x,y de 100 pixels sur 100 pixels
(1*100)*(1*100)= 100 pixels sur 100 pixels.
Notons que : un pouce=2,54 centimètres.

II-3-3 Bruit :

Un bruit (parasite) dans une image est un phénomène de brusque variation d'un pixel par rapport à ses voisins. Il provient généralement des dispositifs optiques et électroniques.

II-3-4 Histogramme : [6] [9]

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (ou couleur) dans l'image. Il permet de donner un grand nombre d'information sur la distribution des niveaux de gris (ou couleur) et de localiser entre quelles bornes sont réparties la majorité des niveaux de gris. Pour diminuer l'erreur de quantification, pour comparer deux images obtenues sous des éclairages différents ou encore pour mesurer certaines propriétés sur une image, on utilise souvent l'histogramme correspondant. L'histogramme peut être utiliser aussi pour améliorer la qualité d'une image (Rehaussent d'image) en introduisant quelques modifications, pour pouvoir en extraire les informations utiles.

II-3-5- Luminance : [9]

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par unité de surface perpendiculaire à la direction d'émission. Souvent le mot luminance est substitué au mot brillance.

II-3-6- Contraste :

C'est la variation relative de la luminance entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Si L_1 *et* L_2 sont les degrés de luminosité respectivement de deux zones voisine A_1 *et* A_2 d'une image, le contraste C est défini par le rapport :

$$C = \frac{L_1 - L_2}{L_1 + L_2}$$

Notons qu'il existe beaucoup d'autres définitions du contraste dans la littérature.

II-3-7- Image à niveaux de gris : [10]

Le niveau de gris est la valeur de l'intensité lumineuse en un point. Le pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaire. Donc pour représenter les images à niveau de gris, on peut attribuer à chaque pixel de l'image une valeur correspondante à la qualité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255. Chaque pixel n'est donc plus représenté par un bit comme dans les images monochromes, mais par octet. Le nombre de niveaux de gris dépend du nombre de bits utilisés pour décrire l'intensité lumineuse de chaque pixel de l'image. Plus ce nombre est important, plus les niveaux possibles sont nombreux.

II-3-8- Image en couleur : [5]

La couleur a envahit le domaine du traitement d'images, depuis que les applications multimédias utilisent le plus souvent des images en couleurs. Une image numérique en couleur est un ensemble de points colorés disposés les uns à coté des autres. On peut montrer qu'un point coloré peut être obtenu de trois couleurs appelées composantes ou primaire mélangées en doses ou intensités . Les systèmes émettant de la lumière (écran d'ordinateur,.....) sont basés sur le principe de la synthèse additive : les couleurs sont composées d'un mélange de trois composantes : Rouge, Vert et Bleu (modèle RVB) ou RGB (red, green, blue).

En standard, on utilisera des systèmes dans lesquels chaque composante de chaque pixel est stockée sur 8 bits (aussi dit true color) ce qui donne au total 24 bits pour chaque pixel; il y a alors environ 16,7 millions de teintes possibles. On utilise aussi des systèmes avec 5 bits par composante (32768 couleurs), voire 6 bits pour le vert, 5 bits pour le bleu et 5 bits pour le rouge (65536 couleurs).

II-4- Stockage des images :

Afin d'être convenablement représentée, une image est stockée sous forme d'un fichier. Ce dernier est composé principalement de deux parties. La première appelée l'entête du fichier et contient des informations générales sur l'image (hauteur, largeur, nombre de couleurs utilisées, ...). La deuxième partie représente l'image proprement dite (la couleur des pixels).

Parmi les formats standards de fichiers image existant, on cite : TIFF(Tagged image file format), BMP, GIF(Graphics Interchange Format), PNG(Portable Network Graphics), EPS(Encapsuled PostScript), WMF (Windows MetaFile), Pict, PSD, TGA, PCX ... sans oublier la norme JPEG [9] qui se base sur la technique de compression par DCT. Son principe part du fait que la répartition énergétique des images est complètement localisée au niveau des basses fréquences, ce qui donne des coefficients transformés de très faibles valeurs pour les haute fréquences et donc, permettant une certaine dégradation du signal, plus au moins grande selon le cas, on peut négliger ces coefficients, ce qui permet d'aboutir à un ordre de compression qui peut être considérable.

II-5- Mesure de la qualité d'une image : [5] [11]

Nous avons dit auparavant que les techniques de tatouage apportent des distorsions (dégradations) aux images. Pour juger la performance d'un tatoueur en terme de qualité visuelle de l'image tatouée, plusieurs méthodes d'évaluation ont été utilisées (ces méthodes sont très utilisées dans le domaine de la compression d'images : pour évaluer la qualité des images compressées) :

II-5-1- Les méthodes objectives :

Des mesures de la qualité d'image ont été standardisées, ce sont des critères dits objectifs, c-à-d obtenus à partir des calculs simples.

L'erreur quadratique moyenne (EQM) :

$$EQM = \left(1/N^2\right)\sum_{n=1}^{N}\sum_{m=1}^{N}\left(X(m,n)-X'(m,n)\right)^2$$

Tel que :

N : Dimension de l'image (N×N pixels)
X : Image d'origine ($X(m,n)$: niveau de gris du pixel dont les Coordonnées sont (m , n))
X' : Image tatouée.

Toutefois la mesure de l'EQM normalisée (EQMN) donne de meilleurs résultats.

$$EQMN = \frac{\sum_{n=1}^{N}\sum_{m=1}^{N}(X(m,n)-X'(m,n))^2}{\sum_{n=1}^{N}\sum_{m=1}^{N}(X(m,n))^2}$$

Une image tatouée est dite de bonne qualité si : EQMN $\leq$ 0.25.

Le rapport signal sur bruit (SNR).

C'est une mesure simple qui a montré de bonnes performances. Elle est définie par :

$$SNR_{db} = 10\log\frac{E\left[X(m,n)^2\right]}{EQM}$$

avec : $E[X(m,n)^2] = (1/N^2)\sum_{n=1}^{N}\sum_{m=1}^{N}(X(m,n))^2$

Le rapport signal sur bruit crête (PSNR).

Le PSNR (*peak signal- to- noise ratio)* est plus souvent utilisé en traitement d'images et est donné par :

$$PSNR_{db} = 10\log_{10}\frac{NdG^2{}_{\max}}{EQM}$$

Où :

$NdG_{\max}$: est le niveau de gris maximum (image numérique sur 8 bits on a : $NdG_{\max}$=255).

Ces mesures de qualité citées ci-dessus sont très utilisées car elles sont très simples à calculer. Mais ne correspondant pas à des mesures fiables de ressemblance visuelle entre deux images.

II-5-2- Les méthodes subjectives :

L'EQM est le critère objectif le plus commun, seulement il ne s'adapte pas bien avec les mesures subjectives. Des recherches récentes ont cependant donné une analyse profonde du système visuel humain (HVS). Elles nous ont permis de distinguer deux méthodes basées sur le calcul de l'opinion moyenne d'un groupe d'observateurs humains.

Méthode de dégradation :

Un groupe de personnes examine un ensemble d'image selon des conditions de visualisation prédéfinis. Les personnes choisies, associent à chaque image une valeur subjective.

Ces valeurs correspondent à des catégories de qualités générales ou des distorsions, selon une échelle donnée dans le tableau suivant :

CATEGORIE	DEGRADATION	QUALITE
5	IMPERCEPTIBLE	EXELLENTE
4	PECEPTIBLE MAIS NON GENANTE	BONNE
3	LEGEREMENT GENANTE	PASSABLE
2	GENANTE	MEDIOCRE
1	TRES GENANTE	MAUVAISE

Tableau 2.1 Echelle de comparaison.

Méthode comparative :

Deux images A et B sont représentées, l'une est la référence l'autre est à évaluer. L'observateur qui ignore laquelle est la référence, évalue la qualité de A et B suivant une échelle continue et bornée

Après avoir donner des généralités sur les images numériques, on va présenter dans le chapitre suivant l'état de l'art des systèmes de tatouage d'images.

Chapitre : III

Etat de l'art

Etat de l'art

III-1- Introduction :

Les différents algorithmes de tatouage d'images numériques se distinguent essentiellement selon les critères suivants [19] :

- **Le type de schéma d'insertion de la signature :** soit un schéma additif (la marque est ajoutée sans modifier l'image originale) soit un schéma substitutif appelé aussi « virtuel » (on supprime dans l'image certaines de ses composantes, cette substitution formant le support de la marque) .
- **Le type de schéma d'extraction de la signature :** le besoin ou non de fournir à l'extracteur : une marque(algorithme de type I, de type II), l'image originale(marquage privé, aveugle, semi privé, public ..), une clef secrète (marquage symétrique, asymétrique).

- **La stratégie sur la marque :** la manière de transformer la signature (ou le message) en marque numérique et la mise en forme de celle-ci vis-à-vis de l'image à marquer (utilisation d'un masque psychovisuel adaptant la marque à l'image à tatouer, sélection de sites prépondérants dans l'image pour l'insertion, utilisation de codes correcteurs ..).

- **Le choix de l'espace de travail :** la marque peut soit être insérée dans le domaine spatial, soit dans le domaine transformée (DCT, DFT, Ondelettes, fractales)

Nous avons opté pour ce dernier critère pour l'étude de l'état de l'art du watermarking des images. Nous allons présenté deux grandes familles de méthodes : celles qui opèrent dans le domaine spatial et celles qui opèrent dans un domaine transformé (fréquentiel).

III-2- Méthodes spatiales :

III-2-1 Modification des bits de poids faible : [3]

Pour s'assurer de l'invisibilité de la marque, les premiers algorithmes allaient inscrire la marque dans les bits de poids faible de la luminance de l'image . Cette technique, aisée à mettre en œuvre permet de stocker n'importe quel type d'information avec une dégradation négligeable de l'image .

Elle ne résiste cependant ni à l'ajout d'un bruit blanc ni à la compression JPEG . Il est donc très facile de supprimer ou du moins de rendre illisible une marque dissimulée de cette manière .

Cette technique peut donc éventuellement servir à véhiculer une information mais sans que cette dernière soit protégée .

III-2-2 Inscription d'information dans des blocs de l'image :

Une deuxième méthode consiste en la définition de blocs de pixels, puis en la modification des valeurs des pixels de ces blocs suivant l'information que l'on souhaite y inscrire : pour un bloc donné, on augmente par exemple les valeurs des pixels lorsque l'on désire inscrire1, et on les diminue pour inscrire 0.

Le choix de l'emplacement des blocs dans l'image peut être fixe ou bien paramétré par une clef secrète (voir par exemple la technique du *patchwork*). L'introduction d'une telle clef est particulièrement importante si l'on utilise des marques qui sont des empreintes digitales (fingerprint) : en effet, si les blocs sont pris aux mêmes endroits pour tous les marquages, alors on peut par une simple différence de deux versions marquées d'une même image déterminer l'emplacement d'un certain nombre de ces blocs ; il suffirait alors de modifier légèrement la valeur des pixels dans ces blocs pour rendre la marque illisible .

Cette technique permet de dissimuler une marque qui résiste assez bien aux compressions avec perte ainsi qu'à la numérisation après impression. Elle ne permet cependant que l'inscription de peu d'information (on inscrit un seul bit par bloc); en plus de ça, elle ne résiste pas aux déformations géométriques .

III-2-3- La méthode du *Patchwork* : [19] [20]

Cette méthode, introduite par Bender et al, est classée dans la catégorie des méthodes à schéma semi-privé. Elle est basée sur le principe suivant :

A l'implémentation, l'algorithme sélectionne pseudo-aléatoirement (avec une clef secrète K, employée pour initialiser un générateur pseudo-alèatoire) deux ensembles de pixels D_+ D_- de N éléments chacune. Les valeurs des luminances $I_{n,m}$ de ces pixels sont alors modifiées selon les formules suivantes :

$$I^*_{n,m} = I_{n,m} - \alpha \quad \text{si } (n,m) \in D_+$$
$$I^*_{n,m} = I_{n,m} + \alpha \quad \text{si } (n,m) \in D_-$$

Où α est une constante fixée appelée « force du tatouage » ou « facteur d'accroissement » .
Considérons la quantité S suivante :

$$S = \frac{1}{N}\left(\sum_{(n,m)\in D_+} I_{n,m} - \sum_{(n,m)\in D_-} I_{n,m}\right)$$

si les pixels considérés sont bien répartis dans l'image, on aura $S=\mu$ où μ est une quantité proche de 0 .

A la détection on calcule la quantité $S^* = \frac{1}{N}\left(\sum_{(n,m)\in D_+} I^*_{n,m} - \sum_{(n,m)\in D_-} I^*_{n,m}\right)$

Si l'on connaît la clef définissant les deux ensembles D_+ et D_-, la valeur attendue de la somme est $S^* = S+2\alpha = \mu+2\alpha \cong 2\alpha$.

Si l'on ne connaît pas cette clef, on ne peut pas retrouver les deux ensembles, on ne peut que générer deux ensembles différents. Si ces ensemble sont générés pseudo-aléatoirement (avec une autre clef K'), S* est alors nulle($S^* = \mu' \cong 0$) .

Ce principe de détection est fondé sur le résultat statistique suivant : si l'on choisit pseudo-aléatoirement deux ensembles de pixels de même cardinal, l'espérance de la somme de leur différence est nulle. Les deux sous-ensembles sélectionnés par les clefs doivent être grands et bien repartis dans l'image pour que cette propriété soit vérifiée.

On peut remarquer que l'implantation de la marque peut se résumer à l'addition de l'image avec une matrice W, de même taille que l'image et contenant la valeur $+\alpha$ pour les pixels de l'ensemble D_+, $-\alpha$ pour les pixels de D., 0 sinon. Si I est l'image originale, I* l'image tatouée, on obtient :

$$I^* = I + W$$

où W est une matrice pseudo-aléatoire obtenue à partir de la clef K.

Dans cette méthode on ne cherche en aucun cas à extraire le tatouage, on répond seulement par oui ou par non à la question : une personne est-elle en possession de l'information secrète (la clef K) ayant permit de générer le tatouage ?

Cette méthode de base est facile à mettre en œuvre mais elle n'est bien sûr pas très robuste (Elle ne résiste pas aux petites déformations géométriques ni au filtrage). Cependant, différentes extensions de cet algorithme ont vu le jour, elles permettent par exemple d'accroître la résistance du système à des opérations de filtrage sur l'image en considérant non plus des ensembles de pixels mais des ensembles de blocs.

III-2-4- La méthode de l'étalement de spectre (Spread Spectrum): [21] [22]

Il est possible de voir le problème de tatouage comme un problème de communication. De ce point de vue, le tatouage consiste à transmettre un message dans un environnement bruité, où l'image hôte est considérée comme un canal de transmission, la marque comme le message à transmettre et les attaques comme du bruit. Les outils utilisés en télécommunication s'imposent donc d'eux même.

Une des techniques largement utilisées en télécommunication est l'étalement de spectre[1]. Son principe est d'étaler le spectre d'un message (la marque) afin de se servir de toute la bande passante du canal(dans notre cas : pour se servir de toute l'image).

L'étalement du spectre du message est classiquement effectué en modulant la donnée par une séquence pseudo-aléatoire de fréquence bien supérieure. Cette méthode peut être utilisée dans les deux domaines spatial ou fréquentiel .

[1] Cette technique qui date des années 40 a d'abord été utilisée pour des applications militaires et est très utilisée aujourd'hui en télécommunication, par exemple pour les téléphones cellulaires, le GPS (Global Positioning Satellite) et le VSAST (Very Small Aperture Satellite Terminals).

L'insertion et la détection selon cette méthode suivent dans la majorité des cas l'exemple décrit ci-dessous :

Exemple : (étalement par séquence directe)

Pour insérer un message M de 8 bits dans une image 64*64, la démarche à suivre se présente comme suit :

- On découpe l'image en 8 blocs de taille 16*32 .
- On génère une Séquence Binaire Pseudo Aléatoire S (SBPA) à l'aide d'une clé secrète, uniquement connue du propriétaire. Cette séquence S de longueur 512=16*32 est composée uniquement de +1 et de –1 et a une moyenne nulle (c'est à dire autant de –1 que de +1).
- On transforme la Séquence S en un signal à deux dimensions(SBPA 2D) de taille 16*32 : pour cela on remplit ligne par ligne ce signal 2D.
- On forme la marque W : on remplit chaque bloc *i* par +S (si le bit *i* du message est égal à 1) ou par –S (si le bit *i* du message est égal à 0). C.a.d chaque bit *i* est étalé par la séquence S (modulation du message M par la séquence S).
- La marque W ainsi formée (que l'on peut moduler par un coefficient α pour l'intensifier) est ajoutée à l'image.

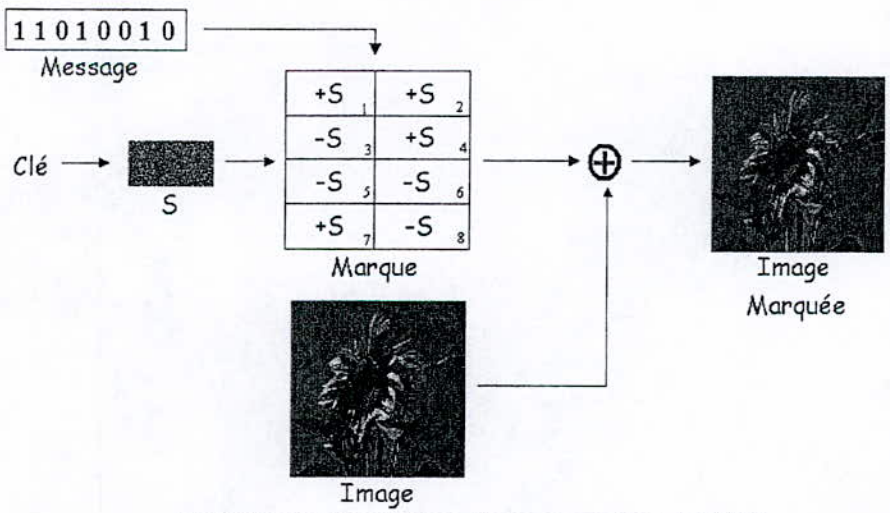


Figure3.1 Insertion pour un découpage en blocs de16*32

- La détection se fait par corrélation: il suffit de calculer l'intercorrélation de la marque avec l'image marquée. Ce calcul se fait simplement en multipliant pixel par pixel les deux images et en faisant ensuite la somme des produits.

Appelons I l'image initiale, W la marque, W_1 une marque différente et I_w l'image marquée ($I_w = I + W$)

- On calcule l'intercorrélation $<I_w,W> = <I+W,W> = <I,W> + <W,W>$
$= \varepsilon + 4096$ (avec $\varepsilon << 64*64=4096$)
- Pour une marque différente on aurait $<I_w,W_1> = <I,W> + <W_1,W>$
$= \varepsilon + \varepsilon << <I_w,W>$

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

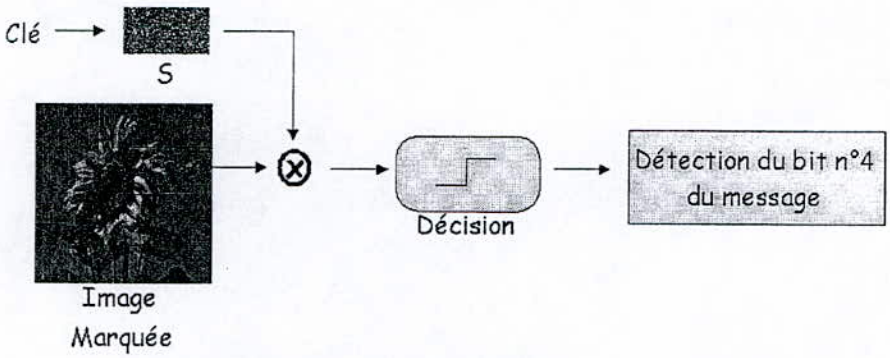


Figure3.2 Détection pour un découpage en blocs de 16*32

III-2-5- Tatouage d'image utilisant le Système Visuel Humain (SVH) : [23]

Dans les méthodes présentées ci-dessus la marque est ajoutée uniformément à la valeur des pixels de l'image. La contrainte d'invisibilité n'est pas considérée. L'idée permettant de remédier à ce manquement est de pondérer l'insertion de la marque par une matrice dépendant des caractéristiques de l'image et de considérations psychovisuelles. Les amplitudes des éléments constituant la marque seront augmentées dans les zones où l'image est très texturée, elles seront diminuées dans les zones très uniformes.

