République Algérienne Démocratique et Populaire
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOHAMED BOUDIAF-M'SILA
FACULTE DE TECHNOLOGIE
DEPARTEMENT DE L'ELECTRONIQUE

MEMOIRE DE MASTER

DOMAINE : SCIENCES ET TECHNOLOGIES

FILIERE : TELECOMMUNICATIONS

OPTION : SYSTEMES DES TELECOMMUNICATIONS

Présenté par : SELLAMI Chaima

SAHRAOUI Soumia

Thème:

TATOUAGE FRAGILE DES IMAGES NUMERIQUES

Devants les jury suivants:

Mr KHALFA Ali	**Université de M'sila**	**Président du jury**
Mme HAMADOUCHE Loubna	**Université de M'sila**	**Rapporteur**
Mr CHALABI Azzedine	**Université de M'sila**	**Examinateur**

Promotion : juin 2017/2018

Dédicace

Je dédie ce travail à mes chers parents

SELLAMI *Abdel Fatih*, **BENYAHIA** *Hafssa*

Qu'ils trouvent ici toute ma gratitude, pour leur

Soutien tout au long de mes études.

A mon cher frère **SELLAMI** *zain el abiddine et toutes*

mes sœurs que dieu les protège

A tous mes collègues de la promo 2017/2018

A tous mes cousins et ma grande famille

A tous mon amie Chahrazed et tous mes êtres chers.

A tous ceux que j'aime.

SELLAMI Chaima

Je dédie ce travail

A mes chers parents « SAHRAOUI nadir et

BOUROUIS meriem »,

Pour tous leurs sacrifices, leurs amours, leur soutien et leurs prières tout au long de mes études.

A mes chères frères et pour leurs encouragements et leur soutien.

A celui que j'aime beaucoup et qui m'a soutenue moralement tout au long de ce travail, mon très cher mari **« DELLOUM *Imad* ».**

A tout ma famille et mes amis et toux ceux qui ont contribué pour que projet soit possible.

Je vous dis merci

SAHRAOUI Soumia

Remerciement

Dieu, Merci de nous avoir guidé sur le meilleur des chemins.

En cette occasion de soutenance de mémoire de Master;

nous avons le plaisir de formuler ma plus humbles remerciements à :

En premier lieu, à HAMADOUCHE Loubna , notre encadreur dans ce travail et mon maître. On la remercie pour ses conseils, sa compréhension, sa disponibilité, son aide ainsi que sa patience.

En second lieu, tous les enseignants, sans exception, qui j'ai honoré lors de notre cursus en nous prodiguant le savoir avec dévouement.

Ensuite, tout le corps enseignants de la faculté de Technologie en général, et ceux du département d'électronique en particulier.

Enfin, Messieurs les membres du jury, qui ont accepté de nous honorer en acceptant d'examiner, de juger et d'évaluer notre mémoire de fin d'études pour l'obtention du Master .

Merci à ceux qu'on oublie toujours : mes maîtres d'école, de collège, et de lycée. Je vous suis très reconnaissante.

A toute personne qui a contribué de près ou de loin à l'élaboration de ce travail, Nous disons, MERCI.

SELLAMI Chaima, SAHRAOUI Soumia

résumé

Le « watermarking » ou tatouage d'image a connu ces dernières années, un essor spectaculaire. L'utilisation accrue des applications multimédia pose de plus en plus des problèmes concernant la préservation de la confidentialité et de l'authenticité de la transmission des données numériques. Ces données, et en particulier les images doivent être protégées de toute falsification. La solution adaptée à ce problème est l'utilisation du tatouage fragile. Plusieurs méthodes efficaces de tatouage des images numériques ont en effet été développées., cette méthode est basée sur l'utilisation de la décomposition en valeur singulières (SVD) et l'opérateur XOR en tant qu'une fonction de hachage pour la vérification les données d'authentification et d'intégrité des images. Les résultats expérimentaux ont montré la faisabilité de notre algorithme proposé, et que notre approche permet d'obtenir une bonne imperceptibilité et sensibilité face aux divers types d'attaques.

Mots clés : tatouage fragile, tatouage numérique, intégrité, authentification, LSB, SVD, XOR.

Table de matières

Dédicace……..……....i

Remerciements……..……...ii

Résume…….....iii

Table des matières…….……i

Table d'abréviations …….……..…v

Liste des figures..……..x

Introduction générale……..…..1

Chapitre I Concepts de base sur l'image numérique

1.1 introduction ……..……...3

1.2 Système de traitement d'images**.....**3

1.2.1 L'acquisition**.....**…3

1.2.2. Le pré traitement**.....**4

1.2.3 L'analyse**.....**4

1.2.4 L'Interprétation**.....**4

1.3 Définition de l'image**.....**5

1.4 Images numériques**.....**5

1.4.1 Les images matricielles **.....**

1.4.2 Les images vectorielles **.....**

1.4.3 La différence entre images matricielles et vectorielles**.....**7

1.5 Caractéristiques d'une image numérique……..7

1.5.1 le pixel ……...7

1.5.2 Voisinage de pixels ……..…..7

1.5.3 Résolution d'une image……8

1.5.4 Poids d'une image…….……..8

1.5.5 Histogramme……8

1.5.6 Luminance…….....9

1.5.7 Contraste……..……9

1.6 Les différents types d'images numériques…….……...…10

1.6.1 Les images binaires .. ……..……...…10

1.6.2 Image à niveaux de gris……...…..…11

1.6.3 Image couleur……...11

1.7 Formats d'image numérique ……..….12

1.7.1 BMP (BitMaP) ……..…..12

1.7.2 GIF (Graphical Interchange Format) …….……12

1.7.3 TIFF (Tagged Image File Format) ……...……12

1.7.4 JPEG …….……12

1.8 Conclusion ……. ……...13

Chapitre II Tatouage des images numériques

2.1 Introduction……..…14

2.2 Historique et Terminologies……...…14

2.3 Un peu de terminologie……...…16

2.4 Définition du tatouage numérique ……..…….....16

2.5 Différences avec la cryptographie ……..……...17

2.6 Tatouage visible et invisible ……...…17

a) Tatouage visible…….……..17

b) Tatouage invisible ……..……..18

2.3 Caractéristiques d'un marquage numérique invisible…….....18

2.3.1 Imperceptibilité ……..18

2.3.2 Robustesse ……..……...19

2.3.3 Capacité ……..……..….20

2.3.4 Sécurité ……..……...20

2.4. Modèle générique du tatouage……..……..….21

2.5 Domaines d'applications ……..……...22

5.1 Protection du droit d'auteur ……..……..23

5.2 Authentification du contenu d'une image……..……..…...23

5.3 Contrôle du nombre de copies…….……...…23

2.6 Classification selon le domaine d'insertion ……..……....24

2.6.1 Domaine Spatial ……24

2.6.2 Domaine Fréquentiel ……..24

2.7 Les Attaques ……..24

2.8. Conclusion ……25

Chapitre III Tatouage fragile des images numérique

3.1 Introduction……..…..27

3.2 Principe du tatouage fragile…….…..27

3.2.1L'authentification…….……28

3.2.2 La sécurité…….....28

3.2.3 La complexité algorithmique (Le coût) ……..28

3.2.4 L'intégrité des images numériques……...……..29

3.3 Schéma générique d'un système d'authentification d'image…….....…30

3. 4 Modèle générique d'une technique de tatouage fragile……..……..30

3.5 Caractéristiques d'un système de tatouage fragile……..…….30

3.5.1 Détection des falsifications……..……..…..31

3.5.2 Imperceptibilité…….……..31

3.5.3 La nécessité de l'image originale pour la détection de la marque…….31

3.5.4 La détectabilité du watermark après le recadrage (cropping) d'image……..…..31

3.5.5 L'insertion du watermark par des personnes non autorisées doit être difficile……...31

3.6 Types des attaques……. ……31

3.6.1 Copy attack ……..……..32

3.6.2 Collage attack : ……..……32

3.6.3 StirMark2……32

3.6.4 Brute Force Attack……..……..32

3.6.5 Attaques malveillantes……..……...32

3.7 Algorithmes de tatouage fragile……..……33

3.7.1 Utilisation des bits de poids faible (LSB) ……..……..…33

3.7.2 L'algorithme de Walton……..……..…33

3.7.3 Algorithme de Fridrich et Goljan……...……..…34

3.7.4 Utilisation de la méthode Self-embedding ……..34

3.8 Conclusion……...……..…..35

Chapitre IV Algorithme de tatouage fragile pour l'authentification d'images

4.1 Introduction ……..36

4.2 Algorithme de tatouage en utilisant la SVD ……..……36

4.3 La décomposition de la valeur singulière (SVD……...……...…36

4.4 Algorithme d'insertion…… ……..37

4.5 Algorithme d'extraction et de vérification……..…38

4.6 Algorithme extraction de la marque et la localisation……..…39

4.7 Mesure de qualité……..…40

4.8 Rapport crête signal sur bruit (PSNR) ……..…....41

4.9 Résultats expérimentaux ……..…..……...42

4.9.1: Application de l'algorithme pour l'authentification et l'intégrité……..…..42

4.9.2 application de l'algorithme de la localisation……..43

a) Recadrage ……...……..…43

b)La compression……...……...43

c) Modification ……44

d) le filtrage ……..……...……44

4.10 Exemple pour autre image ……...……45

a) Modification …..…….....…45

b) Compression ……..45

c) Filtrage ……...46

d) Recadrage ……..……...46

4.11 Les résultats... ……...……46

4.12 Conclusion ……..……..47

Conclusion générale ……..…….....48

Bibliographie……...……..……..49

Table d'abréviations

SVD: décomposition valeur singulière

pixel :petite élément d'image

BMP : Bitmap

GIF: Graphical Interchange Format

TIFF :Tagged Image File Format

JPEG: Joint Photographic Experts Group

DFT :transformée de Fourier discrète

DCT :transformée en cosinus discrète

DWT :la transformée en ondelettes

LSB :bits de poids faible

XOR: operateur logique

PSNR : rapport signal sur bruit (Peak Signal to Noise Ratio)

EQM :l'erreur quadratique moyenne

Image hôte :Image originale

liste Figures

Figure 1.1 1839 : photographie (Louis Jacques Mandé Daguerre) I 1895 : cinématographe (frères Lumière) I 1885 : rayons X (Röntgen) ……..……..3

Figure 1.2 Figure 1.2 Schéma d'un système de traitement d'images ..…….. 5

Figure 1.3 code génétique" de l'image numérique…….……...6

Figure 1.4 images matricielles (Bitmap) composées de pixels……..……7

Figure 1.5 image vectorielle……7

Figure 1.6 la taille d'image (nombre de pixels) divisé par 4. ……..……..8

Figure 1.7 Les bornes de répartition des niveaux de gris . ……..…9

Figure 1.8 Deux images différentes avec même histogramme……..10

Figure 1.9 Exemple de Contraste ……..……...10

Figure 1.10 exemple image binaire……..……..…..10

Figure 1.11 Variation de nombres de niveau de gris pour même image…….……11

Figure 1.12 Principe additif des couleurs R.V.B…….……11

Figure 2.1 Exemple de sténographie réalisé à l'aide de lait . ……..……15

Figure 2.2 Nombre de publications sur le tatouage numérique (INSPEC - juin 2010) …. ….16

Figure 2.3 Exemple d'un tatouage visible . ……..……...17

Figure 2.4 Exemple d'un tatouage invisible. ……..……..……18

Figure 2.5 Contraintes du tatouage numérique ……..……..…20

Figure 2.6 Modèle générique d'un système du tatouage. ……..……...22

Figure 2.7 Classification des attaques selon Voloshynovskiy et al ……..……..25

Figure 3.1 Schéma général d'un système d'intégrité basé sur un tatouage fragile . ……..28

Figure 3.2 Le modèle général d'un système d'authentification basé sur le tatouage fragile.....30

Figure 4.1 schéma d'insertion de la marque……38

Figure 4.2 Schéma d'extraction et vérification……39

Figure 4.3 : algorithme de extraction et localisation ……..40

Figure 4. 4 (a) Image originale et (b) Image tatouée avec l'algorithme utilisant la SVD ……..42

Figure 4.5 Image tatouée après le recadrage et la marque extraite……43

Figure 4.6 Image tatouée après la compression et la marque extraite……...44

Figure 4.7 Image tatouée après la modification et la marque extraite……4

Figure 4.8 Image tatouée après le filtrage et la marque extraite……45

Figure 4.9 Image tatouée après (modification, compression, filtrage , recadrage)et la marque extraite……46

Introduction générale

Les réseaux numériques sont tellement développés qu'ils sont devenus un mécanisme primordial de communication. Ils permettent de transmettre toute sorte d'informations : textuelles, sonores, et principalement des images. Les images constituent la grande partie de l'ensemble des documents numériques manipulés et échangés dans le monde de l'Internet.