Ainsi, l'utilisation de modèles psychovisuels en tatouage d'images permet de répondre à deux contraintes :

_ L'algorithme garantit l'invisibilité du marquage

_ Le compromis invisibilité-robustesse est optimisé

Le principe est de maximiser la force de tatouage pour chaque pixel selon les caractéristiques de l'image et des critères psychovisuels. L'implémentation de la marque est alors donnée par la relation :

$$I^*(i, j) = I(i, j) + \alpha_I(i, j) .W(i, j)$$

Le calcul de la matrice des forces de tatouage α_I est fondé sur une particularité du système visuel humain (SVH) appelée effet de *masquage*. Le masquage a lieu lorsqu'un signal (la marque) est rendu imperceptible par la présence d'un autre signal dit masquant (l'image). Plusieurs modèles de masque ont été utilisé en tatouage d'image, certains sont dans le domaine spatial, d'autres dans le domaine fréquentiel .

Pour une image donnée I de taille (N * N), le masque M_I est une image de même taille dont la valeur au pixel (i, j) donne l'amplitude maximale de la modification que le pixel (i, j) de

l'image peut supporter sans que les dégradations résultantes ne soient perceptibles. En d'autres termes, le masque d'une image I est une matrice M_I telle que si I* est une image de même taille que I, et si la relation :

$$| I(i, j) - I^*(i, j) | \leq M_I (i, j)$$

est respectée pour tous les pixels (i, j) de l'image, l'image I* sera perceptuellement identique à I .

III-3- Méthodes fréquentielles :

III-3-1- Cas général : [21] [19]

Les méthodes fréquentielles sont des méthodes plus récentes dont le principe est d'insérer la marque non pas directement dans l'image mais dans le domaine transformé : DFT[2], DCT[3], DWT[4].. . Pour retrouver l'image marquée, on effectue la transformée inverse. La figure suivante décrit le schéma d'insertion dans le domaine transformé (la détection se fait généralement par corrélation) :

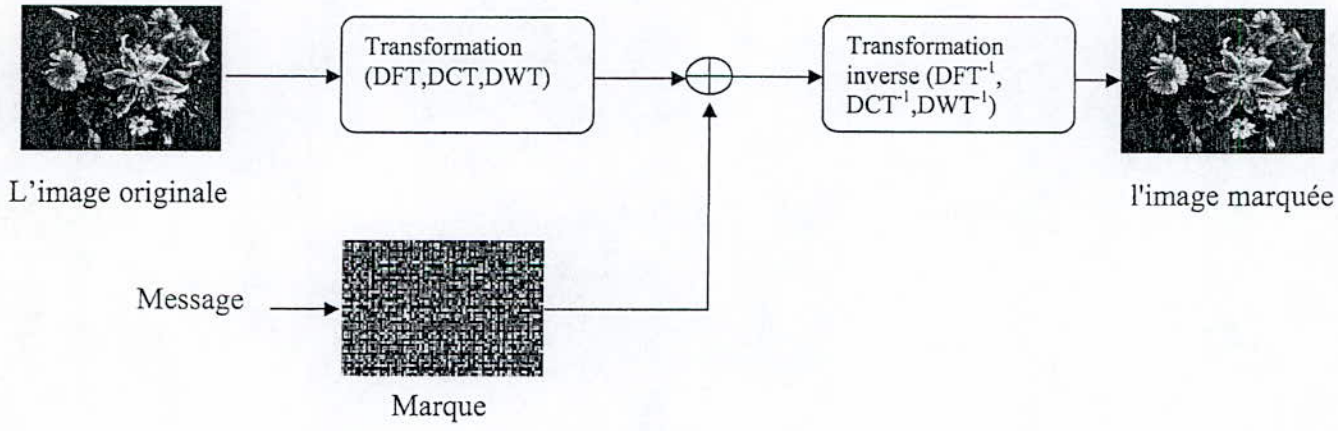


Figure3.3 Insertion d'une marque dans le domaine transformé

Intérêt de l'utilisation de domaines transformés :

Ces méthodes ont été développées à partir des connaissances acquises auparavant en codage de source. Les auteurs de ces méthodes espèrent ainsi en travaillant dans le domaine transformé, anticiper et prévenir au moins les attaques liées à une compression avec perte (comme la compression jpeg pour la DCT, ou jpeg2000 pour la DWT).Ils espèrent également pouvoir travailler plus rapidement en couplant le tatouage d'images avec le codage de source. En d'autres termes, le tatouage est réalisé directement sur le flux compressé. Le dernier point opérant en faveur d'un tatouage dans le domaine transformé est qu'il est possible de bénéficier

[2] Transformée de Fourier discrète .
[3] Transformée en cosinus discrète .
[4] Transformée en ondelettes discrète .

des études psychovisuelles déjà menées en codage de source pour gérer les problèmes de visibilité.

Notons que l'utilisation du domaine fréquentiel (en utilisant ces trois transformées) ne nécessite pas trop de temps de calculs grâce aux algorithmes de transformations rapides .

Dans cette section, nous allons présenter quelques exemples de schémas de tatouage utilisant des domaines transformés.

III-3-2- Insertion dans le domaine DCT :

III-3-2-1- La Transformée par Cosinus Discrète :

La DCT (= Discret Cosinus Transform) est une dérivée des transformées de Fourier. Elle transforme une matrice NxN en une autre matrice NxN, dont les valeurs sont rangées selon leur fréquence : les basses fréquences sont situées en haut a gauche et les hautes fréquences en bas a droite. Les basses fréquences sont les plus importantes pour l'image, tandis que les hautes fréquences sont moins importantes. La valeur de coordonnées (0 , 0) correspond à la valeur moyenne des éléments de la matrice .

Si N désigne le nombre d'"échantillons" x et y, la DCT fait correspondre à chaque valeur de Y(x,y) une valeur de F(u,v) donnée par la formule :

$$F(u,v) = \frac{2}{N} c(u).c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Y(x,y) \cos(\frac{\pi}{N} u(x+\frac{1}{2})).\cos(\frac{\pi}{N} v(y+\frac{1}{2}))$$

avec : $\nu, \mu, x, y = 0...N-1$

$c(j) = \frac{1}{\sqrt{2}}$ si j=0

$c(j)=1$ si j>0

Le calcul de la DCT a pour but de préparer la matrice a l'étape suivante[5] : l'insertion de la marque

Pour revenir à l'image, on utilise la formule suivante :

$$Y(x,y) = \frac{2}{N} \sum_{v=0}^{N-1} \sum_{u=0}^{N-1} c(u)c(v)F(u,v) \cos(\frac{\pi}{N} u(x+\frac{1}{2})).\cos(\frac{\pi}{N} v(y+\frac{1}{2}))$$

[5] La DCT est aussi l'étape caractéristique du format JPEG, elle est propre à ce format et c'est autour de cette étape que tourne tout le fonctionnement de la compression JPEG.

III-3-2-2 Tatouage basé sur la modification des coefficients DCT de plus grandes amplitudes : [22]

Cox et al ont présenté une méthode de tatouage à étalement de spectre dans les coefficients DCT de l'image. On applique la DCT à toute l'image puis on insèrent la signature dans les basses fréquences, c'est à dire dans les composantes les plus significatives(celles qui sont nécessaires à la compréhension de l'image).

La marque W, générée à l'aide d'une clef secrète K, modifie les coefficients DCT de plus grandes amplitudes (exceptée la composante continue I(0,0)) selon l'une des relations suivantes :

$$I^*(i,j) = I(i,j) + \alpha\, w(i,j) \quad (1)$$
$$I^*(i,j) = I(i,j)\,(1 + \alpha\, w(i,j)) \quad (2)$$
$$I^*(i,j) = I(i,j)\, e^{\alpha\, w(i,j)} \quad (3)$$

avec :

$I^*(i,j)$: coefficient DCT de l'image marquée .
$I(i,j)$: coefficient DCT de l'image originale .
α : force du tatouage .
$w(i,j)$: les éléments de la marque W .

Le schéma ci-dessous illustre l'étape d'insertion :

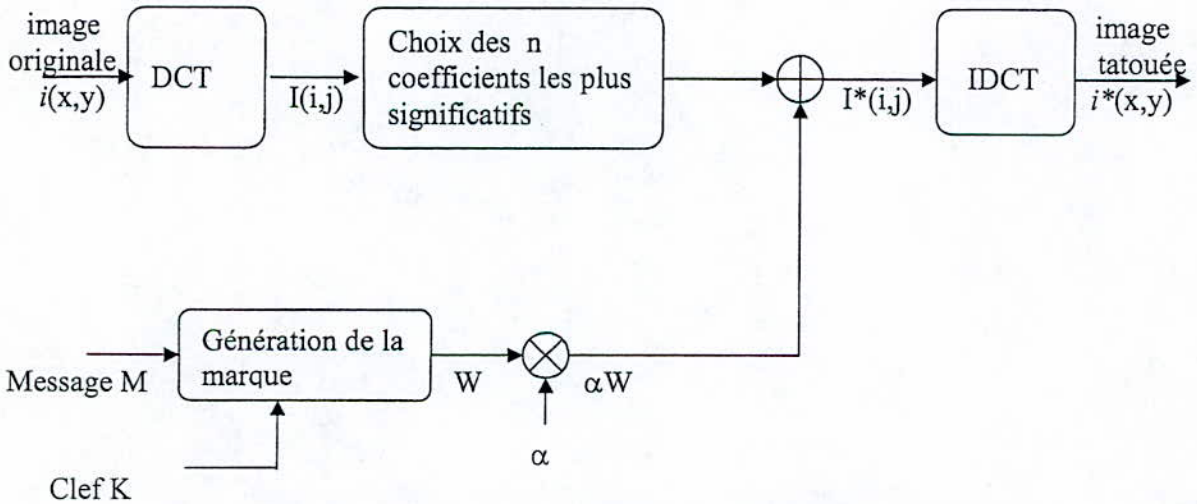


Figure3.4 Insertion de la marque dans le domaine DCT selon la relation (1)

L'extraction se fait en inversant le processus d'insertion et en utilisant l'image originale pour retrouver la marque. La marque W' extraite est comparée à la marque originale W par un calcul de corrélation(coefficient de corrélation *cc*). La décision est de type « oui ou non ».

$$cc = \frac{\sum_i \sum_j w'(i,j) w(i,j)}{\sqrt{\sum_i \sum_j [w'(i,j)]^2} \sqrt{\sum_i \sum_j [w(i,j)]^2}}$$

La décision se fait en comparant cc avec un seuil s (si W et W' sont identiques on aura cc=1) .

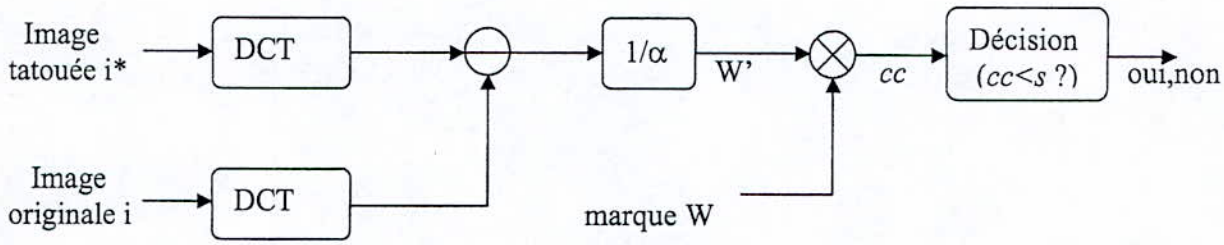


Figure3.5 détection de la marque

Cette méthode est très robuste et donne de bons résultats face aux attaques de type changement d'échelle, compression JPEG, passage à l'analogique puis au numérique, et attaque par collusion. Le principal désavantage de cette méthode est que l'image originale doit être connue pour permettre l'extraction de la marque.

III-3-2-3 Algorithme de Koch et Zhao : [31] [24]

L'idée de base est de décomposer l'image en blocs de 8 * 8 pixels, dont certains sont choisis par une clef K pour porter le message.

Les blocs sont ensuite transformés par DCT, puis les modifications se font sur un triplet (déterminé lui aussi par la clef) de coefficients basses fréquences (C1, C2, C3). Pour assurer l'invisibilité de la marque, on ne modifiera jamais les trois coefficients des plus basses fréquences. Le triplet modifié doit respecter des contraintes d'ordre différentes selon que la marque à implanter W porte le bit 0 ou 1 :

Si : wi = 1 on modifie les trois coefficients pour avoir $C1 > C3 + C^{te}$ et $C2 > C3 + C^{te}$
(si ces deux relations sont déjà vérifiées ; les trois coefficients ne seront pas modifiés)

si : wi = 0 on modifie les trois coefficients pour avoir $C1 < C3 - C^{te}$ et $C2 < C3 - C^{te}$
(si ces deux relations sont déjà vérifiées ; les trois coefficients ne seront pas modifiés)

Pour améliorer la robustesse, la modification se fait sur les valeurs quantifiées du triplet . L'insertion n'est possible que si la différence entre les composantes pointées n'est pas trop importante (ce qui est généralement le cas pour des images réelles).

La détection consiste à la lecture de l'ordre des coefficients, elle ne fait pas appelle à l'image originale.

III-3-2-4 La méthode DCT-PM (DCT phase modulation) : [25]

Cette méthode est basée sur la modification des signes de quelques coefficients DCT de grandes et de moyennes amplitudes .

Pour insérer, par exemple, un message de 100 bits dans une image 512x512 avec cette méthode, on effectue les étapes suivantes :

On décompose l'image x(i,j) en deux parties : xa(i,j) et xb(i,j) . L'image xa de taille 384x384 contient la partie centrale de l'image originale, xb contient le reste de l'image . la figure ci-dessous montre les deux parties obtenues :

l'image original x(i,j) xa(i,j) xb(i,j)

Figure3.6 décomposition de l'image en deux parties

La même marque sera insérée dans les deux parties. La raison pour laquelle on a décomposé l'image de cette manière est d'atténuer l'effet des attaques qui visent les bords de l'image (comme le cropping) ou celles qui affectent son centre. L'utilisation de ce double tatouage augmentera la robustesse du système de marquage .

La partie xa est entièrement transformée par la DCT, les coefficients obtenus sont ensuite classés par ordre décroissant . On choisit pseudo aléatoirement 100 coefficients de plus grandes amplitudes dont on changera le signe selon le bit à insérer . Pour avoir xa* en effectue la DCT^{-1} .

Pour xb, on procède d'une manière similaire seulement on le fait sur des blocs 32x32 : on choisit 100 bloc d'une façon pseudo aléatoire et pour chaque bloc on sélectionne un coefficient dont on changera le signe (selon le bit à insérer) .

L'image marquée résultante sera donc :

$$x^*(i,j) = xa^*(i,j) + xb^*(i,j) .$$

Pour détecter la marque on doit connaître les positions des coefficients porteurs d'information . Il faut donc être en possession de la clef secrète qui a été utilisée dans la phase d'insertion .

III-3-2-5 Algorithme BNA-CDMA : [26] [27]

Cette méthode a été conçue essentiellement pour résister aux attaques géométriques (rotation, translation, changement d'échelle ..) qui mettent en défaut la plupart des systèmes de tatouage : par exemple, une simple rotation de quelques degrés de l'image tatouée entraîne une désynchronisation qui rend la marque totalement indétectable .

La méthode de tatouage (combinaison de plusieurs techniques BNA, DCT, CDMA) est composée des trois étapes suivantes :

1- la normalisation de l'image originale en utilisant un « algorithme de normalisation aveugle » BNA[6] : cette technique de normalisation a été utilisée depuis longtemps dans le domaine de la reconnaissance des formes (reconnaître les mêmes formes avec des tailles et des orientations différentes), M.ALghoniemy et A.H.Tewfik étaient les premiers à l'utiliser dans le domaine du watermarking .

2- La transformation par DCT de l'image normalisée puis l'insertion de la marque dans les moyennes fréquences en utilisant la technique CDMA : Code Division Multiple Access (technique utilisée en communication). Une clef secrète est utilisée pour générer la marque .

3- Retour à l'orientation et à l'échelle originale en effectuant les transformations inverses de celles utilisées dans l'étape 1 .

Pour la détection :

a) On détermine l'image normalisée à l'aide de l'algorithme BNA .
b) On extrait la maque par un calcul de corrélation (en utilisant la clef secrète) .

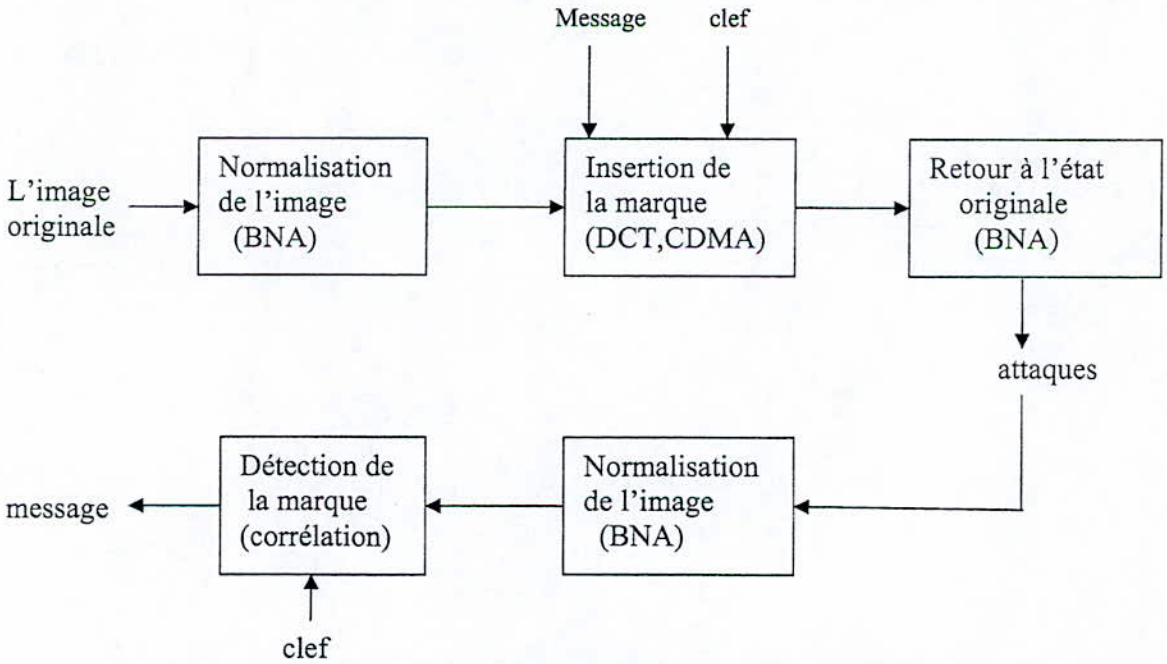


Figure3.7 système de tatouage basé sur la normalisation d'image

[6] BNA : Blind Normalisation Algorithm , c'est un algorithme basé sur le calcul des moments géométriques de l'image .

III-3-3- Insertion dans le domaine DFT :

III-3-3-1- La transformée de Fourrier discrète 2D :

La transformée de Fourrier discrète 2D d'une image $I(x,y)_{0\le x,y\le N-1}$ est donnée par :

$$F(u,v)=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} I(x,y)e^{-j\frac{2\pi}{N}(xu+yv)} \qquad u,v = 0,1,2\ldots N\text{-}1$$

les valeurs F(u,v) sont les coefficients DFT de l'image I(x,y) . Le coefficient F(0,0) est appelé « la composante continue » .

la transformée inverse IDFT est donnée par :

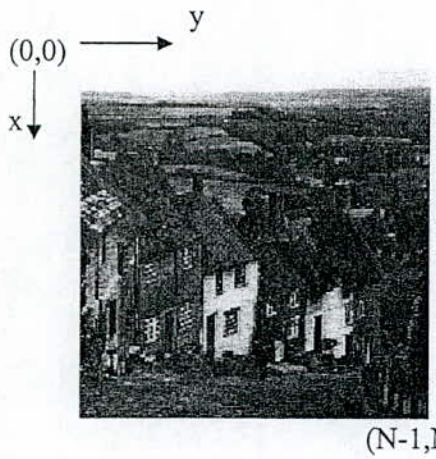
$$I(x,y)=\frac{1}{N^2}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} F(u,v)e^{j\frac{2\pi}{N}(xu+yv)} \qquad x,y = 0,1,2\ldots N\text{-}1$$

Quelques propriétés de la DFT :

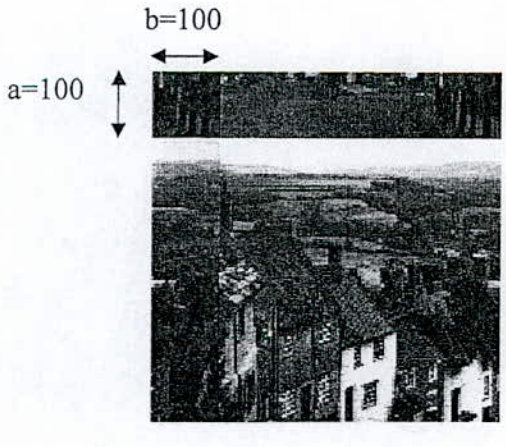
$$F(u,v) = F(u+N,v+N)$$
$$I(x,y) = I(x+N,y+N)$$
$$F(u,v) = \overline{F(-u,-v)} = \overline{F(N-u,N-v)} \quad \text{, (pour } I(x,y)\in R)$$

Translation : une translation dans le domaine spatial se traduit par un changement de phase dans le domaine fréquentiel :

$$I(x+a,y+b) \leftrightarrow F(u,v)e^{-j\frac{2\pi}{N}(au+bv)}$$



l'image originale (N=512)



l'image après translation

changement d'échelle : un changement d'échelle dans le domaine spatial provoque un changement d'échelle inverse dans le domaine fréquentiel :

$$I(ax,by) \leftrightarrow \frac{1}{ab} F(\frac{u}{a},\frac{v}{b})$$

Rotation : une rotation dans le domaine spatial se traduit par une rotation de même angle dans le domaine fréquentiel :

$$I(r,\theta+\theta_0) \leftrightarrow F(\omega,\varphi+\theta_0)$$

avec : I(r,θ) , F(ω,φ) la représentation de I(x,y) , F(u,v) en coordonnées polaires

($r=\sqrt{x^2+y^2}$, θ=arctan(y/x))

III-3-3-2- La technique DFT-AM (DFT Amplitude Modulation) : [19] [28] [34]

Dans cette méthode l'insertion de la marque se fait par une modulation d'amplitude des coefficients DFT selon l'équation suivante :

$$|F^*(u,v)| = |F(u,v)| (1 + \alpha W(u,v)) \quad (*)$$

avec F(u,v) la DFT de l'image originale et F*(u,v) celle de l'image tatouée . α est le coefficient d'accroissement .

Il faut que W(u,v)=W(N-u,N-v) pour que la propriété $F^*(u,v) = \overline{F^*(N-u,N-v)}$ reste vérifiée (c.a.d pour que les I*(x,y) soient réels) .

L'équation (*) nous permet de faire des modifications qui dépendent du contenu de l'image. Si on choisit par exemple α=0.2 on aura :

F*(u,v) =0.8F(u,v) si W(u,v)=+1
F*(u,v) =1.2F(u,v) si W(u,v)=-1

En général ce sont les coefficients de moyennes fréquence qui sont modifiés : la modification des coefficients basse fréquence rend la marque visible et les coefficients haute fréquence sont très sensibles au bruit, au filtrage et à la compression avec perte. La détection se fait d'une façon classique (par calcul de corrélation) .

Cette technique résiste bien aux translations car ce type de transformation géométrique n'affecte pas le module de la DFT .

Des études expérimentales ont montré que l'information contenue dans la phase de la DFT d'une image est prépondérante sur celle contenue dans l'amplitude . Donc la technique de modulation d'amplitude est utilisée dans les systèmes de tatouage qui privilégient à priori l'aspect invisibilité sur l'aspect robustesse .

III-3-3-3- La technique DFT-PM (DFT-Phase Modulation) : [32]

De faite que la phase de la transformée de Fourier content des informations plus significatives que son amplitude, beaucoup de tatoueurs d'image préfèrent introduire la marque au niveau de la phase pour, d'une part s'assurer qu'une tentative de suppression du tatouage

engendrera inévitablement des dégradations importantes de l'image ; d'autre part les techniques de modulation de phase sont reconnues comme étant plus robuste au bruit que les techniques de modulation d'amplitude.

L'insertion de la marque se fait à l'aide des équations suivantes :

$$\varphi^*(u,v)=\varphi(u,v)+m$$
$$\varphi^*(u,v)=\varphi(N-u,N-v)-m$$

Avec φ(u,v) est la phase du coefficient F(u,v) et m le niveau du tatouage .

La dernière équation est utilisée pour garder la symétrie qui caractérise la DFT d'une image ($F(u,v)=\overline{F(N-u,N-v)}$) : pour assurer que les I*(x,y) resteront réels après l'application de la DFT inverse . Notons que si cette équation est respectée, la composante continue F(0,0) et le coefficient F(N/2,N/2) resteront inchangés .

Pour augmenter la robustesse de la marque la phase φ(u,v) ne sera modifiée que si :
$|F(u,v)|/\sum_i\sum_j|F(i,j)| > T$ est vérifiée ou T est un seuil prédéterminé .

III-3-3-4- Utilisation de transformée de Fourrier-Mellin : [29] [35]

Ruanaidh et Pun [29] étaient les premiers à proposer un schéma de tatouage basé sur la transformée de Fourrier-Mellin pour résister aux attaques géométriques. La figure ci-dessous représente le schéma de tatouage contenant les étapes de transformations de l'image du domaine spatial jusqu'au domaine invariant par translation, rotation et changement d'échelle. Cette transformation est composée d'une transformée de Fourier suivie d'une transformée de Fourrier-Mellin. Pour que la transformation soit inversible, les signaux de phases de l'image originale sont conservés et réutilisés lors du retour au domaine spatial.

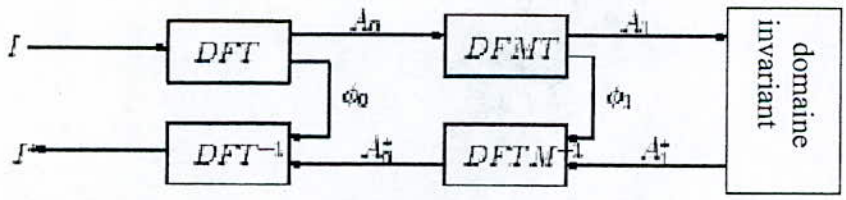


Figure3.8 Schéma du tatouage dans le domaine d'invariance. La DFT est la transformée de Fourier discrète, la DFMT celle de Fourrier-Mellin. Les signaux Ai représentent les amplitudes, ϕ i les phases des transformées de l'image.

L'invariance par translation est obtenue par la transformation de Fourier de l'image dont on ne prend que le module. Les invariances par rotation et changement d'échelles sont obtenues par transformation de Fourrier-Mellin du module. En effet, cette transformation peut être vue comme la composée d'un changement de repère de cartésien en log-polaire et d'une transformée de Fourier. Le changement de repère a la propriété de transformer les rotations et changement d'échelles en translation, la transformée de Fourier, dont on ne prend que le module, rend le tout invariant.

Cette méthode marche théoriquement, mais elle pose beaucoup de problèmes lors de son implémentation. C.Lin et M.Wu [35] ont proposé des améliorations pour faciliter l'implémentation en travaillant sur un signal à 1D extrait de l'image, malgré ça, l'implémentation reste toujours loin d'être praticable .

Remarque : la transformée de Fourrier-Mellin $F_M(k_1,k_2)$ d'un signal $f(x,y)$ est donnée par :

$$F_M(k_1,k_2) = \int_{-\infty}^{+\infty} \int_{0}^{2\pi} f(e^{\mu}\cos\theta, e^{\mu}\sin\theta)\exp[i(k_1\mu + k_2\theta)].d\mu.d\theta$$

II-3-4- Autres algorithmes utilisant la DFT :

a)Insertion d'une grille secrète : [30]

Afin de pouvoir détecter les transformations géométriques(que l'image peut subir), un ensemble de positions du spectre de module de la transformée de Fourrier, que l'on appelle grille de référence, est modifiés de manière à y insérer des maxima locaux. Les positions de ces amplitudes dépendent d'une clef secrète . Ainsi, la grille de référence n'est connue au moment de l'extraction que si l'on possède cette clef. Pour décoder le message, les maxima locaux de la DFT sont extraits, et la transformation géométrique à calculer correspond à la transformation mettant en correspondance un maximum de points de la grille de référence avec les maxima locaux détectés. Grâce à ce calcul de transformation, la synchronisation de la marque devient possible, et le message peut être extrait .

b)Insertion d'une marque circulaire symétrique : [28]

Dans cette méthode, les amplitudes (de moyennes fréquences) de la DFT de l'image sont modulés par une marque $W(k_1k_2)$ symétrique qui a la forme d'un anneau :

$$W(k_1,k_2) = W(N-k_1,N-k_2)$$

$$W(r,\theta) = \pm 1 \quad \text{si } R_1<r<R_2$$
$$= 0 \quad \text{si } r>R_2 \text{ ou } r<R_1$$

Avec : $r = (k_1+k_2)^{1/2}$ $\theta = \arctan(k_2/k_1)$

L'aspect circulaire de la marque est utilisé dans la détection pour déterminer l'angle de rotation que l'image a subit : on calcul la corrélation entre la marque et l'image tatouée et on essaye de maximiser la valeur de cette corrélation en faisant tourner la marque plusieurs fois d'un angle $0 \le \theta \le \pi$.

III-3-4- Insertion dans le domaine ondelettes : [31] [33]

Comme la DCT ou la DFT, la transformée en ondelettes discrète DWT (Discrete wavelet transform) a été utilisée par la communauté du tatouage d'image. Parmi les algorithmes qui utilisent cette transformée, on a par exemple celui proposé par Kundur : La marque, une matrice binaire dans {-1,1}, est décomposée en quatre sous-marques par DWT au niveau 1. L'image est

décomposée en ondelettes jusqu'à un niveau L (en pratique L = 4). Les coefficients de détails de tous les niveaux sont alors modifiés : on y ajoute les sous marques pondérées par un seuil psychovisuel adaptatif. L'image marquée est alors reconstruite par transformation inverse. La détection se fait avec l'image originale, on extrait les valeurs de la marque à chaque résolution, la marque extraite finale étant la moyenne des valeurs obtenues. Cette méthode est très robuste à la compression et à l'ajout de bruit blanc.

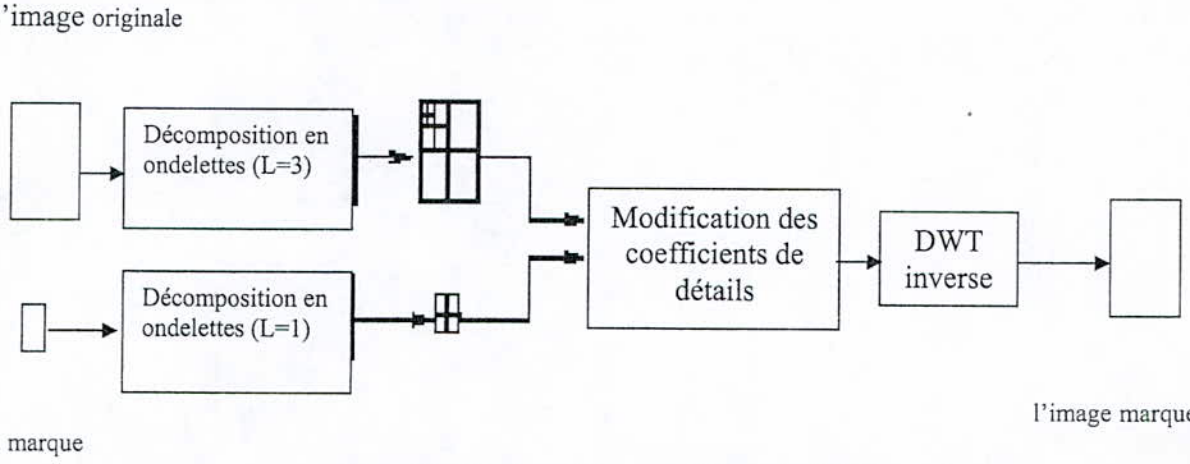
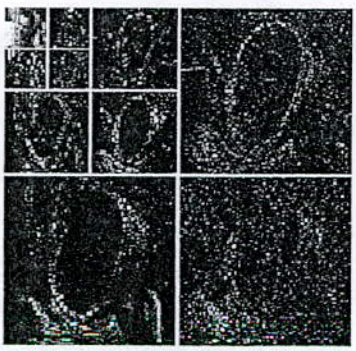


Figure3.9 tatouage d'image utilisant la DWT

Exemples de décomposions par DWT *de l'image « Barbara » jusqu'à un niveau* L (la décomposition à été faite avec MATLAB : en utilisant Wavelet Toolbox) :


l'image originale


décomposition jusqu'à L=1


décomposition jusqu'à L=3

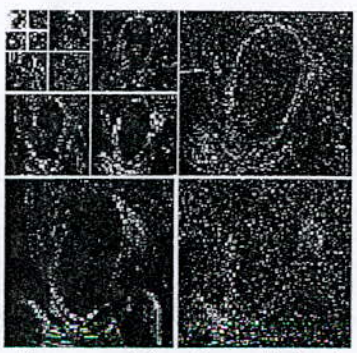

décomposition jusqu'à L=4

Figure3.10 *Exemples de décomposions par* DWT

III-3-5- Autres techniques : [21]

Beaucoup d'autres techniques sont étudiées ou en cours d'investigation. Des chercheurs s'intéressent notamment au domaine fractal, l'objectif étant de profiter de certaines propriétés d'invariance propres aux fractales afin de pouvoir prévenir certaines attaques et récupérer la marque sans recourir à l'image originale.

Actuellement un intérêt grandissant est porté aux schémas dits substitutifs qui représentent les méthodes pour lesquelles la marque est formée par la suppression de certaines composantes de l'image. Ces composantes sont choisies, comme pour le schéma additif, par une clé secrète; la signature est ensuite adaptée à l'image originale (par un masque psychovisuel par exemple). La détection de la signature s'effectue en examinant la répartition des caractéristiques extraites .

III-4- Codes correcteurs

De nombreuses méthodes utilisent potentiellement les codes correcteurs d'erreurs afin d'augmenter les performances en termes de robustesse des algorithmes de tatouage. L'emploi de tels codes apparaît en effet naturel si l'on examine le problème de la robustesse du tatouage sous l'angle de la communication d'un signal sur un canal bruité.

Parmi les codes utilisés, on a :

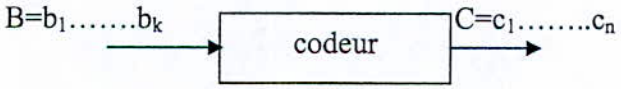
Le code répéteur :

c'est la plus simple et la plus ancienne méthode de correction d'erreurs. Elle consiste tout simplement à répéter m fois chaque bit du message à insérer.

Le code cyclique :

on va décrire ici le principe de codage/décodage de ce code sans rentrer dans les détails mathématiques, car ce serait trop long.

Soit un message $M=\{b_i|\ b_i \in \{0,1\}_{,i=1...64}\}$ à coder avec un code cyclique de paramètres (k,n). Pour cela, chaque bloc de k bits de M sera remplacé par un bloc de n bits à la sortie du codeur (avec n>k) :



C : est appelé *mot de code,* B : est le bloc message à coder .
n : est appelé longueur du code, k est la longueur initial du mot.
k/n :est le rendement.

L'ensemble des mots de code est l'ensemble des valeurs possibles de C (le nombre de ces valeurs est très $<2^n$), on détecte une erreur si on reçoit une chaîne qui ne correspond à aucun mot de code.

Dans un code cyclique toute permutation circulaire d'un mot du code est encore un mot du code. Exemple : un code cyclique (1,2) possède les mots de code suivantes :{01,10} ou {00,11}, mais pas {01,11}.

Dans les processus de codage et de décodage on utilise la représentation polynomiale de B et de C, plus un polynôme g(x) dit polynôme générateur qui doit être connu par le codeur et le décodeur :

$$B=b_1 \ldots . b_k \quad \rightarrow \quad B(x) = \sum_{j=1}^{k} b_j x^{k-j} = b_1 x^{k-1} + b_2 x^{k-2} + \ldots\ldots\ldots + b_k$$

$$C=c_1 \ldots . c_n \quad \rightarrow \quad C(x) = \sum_{j=1}^{n} c_j x^{n-j} = c_1 x^{n-1} + c_2 x^{n-2} + \ldots\ldots\ldots + c_n$$

g(x) est un polynôme de degré n-k : $g(x) = x^{n-k} + g_2 x^{n-k-1} + \ldots\ldots + g_{n-k} x + 1$ $(g_i \in \{0,1\})$.

Le codage se fait par la multiplication de g(x) avec B(x) :

$C(x) = B(x) .g(x)$ (notons que l'addition utilisée est une addition modulo 2)

Le décodage se fait par la division :

- Si C'(x) divise g(x) :il n'y a pas d'erreurs (C' :est le mot code reçu par le décodeur, C'(x) est son polynôme correspondant).
- Si C'(x) ne divise pas g(x) :il y a erreur (la correction se fait en cherchant le mot code le plus proche de B' tel que B'(x) est le quotient de la division C'(x)/g(x)).

Notons que l'usage des codes correcteurs dans le cadre du tatouage d'image reste un problème ouvert, requérant la conception de codes compacts capables de prendre en compte la diversité des attaques.

Après la présentation de l'état de l'art des méthodes de watermarking des images, il ressort que le souci majeur des algorithmes de tatouage est comment résister aux différentes attaques ? Ainsi la connaissance des modes d'action des attaques est nécessaire pour élaborer des algorithmes robustes et efficaces (du moins vis-à-vis certaines attaques), se sera l'objet du chapitre suivant .

Chapitre : IV

Les attaques contre les systèmes de tatouage d'images

Les attaques contre les systèmes de tatouage d'images

IV-1- Introduction :

Les manipulations que peut subir une image sont très diverses et se regroupent en quelques grandes familles qu'on va présenter . Soulignons que la plupart d'entre elles sont très faciles à mettre en oeuvre à l'aide d'outils simples de traitement d'images .