Cette extraordinaire révolution technique de l'analogique vers le numérique ne s'est pas faite sans engendrer des inquiétudes puisque n'importe qui peut facilement copier, modifier et distribuer les documents numériques sans risque de les détériorer. Il est très difficile de trouver un compromis entre le libre accès à l'information et le respect des droits d'auteurs, donc, il est préférable de protéger les documents numériques avant de les transmettre[1].

Après l'explosion de l'internet, le commerce électronique et les services de partage des fichiers électroniques sont devenus très populaire, des milliards des fichiers électroniques se trouvent dans l'internet, aussi la banalisation des outils de traitement et de transmission d'images et de vidéo a également ouvert le champ à la copie, l'altération et la distribution illégale. Les premiers à en souffrir sont les artistes, l'économie et l'emploi de façon générale.

Il existe plusieurs techniques pour l'authentification des images numériques, le tatouage numérique est parmi les solutions les plus efficaces face à ce problème.

En générale, l'authentification d'une image numérique est réalisée en utilisent un tatouage fragile. Avec le tatouage fragile, l'information cachée est perdue ou modifiée dès que l'image hôte subit une modification, la perte du watermark ou son altération sera prise comme une preuve que les données ont été falsifiées, alors que la récupération du watermark contenu dans les données est utilisée pour démontrer l'intégrité des données [2].

Nous nous intéressons dans ce mémoire au tatouage numérique des images dans le but d'étudier et d'implémenter des méthodes de tatouage d'images basé sur la décomposition en valeurs singulières (SVD). Cette transformée (la SVD) a été découvert indépendamment par Beltrami en 1873. Elle n'a été employée comme outil informatique qu'aux années 60. Maintenant, la SVD est un des outils les plus utiles de l'algèbre linéaire avec plusieurs applications dans la compression d'image, le tatouage d'image et d'autres champs de traitement des signaux [1].

Le présent mémoire est organisé en quatre chapitres :

- chapitre1: présente une introduction aux images numériques. Plus précisément, nous présentons quelques terminologies et quelques notions pertinentes dans le domaine des images numériques.
- chapitre 2: définit et décrit le principe général du tatouage et ses applications.
- chapitre 3: décrit le principe du tatouage fragile et ses caractéristiques.
- chapitre 4: nous étudions et implémentons des algorithmes de tatouage basés sur la SVD et nous présentons quelques résultats expérimentaux obtenus par notre algorithme de tatouage fragile des images numériques.

Chapitre I

Concepts de base sur l'image numérique

1.1 introduction

Le traitement d'images est un domaine très vaste qui a connu, et qui connaît encore un développement important depuis quelques dizaines d'années. On désigne par *traitement d'images numériques* l'ensemble des techniques permettant de modifier une image numérique, d'améliorer son aspect visuel ou d'en extraire des informations jugées pertinentes. [3]

Les applications du traitement d'images sont multiples et interviennent dans de nombreux aspects de la vie courante et professionnelle. Avec l'ère de l'information, l'internet haut-débit, de l'audiovisuel et du numérique, l'expansion et la circulation des supports multimédia ont beaucoup augmenté. La plupart des appareils scientifiques fournissent des images (appareils photographiques, caméra, radio-graphe, scanner, sonar,…..).[4]

Figure 1.1 1839 : photographie (Louis Jacques Mandé Daguerre) I 1895 : cinématographe (frères Lumière) I 1885 : rayons X (Röntgen) [4]

Dans ce chapitre, nous aborderons les notions de base nécessaires à la compréhension des techniques de traitement d'images.

1.2 Système de traitement d'images

Un système de traitement numérique d'images est composé de :

1.2.1 L'acquisition

L'acquisition est la première étape dans le système de traitement d'images, à partir de laquelle une image numérique est produite, elle consiste en deux étapes l'échantillonnage et le codage. L'échantillonnage correspond au

décodage de signal en pixels et le codage correspond à la quantification de l'intensité de chaque pixel en une valeur numérique appelée niveau de gris.

1.2.2. Le pré traitement

Regroupe toutes les opérations de manipulation de l'image qui permettent d'en améliorer la qualité. Ces manipulations produisent une nouvelle image. On trouve différentes techniques :

- **La compression** : Réduction du volume de l'image, la compression d'images est donc encore plus d'actualité aujourd'hui .
- **La restauration** : correction des défauts dus à une source de dégradation.
- **L'amélioration** : Modification de l'image dans le but de la rendre plus agréable à l'œil.
- **Codage et décodage** : à des fins de stockage ou de transmission, est la transformation des images du monde physique en une forme comprise par l'ordinateur et l'inverse.
-

1.2.3 L'analyse

Elle a pour but d'analyser les objets contenus dans l'image. Elle est essentiellement composée par la phase de segmentation. Elle consiste à construire une représentation symbolique de l'image c'est-à-dire définir une carte de l'image qui décrit les régions homogènes selon un critère de similarité.

1.2.4 L'Interprétation

Où la compréhension a pour but le passage de la description structurelle à la description sémantique en regard à certains objectifs. Cet objectif peut être très simple (mesure de certains paramètres sur des formes) ou beaucoup plus complexe (description du contenu de la scène en terme de concepts non mathématiques).[2]

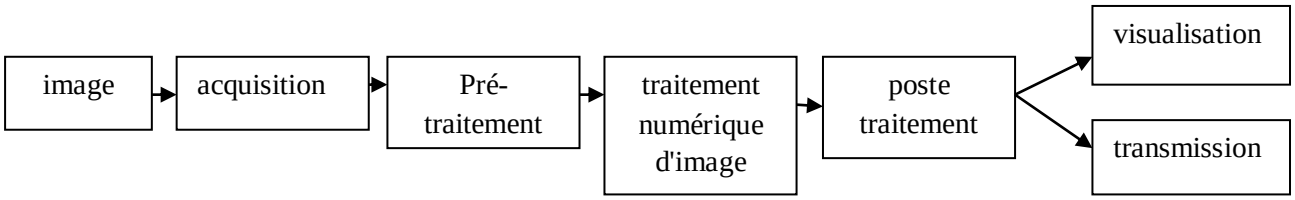

Figure 1.2 Figure 1.2 Schéma d'un système de traitement d'images [2]

1.3 Définition de l'image

L'image est une représentation d'une personne ou d'un objet par la peinture, le dessin, la photographie, le film... etc. Les chercheurs en imagerie disent qu'une image est la conscience que nous prenons d'un aspect du monde extérieur par l'intermédiaire d'un capteur.

En Informatique, une image désigne une structure de données matricielle contenant des pixels. Elle est décrite comme une fonction discrète I(x, y) à deux dimensions, tel que x, y sont les coordonnées spatiales d'un point de l'image I. Cette fonction donne l'intensité lumineuse de chaque pixel de coordonnées spatiales(x, y)[2].

1.4 Images numériques

L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevés à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter.

Exemples d'images numériques :

- image "web".
- image d'un film d'animation.
- sortie des appareils photos et caméscopes numériques.

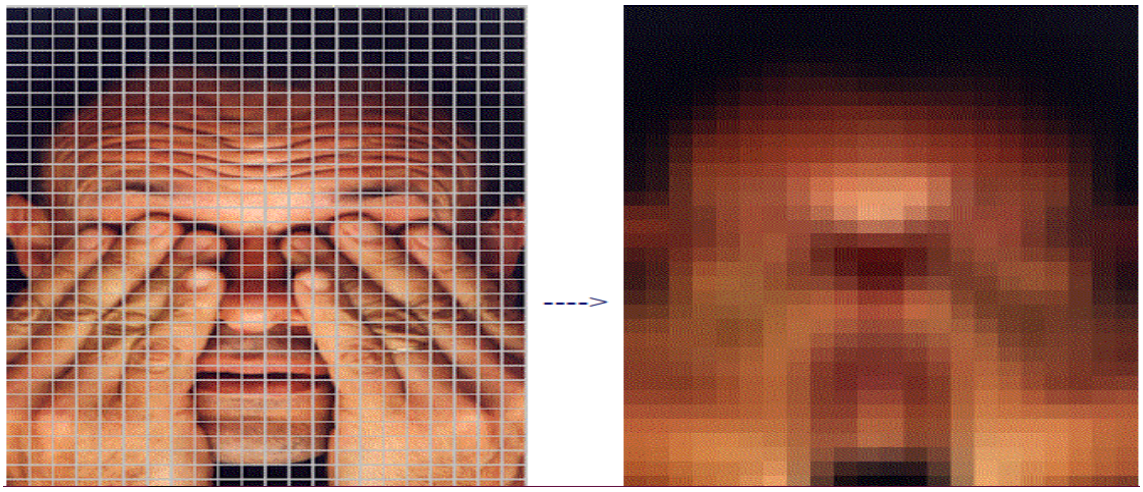

Figure 1.3 code génétique" de l'image numérique[4]

1.4.1 Les images matricielles

Une image matricielle est composée d'un ensemble de points (pixels). Chacun d'eux a une position et une couleur bien précise. Les photos numériques et les documents scannés sont des images matricielles. En cas d'agrandissement, une perte de qualité peut être remarquée.

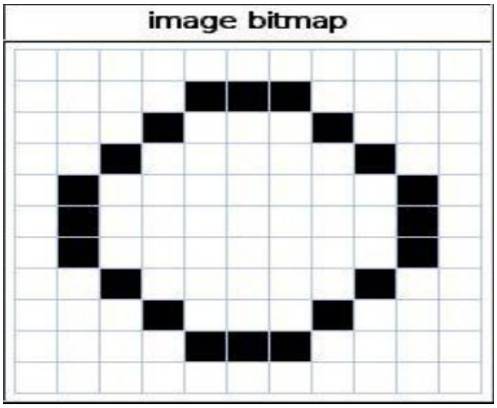

Figure 1.4 images matricielles (Bitmap) composées de pixels.[6]

1.4.2 Les images vectorielles :

Une image vectorielle est composée de formes géométriques pouvant faire l'objet d'une description mathématique (droites, cercles, points, …). Une image vectorielle se redimensionne aisément, sans aucune perte de qualité. Ces images sont très utiles pour des reproductions à grande échelle, des calculs pouvant être réalisés à chaque fois, afin d'obtenir l'image exacte, quelle que soit la taille choisie**. [5]**

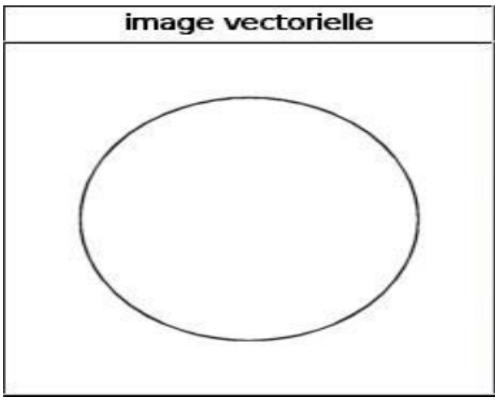

Figure 1.5 image vectorielle

1.4.3 La différence entre images matricielles et vectorielles

La principale différence entre ces deux formats est qu'une image vectorielle peut être agrandie sans perdre sa qualité alors qu'une image matricielle perd en netteté à l'agrandissement.