Il est important de remarquer que certaines de ces manipulations peuvent être appliquées en toute honnêteté tandis que d'autres ne concernent que les tentatives d'altération volontaire de la marque dans un but malhonnête .

IV-2- Définition : [11] [12]

On appel **attaque** tout traitement susceptible d'altérer le filigrane ou de provoquer des ambiguïtés lors de son extraction. L'attaque est dite réussie si elle arrive à rendre la détection du filigrane impossible, sans endommager trop considérablement l'image tatouée .

Dans le domaine de la cryptographie, les progrès ont été itératifs : des algorithme ont été proposés, des attaques ont été trouvées, de meilleurs algorithmes ont apparu, et ainsi de suite. Cette façon de procéder est appliquée aussi dans le watermarking .

IV-3- Classification des attaques : [13]

Les attaques contre les systèmes de watermarking peuvent être classés de plusieurs façons :

1ère Classification :

On peut séparer les attaques de la manière suivante : Les transformations usuelles de l'image comme la compression, ne visent pas forcément à attaquer le tatouage, ce sont des attaques « non intentionnelles ». Le deuxième groupe d'attaques est constitué d'attaques génériques, i.e qui ne visent pas un algorithme en particulier. Le troisième ensemble concerne les attaques ciblées sur une méthode de tatouage déterminée.

2ère Classification :

Une autre idée est d'étudier les attaques selon l'étape du tatouage qu'elle mettent en défaut. En effet, si des pirates tentent par exemple d'enlever la marque, c'est l'étape d'implémentation qui est visée. Ils peuvent aussi vouloir invalider le marquage, en noyant par exemple le message dans du bruit, c'est alors l'étape de détection qui est visée. Le tableau ci-dessous donne une classification des diverses attaques selon cette distinction. (On va détailler certaines de ces attaques plus tard) .

Attaques sur l'implémentation	Attaque sur la détection
Filtrage Compression Cropping	Ajout de bruit , transformations géométriques, passage à l'analogique , surmarquage, mosaïque , collusion

Tableau 4.1 Attaques sur l'implémentation, attaque sur la détection

3ère Classification :

Ici les attaques sont classées selon le domaine visé . On aura les classes suivantes :

Traitement d'images ;
Les attaques géométriques ;
Les attaques cryptographiques ;
Les attaques sur le protocole .

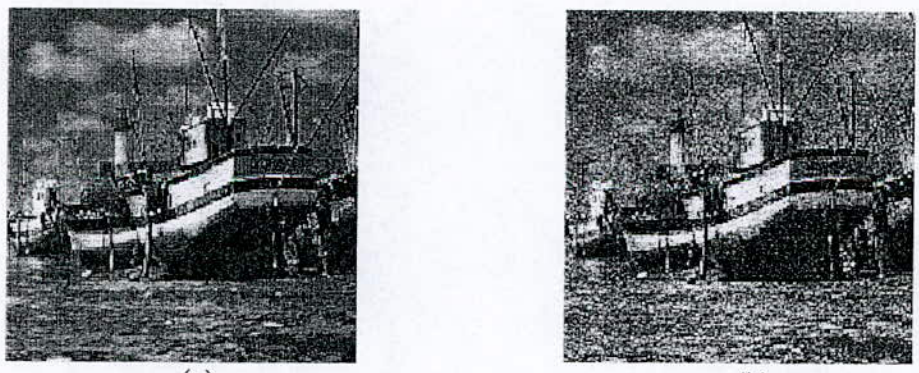
Dans ce travail nous allons utilisé la 3ère Classification .

IV-4- Les techniques d'attaques :

IV-4-1- Traitement d'images : [11] [9] [14]

1- Ajout d'un bruit à l'image :

on ajoute à l'image une deuxième image qui consiste en un bruit blanc . Ceci a pour effet de légèrement modifier des pixels uniformément répartis dans l'image et peut éventuellement rendre le filigrane inséré indétectable .



(a) (b)

figure4.1 L'image *boat.bmp 512x512* (a)avant l'ajout de bruit, (b)après l'ajout d'un bruit gaussien de moyenne nulle et de variance égale à 0.005 on a utilisé la fonction *imnoise* de MATLAB6.1 (PSNR=23dB)

2- Impression/renumérisation :

Ce procédé consiste en l'impression du document puis en sa renumérisation à l'aide d'un scanner . Il peut aussi simplement signifier la numérisation d'une image imprimée présente dans un livre ou un magazine .

3- Compression avec perte :

Les algorithmes de compression avec perte sont particulièrement dangereux pour les processus de tatouage puisque leur objectif est exactement l'opposé de celui du tatouage. On veut en effet, par l'utilisation de ces algorithmes ne garder de l'image que les composantes essentielles à leur compréhension (une marque invisible n'est évidement pas essentielle). C'est pourquoi certains auteurs proposent d'insérer la marque dans des endroits perceptuellement significatifs de l'image. Ces lieux de marquage seront souvent choisis directement dans les domaines transformés utilisés par les algorithmes de compression : Le domaine DCT pour la norme JPEG[1] (Joint Photographic Expert Group), la transformée en ondelette pour la norme JPEG2000 .

(a) (b) (c)

figure4.2 L'image *lena 512x512* (a) avant compression
(b) après compression JPEG de 50% : PSNR=35,8dB
(c) après compression JPEG de 5% : PSNR=27.3dB
on a utilisé la fonction *imwrite* de MATLAB6.1

En générale, les utilisateurs choisissent un taux de compression souvent $\geq 50\%$, pour lequel la qualité de l'image compressée est très acceptable .

Notons que cette opération ne résulte pas forcément d'une intention malhonnête, elle est généralement utilisée pour optimiser les capacités de stockage .

4- Modification d'histogramme :

L'***histogramme*** est une fonction qui donne pour chaque niveau de gris (ou couleur) i d'une image, le nombre d'échantillons (pixels) possédant la valeur de niveau i (i=1...Q si chaque pixel est codé sur un octet : Q=256) .

La modification d'histogramme est l'une des opération qu'on utilise souvent dans le traitement d'images et qui peut être considérée comme une attaque contre les systèmes du

[1] La norme J.P.E.G. définie en 1991 par un groupe d'experts du monde de la photographie est actuellement la méthode de compression d'images fixes avec pertes la plus utilisée.

watermarking . Parmi les modifications qu'on peut rencontrer , on a *l'égalisation d'histogramme* et *la correction Gamma* .

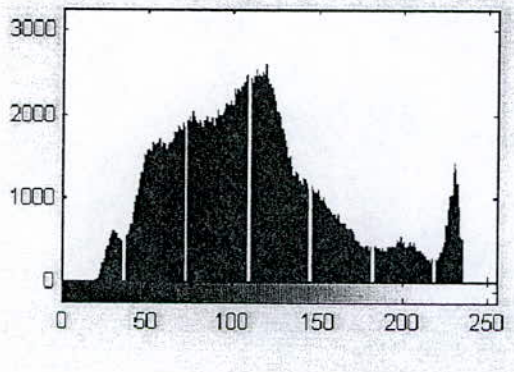
a) Egalisation d'histogramme :

Cette transformation consiste à rendre le plus plat possible, l'histogramme des niveaux de gris (ou couleurs) de l'image .

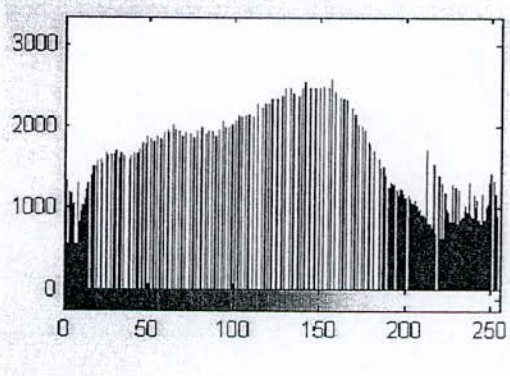
Exemple : cet exemple a été effectué sous MATLAB6.1 sur l'image *goldhill.tif 512x512.* On a utilisé les fonctions *: histeq* et *imhist* :

(a)

(c)



(b)



(d)

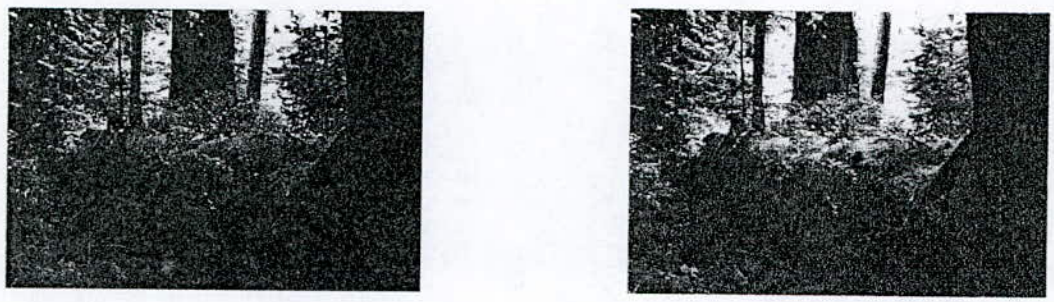
figure4.3
(a) L'image avant égalisation (b) son histogramme
(c) L'image après égalisation (d) son histogramme

b) Correction Gamma :

On peut modifier les niveaux de gris (ou les couleurs) de l'image de la manière suivante : on défini une application de [0..255] dans [0..255] qui va modifier pour tous les pixels la valeur de niveau de gris correspondant. Des outils de traitement d'images proposent par exemple la fonction suivante :

$$[0..255] \rightarrow [0..255]$$
$$i \rightarrow 255*(i/255)^{1/\gamma}$$

où γ est un paramètre donné par l'utilisateur .



(a) (b)

figure4.4 L'image *forest.tif* (a) avant correction Gamma
(b) après correction Gamma γ=0.5
on utilisé la fonction *imadjust* de MATLAB6.1

5- Filtrage :

La marque insérée dans l'image ressemble souvent à du bruit, c'est donc tout naturellement que les pirates appliquent au document marqué des méthodes classiques de débruitage (filtrage) pour lui retrancher l'estimée de la marque. Sous certaines conditions, le signal résultant sera proche du signal original.

Le filtrage ne résulte pas forcément d'une intention malhonnête, il est souvent utilisé pour la restauration[2] d'images. Il peut consister en :

-une méthode spatiale : on applique un masque à l'image consistant par exemple en un moyennage (filtre moyenneur) ou un filtre médian .
- une méthode fréquentielle : on supprime alors les hautes fréquences dans la transformée de Fourier de l'image .

[2] La ***restauration d'images*** est l'ensemble des méthodes développées pour compenser les dégradations connues ou estimées et rétablir la qualité initial de l'image . Il ne faut pas le confondre avec le ***rehaussement d'images*** qui est l'ensembles des méthodes (exemple: modification d'histogramme) qui modifient l'apparence d'une image pour qu'un observateur ou une machine puisse plus facilement certaines informations désirées [9].

(a) (b) (c)

figure4.5 L'image *barbara.bmp512x512* (a) avant filtrage
(b) après application d'un filtre médian (15x15)
(c) après application d'un filtre moyenneur (15x15)
on a utilisé les fonctions *medfilt2* et *imfilter* de MATLAB6.1

IV-4-2- Attaques géométriques : [11] [12] [14]

Ces attaques sont très simples et très dangereuses pour la plupart des schémas de tatouage, ils ne cherchent pas à ôter la marque mais plutôt à la désynchroniser. Dans ces attaques, la marque est décalée, le détecteur ne la retrouve pas aux endroits attendus et conclut à l'absence de la marque. Cette désynchronisation se fait la plupart du temps par le biais de transformations géométriques de l'image ou de parties de cette image, telles que la rotation , la translation, la symétrie, la réduction, l'agrandissement ou encore l'extraction de morceaux de l'image .

1- Rotation :

Cette attaque consiste en une rotation plus ou moins importante de l'image ou d'un détail de cette image .La rotation doit être le plus faible possible pour qu'elle ne soit pas décelable à l'oeil nu .

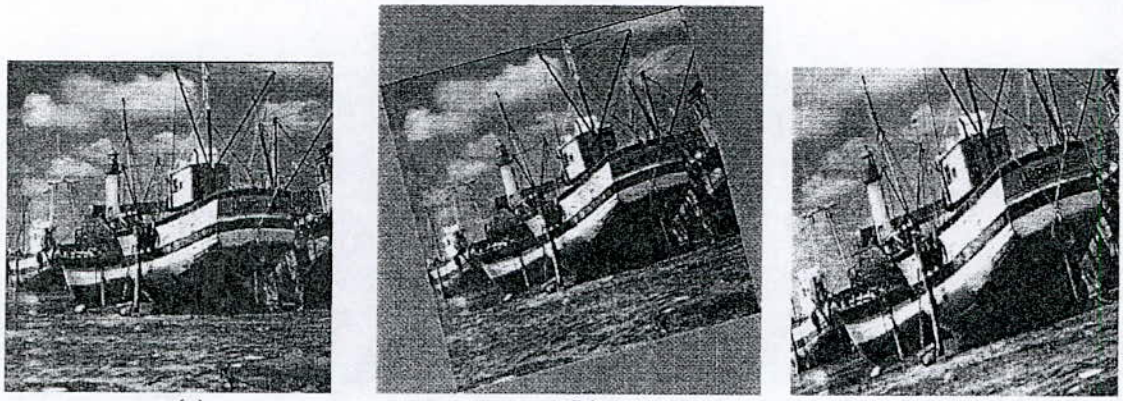
2- Changement d'échelle :

Cette opération peut ne pas résulter d'une intention de piratage (par exemple mettre des images à la bonne échelle pour quelqu'un qui publie un livre) . On distingue deux types de changement d'échelle :

- *Le changement d'échelle uniforme :* Les échelles en X et en Y varient de la même manière (il y a conservation des proportions) .
- *Le changement d'échelle non uniforme :* il n'y a pas de conservation des proportions (les échelles en X et en Y ne varient pas de la même manière) .

3- Recadrage :

Appelé aussi fenêtrage, émargement ou encore 'cropping' . Comme son nom l'indique, cette opération consiste à recadrer l'image en supprimant quelques lignes ou colonnes sur ses bords .



(a) (b) (c)

figure4.6 L'image *boat* (a) l'image originale (b) après rotation de 15°
(c) après rotation de 15° + cropping + changement d'échelle .
on a utilisé les commandes *rotate* , *crop* et *resize du* logiciel PhotoImpact6.0

4- Montage :

Dans cette attaque on colle des morceaux d'images sur une autre image (par exemple on remplace le visage d'un personnage par un autre) .

5- Extraction de détails :

Cette opération ressemble à celle de recadrage, mais beaucoup plus chirurgicale , le détail extrait peut être un visage par exemple .

6- La symétrie axiale :

Cette attaque peut ne pas être perceptible si l'image tatouée présente naturellement une symétrie par rapport à un axe donné .

7- La symétrie horizontale – La symétrie verticale :

Certaines images peuvent subir une inversion horizontale ou verticale sans perdre leurs sens . Ces symétries sont des cas particuliers de la symétrie axiale .

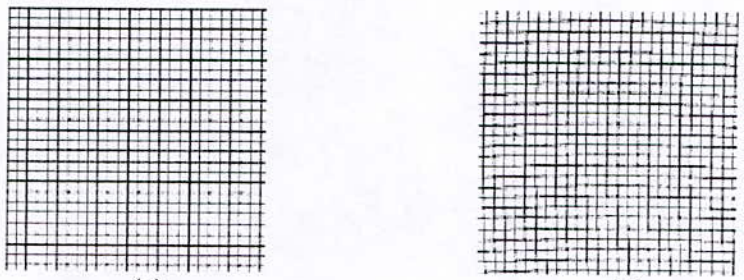
(a) (b) (c)

figure4.7 L'image *boat* (a) avant flipping,
(b) après flipping horizontal, (c) après flipping vertical .
on a utilisé la commande *flip du* logiciel PhotoImpact6.0

8- Attaques de StirMark :

StirMark est un logiciel d'attaque de marques disponible gratuitement sur Internet (avec son code source) . Il a été développé à Cambridge, est maintenu par Fabien Petitcolas . Il combine plusieurs transformations géométriques au même temps

Le logiciel StirMark est devenu une référence pour tester la robustesse d'un algorithme de tatouage d'images et jusqu'à maintenant aucun schéma de tatouage ne résiste à cette attaque .



(a) (b)

figure4.8 L'effet d'une attaque de StirMark sur une grille
(a)avant attaque (b)après attaque

9- Attaques de UnZign :

UnZign est lui aussi un logiciel d'attaque de marques dont seuls les exécutables sont disponibles sur Internet (ni le code source, ni même l'algorithme utilisé ne sont donnés) . Il permet également d'effectuer des déformations invisibles sur l'image afin de craquer une marque. UnZign est très efficace sur les schémas concernant le domaine spatial .

IV-4-3- Attaques cryptographiques : [15] [16] [17]

Ces attaques s'inspirent largement du domaine de la cryptographie et en utilisent ses principes. Par exemple beaucoup de schémas de tatouage utilisent des clés secrètes uniquement connues du propriétaire; pour être en parfaite sécurité il est donc déjà nécessaire d'avoir à sa disposition un jeu de clés conséquent.

1- Attaque par collusion :

L'attaque dite de collusion[3] a lieu lorsque plusieurs utilisateurs sont en possession du même document portant différentes marques. La mise en commun de ces documents permet de nombreuses opérations : moyenne, recherche de propriétés statistiques communes dans différents domaines, recherche d'informations sur la localisation de la marque...

Décrivons ***une attaque par moyenne*** : l'image résultante de la moyenne des images tatouées en circulation aura la même qualité que ces dernières. Elle contiendra toutes les marques, leurs amplitudes étant fortement diminuées. La détection sera alors perturbée à la fois par cette baisse d'amplitude et de possibles interférences entre les marques. Plus le nombre d'images utilisé sera grand et plus il y aura de chances de faire disparaître la marque .

2- Attaque par recherche exhaustive :

[3] entente secrète en vue de tromper quelqu'un (Larousse) .

Cette attaque a besoin de calculateurs très puissant afin d'essayer de retrouver la clé utilisée dans le processus de tatouage . Le calculateur teste toutes les clés possibles jusqu'à en trouver la bonne .

Cette technique d'attaque est très peu utilisée du fait qu'elle nécessite beaucoup de temps de calcul, surtout lorsque la longueur de la clé n'est pas connue.

IV-4-4- Attaques sur le protocole : [12] [17] [18]

1- Attaque par surmarquage (surtatouage) :

L'attaque par surmarquage consiste à tatouer à nouveau une image déjà tatouée. Pour certains schémas, en particulier si les lieux de tatouages sont fixés, cette attaque peut être très dangereuse. Certains protocoles[4] de tatouage se protègent en vérifiant, avant l'insertion de la marque, que l'image originale proposée n'est pas tatouée. Cette protection n'est utile que si le schéma de tatouage demeure inconnu. En effet, s'il est connu, un pirate peut ajouter une marque de sa fabrication qui invalidera la détection.

Un exemple d'attaque par surmarquage est celui visant particulièrement l'algorithme de tatouage de Digimarc (qui marque uniquement les images non tatouées). Dan cette attaque, les pirates commencent par éviter l'interdiction au surtatouage : une image est dégradée jusqu'à ce que l'on puisse la surtatouer (la première marque n'étant plus lisible). On ajoute à l'image originale l'image ainsi surtatouée (en diminuant son amplitude pour que les dégradations n'apparaissent plus). L'image résultante porte alors les deux tatouages, mais le détecteur n'en lit qu'un, le nouveau : le pirate s'est donc approprié l'image .

2- Attaque par copiage :

Ici, on propose d'estimer une marque sur l'image marquée par des méthodes de prédiction connues (La prédiction de Wiener par exemple), et d'ensuite insérer cette marque sur une autre image non marquée (Watermark Copy Attack). Le but est toujours de créer une ambiguïté lors de l'authentification du propriétaire : en effet lors de la confrontation avec le propriétaire, le pirate pourra répondre que le logiciel de détection retrouve la marque sur beaucoup d'autres images qui n'appartiennent cette fois qu'au pirate.

Pour résister à ce type d'attaque , l'algorithme de tatouage doit générer des marques liées aux images originales . Ainsi même le pirate arrive à estimer la marque , il lui sera impossible de l'insérer dans une autre image sans dégrader la qualité de celle-ci .

3- Attaque de l'impasse (Attaque par inversion) :

Cette attaque porte aussi le nom d' ***attaque IBM*** , elle utilise le fait que beaucoup de systèmes de tatouage ne permettent pas de savoir quel filigrane parmi plusieurs a été ajouté le premier (le processus de tatouage est souvent additif et donc inversible) .

Soit une image tatouée I* (I*=I+W , I étant l'image originale et W la marque) , un pirate qui a enregistré une marque W' peut très bien prétendre que l'image est la sienne et que la version originale est I+W-W' .

[4] ensemble des règles à respecter au cours de certains traitements ou de certaines opérations

Deux solutions ont été proposées : utiliser des systèmes de marquage non inversibles, ou concevoir des mécanismes d'enregistrement pour stocker les copies tatouées et la date de tatouage en vue d'une vérification ultérieure . La deuxième solution est à éviter car elle implique l'utilisation d'une base de données gigantesque .

IV-4-5- Autres attaques (attaque mosaïque) : [12]

L'objectif de l'attaque mosaïque est de tremper le détecteur du filigrane, il faut bien se rendre compte que cette attaque ne détruit pas le filigrane qui peut alors être retrouvé par des algorithmes plus performants et donc plus complexes .

Cette attaque a été proposée par F.Petitcolas , elle vise la vérification automatique des marques dans les images sur l'Internet via des *robots traqueurs* (petits programmes parcourant automatiquement le réseau ; ils téléchargent image après image et vérifient si elles contiennent une marque).

L'idée est d'empêcher ces *robots* de retrouver la marque en présentant l'image tatouée de manière détournée (sachant que tout algorithme de watermarking requiert une taille minimale de l'image) :

on la découpe en plusieurs petits morceaux , telle une mosaïque, et on les assemble ensuite dans une page HTML. La plupart des navigateurs acceptant qu'il n'y ait aucun espace entre plusieurs images, il suffit de reconstituer l'image à l'aide de ces petits morceaux (dans certains cas le chargement de la mosaïque est même plus rapide que l'image entière) . Cette image est alors affichée correctement par un navigateur sans être dégradée, mais un *robot traqueur* la voit comme un ensemble d'images indépendantes de très petite taille .

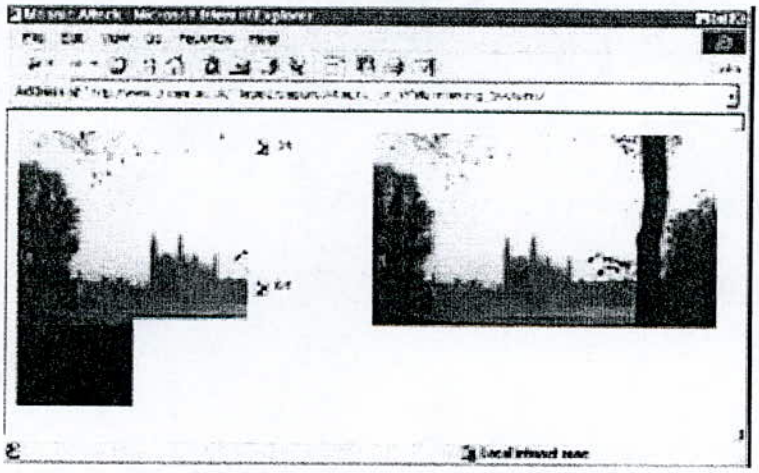


figure4.9 téléchargement d'une image après et avant attaque mosaïque
http://www.cdt.luth.se/~peppar/kurs/smd074/lekt/7/slide43.html

IV-5- Conclusion :

Dans ce chapitre, on n'a pas fait une description exhaustive de toutes les attaques existantes. En particulier, on n'a pas présenté les attaques spécifiques à certains algorithmes. Les différentes attaques présentées ici montrent la nécessité de faire la conception de l'algorithme de tatouage en fonction des applications: une fois ces applications définies, il devient possible d'anticiper les attaques qui seront utilisées et de les contrer.

Ce qu' il faut retenir, c'est que quelques soient les attaques qui auront été portées sur une image afin de détruire ou de fausser un filigrane , elles n'ont de sens que si la qualité de l'image est préservée . C'est sur cette hypothèse que toutes ces attaques peuvent être évités . Hélas, si à chaque méthode une nouvelle attaque a été déterminée , à chaque attaque correspond une nouvelle méthode pour y résister . Ce cercle n'a pas encore été rompu jusqu'à ce jour , rendant toutes les méthodes de watermarking inefficaces .

Chapitre : V

Etude et implémentation de quelques algorithmes de watermarking des images

Etude et implémentation de quelques algorithmes de watermarking des images

V.1. Introduction :

Ce chapitre est consacré à l'étude et l'implémentation de deux méthodes de watermarking des images, l'une opère dans le domaine spatiale et l'autre dans le domaine fréquentiel. Mais avant d'entamer cette étude, on va présenter des tests qui ont été effectués sous MATLAB en utilisant quelques algorithmes de tatouage de base (DFT-AM, DFT-PM, DCT) pour voire l'effet de l'insertion d'une marque sur la qualité de l'image.

V.2. Test de quelques algorithmes de tatouage de base :

Les images utilisées (lena.tif , goldhill.tif , barbara.tif) sont des images à niveaux de gris et de taille 128x128. La marque insérée est un message de 8 bits bipolaire {1,-1} étalé par une séquence pseudo aléatoire pour couvrir toute l'image.

Voici un résumé des équations utilisées pour chaque algorithme de base (pour les résultats, consulter les annexes A, B, C) :

A) La technique DFT-AM :

L'équation d'insertion utilisée est :

$$|F^*(u,v)| = |F(u,v)| \, (1 + \alpha \, W(u,v)) \quad , \quad [W(u,v)=W(N-u,N-v)]$$

avec F(u,v) la DFT de l'image originale et F*(u,v) celle de l'image tatouée . α est le coefficient d'accroissement. (les résultats sont donnés dans l'annexe A)

B) La technique DFT-PM :

Les équations d'insertion utilisées sont :

$$\varphi^*(u,v)=\varphi(u,v)+m$$
$$\varphi^*(u,v)=\varphi(N-u,N-v)-m$$

Avec $\varphi(u,v)$ est la phase du coefficient F(u,v) et m le niveau du tatouage .
$F(u,v)_{u,v=1..128}$: les coefficients DFT de l'image originale .
(les résultats sont donnés dans l'annexe B).

C) Insertion dans le domaine DCT:

L'équation d'insertion utilisée est :

$$I^*(i,j) = I(i,j) \, (1 + \alpha \, w(i,j))$$

avec :I*(i,j) : coefficient DCT de l'image marquée ;

I(i,j): coefficient DCT de l'image originale

α :le coefficient d'accroissement .
(les résultats sont donnés dans l'annexe C)

Après les tests effectués sur les algorithmes de base les plus simples, on va faire maintenant l'étude et l'implémentation de deux méthodes plus complexes :

V.3. Description des méthodes implémentées :

Comme il a été dit, les deux méthodes implémentées opèrent dans deux domaines différents (spatial/fréquentiel). Le point commun de ces deux méthodes est qu'elles utilisent la même stratégie : la technique multicouche, appelée aussi la technique CDMA (Code Division Multiple Access : Accès Multiple à répartition par code) ou encore SS-CDMA (Spread spectrum CDMA).

L'utilisation de la même stratégie pour les deux méthodes facilitera la comparaison et la déduction par la suite des avantages et des inconvénients de chaque une .

En communication la technique CDMA permet notamment de pouvoir mélanger plusieurs signaux à l'émission, le but étant de pouvoir transmettre plusieurs communications en même temps et non pas l'une après l'autre. Appliquée au tatouage d'images cette méthode peut nous permettre d'insérer une quantité d'information plus importante dans l'image sans pour autant la dégrader.

Un masque psychovisuel peut être utilisé dans la première méthode (spatial) pour minimiser les distorsions visibles introduites à l'images lors de l'insertion de la marque(surtout pour les images très texturées .

Pour la deuxième méthode, le domaine fréquentiel est obtenu en utilisant la DCT comme transformation de domaine et en insérant la marque dans les coefficients DCT de basses et moyennes fréquences (les coefficients hautes fréquences sont très sensibles aux bruits et la compression avec perte). Cette transformée a été appliquée à toute l'image pour que l'effet de la marque soit étalé sur tout le document hôte (c.à.d l'image hôte). L'utilisation de la DCT permettra à la marque de mieux résister à la fameuse compression JPEG puisque cette dernière utilise aussi la DCT dans son processus de compression.

En fin, on a utilisé dans les deux méthodes des codes correcteurs d'erreurs pour augmenter les performances de détection .

V.4. Application de la technique CDMA dans le tatouage d'images :

La technique CDMA en communication propose de mélanger plusieurs signaux à l'émission ; pour différencier les différents signaux à la réception, la détection se fait par un calcul de corrélation. On applique donc cette méthode au tatouage d'images pour pouvoir insérer un nombre de bits plus conséquent dans l'image (en ajouter plusieurs marques pour former la marque définitive) .

Soit un message M, de 64 bits, à insérer dans une image I en utilisant un marquage à N couches ($N \in \{1,2,4,8\}$).

$M=\{ bk \mid b_k \in \{0,1\}, k=1...64 \}$ en général on utilise une représentation bipolaire :

$M=\{ bk \mid b_k \in \{+1,-1\}, k=1...64 \}$

Le message M est devisé en N 'sous messages' de m bits chacun :

$M=\{ M_j \mid j=1...N \}$

$M_j=\{ b_{i,j} \mid b_{i,j} \in \{+1,-1\}, i=1...m , m=64/N \}$

Chacun de ces N messages sera inséré dans l'image I en utilisant une séquence pseudo aléatoire différente . Pour cela on divise l'image (ou la DCT de l'image) en m blocs $I_{i\ (i=1..m)}$, chaque bloc sera modifié comme suit :

$$I_i^*(x,y) = I_i(x,y) + \alpha\, w_i(x,y) \quad \text{avec} \quad w_i(x,y) = \sum_{i=1}^{N} S_j^{(2D)}(x,y)\, b_{i,j}$$

Où

α : la force du tatouage .

$b_{i,j}$: le i^{eme} bit du j^{eme} 'sous message' .

$S_j^{(2D)}$: est une Séquence Binaire Pseudo Aléatoire à 2 Dimensions (SBPA 2D) de taille égale à celle des blocs I_i .

Notons que dans le cas fréquentiel les coefficients DCT sont modifiés de la façon suivante :

$$F_i^*(u,v) = F_i(u,v)\,(1+\alpha\, w_i(u,v)) \quad i=1...m$$

$$\text{avec : } w_i(u,v) = \sum_{i=1}^{N} S_j^{(2D)}(u,v)\, b_{i,j}$$

$$F = DCT(I)$$

La détection se fait par calcul de corrélation. prenons le cas de la méthode spatiale :

Pour trouver le bit $b_{i,n}$ (le i^{eme} bit du n^{eme} sous message, c.a.d le bit $b_{i+m(n-1)}$ du message M) on calcul la corrélation $C_{i,n}$ entre le i^{eme} bloc I_i^* de l'image tatouée et la $n^{eme}_{(1\le n\le N)}$ séquence pseudo aléatoire $S_n^{(2D)}$:

$$C_{i,n} = \sum_{x,y} S_n^{(2D)}(x,y) \,.\, I_i^*(x,y) = \sum_{x,y} S_n^{(2D)}(x,y) \,.\, I_i(x,y) + \alpha \sum_{x,y} S_n^{(2D)}(x,y) \sum_{i=1}^{N} S_j^{(2D)}(x,y)\, b_{i,j}$$

$$= \sum_{x,y} S_n^{(2D)}(x,y) \,.\, I_i(x,y) + \alpha \sum_{i=1}^{N} \sum_{x,y} S_n^{(2D)}(x,y)\, S_j^{(2D)}(x,y)\, b_{i,j}$$

$$\approx \sum_{x,y} S_n^{(2D)}(x,y) \cdot I_i(x,y) + \alpha \sum_{x,y} [S_n^{(2D)}(x,y)]^2 b_{i,n}$$

$$\approx \alpha \sum_{x,y} [S_n^{(2D)}(x,y)]^2 b_{i,n}$$

Car : $\sum_{x,y} S_n^{(2D)}(x,y)\, S_j^{(2D)}(x,y) \approx 0$ pour $j \neq n$ (les séquences S_j sont décorrélées 2 à 2)

$\sum_{x,y} S_n^{(2D)}(x,y) \cdot I_i(x,y) \ll \alpha \sum_{x,y} [S_n^{(2D)}(x,y)]^2 b_{i,n}$ (S_n et Ii sont indépendantes puisque S_n est générée d'une façon pseudoaléatoire)

Donc le bit $b_{i,n}$ sera obtenu par : $b_{i,n} = \text{sign}(C_{i,n})$

Le même principe sera utilisé dans le cas fréquentiel .

V.5. Génération des séquences pseudoaléatoires :

Pour garantir les approximations faites précédemment, il faut choisir les séquences Sj d'une façon appropriée, car elles ont une influence directe sur la phase de détection et donc sur tout le processus de tatouage.

Pour cela on utilise généralement des séquences pseudoaléatoires dites « m-séquences ». d'autres séquences peuvent être utilisées comme les gold-séquences par exemple.

Une m-séquence est une suite de valeurs binaires. Elle est générée au moyen de dispositifs appelés registres à décalage à rétroaction linéaire (LFSR :Linear Feedback Shift Registers)

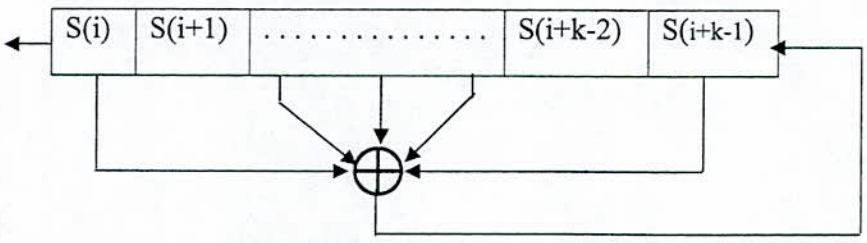


Figure 5.1 Cas général d'un LFSR de longueur k

Chaque fois qu'on a besoin d'un bit pour la séquence, tous les bits du registre sont décalés à gauche. Le nouveau MSB (bit le plus significatif) est calculé par une fonction dépendante des autre bits. Le LSB (bit le moins significatif) sorti suite au décalage est le bit demandé.

La période d'un registre à décalage est la longueur de la séquence de sortie avant que le registre retrouve son état initiale (S(0) . . . S(k-1)). Quand la longueur d'un de ces registres est k, la période P de la séquence équivaut à : $P=2^k-1$. Dans cette période P on trouve 2^{k-1} uns et $2^{k-1}-1$ zéros.

Notons qu'au moins un élément de l'état initiale du registre doit être non nul et au moins deux de ces k étages doivent être reliés à l'additionneur modulo-2 .

En pratique, les m-séquences sont généralement utilisées sous leurs forme bipolaire : les zéros sont remplacés par des -1. Une caractéristique importante d'une séquence pseudoaléatoire S, est sa fonction d'autocorrelation R(m) qui est généralement définie en utilisant la représentation bipolaire :

$$R(m)=\sum_{i=1}^{P} S(i)\, S(i+m)$$

Où : $0 \le m \le P-1$, $S(i)=\pm 1$, P est la période de la séquence.

Dans le cas des m-séquences, cette fonction vérifie la propriété suivante :

$$R(m)=\begin{cases} P & m=0 \\ -1 & 1\le m\le P-1 \end{cases}$$

C.à.d $R(m\neq 0) << R(0)$

Donc $S(i)_{i=1...P}$ et $S(i+m)_{i=1...P,\, m\neq 0}$ sont décorrélées.

La séquence S est séquence à une dimension, pour avoir une séquence à 2 dimensions $S^{(2D)}$, il suffit de transformer S en un signal à 2D en remplissant ligne par ligne ce signal.

V-6- Génération de la marque dans un schéma multicouche :

L'idée utilisée est de superposer plusieurs couches pour pouvoir augmenter la taille des SBPAs 2D (Séquences Binaires Pseudo Aléatoires à 2 Dimensions : les $S_j^{(2D)}$ utilisées dans §V.2) de départ et donc d'améliorer la détection de chaque bit du message. Cette méthode permet par ailleurs de pouvoir insérer plus d'information dans l'image.

Pour chaque couche on affectera une SBPA 2D différente: en effet si deux couches avaient la même SBPA 2D initiale, il arriverait que sur certains blocs de l'image on ajoute la SBPA 2D avec la première couche puis on la retranche avec la seconde ; finalement la marque ne serait pas présente pour ce bloc et la détection serait donc fausse dès le départ.

La figure ci-dessous décrit la méthode pour un schéma à 1, 2, 4 ou 8 couches pour une image 512*512 et pour l'insertion d'un message de 64 bits :

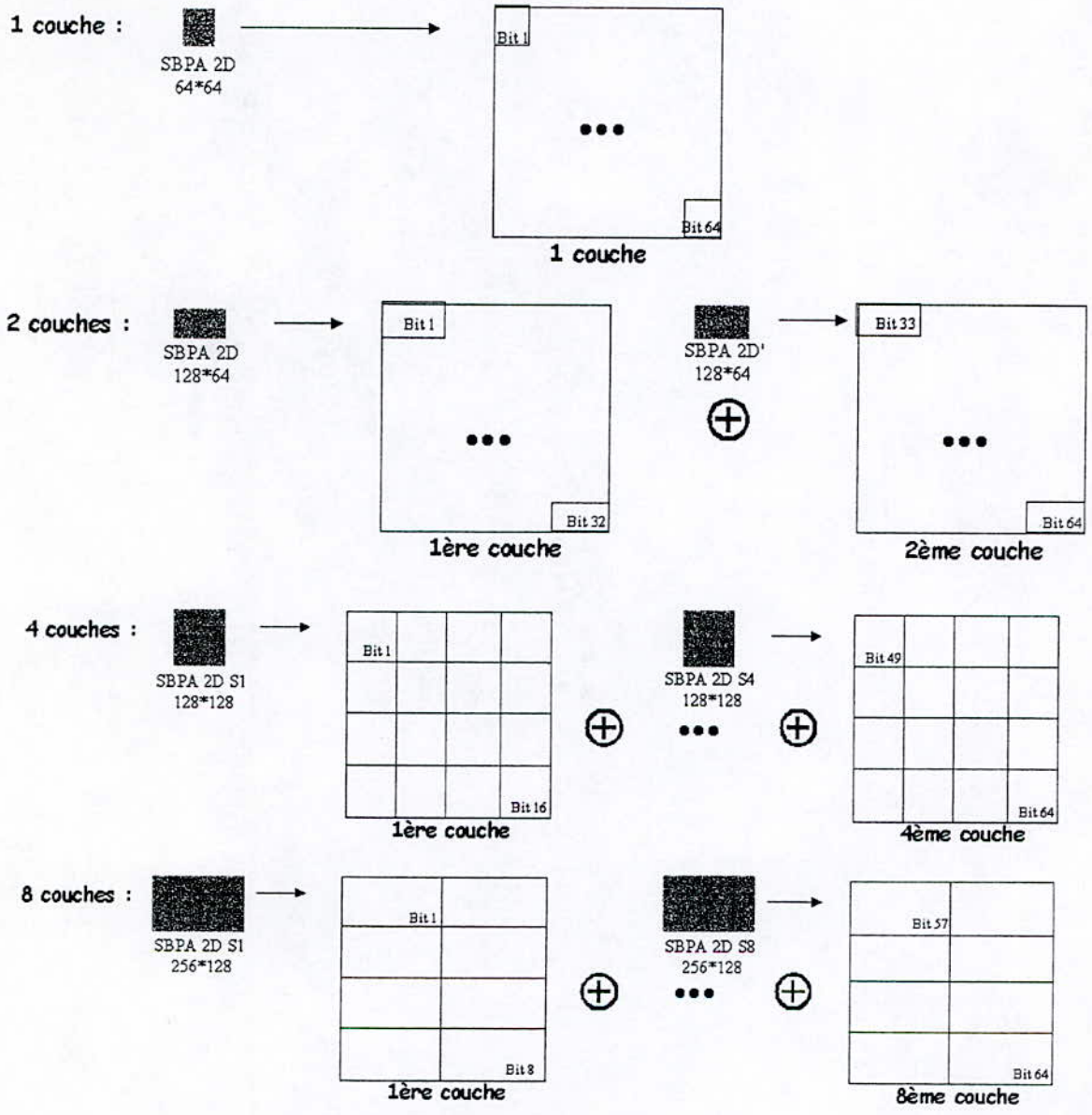


Figure 5.2 Construction de la marque dans un schéma multicouche

Donc, plus il y a de couches et plus les dimensions de chaque SBPA 2D augmentent et plus la détection de chaque bit s'améliore :

	1 couche	2 couches	4 couches	8 couches
Nombre de blocs par couche	64	32	16	8
Taille de chaque SBPA 2D	64*64	128*64	128*128	256*128

Tableau5.1 Nombre de blocs et tailles des SBPA 2D pour 1, 2, 4, 8, couches

Ces chiffres sont toujours pour une image 512x512 et un message de 64 bits .