Les professionnels (graphistes, illustrateurs ou concepteurs) réalisent la majorité de leurs visuels en vectoriel afin de pouvoir les modifier à volonté sans les altérer.[6]

1.5 Caractéristiques d'une image numérique

1.5.1 le pixel

Une image numérique contient un nombre fini de points. Ces points sont appelés pixels (contraction des mots anglais *"picture element"*, c'est à dire élément d'image). Les pixels sont situés sur une grille régulière. A chaque pixel de la grille est associée une couleur ou une nuance de gris.

1.5.2 Voisinage de pixels

On définit le voisinage de tout composante A de l'image I, par l'union de tout les voisinages des pixels de A.

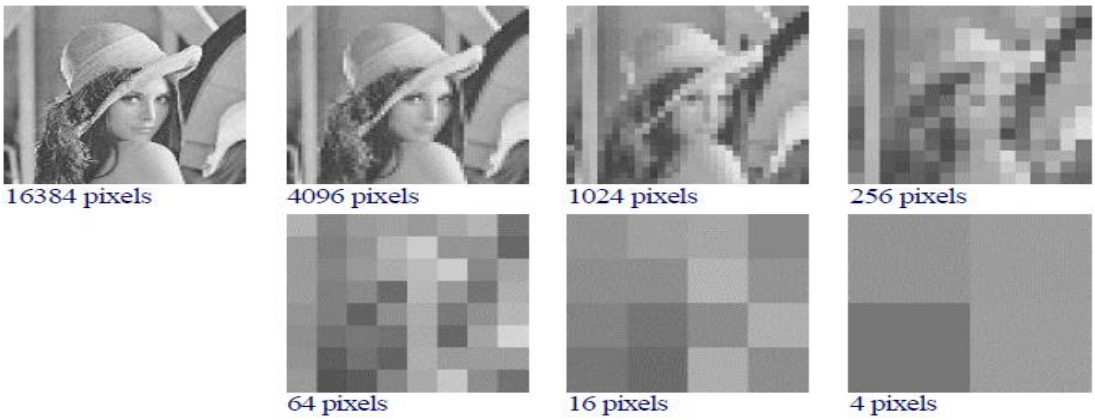

Figure 1.6 la taille d'image (nombre de pixels) divisé par 4 [5]

1.5.3 Résolution d'une image

La résolution d'une image composée de points est définie par la densité des points par unité de longueur. La résolution permet de définir la finesse de l'image. Plus la résolution est grande, plus la finesse de l'image est grande.

Les points d'une image ont différents noms dépendant du média. Sur les écrans on parle de pixel, les médias imprimés parlent de points ou *dots*. Par conséquent la résolution dans le domaine de l'écran est **ppi** - **p**ixels **p**er **i**nch (**PPP** en français :**p**ixels **p**ar **p**ouce). La résolution dans le domaine des médias imprimés est **dpi** - **d**ots **p**er **i**nch.

1.5.4 Poids d'une image

La définition d'une image est le nombre de pixels total, c'est-à-dire le nombre de colonnes de l'image que multiplie son nombre de lignes. Une image possédant 640 pixels en largeur et 480 en hauteur aura une définition de 640 pixels par 480 notée 640x480 = 307200 pixels. Puisqu' un pixel = 3 octets pour une image en couleurs, cette image pèse 921600 octets (1 Mo).

1.5.5 Histogramme

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 (couleur) dans l'image. Il permet de donner un grand nombre d'information sur la distribution de ces niveaux et de voir entre quelles bornes sont reparties dans le cas d'une image trop claire ou d'une image trop foncée.

Il peut être utilisé pour améliorer la qualité d'une image (Rehaussement d'image) en introduisant quelques modifications, pour pouvoir extraire les informations utiles de celle-ci.

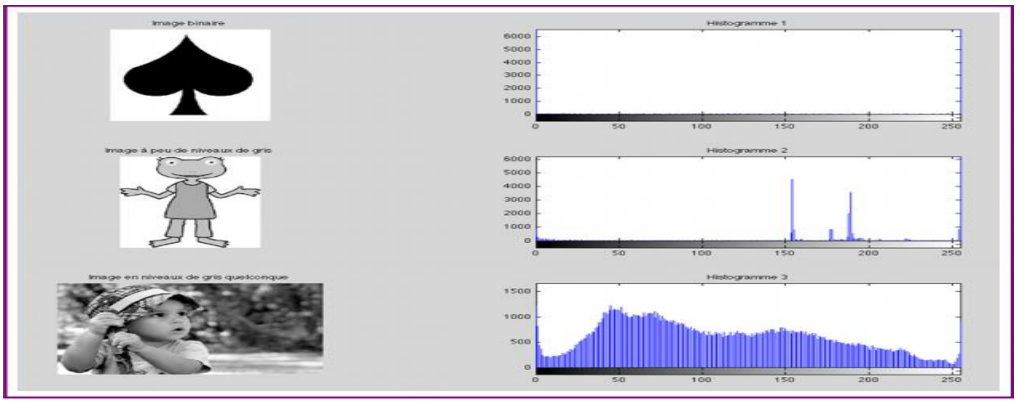

Figure 1.7 Les bornes de répartition des niveaux de gris [4]

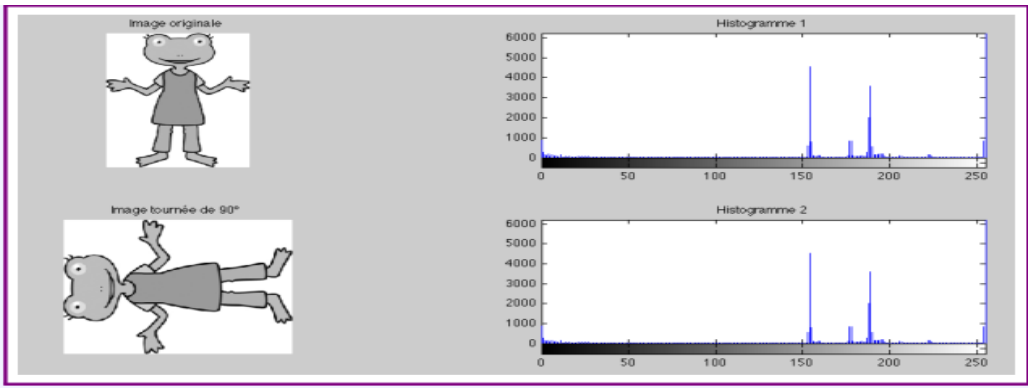

Figure 1.8 Deux images différentes avec même histogramme[4]

1.5.6 Luminance

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 l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance.

1.5.7 Contraste

C'est l'opposition marquée entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Le contraste est défini en fonction des luminances de deux zones d'images. Si L1 et L2 sont les degrés de

luminosité respectivement de deux zones voisines A1 et A2 d'une image, le contraste C est défini par le rapport :

$$C = \frac{L1 - L2}{L1 + L2} \quad [2]$$

Figure 1.9 Exemple de Contraste [2]

1.6 Les différents types d'images numériques

A l'issue de la numérisation, une image numérique est constituée d'un tableau de valeurs entières. Pour pouvoir stocker et transmettre cette image comme n'importe quelle autre donnée informatique, il faut la coder en binaire, c'est-à-dire la décrire par une suite de 0 et de 1. [5]

1.6.1 Les images binaires :

Une image binaire est une image pour laquelle chaque pixel ne peut avoir pour valeur que 0 ou 1.

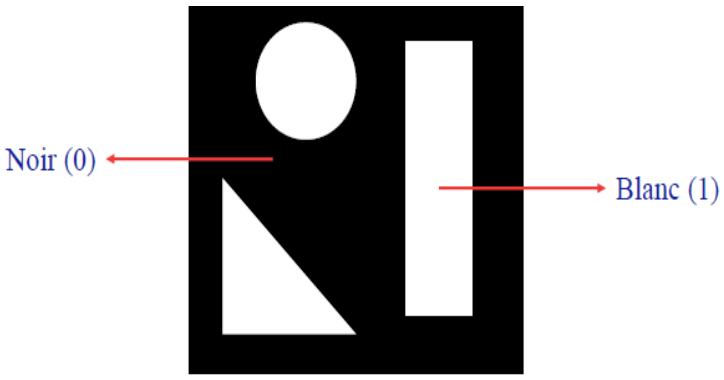

Figure 1.10 exemple image binaire

1.6.2 Image à niveaux de gris

Le niveau de gris est la valeur de l'intensité lumineuse en un point. Il peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Donc pour représenter les images à niveaux de gris, on peut attribuer à chaque pixel de l'image une valeur correspondant à la quantité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255. Chaque pixel n'est donc plus représenté par un bit, mais par un octet. Pour cela, il faut que le matériel utilisé pour afficher l'image soit capable de produire les différents niveaux de gris correspondant. Le nombre de niveaux de gris dépend du nombre de bits utilisés pour décrire la luminance de chaque pixel de l'image. Plus ce nombre est important, plus les niveaux possibles sont nombreux [3].

Figure 1.11 Variation de nombres de niveau de gris pour même image

1.6.3 Image couleur

Une image en couleur correspond à la synthèse additive de 3 images, rouge, vert et bleu. Chaque pixel est donc codé sur $3\times N$ bits.

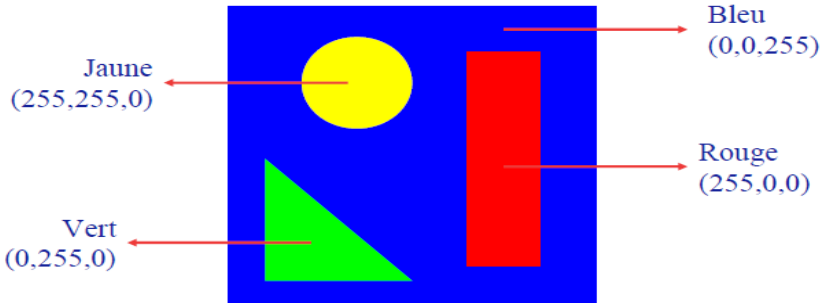

Figure 1.12 Principe additif des couleurs R.V.B

1.7 Formats d'image numérique :

➢ 1.7.1 BMP (BitMaP)

Le BMP est un des formats les plus simples développé conjointement par Microsoft et IBM, ce qui explique qu'il soit particulièrement répandu sur les plates formes Windows et OS/2. C'est un format ouvert et non compressé. Sa taille rédhibitoire rend son utilisation en ligne difficile, mais sa grande compatibilité le rend un format de travail efficace.

➢ 1.7.2 GIF (Graphical Interchange Format)

Le format GIF (*Graphical Interchange Format)* été créé en 1987 par Compuserve pour que les utilisateurs puissent s'échanger des images de façon efficace et moins onéreuse. Ce format permet une compression sans perte (algorithme LZW). Il autorise une bonne compression et une décompression très rapide grâce à la méthode LZW. Cette compression est plus efficace pour les dessins et graphiques que pour les photographies numériques [5].

➢ 1.7.3 TIFF (Tagged Image File Format)

Le TIFF pour (Tagged Image Filea) été mis au point en 1987. C'est un ancien format graphique, permettant de stocker des images bitmap de taille importante (plus de 4 Go compressées), sans perdition de qualité et indépendamment des plates formes ou des périphériques utilisés. Il supporte différents types de compression autant avec que sans perte de données.

Le format TIFF permet de stocker des images en noir et blanc, en couleurs réelles (True color, jusqu'`a 32 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de couleurs.

➢ 1.7.4 JPEG

Ce format est l'un des plus complexes, son étude complète nécessite de solides bases mathématiques, cependant malgré une certaine dégradation, il offre des taux de compressions plus qu'intéressants. JPEG est la norme internationale (ISO 10918-1) relative à la compression d'images fixes, notamment aux images photographiques. La méthode de compression est "avec pertes" et s'appuie sur l'algorithme de transformée en cosinus discrète DCT. Un mode "sans perte" a ensuite été développé mais n'a jamais été vraiment utilisé. Cette norme de compression a été développée par le comite JPEG (Joint Photographic Experts Group) et normalisée par l'ISO/JTC1 SC29.

Ce type de compression est très utilisé pour les photographies, car il est inspiré des caractéristiques de perception visuelles de l'œil humain.

1.8 Conclusion :

Dans ce chapitre, nous avons essayé de présenter quelques notions de bases liées au domaine de l'image numérique et de son traitement, en donnant quelques définitions élémentaires portant sur ce sujet, et qui seront sûrement des points essentiels dans la suite de notre travail, qui s'intéressera dans la prochaine phase, à aborder le sujet de tatouage numérique, son état de l'art, ainsi que les différentes techniques utilisées.

Chapitre II

Tatouage des images numériques

2.1 Introduction

Le tatouage numérique est un domaine scientifique récent apparu au début des années 90 et qui présente de multiples intérêts. Dans ce chapitre, nous présenterons le principe du tatouage numérique des images ainsi que quelques-unes de ses applications. Après avoir donné un aperçu historique sur cette technique et sur les techniques de dissimulation de l'information, nous présenterons le tatouage numérique et ses différentes étapes qui conduisent à l'insertion de la marque. Ensuite nous décrirons quelques représentations de l'image dans le domaine spatial et fréquentiel. Nous présenterons les différentes applications possibles du tatouage numérique pour les images à la fin de ce chapitre et nous présenterons brièvement l'évaluation en terme d'imperceptibilité et de robustesse des schémas de tatouage numérique des images .

2.2 Historique et Terminologies

Une Part d'histoire

L'apparition de la stéganographie est très ancienne, elle remonte à l'antiquité. En effet, les premiers exemples connus nous viennent directement des Grecs. Ils rasaient les cheveux d'un esclave, puis tatouaient sur son crâne un message. Une fois les cheveux repoussés, l'esclave pouvait traverser les territoires ennemis sans éveiller les soupçons. Une fois à destination, il suffisait de raser à nouveau le crâne pour récupérer le message. Bien sûr, il ne fallait pas être pressé... Au cours de l'histoire, les techniques ont évoluées sans cesse, et on a vu au fur et à mesure du temps la naissance de nouveau procédés plus efficaces. Par exemple les encres sympathiques, qui fut la méthode la plus utilisée au cours des siècles. On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait ou de certains produits chimiques. Il est invisible à l'œil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message .

Figure 2.1 Exemple de sténographie réalisé à l'aide de lait .

Les tatouages du papier sont apparus dans l'art de la fabrication du papier, il y a presque 700 ans. Le plus ancien document tatoué trouvé dans les archives remonte à 1292 et a son origine dans la ville de Fabriano en Italie, qui a joué un rôle important dans l'évolution de l'industrie papetière.

A la fin du troisième siècle, environ 40 fabricants du papier partageaient le marché du papier. La concurrence entre ces fabricants était très élevée et il était difficile que n'importe quelle partie maintienne une trace de la provenance du papier et ainsi que son format et sa qualité. L'introduction des tatouages était la méthode parfaite pour éviter n'importe quelle possibilité de confusion .Après leur invention, les tatouages se sont rapidement étendus en Italie et puis en Europe et bien qu'au commencement utilisé pour indiquer la marque ou le fabricant du papier, ils ont servi plus tard pour indiquer le format, la qualité, et la force du papier, et ont été également employés comme une base pour dater et authentifier le papier.

L'analogie entre le tatouage du papier et le tatouage numérique est évidente : les tatouages du papier des billets de banque et de timbres ont inspiré la première utilisation du terme «Marque d'eau» dans le contexte de données numériques. Les premières publications portant sur le tatouage d'images numériques ont été publiés par Tanaka et al. en 1990 et par Tirkel et al. en 1993.

En 1995, le temps est évidemment bien de prendre ce sujet, et il a commencé à stimuler l'augmentation des activités de recherche. Depuis 1995, le tatouage numérique a gagné beaucoup d'attention et a évolué très rapidement et alors qu'il y a beaucoup de sujets ouverts pour davantage de

recherches, des méthodes de travail et des systèmes pratiques ont été développés .

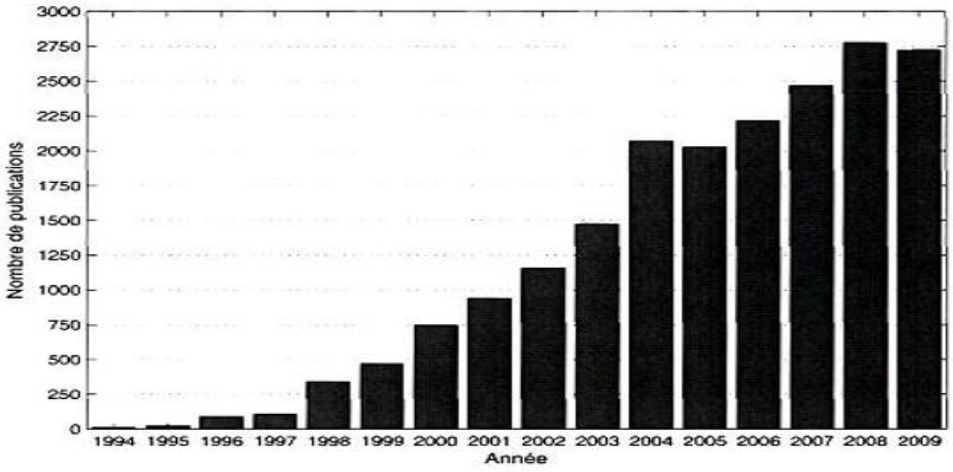

Figure 2.2 Nombre de publications sur le tatouage numérique (INSPEC - juin 2010) .

2.3 Un peu de terminologie

Pour nommer le tatouage d'images dans le monde, on utilise généralement le mot anglais "Watermarking". Ce terme anglo-saxon, signifiant "filigranne" à la base, correspond au fait même de masquer des données sur un autre support. Cela regroupe par conséquent des notions plus précises et restrictives de marques, invisibles et robustes, appliquées au service de protection des droits d'auteurs. Ce qui nous amène donc à employer une expression associant davantage cette idée d'enfouissement de données, le "data embedding" .

2.4 Définition du tatouage numérique

Le tatouage numérique ou watermarking est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. Le message inclus dans le signal hôte, généralement appelé marque ou bien simplement message, est un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant du créateur, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le signal hôte. [1]

2.5 Différences avec la cryptographie

En cryptographie, l'objectif n'est pas de dissimuler des informations dans d'autres, mais plus simplement de rendre l'information que l'ont désiré transmettre complètement illisible à toute personne ne possédant pas la donnée nécessaire à son décodage. De plus en cryptographie si le message primaire est modifié, il devrait être impossible de le recouvrer, tandis qu'en sténographie, le message secondaire est supposé rester accessible et ce même après de multiples recopies et manipulations diverses du message primaire [1].

2.6 Tatouage visible et invisible

On distingue généralement deux classes du tatouage : visible et invisible.

a- Tatouage visible

Le tatouage visible est très simple. Il est équivalent à l'estampage d'un watremark sur le papier, et pour cette raison il est appelé parfois estampage numérique. Le tatouage visible altère le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre). Il est fréquent que les agences de photo ajoutent un watermark visible en forme de copyright (©) aux versions de prévisualisation (basse résolution) de leurs photos. Ceci afin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watermark est visible, alors elle peut être facilement attaquée. Néanmoins, nous trouvons des applications qui demandent que le watermark soit visible, c'est le cas du logo des sociétés dans les programmes télévisuels [7].

Figure 2.3 Exemple d'un tatouage visible [2].

b-Tatouage invisible

En revanche, le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le signal d'une manière imperceptible par l'utilisateur final. Pour reprendre l'exemple de l'agence de photo, les photos hautes résolutions vendues par l'agence possèdent elles au contraire un watermark invisible, qui ne dégrade donc pas le contenu visuel, mais qui permet de détecter l'éventuelle source d'un vol. Le message caché par le tatouage peut être un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur .

Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs . La majorité des techniques concernant la protection des propriétés intellectuelles suivent cette branche.

Dans ce qui suit, nous nous concentrons sur cette dernière catégorie, et le mot « Tatouage » est pris au sens du tatouage invisible [2].

Figure 2.4 Exemple d'un tatouage invisible.

3 -Caractéristiques d'un marquage numérique invisible

Les performances d'un marquage sont appréciées sous les trois critères suivants : Imperceptibilité, Robustesse, Capacité [2].

3-1 Imperceptibilité

La notion d'imperceptibilité est liée à la perception visuelle ou auditive des distorsions résultant à l'insertion de la marque dans un document. Le tatouage doit être invisible pour un observateur humain. De plus, la marque insérée ne devrait pas affecter la qualité du document.

L'évaluation de la qualité visuelle ou auditive des documents après le tatouage devient un critère important pour la validation des algorithmes de tatouage. En ce qui concerne les images, une telle évaluation nécessite une analyse du système visuel humain (HVS). Plusieurs mesures objectives ont été proposées dans la littérature pour mesurer la qualité visuelle d'un document tatoué. Une description détaillée des mesures objectives peut être trouvée dans [Nguyen 2011][2].

3-2 Robustesse

La robustesse représente la capacité du tatouage à résister aux dégradations du document tatoué. Ces modifications définissent l'ensemble des attaques qu'elles soient intentionnelles ou non intentionnelles. Le premier type d'attaques vise à supprimer la marque insérée dans un document, tandis que le deuxième type d'attaque n'a pas pour objectif de supprimer la marque mais plutôt l'altérer. Selon le critère de robustesse on distingue trois types du tatouage numérique :

- **Tatouage robuste** : Un système de tatouage est dit robuste, si la détection de la marque est effective même si le document tatoué a été altéré ou attaqué. Un système de tatouage robuste doit résister aux opérations licites effectuées sur le document numérique (compression, conversion analogique-numérique, filtrage, etc.) et celles illicites (attaques malveillantes des pirates).
- **Tatouage fragile** : Dans le tatouage fragile, la marque est très sensible aux modifications du document tatoué. Cette technique sert à prouver l'authenticité et l'intégrité d'un document tatoué. Une technique de tatouage fragile devrait détecter (avec une forte probabilité) toute altération du document tatoué. Une comparaison de la marque extraite et de la marque originale est effectuée afin d'identifier si le document est manipulé ou pas.
- **Tatouage semi-fragile** : Il combine les caractéristiques du tatouage robuste et fragile pour avoir une situation intermédiaire, dans laquelle la marque est robuste pour un ensemble défini de dégradations, et fragile à d'autres.

3.3 Capacité

C'est la quantité d'information (en bits) que l'on peut insérer dans une image. Il faut que le nombre de bits insérés soit suffisant pour résister aux attaques [5]

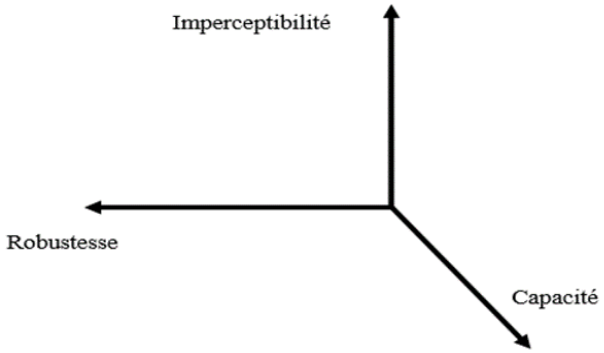

Figure 2.5 Contraintes du tatouage numérique [1]

Ces trois contraintes (imperceptibilité, capacité et robustesse) sont contradictoires Figure 2.5

Si l'on augmente par exemple la force du marquage dans le but de rendre le tatouage plus robuste, cela aura en contrepartie pour effet de rendre le tatouage plus visible. De la même manière, si l'on augmente la quantité d'information à insérer, on aura en contrepartie un tatouage visible et moins robuste.