En outre, cette méthode a l'avantage de ne pas trop détériorer l'image; en effet sur un schéma à 8 couches, on ajoutera sur chaque bloc de l'image des coefficients égaux à +8, +6, +4 ,+2, 0, -2, -4, -6, -8, mais avec une probabilité plus importante pour le coefficient 0 et une probabilité qui décroît d'autant plus que le coefficient a une valeur élevée :
Dans le schéma à 8 couches la marque finale à ajouter à l'image est obtenue par la superposition de 8 autres marques : si on considère chaque marque comme une matrice composée de +1 et de -1 ; la matrice correspondante à la marque finale sera obtenue par la sommation des 8 autres matrices et ses éléments peuvent donc prendre les valeurs +8, +6, +4, +2, 0, -2, -4, -6, -8 avec les probabilités suivantes :

Coefficient ajouté	+8	+6	+4	+2	0	-2	-4	-6	-8
Probabilité	1/256	8/256	28/256	56/256	70/256	56/256	28/256	8/256	1/256

Tableau5.2 Probabilités des coefficients à ajouter

Dans l'implémentation on se limite à un nombre maximal de 8 couches ; au delà de 8 couches il y aurait en effet un risque de trop détériorer l'image. Si on prend 16 couches par exemple, il est possible sur un bloc d'ajouter à l'image des valeurs égales à +16 ou –16 .

V.7. Codes correcteurs d'erreurs :

Pour les deux méthodes (spatial et fréquentielle), on a utilisé des codes correcteurs d'erreurs pour augmenter les performances de détection. On a le choix entre un code répéteur (avec un nombre de répétition allant de 1 à 10) ou un code cyclique (avec un rendement de 1/2 , 1/3 ou 2/3). En plus, ces deux codes ont été associés avec un 'interleaving' (éparpillement).

L'idée de l'éparpillement est de répartir les bits consécutifs des blocs formant le message à insérer, dans des paquets différents. Ainsi grâce à cet entrelacement, un groupe d'erreurs (affectant un paquet) affecte uniquement quelques bits dans plusieurs blocs, ce qui nous permis de corriger indépendamment ces quelques bits erronés dans chacun de ces blocs.
Dans l'application , la séquence à éparpiller sera écrite dans une matrice suivant les colonnes puis retranscrite suivant les lignes pour donner le message final à insérer dans l'image.

Pour ce qui concerne le code cyclique, on a utilisé les fonctions *encode* et *decode* de MATLAB de la manière suivante :
Mc= encode(M , n , k ,'cyclic') pour le codage.
M = decode(Mc , n , k ,'cyclic') pour le décodage.

V.8. Utilisation de masque psychovisuel :

On a utilisé, dans la méthode spatiale, un masque psychovisuel $M_\sigma(x,y)$ basé sur le calcul de la variance locale . Pour chaque pixel (x,y) de l'image originale I, on calcule la variance du bloc B de taille N_BxN_B (N_B=3,5,7,9,..) centré sur le pixel (x,y). A la fin, on normalise en divisant toutes les variances obtenues par la variance maximale (on aura pour tout (x,y) $0 \leq M_\sigma(x,y) \leq 1$) :

$$M_\sigma(x,y) = M(x,y)/M_{max} \qquad \text{avec : } M(x,y) = \frac{1}{N_B^{\,2}} \sum_{(i,j)\in B} \left[I(i,j) - m_B(x,y)\right]^2$$

Où :

$m_B(x,y) = \frac{1}{N_B^{\,2}} \sum_{(i,j)\in B} \left[I(i,j)\right]$: la moyenne du bloc B centré sur le pixel (x,y) .

$M_{max} = \max_{m,n}[M(m,n)]$: le maximum de toute les variances calculées sur toute l'image .

L'image tatouée I* sera donc donnée par :

$$I^*(x,y) = I(x,y) + \alpha\, M_\sigma(x,y)\, W_M(x,y)$$

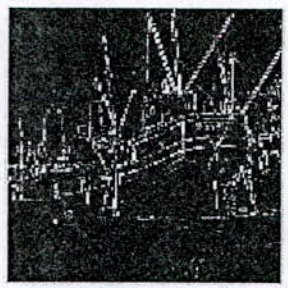
Où :

α : la force du tatouage .

W_M : la marque multicouche.

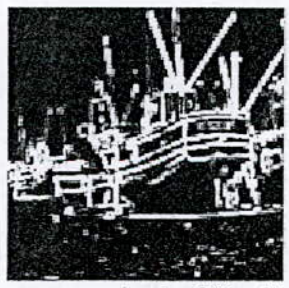
Exemple :

l'image originale



masque psychovisuel(N_B=3)

masque psychovisuel(N_B=5)



masque psychovisuel(N_B=9)

figure 5.3 *exemples de calcul de masque psychovisuel basé sur un calcul de variances locales.*
Les calculs ont été faits avec MATLAB6.1

Remarque :

En utilisant ce masque la marque sera concentrée seulement dans les zones texturées. Mais, par contre, le temps de calcul sera grand et la robustesse de la marque diminuera surtout pour les image faiblement texturées car le masque fera diminuer la force du tatouage dans les zones non texturées de l'image. (donc l'utilisation de ce masque sera efficace seulement pour les images texturées) .

V.9. Schémas d'insertion / schémas de détection :

Après avoir décri les différentes techniques utilisées pour la génération de la marque, son insertion puis sa détection, on va maintenant résumer les schémas définitifs d'insertion et d'extraction dans les deux domaines , spatial et fréquentiel :

La figure**5.4** résume le schéma d'insertion de la marque dans le domaine spatial : la marque multicouche W_M est obtenue par la superposition des N autres marques : $W_M = \sum_{i=1}^{N} W_{Mi}$ (la taille de chaque W_{Mi} = la taille de l'image à tatouer) . pour générer les N séquences pseudoaléatoires $S_j^{(1D)}$ on a utilisé la méthode décrite dans [38] : on génère une longue séquence pseudoaléatoire S puis on la décompose en N autres séquences (la longueur des $S_j^{(1D)}$, donc de S, dépend de la taille des blocs constituant les W_{Mi}) .

Notons que les messages $Mc_{j\ (j=1..N)}$ sont sous une forme bipolaires : $b_{i,j} = \pm 1$ et que $m=\frac{64}{N}\frac{n}{k}$ (avec k/n est le rendement du code correcteur) .

La figure**5.5.** décrit le schéma de détection du message toujours pour le cas spatial . Les séquences $S_j^{(1D)}$ sont générées de la même façon que dans la phase d'insertion . La détection se fait par calcul de corrélation entre les $S_j^{(2D)}$ et les différents blocs de l'image tatouée .

La figure**5.6.** résume le schéma d'insertion de la marque dans le domaine fréquentiel . La marque multicouche W_M est générée comme dans la figure**5.4.** mais , cette fois ci , sa taille n'est pas égale à celle de l'image à tatouer, elle est égale à celle de la partie F' (qui correspond aux coefficients DCT de basses et moyennes fréquences) .

Le paramètre ***e*** représente la distance entre la composante continue F(0,0) et le premier coefficient DCT extrait (qui sera modifié par la suite). Plus ***e*** est grand, plus la marque sera invisible et plus sa robustesse diminue .

La figure**5.7.** représente le schéma de détection du message dans le cas fréquentiel. La détection se fait toujours par calcul de corrélation .