Donc il faut respecter un compromis entre ces trois critères pour construire une méthode de tatouage [1].

3.4 Sécurité

La sécurité constitue une contrainte indépendante des quatre premières. Elle concerne par exemple la génération de la clé secrète, ainsi que le protocole d'échange général. La méthode du tatouage doit également respecter le principe suivant énoncé par Kirchhoff : " l'algorithme lui-même doit pouvoir être rendu public, la sécurité ne dépendant pas de son caractère secret". Cela signifie que l'efficacité d'un algorithme du tatouage ne peut pas être fondée sur l'hypothèse que les attaques possibles ne savent pas le processus du tatouage [5].

4. Modèle générique du tatouage

Le schéma du tatouage numérique est résumé dans la figure 2.8. Le système typique du tatouage numérique comprend deux sous-systèmes : le sous-système d'insertion du watermark (appelé aussi la phase de codage) et le sous-système de détection/extraction (appelé aussi la phase de décodage). Le sous-système d'insertion (Embedding) comprend en entrée un watermark W, un document hôte (porteur) I et une clé secrète K spécifique au tatoueur. Cette dernière est utilisée pour renforcer la sécurité de tout le système. La phase d'insertion génère en sortie un document tatoué I_w. Cette phase est modélisée par la fonction suivante **:**

$$\mathbf{I_w = E\ (I,W,K)} \quad \mathbf{(2.1)}$$

Le document tatoué I_W est ensuite copié et attaqué, ce qui est modélisé par la transmission dans un canal soumis à bruit. Le document reçu est appelé I^*_w. La réception du document consiste en deux parties : d'une part la détection du watermark et d'autre part, s'il est présent son décodage (extraction).

La phase de (détection/extraction) prend en entrée le document tatoué et éventuellement attaqué I^*_w, la clé K et éventuellement le document original I et/ou le watermark originel W. La phase de détection consiste à prouver la présence d'un watermark en utilisant une mesure de confidentialité ρ. Elle est modélisée par la fonction :

$$\mathbf{\rho = D\ (I^*_w,\ K,..)} \quad \mathbf{(2.2)}$$

La phase d'extraction consiste à calculer une estimation W ′ de W. Elle est modélisée par la fonction :

$$\mathbf{W' = D\ (I*_w,K,..)} \quad \mathbf{(2.3)}$$

- I et W sont des paramètres optionnels pour la fonction D.

Pour un système de tatouage typique, plusieurs conditions doivent être satisfaites :

- Le watermark W ′ doit être détecté à partir de I_w avec/ou sans la connaissance explicite du I.
- Si I_w n'est pas modifié (attaqué), alors W ′ correspond exactement à W [7].

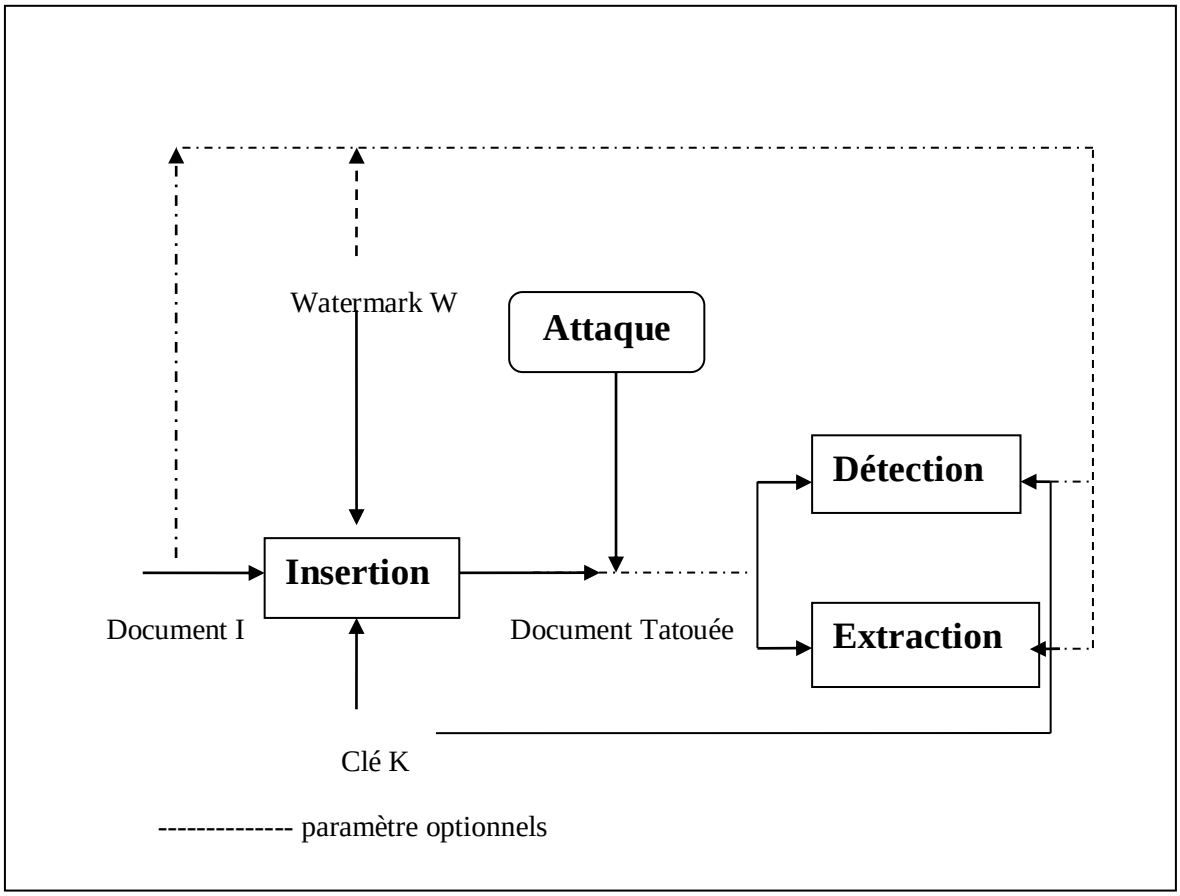

Figure 2.6 Modèle générique d'un système du tatouage[5].

– Pour un tatouage robuste, si I_w est attaqué, W ′ doit correspondre à W, à fin de donner un jugement clair de l'existence du watermark.

– Pour un tatouage fragile, W ′ doit être partiellement ou totalement différente à W, après des petites modifications de I_w.

5. Domaines d'applications

Le tatouage numérique est utilisé dans une variété d'applications où il est nécessaire d'associer certaines informations à un document numérique. Le tatouage inséré dans un document est essentiellement caractérisé par l'invisibilité, l'inséparabilité du document, et enfin il subit les mêmes transformations que le document. Ces trois aspects sont les principales raisons qui permettent l'intégration du tatouage dans diverses applications.

D'autre part, les objectifs contradictoires rendent impossible la création d'un algorithme universel adaptable à toutes les applications. Jusqu'à ce jour il n'existe pas une méthode de tatouage qui soit à la fois imperceptible, robuste et qui puisse insérer une grande quantité d'information. Il est nécessaire de prendre en compte les besoins de l'application visée lors de la conception d'un algorithme de tatouage numérique [2].

Les applications du tatouage numérique sont nombreuses, parmi celle-ci on peut citer :

5.1 Protection du droit d'auteur

la protection des droits d'auteur a été une des premières applications du tatouage numérique. En cas de litige juridique, le propriétaire d'une image est en mesure d'apporter la preuve qu'il est le propriétaire même si celle-ci a subi des dégradations (attaques). Une telle application doit assurer une grande robustesse contre les attaques, éviter toute ambiguïté de la preuve et minimiser les distorsions lié à l'insertion de la marque.

5.2 Authentification du contenu d'une image

L'idée de base de cette application consiste à insérer une marque fragile dans une image, qui sert à alerter l'utilisateur face à une éventuelle modification de l'image par une personne non autorisée et à localiser précisément les régions manipulées. Cette application est généralement utilisée dans le domaine juridique et médical.

5.3 Contrôle du nombre de copies

Les données numériques peuvent être dupliquées sans subir de détérioration de la qualité. Dans ce contexte, si une personne détient en main un document numérique et si elle est malintentionnée, elle peut produire illégalement un nombre illimité de copies de ce document avec une qualité égale au document d'origine. Le tatouage numérique peut faire face à cette situation. Des informations relatives au nombre de copies autorisées sont encryptées dans la marque. Ce principe a été utilisé dans les vidéos où la marque indique si la vidéo peut être recopiée ou non .

6 . Classification selon le domaine d'insertion

Les techniques courantes décrites dans la littérature peuvent être regroupées en deux principales classes : techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

6.1 Domaine Spatial

Dans les techniques spatiales, le watermark est inséré en modifiant directement les valeurs de pixels de l'image hôte. Ce sont des méthodes simples et peu couteuses en temps de calcul. Elles sont consacrées aux tatouages en temps réel demandés dans des environnements de faible puissance. Certaines techniques dans le domaine spatial peuvent être robustes aux attaques de type transformations géométriques.

Plusieurs méthodes, proposées dans la littérature, modifient les bits de poids faible LSB de l'image hôte. L'invisibilité du watermark est obtenue par l'hypothèse que les données contenues dans les bits LSB sont visuellement insignifiantes .

6.2 Domaine Fréquentiel

Les méthodes présentées précédemment permettent en général de retrouver le watermark en faisant la différence entre l'image originale et l'image tatouée. Cela leur confère un sérieux désavantage : une personne qui voudrait attaquer ces images et qui se serait procurée une image originale, ou bien plusieurs personnes mettant en commun leurs images tatouées peuvent détruire le watermark. Des algorithmes incluant le watermark non pas directement dans l'image, mais dans une transformée de l'image seront à cet égard plus robustes, et permettent en plus de choisir les pixels qui seront plus résistants à certains types d'attaques.

Le tatouage dans le domaine fréquentiel est obtenu après l'utilisation de l'une des transformées comme la DFT (transformée de Fourier discrète), la DCT (transformée en cosinus discrète), DWT (la transformée en ondelettes) ou d'autres transformées.