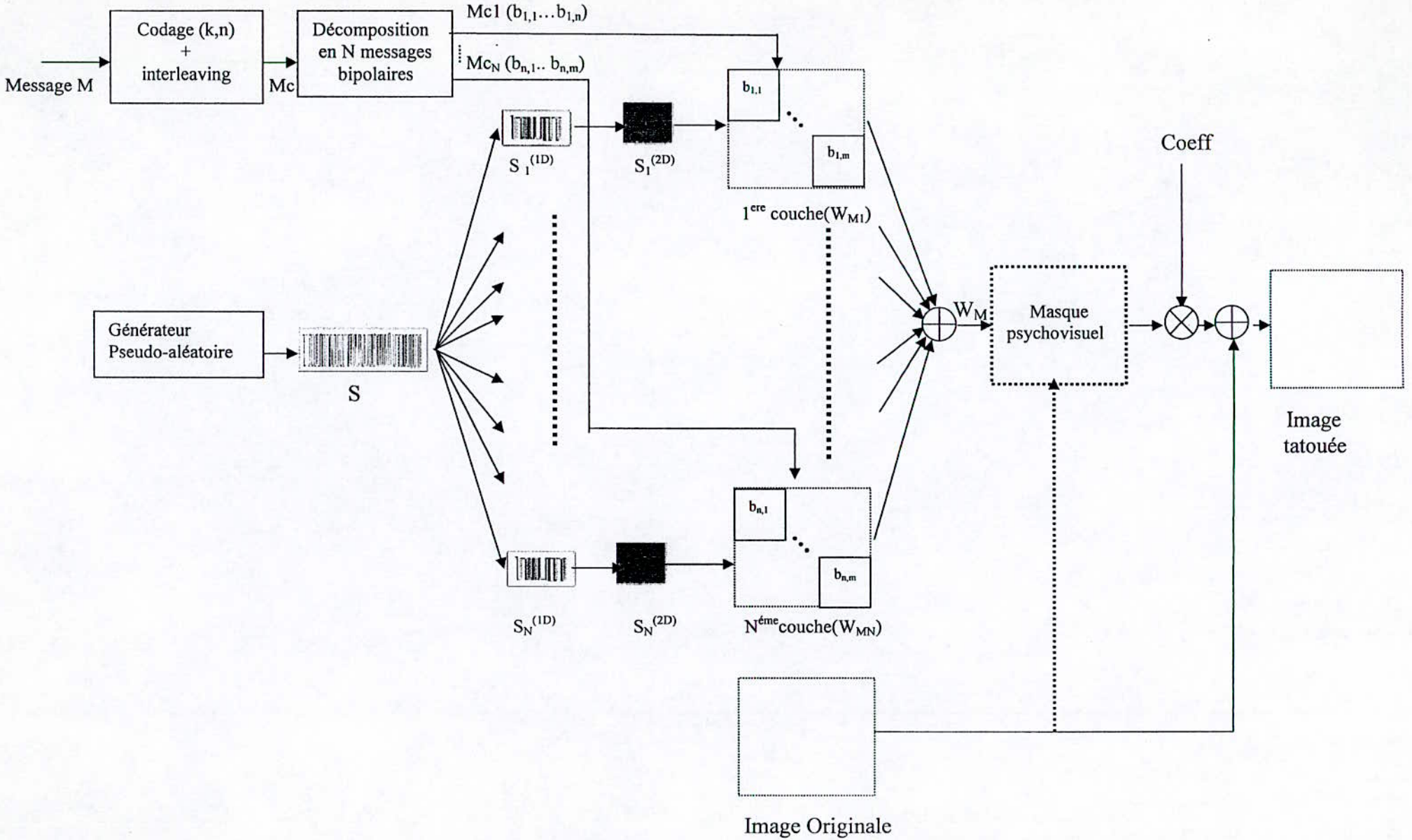


figure**5.4**. *Schéma d'insertion dans le domaine spatial*

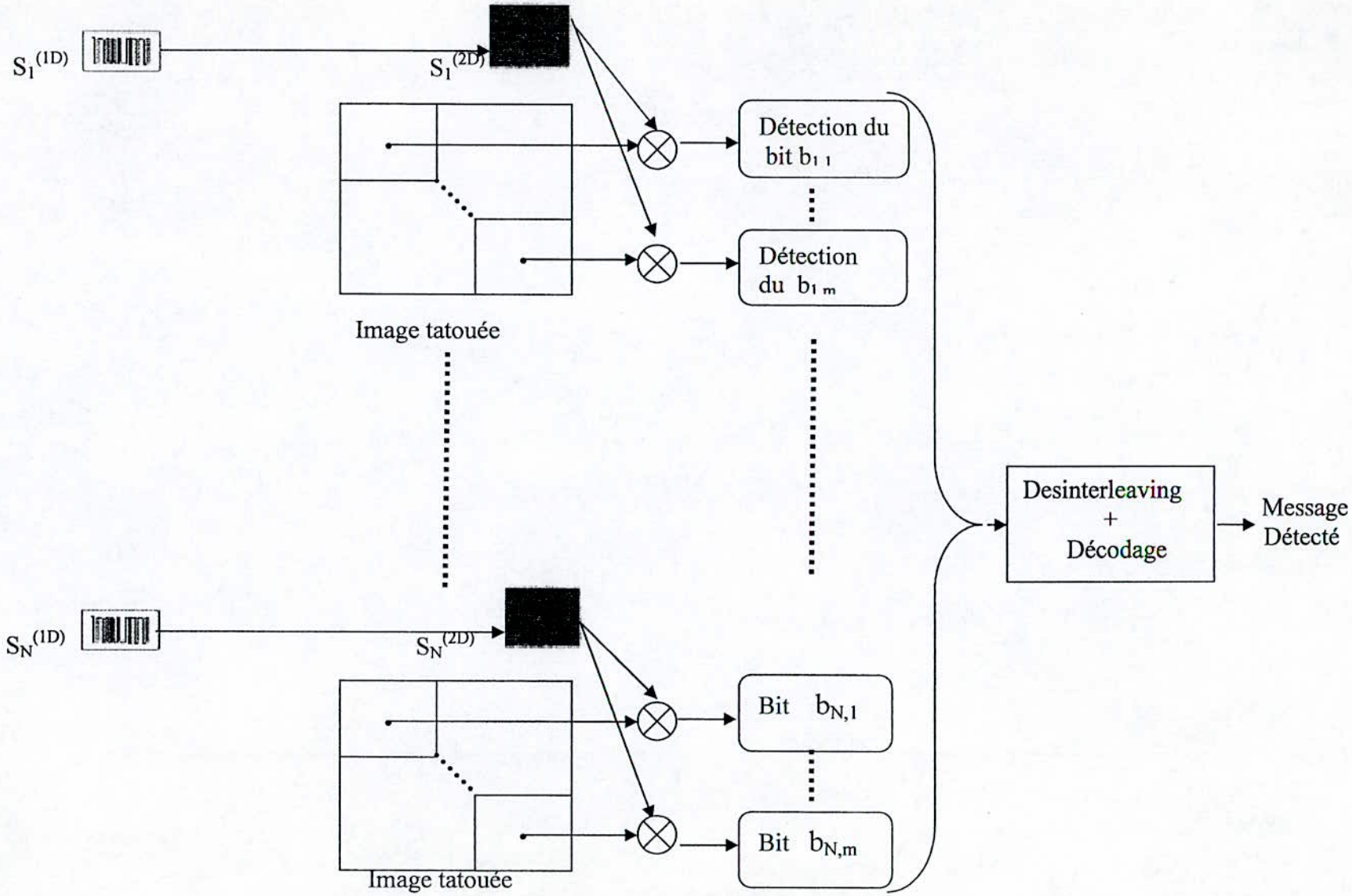


figure5.5 *Schéma de détection dans le domaine spatial*

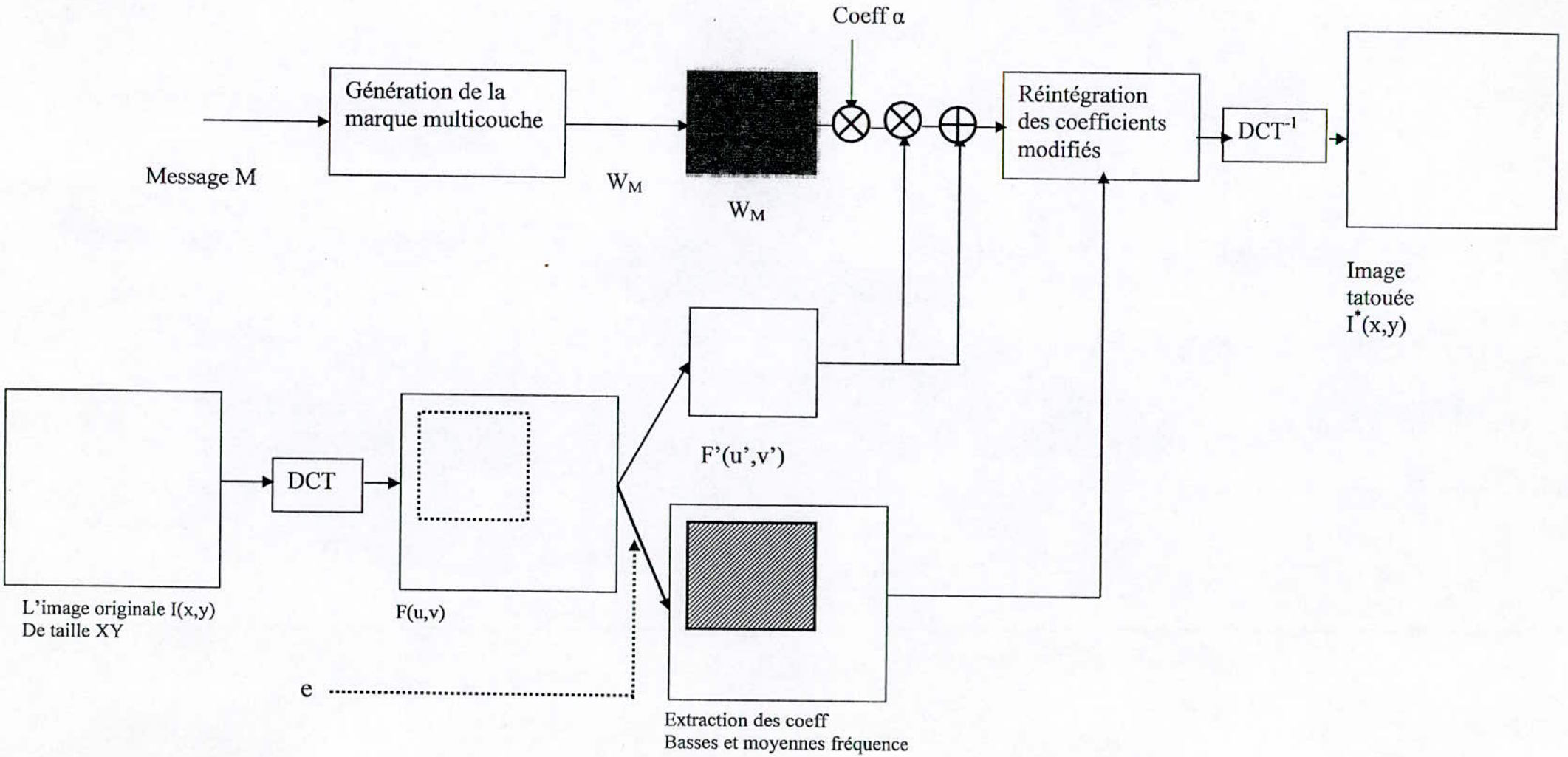


figure5.6 *Schéma d'insertion dans le domaine fréquentiel*

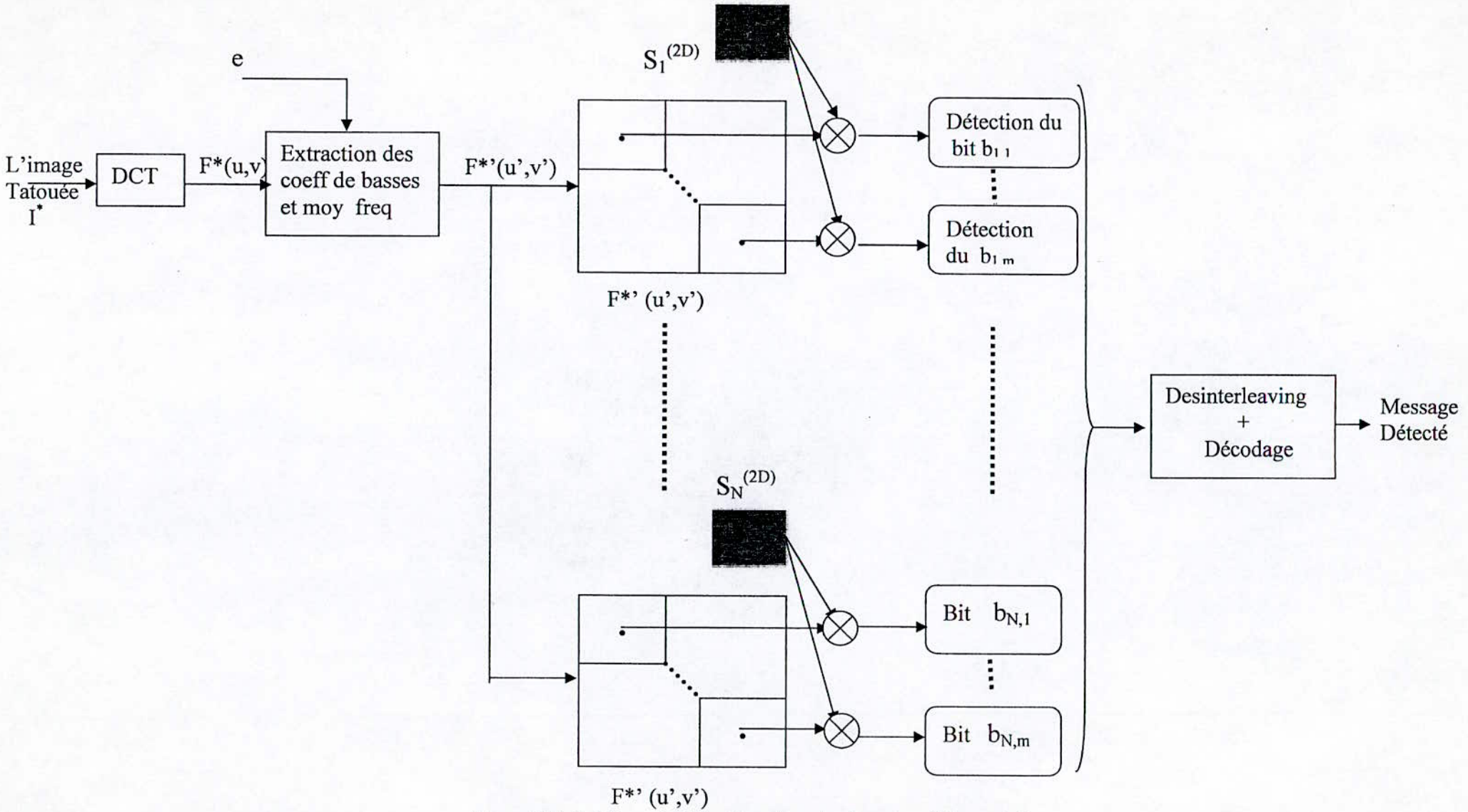


figure5.7. *Schéma de détection dans le domaine fréquentiel*

V.10. Mise en œuvre des méthodes :

L'implémentation effectuée dans le cadre de ce projet a été faite sous l'environnement MATLAB v6.1 en raison de l'existence de fonctions intégrées nécessaires à notre application : lecture d'images (MATLAB reconnaît beaucoup de formats d'images : tif, bmp, jpg, pcx, png), la transformation DCT bidimensionnelle, codage correcteur d'erreurs, filtrage d'images, ajout de bruit, transformation géométriques etc.. Ces fonctions sont disponibles au niveau des deux librairies IMAGE PROCESSING TOOLBOX et COMMUNICATIONS TOOLBOX .

Une interface graphique a été développée afin de simplifier l'entrée des différents paramètres d'insertion/extraction, la visualisation des images avant et après le tatouages ou l'évaluation des messages détectés,

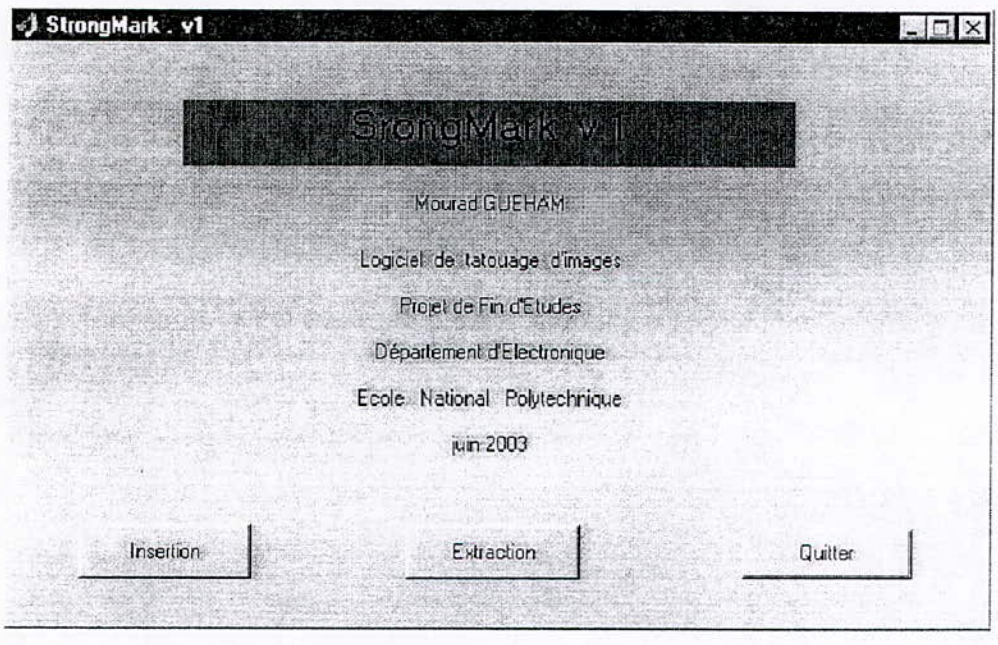


figure5.8. *page d'accueil de l'interface graphique développée.*

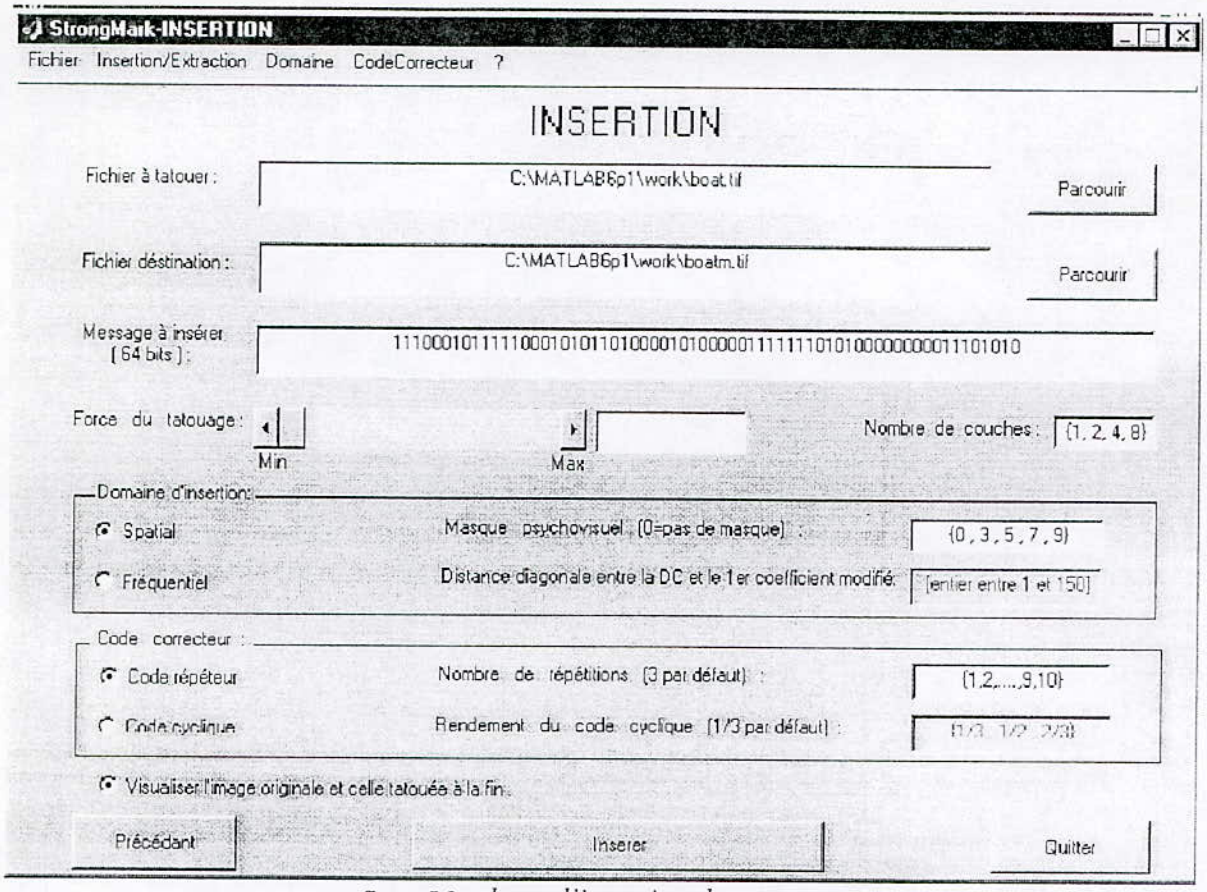


figure5.9. *phase d'insertion du message*

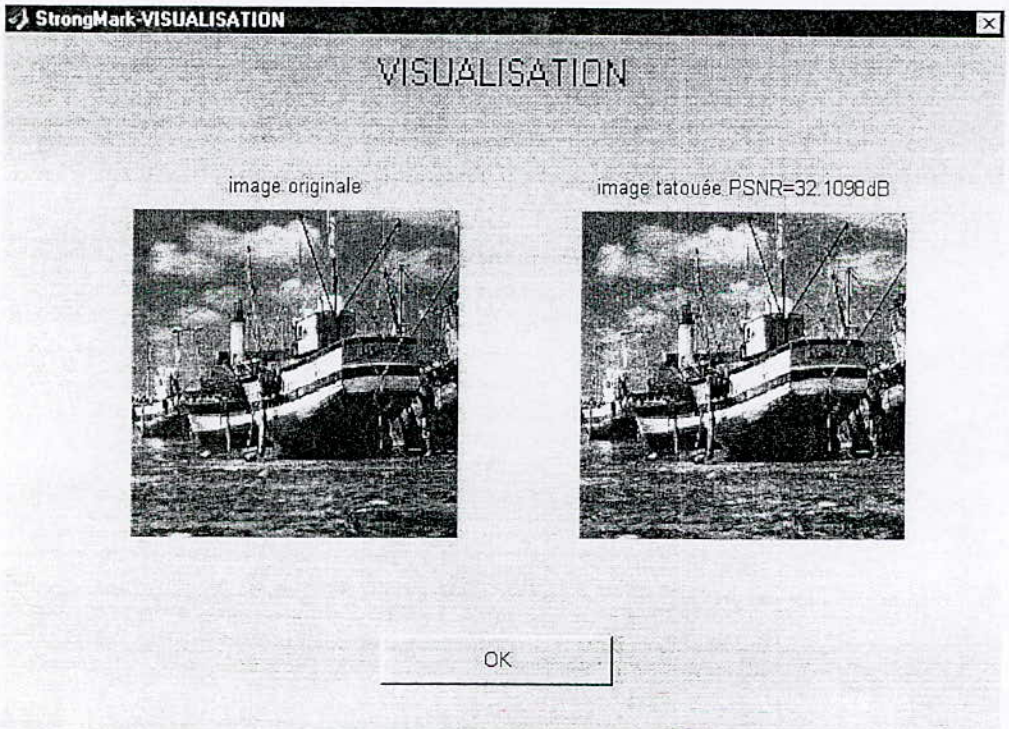


figure5.10. *visualisation des images : originale et tatouée.*

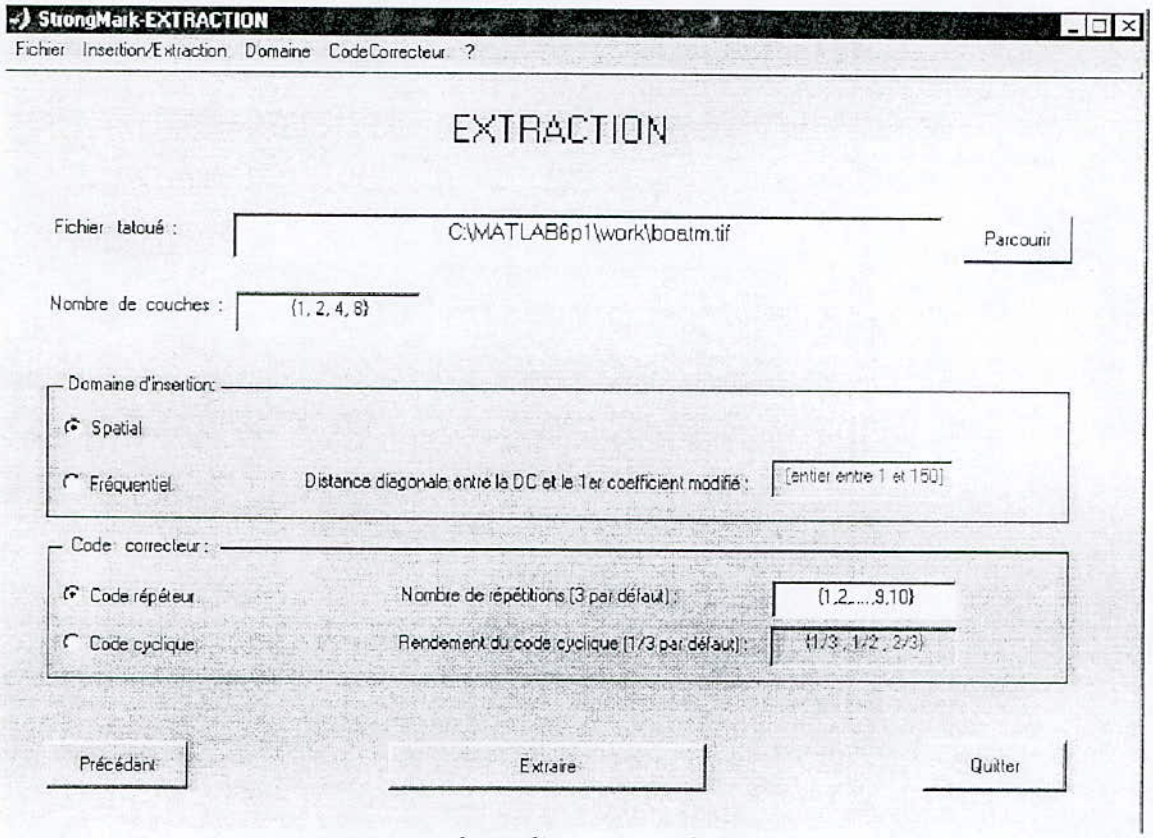


figure5.11. *phase d'extraction du message*

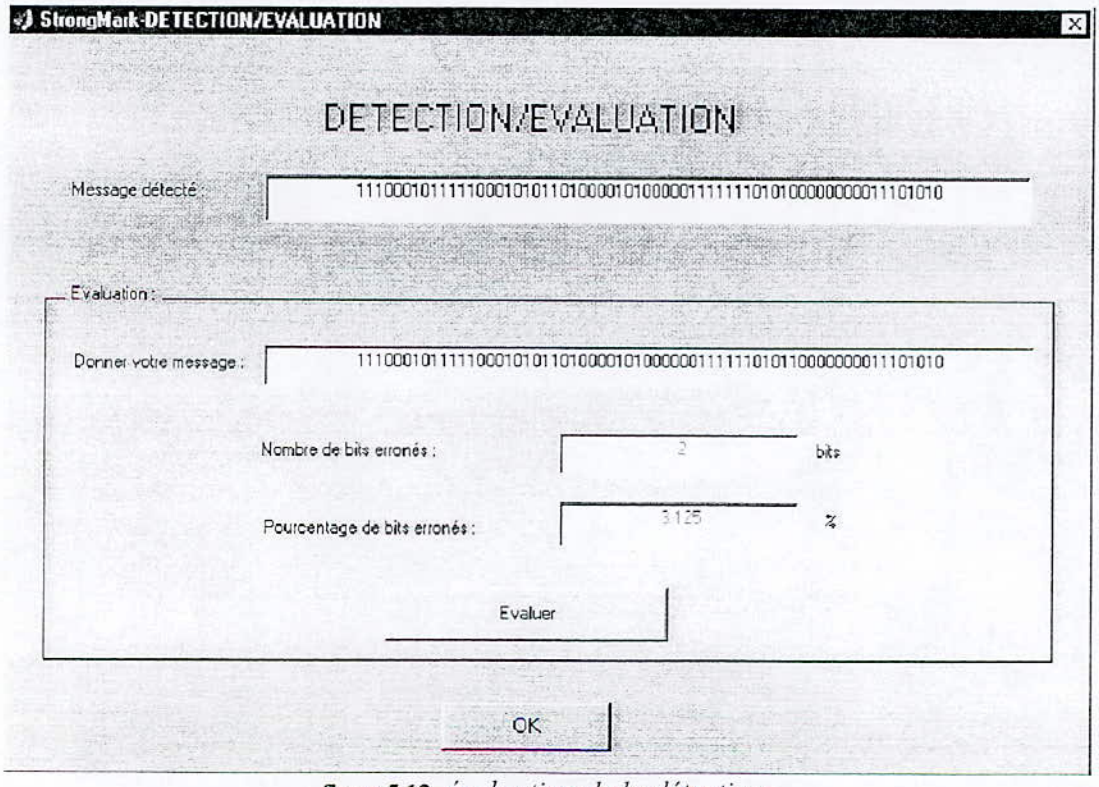


figure5.12. *évaluation de la détection.*

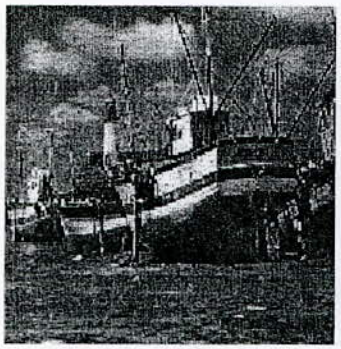
Chapitre : VI

Expérimentations et résultats

Expérimentations et résultats

La plupart des articles traitant le tatouage d'images proposent un algorithme dont les résultats sont présentés relativement à quelques images (souvent Lena). Le problème de l'interprétation de ces résultats, et donc de l'estimation qualitative de l'algorithme de marquage, vient de ce que tous les articles ne prennent ni les mêmes mesures, ni les mêmes images.

Pour ce qui concerne ce travail, on a choisi des images classiques , utilisées dans la plupart des articles de traitement d'images . Ces images sont : Boat, Lena, Baboon, Goldhill, Barbara :



Boat

Baboon

Lena

Goldhill

Barbara

Figure 6.1 images utilisées dans les tests

Notons que les images utilisées sont des images à niveaux de gris au format TIF ou BMP et de taille 512x512 .

Pour évaluer les performances et la qualité des deux méthodes implémentées , on a effectué une batterie de tests sur ces images . Les tests effectués consistent en l'évaluation des messages insérés dans les images , après les avoir subir des attaques différentes : compression JPEG, filtrage, ajout de bruit, redimensionnement, cropping , rotation .

Dans tout les tests, on a effectué le marquage avec les deux méthodes en utilisant les meilleurs paramètres de chacune d'elles : on a utilisé la force de tatouage maximale (celle qui correspond à un PSNR de l'image tatouée d'environ 30 dB) .

Les attaques qu'on a fait subir aux images tatouées sont :

VI.1. Compression JPEG

La compression JPEG est souvent utilisée pour optimiser les capacités de stockage, donc, elle ne résulte pas forcément d'une intention malhonnête

Pour tester la robustesse des deux méthodes vis avis cette opération , on compressé les images tatouées avec différents taux de compression . Les résultats sont donnés dans les deux tableaux suivants :

Taux de compression % / images	60	50	40	30	20	10	5
Lena	100	100	100	100	100	95.31	76.56
Barbara	100	100	100	100	100	100	100
Boat	100	100	100	100	100	93.75	78.12
Baboon	100	100	100	100	100	100	100
Gold hill	100	100	100	100	100	93.75	70.31

Tableau 6.1 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode fréquentielle , après compression JPEG

Taux de compression % / images	60	50	40	30	20	10	5
Lena	100	98.44	98.44	93.75	79.69	64	64
Barbara	100	100	100	98.44	92.18	81.25	75
Boat	100	100	100	100	98.44	89.06	82.81
Baboon	100	100	100	100	100	95.31	81.25
Gold hill	100	100	100	100	100	92.19	71.87

Tableau 6.2 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode spatiale , après compression JPEG

On peut dire que les deux méthodes résistent bien à la compression JPEG : le message a été identifié pour des taux de compression allant jusqu'à 10% (le message est considéré comme identifié si PBI > 80%) . Notons que pour les taux de compression < 10% les images compressées sont de très mauvaise qualité , donc meme si le message n'est identifié , l'attaque est considérée comme non réussie .

Pour cette attaque , la méthode fréquentielle donne des meilleurs résultats que la méthode spatiale .

VI.2. Filtrage :

Comme pour la compression , le filtrage aussi peut ne pas résulter d'une intension malhonnête, il est souvent utilisé dans la restauration d'images (III.4.1.5) . Dans ce test on a utilisé trois type de filtres : Adaptatif(wiener) , médian, moyenneur .

La méthode spatiale n'a pas très bien résisté à ce type d'attaques , cependant, l'autre méthode (fréquentielle) a donné des résultats très satisfaisants comme le montre les deux tableaux suivants :

Filtre / image	Adaptatif(wiener)					médian	moyenneur
	3x3	5x5	7x7	9x9	11x11	3x3	3x3
Lena	100	96.87	100	100	100	100	100
Barbara	100	100	100	100	100	100	100
Boat	100	100	100	100	100	100	100
Baboon	100	100	100	100	100	100	100
Golghill	100	98.43	100	100	100	100	100

Tableau 6.3 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode fréquentielle , après filtrage

Filtre / image	Adaptatif(wiener)					médian	moyenneur
	3x3	5x5	7x7	9x9	11x11	3x3	3x3
Lena	89.06	81.25	79.68	79.68	81.25	84.37	75
Barbara	90.62	89.06	87.5	87.5	87.5	82.81	79.68
Boat	98.43	95.31	90.62	90.62	90.62	95.31	93.75
Baboon	98.43	90.62	89.06	87.5	87.5	87.5	76.56
Goldhill	100	93.75	89.06	87.5	84.37	100	96.87

Tableau 6.4 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode spatiale , après filtrage

VI.3. Ajout d'un bruit :

Cette attaque consiste à ajouter aux images tatouées un bruit blanc gaussien . Les images bruitées avaient un PSNR allant de 30 à 13 dB .

Dans tout ces cas , et pour les deux méthodes , le message a été identifié à 100% même si la qualité visuelle des images a été très affectée par cette opération : surtout pour un PSNR < 20 dB .

image originale

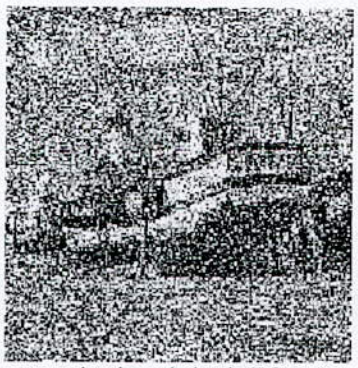


image après ajout de bruit (PSNR=13 dB)

figure 6.2 effet d'un ajout de bruit

VI.4. Redimensionnement (resize) :

Les images tatouées ont été redimensionnées de 512x512 vers 384x384, 256x256, 128x128 correspondant à des réductions de 75%, 50%, 25%. Puis, les images résultantes ont été redimensionnées une 2ème fois vers 512 x 512 par interpolation (on a utilisé la fonction *imresize* de MATLAB6.1) . Le watermark a seulement résisté à des réductions ≥ 50% :

Réduction / image	75%	50%	25%
Lena	100	100	60.93
Barbara	100	100	62.50
Boat	100	100	68.75
Baboon	100	100	53.12
Goldhill	100	100	54.68

Tableau 6.5 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode fréquentielle , après redimensionnement .

Reduction / image	75%	50%	25%
Lena	100	95.31	81.25
Barbara	100	96.87	75
Boat	100	100	82.81
Baboon	100	100	68.75
Goldhill	100	100	73.43

Tableau 6.6 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode spatiale, après redimensionnement .

VI.5. Cropping – Rotation :

Ces attaques ont pour but d'introduire une désynchronisation au niveau de l'image tatouée . L'opération de recadrage (cropping) consiste à supprimer quelques lignes et quelques colonnes sur les bords des images marquées (ce nombre de lignes et de colonnes supprimées varie de 1à 3), pour la 2^{eme} attaque , on fait subir aux images des rotations de 1^0 (on a utilisé les fonctions : *imcrop, imrotate, imresize* de MATLAB6.1) :

Attaques / images	cropping						Rotation de 1^0
	n=1		n=2		n=3		
	Sans 'resize'	Avec 'resize'	Sans 'resize'	Avec 'resize'	Sans 'resize'	Avec 'resize'	
Lena	100	100	56.25	92.18	56.25	37.50	50
Barbara	100	100	42.18	87.50	56.25	45.31	50
Boat	100	100	57.81	92.18	56.25	42.18	46.87
Baboon	100	100	48.43	93.75	46.87	37.50	50
Goldhill	100	100	39.02	89.06	42.18	45.31	50

Tableau 6.7 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode fréquentielle , après 'cropping'- rotation .

'Avec resize': avec redimensionnement de l'image recadrée vers sa taille initiale .
'Sans resize': sans redimensionnement de l'image recadrée .

Attaques / images	cropping						Rotation de 1^0
	n=1		n=2		n=3		
	Sans 'resize'	Avec 'resize'	Sans 'resize'	Avec 'resize'	Sans 'resize'	Avec 'resize'	
Lena	57.81	76.56	56.26	57.81	56.26	50	46.87
Barbara	43.75	79.68	50	71.87	54.68	60.93	60.93
Boat	50	70.31	48.43	67.18	56.25	64.06	54.68
Baboon	39.06	60.93	37.5	51.56	40.62	43.75	53.12
Goldhill	53.12	71.87	54.68	62.5	60.93	57.81	57.81

Tableau 6.8 Pourcentage des Bits Identifiés (PBI) dans les images tatouées par la méthode spatiale, après 'cropping'- rotation .

Ces attaques étaient fatales pour le système de marquage pour les deux méthodes , surtout dans le cas du marquage spatiale . La méthode fréquentielle a seulement résisté à la suppression d'un cadre d'une ligne et d'une colonne .

Conclusion et perspectives

Ce projet nous a permet d'étudier les algorithmes de tatouage d'images à la fois dans le domaine spatial et le domaine des transformées. Nous avons également étudier les différentes attaques qu'un système de marquage d'image peut subir, et à la fin, on a implémenté deux méthodes opérant dans deux domaines différents (spatial - fréquentiel). Ces deux méthodes utilisent la même stratégie : la technique multicouche pour insérer le watermark. Les tests effectués ont montré que ces deux méthodes résistent aux attaques de type traitement d'images (compression, filtrage, ajout de bruit) et que la méthode fréquentielle donne de meilleurs résultats que la méthode spatiale. Cependant, les deux méthodes résistent mal, pour ne pas dire sont très fragiles, aux attaques géométriques .

Il s'avère aussi que la robustesse aux attaques géométriques est un problème de recherche. Plusieurs solutions ont été proposées dans la littérature, par exemple : la normalisation de l'image originale avant son tatouage en utilisant un calcul des moments géométriques de cette image [26] [27], ou l'insertion d'une grille secrète de référence afin de pouvoir détecter les transformations géométriques(que l'image peut subir) [30], ou encore l'utilisation d'une marque circulaire symétrique [28]. On peut aussi changer complètement l'espace de travail en utilisant un espace invariant aux transformations géométriques (en utilisant par exemple la transformée de Fourrier-Mellin[29] [35]).

Il serait aussi très intéressant d'étudier les résultats des deux algorithmes sur des images couleurs, en les appliquant à la luminance; le tatouage d'images ne serait en effet que peu utile si il ne concernait pas les images couleurs.

En fin, on peut dire que jusqu'ici, aucun algorithme de watermarking proposé dans la littérature n'a été concluant. C'est une technologie prometteuse, un domaine en plein ébullition, mais qui s'avance trop rapidement. On y retrouve des notions empruntées des communications, de la cryptographie, de la psychovisualisation, de la théorie des codes, de la compression de données ... . Tellement de sujets pointus qui peuvent dérouter bon nombre d'auteurs qui ne peuvent être spécialistes dans tous ces domaines .

Annexe A

l'image originale
lena.tif 128x128



α=0.2 (PSNR=11.7db) α=0.4 (PSNR=3.5db) α=0.8 (PSNR<1db)

Modification des coefficients HF (sans exception)



α=0.2 (PSNR=23.9db) α=0.4 (PSNR=17.9db) α=0.8 (PSNR=12db)

Modification des coefficients HF (exceptée la composante continue F(0,0))



α=0.2 (PSNR=46.6db) α=0.4 (PSNR=40.6db) α=0.8 (PSNR=34.6db)

Modification des coefficients MF

Résultats d'insertion d'une marque avec la technique DFT-AM

Annexe B

l'image originale
barbara.tif 128x128

m= π /4 (PSNR=1.8db)

m= π /2 (PSNR=0.8db)

m= π (PSNR=0.3db)

Modification des coefficients HF (sans exception)

m= π /4 (PSNR=9.3db)

m= π /2 (PSNR=3.1db)

m= π (PSNR=0.4db)

Modification des coefficients HF (exceptée la composante continue F(0,0))

m= π /4 (PSNR=28.5db)

m= π /2 (PSNR=19.2db)

m= π (PSNR=5.6db)

Modification des coefficients MF

Résultats d'insertion d'une marque avec la technique DFT-PM

Annexe C

l'image originale
goldhill.tif 128x128



α=0.2 (PSNR=12db) α=0.4 (PSNR=4db) α=0.8 (PSNR<1db)
Modification des coefficients HF (sans exception)



α=0.2 (PSNR=23.5db) α=0.4 (PSNR=17.5db) α=0.8 (PSNR=11.7db)
Modification des coefficients HF (exceptée la composante continue I(0,0))



α=0.2 (PSNR=44.5db) α=0.4 (PSNR=38.5db) α=0.8 (PSNR=32.5db)
Modification des coefficients MF

Résultats d'insertion d'une marque dans le domaine DCT

BIBLIOGRAPHIE

[1] F.A.P. Petitcolas ,R.J. Anderson, M.G.kuhn," *Information hiding-A survey*", in proceedings of the IEEE vol.87 no.7,July 99,pp.1062-1078.

[2] J.J.K.O Ruanaidh, W.J.Dowling, F.M.Boland , "*Watermarking digital image for copyright protection* ", IPA95 special section in IEEE Proc-Vis . Image Process, Vol .143, No.4, August 1996, pp.250-256.

[3] . www-rocq.inria.fr\codes\Watermarking\default.html.

[4] A.Marion "*Introduction aux techniques de traitement d'images*", Eyrolles. 1987.

[5] J.P.Guillois "*Techniques de compression des images*", HERMES, Juin 96.

[6] R.C.GANZALES et P.WINTZ "*digital image processing*", Edition WESLEY, 2eme édition novembre 1987.

[7] MICROSOFT "*Encyclopédie ENCAETA*" série 1998.

[8] www.ccr.jussieu.fr/urfist/image numérique/home image.html .

[9] M.KUNT " *Traitement numérique des images* " volume 2.juillet 1993.

[10] Hardancourt "*Fou du multimédia*" Sybex 1995.

[11] M.Kutter and F.A.P.Petitcolas "*A faire benchmark for image Watermarking systems*" Electronic Imaging 99.Security and Watermarking of Multimedia contents, vol.3657 sans Jose, CA,USA,25-27 January 1999 .

[12] F.A.P. Petitcolas, Markus G. Kuhn and Ross J.Anderson," *Attacks on copyright Marking Systems*", David Aucsmith, Ed, Second workshop on information hiding, in vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, USA, 14-17 April, 1998, PP.218-238.

[13] S. Voloshynovskiy, S. Pereia, T. Pun, J.J. Eggers and J.K. Su, "*Attacks on Digital Watermarking: Classification, Estimation-Based Attacks, and Benchmarks*" Procedings in the IEEE Communication Magazine, August 2001.

[14] F.ABTROUN et M.HADDAD "*Watermarking video*" PFE . ENP 2001.

[15] M.BENZITOUNI et L.M.CHOUITER "*Watermarking audio* ", PFE, ENP 2002.

[16] Ingemar J. Cox and jean-PAUL M.G.Linnartz, "*Some general methods for tampering with Watermarking*", appeared in IEEE International conference on image processing, 1997.

Bibliographie :

[17] Guy De Smet " *Etat de l'art de Watermarking, application aux séquences vidéo MPEG* " Mémoire de licence en informatique ULB (Belgique), 1999.

[18] WOLFGANGR.B and DELP E.J "*A Watermarking technique for digital imagery :further studies*" In Int.Conf.on Imaging science, systems and technology .Las Vegas, Nevada, July 1997.

[19] J-L. Degelay, C.Rey, S.Roche "*Introduction au tatouage d'image*", Institut Eurécom, Multimédia Communication DPT. (http : //www.eurecom.fr/~image).

[20] W.BENDER, DGRUHL et MORIMOTO, "*Techniques for data hiding*", In Proc. Of SPIE, February 1995, vol 2420, P40.

[21] Boris Vassaux "*codage et insertion de messages pour le tatouage d'images* ", Rapport DEA, INPGrenoble 2000.

[22] L. Cox, J. Killian, T. Leighton, T. Shamoon, "*Secure Spread spectrum Communication for Multimedia* ", technical report, NEC Research Institute, 1995.

[23] S. Winkler, M. Kutter, "*ver sun tatouage à étalement de spectre optimal utilisant le système visuel humain* ", Laboratoire de traitement des signaux, Ecole polytechnique Fédérale de Lausanne, 1015 lausanne, Suisse.

[24] J. Zhao, E. Koch, "*Embadding robust label into images for copyright protection*", Technical report, fraunhofer Institute for Computer Graphics, Darmsdadt, Allemagne, 1994.

[25] F. Alturki and R. Mersereau "*An oblivious robust digital watermark technique for still images using DCT phase Modulation*", Georgia Institute of Technology. USA. 2000.

[26] P. Dong and N.P. Galarsanos "*Affine Transformation Resistant Watermarking based on image normalisation*", Dpt. of electrical engineering, Illinois Institute of Technology. Chicago 2002.

[27] M. Alghoniemy and A.H.Tewfik "*Geometric distortion correction through image normalisation*", Multimedia and Expo, 2000, ICME 2000.

[28] V. Solachidis and I. Pitas "*Circulary Symetric watermrk embedding in 2D.CFT domain*", University of Thessaloniki, Greece 1999.

[29] J.O. Ruanaidh and T. Pun "*Rotation, Scale and rotation invariant spread spectrum digital image watermarking*", signal processing, vol. 66, no. 3, PP 303-317, 1998.

[30] G.csurka, F.Deguillaune, J.O Ruanaidh et T. Pun "*Tatouage d'image basé sur la transformée de fourrier discrète*", University of Geneva. Switzerland (http://cuiwww.unige.ch/~vision) 2000.

[31] ANNE-MANOURY "*Tatouage d'image numérique par paquets d'ondelettes*", Thèse de doctorat, Ecole centrale de NANTES 2001.

Bibliographie :

[32] J.J.K. O Ruanaidh, W.J. Dowling, and F. M. Boland, "*Phase Watermarking of Digital Images*", Proceedings of the IEEE International Conference on Image Processing, pp. 239-242, September 1996.

[33] D. Kundur and D. Hatzinatos "*A Robust digital image watermarking method using wavelet-based fusion*", University of Taronto, Canada. 1997.

[34] Onur Mutlu "*An Overview of image watermarking algorithms*", Project repport, EE 371R Digital image processing, descember 2001.

[35] C. Y. Lin, M. Wu, etc, "*Rotation, Scale, and Translation Resilient Public watermarking for images*," in IEEE trans. on image processing, vol. 10, no.5, May 2001.

[36] B.VASSAUX, P.BAS, J.M.CHASSERY "*Tatouage d'images par étalement de spectre : Apport de la technique CDMA en mode multicouche*" CORESA2000 19 ET 20 OCTOBRE 2000

[37] F. Bartolini, M. Barni, V. Cappellini, A. Piva "*Mask building for perceptually hiding frequency embedded watermarks*" University of Firenze, Italy 1998

[38] J.Mayer, A.V.Silv´erio and J.C.M.Bermudez "*On the Design of Pattern Sequences for Spread Spectrum Image Watermarking*" International Telecommunications Symposium – ITS2002, Natal, Brazil