7 . Les Attaques

Pour tester la robustesse des algorithmes de tatouage, il faut simuler des attaques aux images reçues après la phase d'insertion. Les attaques que peuvent subir les images tatouées sont:

- Le filtrage.
- L'ajout du bruit, le débruitage car la marque ayant des caractéristiques comme le bruit.
- La compression .
- Le changement de contraste, de lumière.
- Les transformations géométriques usuelles : le but est de pouvoir isoler une partie de l'image, de faire un agrandissement ou une réduction. Dans ces cas, nous observons une perte de synchronisation, c'est-à-dire de possibilité de localisation de la marque.
- la rotation.
- le cadrage.
-

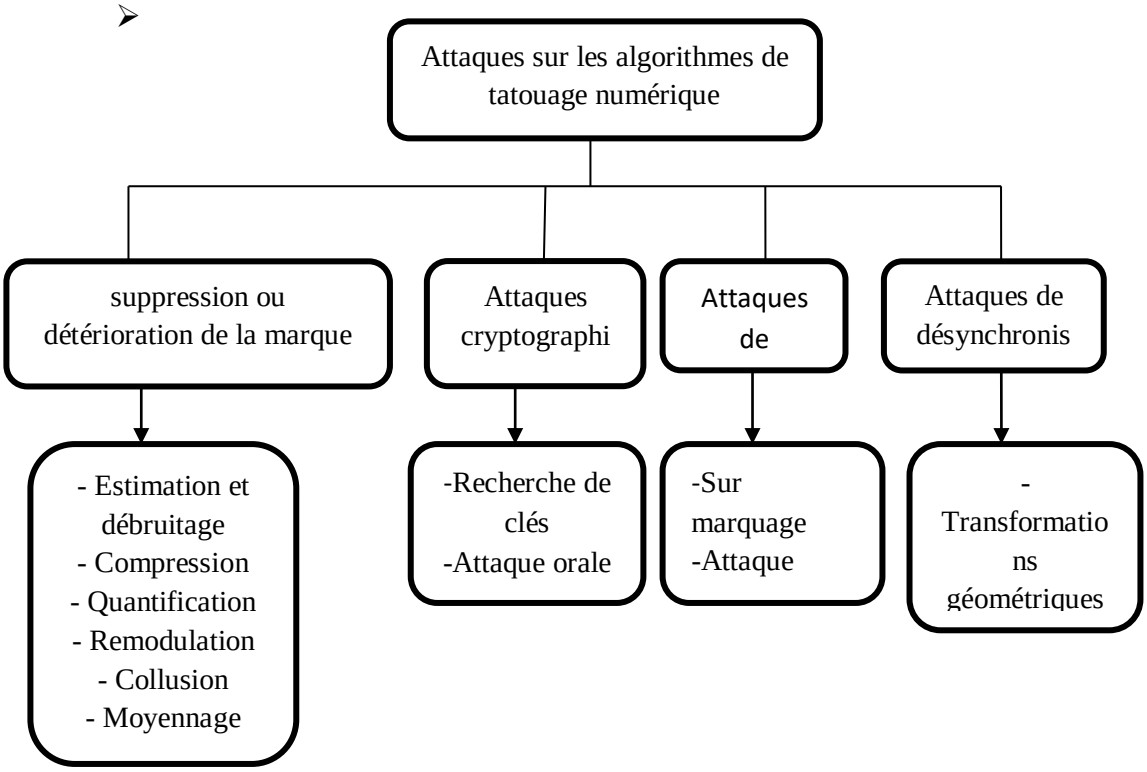

Figure 2.7 Classification des attaques selon Voloshynovskiy et al [8]

8. Conclusion

Dans ce chapitre, nous avons présenté la technique du tatouage numérique d'une manière générale. Nous nous sommes intéressés aux terminologies et notions liées au tatouage invisible des images numériques.

Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptyuè_uelle. Nous avons présenté aussi les techniques du tatouage selon différents critères, les types d'algorithmes, et les domaine d'insertions.

Chapitre III

Tatouage fragile des images numérique

3.1 Introduction

Le tatouage d'images numériques a connu un grand progrès ces dernières années. Développé au début pour la protection des droits d'auteur des documents multimédia, il tend de plus en plus à être utilisé pour remplir d'autres fonctions de sécurité, notamment des fonctions d'intégrité, ou des services d'information. Contrairement aux applications de protection des droits d'auteur, les données insérées pour but d'authentification devraient être fragiles dans le sens où elles devraient être facilement modifiées lorsque les données sont manipulées. Cet objectif peut être atteint avec des techniques de tatouage fragile qui sont peu robustes à certaines modifications. Les méthodes fragiles sont utilisées uniquement pour répondre à des problèmes de contrôle d'intégrité des images.

Dans ce chapitre, nous présentons le tatouage fragile d'images numériques dans l'objectif est d'assurer un service d'authentification et intégrité des images. Nous présentons aussi les différentes techniques utilisées dans ce domaine, ainsi que quelques algorithmes de tatouage fragile les plus populaires [1].

3.2 Principe du tatouage fragile

Les méthodes proposées pour assurer un service d'intégrité sont basées sur l'utilisation d'un tatouage fragile, par opposition au tatouage robuste classiquement utilisé pour la protection des droits d'auteur. Le principe de ces approches est d'insérer une marque ou un logo binaire (généralement prédéfini et indépendant des données à protéger [11]) dans l'image d'origine de telle manière que les moindres modifications apportées à l'image se répercutent également sur la marque insérée (figure3.1). Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence de cette marque . De ce fait, si la marque est altérée, l'image n'est plus considérée comme authentifiée.[1]

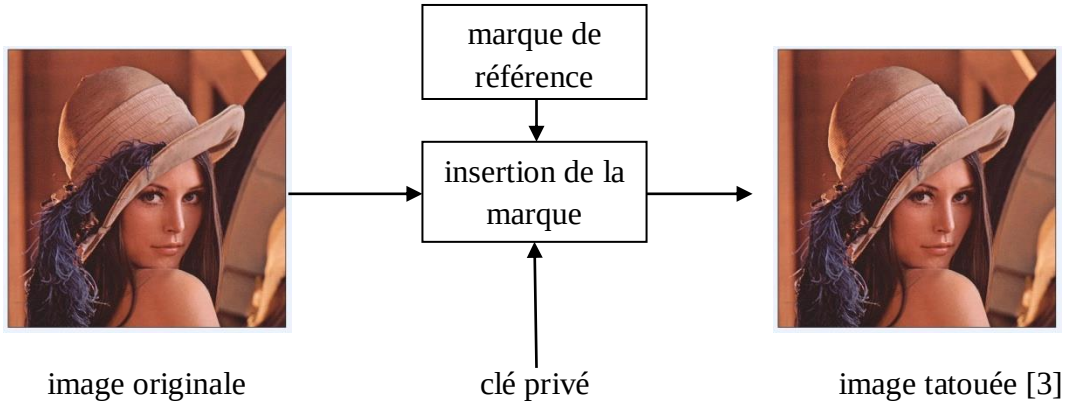

Figure 3.1 Schéma général d'un système d'intégrité basé sur un tatouage fragile [2].

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

3.2.1 L'authentification

Le but de ce tatouage est d'insérer dans une image une marque qui puisse authentifier le document ou apporter la preuve que le contenu de ce document n'a pas été modifié depuis cette insertion. Dans certains cas on préfère assurer une authentification stricte (ou intégrité des données). Pour cela, on utilise des marques fragiles qui deviennent non détectables dès qu'une valeur des données change dans le document [12].

3.2.2 La sécurité

La sécurité constitue une troisième contrainte indépendante des deux premières. Elle concerne par exemple la génération de la clé secrète, ainsi que le protocole d'échange général. La méthode du tatouage doit également respecter le principe suivant énoncé par Kerckhoff : "l'algorithme lui-même doit pouvoir être rendu public, la sécurité ne dépendant pas de son caractère secret". Cela signifie que l'efficacité d'un algorithme du tatouage ne peut pas être fondée sur l'hypothèse que les attaques possibles ne savent pas le processus du tatouage [13].

3.2.3 La complexité algorithmique (Le coût)

Dans certaines applications, comme le contrôle de diffusion et la sécurité des cartes d'accès, la rapidité est primordiale. La lecture doit être effectuée en temps

réel. Généralement, en tatouage numérique, la complexité en écriture est moins cruciale que la complexité en lecture [14].

3.2.4 L'intégrité des images numériques

Le service d'intégrité est un concept bien connu en sécurité. Sa définition repose sur une décision binaire qui garantit que les données reçues sont rigoureusement identiques à celles émises. Cette définition est applicable à tout type de documents numériques, néanmoins, ce service s'avère être trop strict et pas bien adapte aux documents images [15].

Le problème de l'intégrité des images se pose principalement en termes de contenu sémantique, c'est-à-dire la détection des modifications du document pouvant engendrer une gêne dans sa visualisation et/ou une erreur dans son interprétation (modification de la légende, disparition d'un visage, etc.).

3.3 Schéma générique d'un système d'authentification d'image

Le schéma générique d'un système d'authentification d'images doit satisfaire les critères suivants [12]:

- **Sensibilité :** le système doit être capable de déceler des manipulations pouvant modifier l'interprétation que l'on a d'une image.
- **Tolérance:** le système doit être tolérant vis-à-vis des algorithmes de compression avec pertes tels que JPEG, et plus généralement vis-à-vis des manipulations bienveillantes (générées, par exemple, par les fournisseurs de contenu multimédia).
- **Localisation des régions altérées :** Le système doit être capable de donner une information visuelle permettant d'identifier rapidement les régions qui ont été manipulées.
- **Reconstruction des régions altérées :** Éventuellement, le système doit avoir la capacité de restaurer, même partiellement, des zones qui ont été manipulées où détruites, afin de permettre à l'utilisateur de savoir quel était le contenu original des zones manipulées.
- **Mode de stockage :** Les données d'authentification devraient être intégrées dans l'image elle-même, sous la forme d'un watermark, plutôt que dans un fichier séparé, comme dans le cas d'une signature externe.
- **Mode d'extraction :** suivant que les données d'authentification sont dépendantes ou non de l'image, on favorisera pour un mode d'extraction du tatouage aveugle ou semi-aveugle. En mode d'extraction aveugle, le watermark (les données d'authentification) est récupérée en utilisant seulement l'image tatouée (et éventuellement attaquée),

tandis qu'en semi-aveugle il s'agit particulièrement de vérifier la présence de tel watermark dans une image (via un score de corrélation). Il est très clair qu'un mode d'extraction non aveugle n'est pas préféré pour un service d'intégrité dans la mesure où il fait appel à l'image originale [12].

3. 4 Modèle générique d'une technique de tatouage fragile

Le modèle général d'un système d'authentification basé sur le tatouage numérique est illustré dans la Figure 2. Généralement, une clé secrété *K* connue par l'émetteur et le récepteur est utilisée pour générer un watermark *W* qui sera inséré dans l'image hôte f. L'image tatouée f_w est ensuite délivrée par le canal de communication (internet, satellite, etc.) ou stockée dans une base de données. Pour authentifier l'image reçue f^*_w, la même clé secrète est utilisé pour extraire la marque *W** et la comparer avec *W* [16]

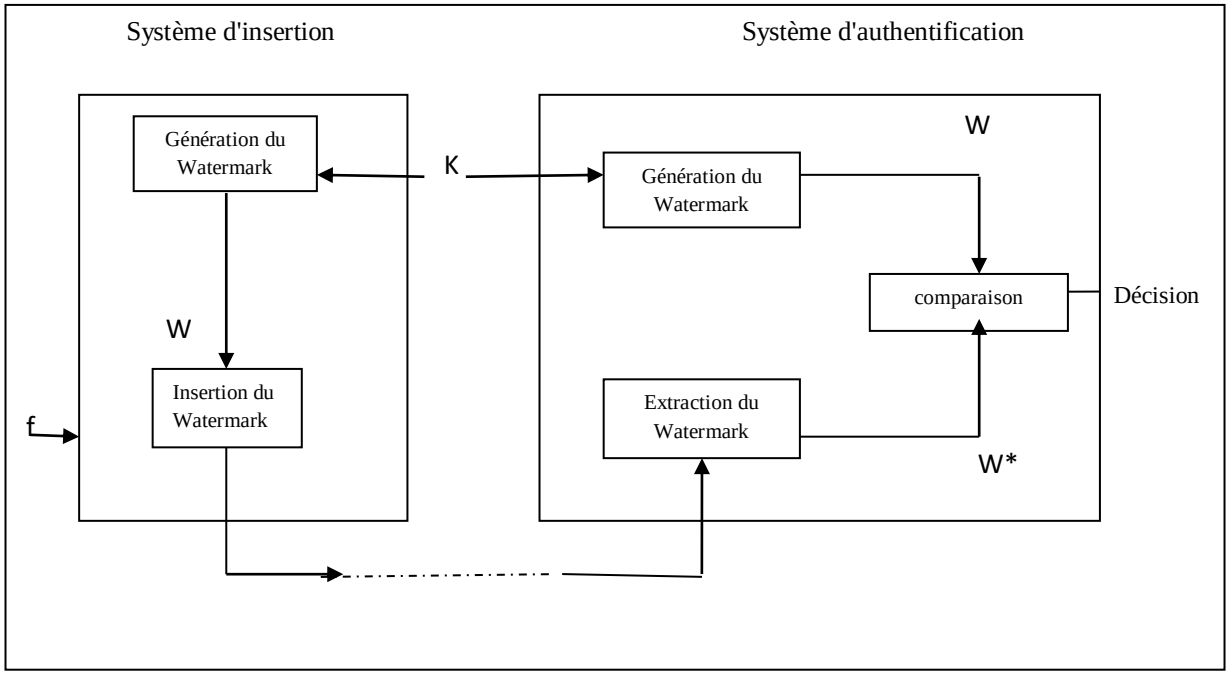

Figure 3.2 Le modèle général d'un système d'authentification basé sur le tatouage fragile [16]

3.5 Caractéristiques d'un système de tatouage fragile

3.5.1 Détection des falsifications

Une technique de tatouage fragile devrait détecter (avec une probabilité élevée) toute altération de l'image tatouée. C'est la propriété la plus fondamentale

d'une méthode de tatouage fragile et elle est une exigence pour tester de manière fiable l'authenticité de l'image. Dans de nombreuses applications, il est également souhaitable de donner une indication de la quantité d'altération et sa localité.

3.5.2 Imperceptibilité

Le watermark inséré ne doit pas être visible par l'observateur. Dans la plupart des cas il s'agit de préserver la qualité visuelle de l'image tatouée [2].

3.5.3 La nécessité de l'image originale pour la détection de la marque

L'image originale peut ne pas être existée ou le propriétaire peut avoir des raisons de ne pas faire confiance à un tiers avec l'original (ce dernier pourrait alors placer son propre watermark sur l'originale et réclamer qu'il en appartient).

3.5.4 La détectabilité du watermark après le recadrage (cropping) d'image

Dans certaines applications, la capacité de détecter le watermark après le recadrage est très souhaitable. Par exemple, un attaquant peut être intéressé par certaines parties (visages, des personnes, etc.) de l'image tatouée. Dans d'autres applications, cette fonctionnalité n'est pas requise, cependant le recadrage est traité comme une modification.

3.5.5 L'insertion du watermark par des personnes non autorisées doit être difficile.

une attaque particulière mentionnée dans consiste en la suppression du watermark d'une image tatouée, et l'insertion de ce dernier dans une autre image.[17]

3.6 Types d'attaques

Une des attaques les plus courantes contre les systèmes à base de tatouage fragile, consiste à tenter de modifier une image protégée sans affecter le watermark qu'elle contient, ou bien encore à tenter de créer un nouveau watermark que le détecteur considérera comme assurée authentique [18].

Prenons par exemple le cas volontairement simplifie ou l'intégrité d'une image est par un watermark fragile, indépendant du contenu, et inséré dans les LSB des pixels. Il est clair que si on modifie l'image sans se préoccuper de savoir quels sont les bits affectés par la manipulation, on a toutes les chances pour que le watermark soit dégradé et l'attaque détectée.

Par contre, si on prend soin de modifier l'image sans toucher aux LSB, le watermark restera intacte et le système ne décèlera aucune falsification.

3.6.1 Copy attack :

D'un point de vue plus général, dès que l'insertion est assurée par un watermark indépendant du contenu de l'image à protéger, il est possible d'imaginer une attaque qui recopie un watermark valide d'une image dans une autre « Copy Attack ». De cette manière, la deuxième image se retrouve alors protégée. Ce type d'attaque peut également être effectuée sur la même image ; dans ce cas, le watermark est dans un premier temps retire de l'image, l'image est ensuite manipulée, et enfin le watermark est réinséré dans l'image [19].

3.6.2 Collage attack :

Dans le même esprit, l'attaque « Collage-Attack », qui consiste à créer une image contrefaite de toutes pièces à partir d'une banque d'images protégées par le même watermark et la même clé. Cette attaque ne présuppose aucune connaissance à priori sur le watermark, ni sur la clé secrète utilisée. Son principe est relativement simple puisqu'il consiste à remplacer chaque pixel de l'image à manipuler par le pixel qui lui est le plus similaire parmi les pixels de même position des images de la base.[20]

3.6.3 StirMark2

La difficulté de cette méthode est de disposer d'une banque d'images suffisamment variées pour obtenir une image falsifiée de bonne qualité visuelle . Un attaquant peut être intéresse par la suppression totale du watermark. Pour ce faire, un attaquant peut ajouter un bruit aléatoire à l'image, en utilisant des techniques visant à détruire des watermark (telles que StirMark2), ou en utilisant une analyse statistique ou de collusion pour estimer l'image originale [19].

3.6.4 Brute Force Attack

Une autre attaque classique consiste à essayer de trouver la clé secrète utilisée pour générer le watermark. Ce type d'attaque est appelé « Brute Force Attack ». Une fois la clé trouvée, il devient alors très facile pour un pirate de falsifier le watermark d'une image protégée avec cette clé. La seule parade efficace est d'utiliser des clés de grande taille de manière à rendre cette attaque très dissuasive en termes de temps de calcul [19].

3.6.5 Attaques malveillantes

Il convient d'aborder le problème des attaques malveillantes de pirates. L'objectif commun de ces attaques, n'est pas de détourner le contenu d'une image mais d'utiliser les failles ou les faiblesses d'un système d'authentification afin de le

tromper, autrement dit faire croire au système qu'une image est intègre alors que son contenu a été modifié (ou l'inverse dans certains cas).

3.7 Algorithmes de tatouage fragile

3.7.1 Utilisation des bits de poids faible (LSB)

L'utilisation des LSB (bits de poids faible) est une méthode très simple, aux limites évidentes. Elle consiste à insérer des données uniquement au niveau des bits de poids faible de l'image. Pour une image codée sur 8 bits, une modification du LSB entraîne une variation du niveau de gris de 1 sur une échelle de 256. [21]

Cette modification est en pratique invisible. Une méthode d'insertion consiste alors à supprimer tous les bits de poids faible de l'image à marquer, puis à y insérer les données voulues. Un bit de donnée est ainsi inséré par pixel de l'image. Si cette méthode obtient de bons résultats pour ce qui est de l'invisibilité, on conçoit aisément qu'elle n'est pas satisfaisante pour ce qui est de la robustesse. Il suffit en effet de mettre à zéro tous les bits de poids faible de l'image marquée pour effacer irrémédiablement la marque.

3.7.2 L'algorithme de Walton

- Choisir un nombre entier suffisamment grand *N*.
- Diviser l'image en blocs de 8x8 pixels.
- Pour chaque bloc *B* :

a) Mettre à zéro le bit de poids faible de chaque pixel du bloc. Noter les 64 pixels résultants du bloc comme suit (*p1, p2, …, p64*).

b) Générer une séquence pseudo-aléatoire de 64 nombres entiers (*a1, a2, ...*) comparables dans la taille à *N*. Utiliser une clé secrète *K*.

c) Calculer le (*check-sum*) S de la manière suivante :

$$\boldsymbol{S = \sum_{j=1}^{64} (a_j\, g(p_j))\ mod\ N} \qquad \textbf{(3.1)}$$

d) Encrypter la forme binaire de *S*. Une autre clé est requise.

e) Insérer la séquence encryptée au niveau des 64 bits de poids faible (*LSB*) de chaque pixel du bloc considéré.

Le processus de détection et de vérification d'authenticité de l'image consiste à comparer pour chaque bloc, le *check-sum* calculée à partir de l'image testée avec le *check-sum* extrait des bits de poids faible. Cette méthode est simple, rapide, sensible

à toute manipulation et capable de localiser les régions touchées dans l'image. Quoique dans le cas d'un échange de deux blocs dans deux images différentes et qui sont protégées par les même clés, le système est vulnérable à ce type d'attaque et peut ne pas détecter cette modification [22]. Une solution simple à ce problème est de rendre le watermark dépendant du contenu de l'image [23].

3.7.3 Algorithme de Fridrich et Goljan

Fridrich et Goljan ont proposé une méthode qui repose également sur l'utilisation des LSB , mais cette fois-ci, dans le but de cacher suffisamment d'informations afin de pouvoir non seulement de déceler d'éventuelles manipulations, mais surtout de permettre une reconstruction partielle des blocs altérés.

Le principe de base consiste à découper l'image en blocs de taille 8×8 pixels, de calculer les coefficients DCT en ne tenant compte que des MSB. Ces coefficients DCT sont ensuite quantifiés à l'aide de la table de quantification correspondant à une compression JPEG d'une qualité de l'ordre de 50%. La matrice quantifiée résultante est alors encodée sur 64 bits et insérée au niveau des LSB des pixels d'un autre bloc. Le bloc servant de support au tatouage doit être suffisamment éloigné afin d'éviter qu'une modification locale de l'image qui altère à la fois l'image et les données de reconstruction.[11]

3.7.4 Utilisation de la méthode Self-embedding :

Dans le but de reconstruire partiellement les régions détériorées après attaques ont proposés d'insérer une grande quantité d'information à l'aide des LSB. Le schéma proposé opère dans le domaine transformé en utilisant la DCT. Cette transformée est appliquée sur des blocs de 8x8 pixels de l'image. La seconde étape consiste à quantifier les coefficients DCT de chaque bloc, à l'aide de la table de quantification correspondant à une compression JPEG d'une qualité de l'ordre de 50%. Après l'étape de quantification de bloc, les coefficients résultats, sont encodés sur 64 bits est incrustés dans les LSB des pixels d'un bloc suffisamment distant du bloc quantifié afin d'assurer que les distorsions locale que peut subir l'image ne détériore à la fois l'image et les informations de reconstruction [25].

3.8 Conclusion

Dans ce chapitre, nous avons présenté la technique du tatouage fragile, qui permet d'assurer un service d'intégrité et d'authenticité adapté aux images numériques. Nous avons présenté le schéma général du tatouage fragile, les principaux algorithmes conçus pour ce type de marquage ainsi que les avantages et les inconvénients de chaque algorithme. Dans le prochain chapitre nous présenterons le tatouage fragile basé sur la décomposition en valeurs singulières SVD, et les résultats obtenus en employant cette méthode.

Chapitre 4

Algorithmes de tatouage fragile pour l'authentification d'images

4.1 Introduction

Dans ce chapitre, nous présenterons les algorithmes et les différents résultats pratiques obtenus du tatouage fragile des images numériques. Le tatouage fragile est considéré comme une solution alternative permettant d'assurer un service d'authentification et d'intégrité des images. En effet toutes perte ou altération de la marque sera prise comme preuve que l'image tatouée a été falsifiée, alors que la récupération de l'information de la marque contenue dans celle-ci sert à certifier l'intégrité ou à localiser la modification dans l'image, si elle a eu lieu.

L'algorithme de tatouage que nous avons réalisé se base sur l'utilisation de la SVD (décompositions en valeurs singulières) de l'image. Dans une première partie, nous avons exploité la SVD pour détecter les modifications dans les images tatouées, cela nous a permis de vérifier leur authenticité. En seconde partie, nous avons étendu l'algorithme pour la localisation du changement possible dans l'image tatoué.

Nous avons évalué les performances de l'algorithme du tatouage réalisé en terme d'invisibilité de la marque et l'efficacité d'assurer l'authenticité et l'intégrité de l'image tatouée. Tout les programmes sont réalisés avec Matlab 2014.

4.2 Algorithme de tatouage en utilisant la SVD

Dans cette section, nous allons présenter les algorithmes de tatouages d'images en niveaux de gris basées sur la SVD. L'idée de base de l'algorithme proposé est d'intégrer des données d'authentification extraites de l'image originale dans l'image elle-même. Pour l'authentification, nous vérifions si le les informations sont modifiées ou non du côté du récepteur.[30]

4.3 La décomposition de la valeur singulière (SVD

Soit A, une matrice $m*n$, la décomposition à Valeur Singulières SVD (Singular Value Decomposition) est une méthode de décomposition numérique qui permet d'exprimer la

matrice A comme le produit de trois matrices particulières, U, V , et S telles que :

$A = USV^T$ (1)

- U est une matrice m ∗ n, orthogonale.
- S est une matrice n ∗ n, diagonale.
- V est une matrice n ∗ n, orthogonale.

$$[A] = [U] \begin{bmatrix} S1 & 0 & 0 \\ & S2 & \\ 0 & 0 & S3 \end{bmatrix} [V]$$

Propriétés

- Les S i sont les valeurs singulières de A.
- Si la matrice A est singulière, il y a des w i nuls.
- En général rang (A) = au nombre de S i non nuls.
- La décomposition SVD est unique. [27]

4.4 Algorithme d'insertion

Considérons une image O de taille MxN pixels comme image originale. La procédure d'insertion de la marque dans cette image est illustrée dans la **Figure (4.1)**. N pixels sont sélectionnés aléatoirement avec une clé. Cette clé sera utilisée dans la procédure d'extraction de la marque. Pour le nombre N, il est égal à la dimension des valeurs singulières de la SVD. Ensuite les LSB des pixels sélectionnés sont mis à zéro. Les données d'authentification (la marque) sont calculés à partir des valeurs singulières de l'image hôte.

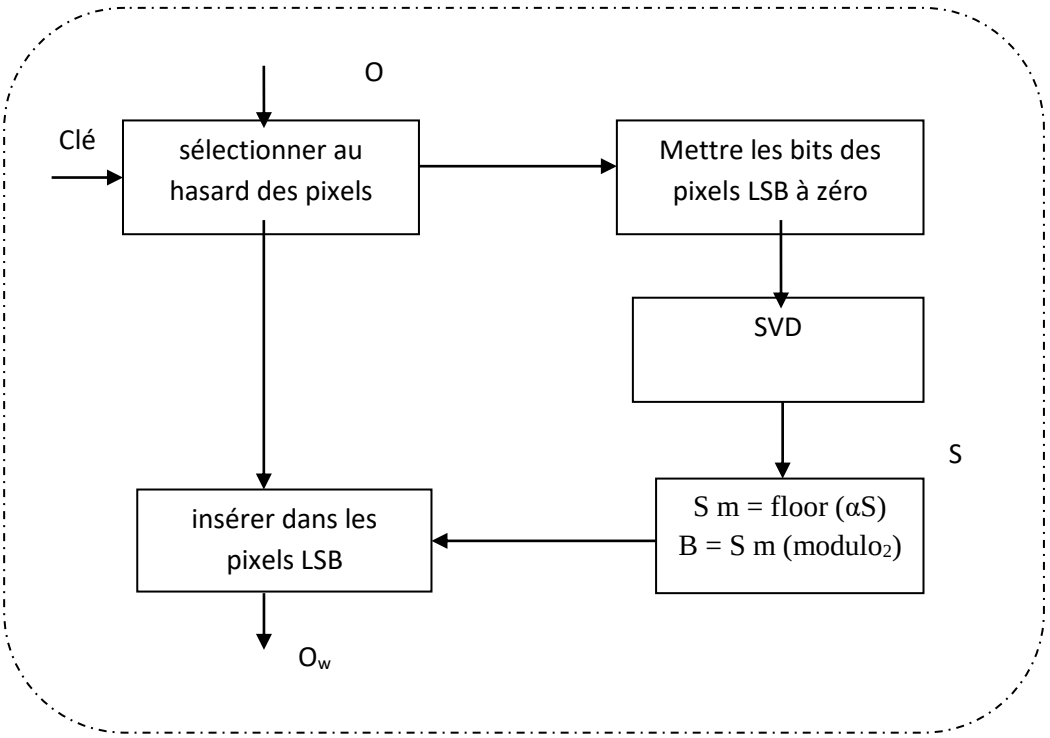

Figure 4.1 schéma insertion de la marque

4.5 Algorithme d'extraction et de vérification

la procédure d'extraction et de vérification pour la marque insérée dans l'image marquée est montrée à la **Figure (4.2).** nous choisissons N pixels dont l'emplacement est donné par la clé utilisée dans le processus d'insertion. ensuite nous obtenons les LSB de ces pixels et nous comparons la chaine LSB résultantes avec les données d'authentifications calculée

.

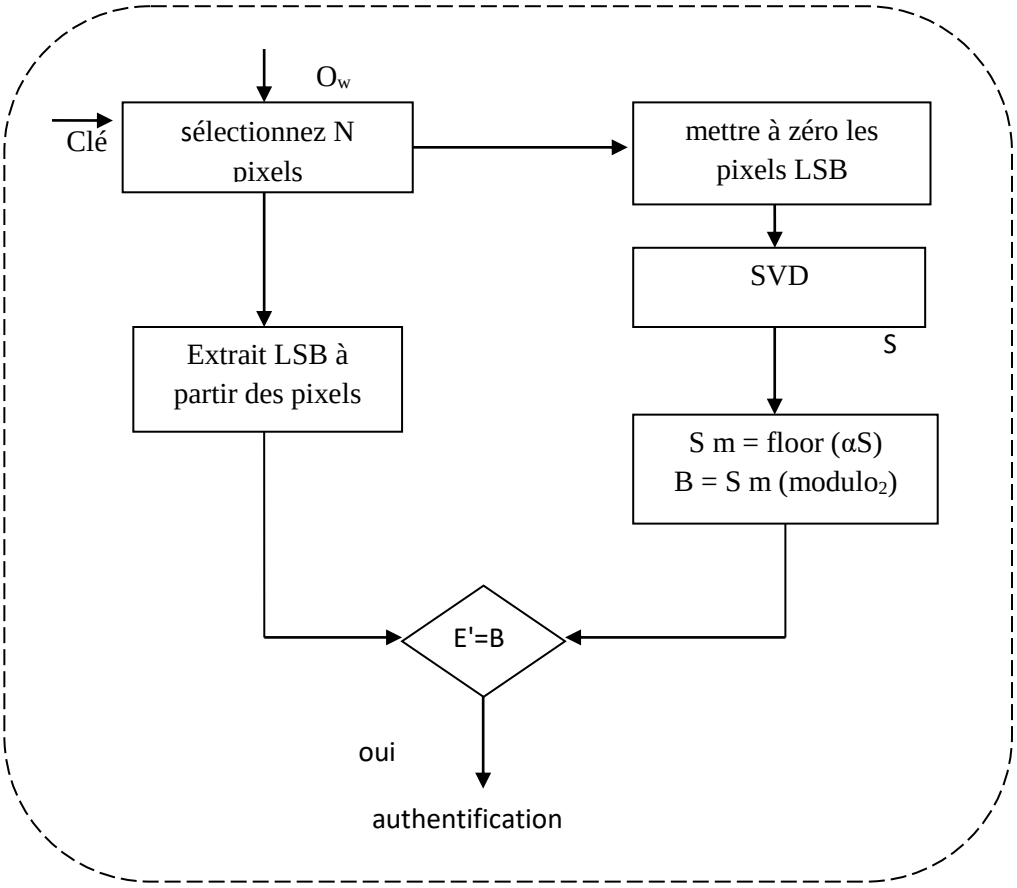

Figure 4.2 Schéma d'extraction et vérification

4.6 Algorithme extraction de la marque et la localisation

Dans le tatouage fragile, les attaquants essaient de changer une image sans laisser de traces visibles. nous devons alors concevoir une marque qui détecte le changement possible ainsi que son emplacement . dans cet algorithme de localisation **Figure 4.3** , tout les LSB d'une image originale sont mis à zéro. la marque est une image binaire W' de taille MxN. une deuxième marque B' (représentant la donnée d'authentification) est générée selon l'algorithme précédant. La donnée d'authentification B' sera ensuite combinée avec la marque binaire W' en utilisant une opération XOR bit par bit pour former L. Autrement dit : $L = B' \oplus W'$. enfin, le résultat L sera intégré dans les LSB des pixels sélectionnées aléatoirement en utilisant une clé. L'extraction de la marque depuis l'image tatouée pour localiser l'emplacement d'un changement possible consiste à inverser l'opération d'insertion. L'opérateur XOR $W''=B'\oplus E'$ est effectué entre les données d'authentifications B' et les bits E'

pour reformer la marque binaire W''. E' représente les bits LSB précédemment extraits.

Si l'image tatouée n'a pas été modifiée, la marque extraite W'' est égale à celle insérée W'. Si Les LSB de l' image tatouée sont modifiés, nous pouvons détecter les endroits de ce changement.

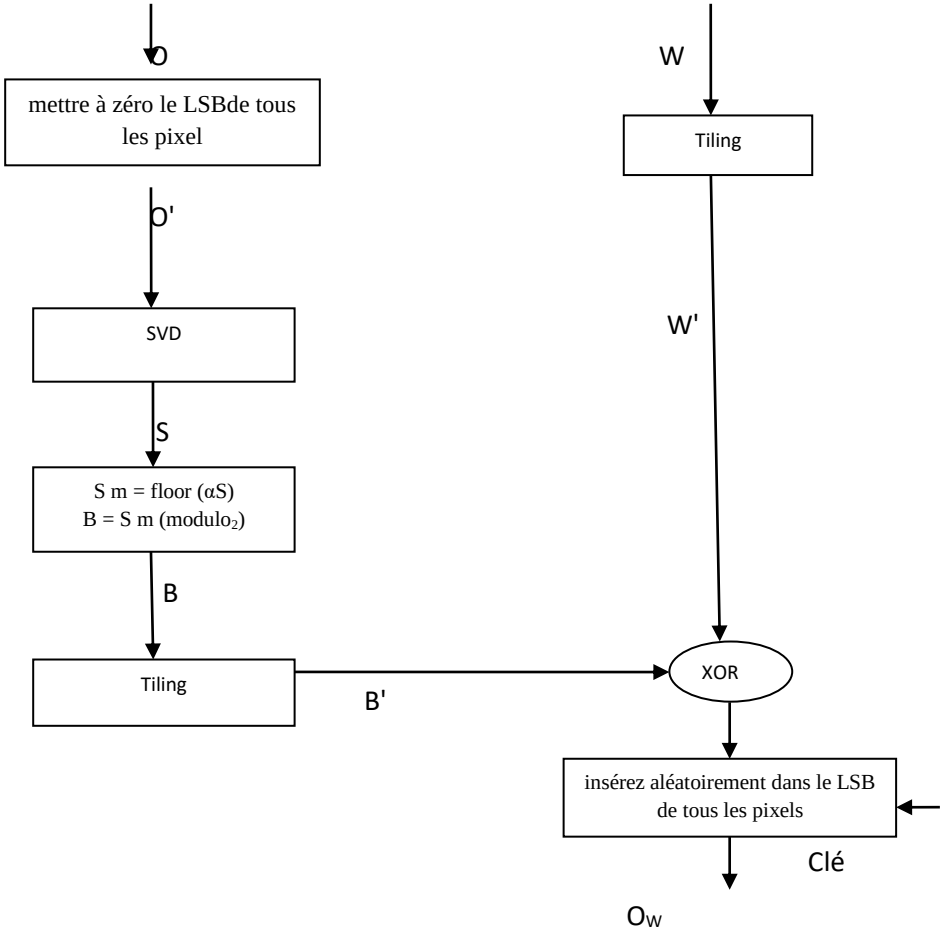

Figure 4.3 : algorithme de extraction et localisation [30]

4.7 Mesure de qualité

la qualité d'une image revient à estimer le changement de certaines caractéristiques de cette image. L'étape d'extraction des caractéristiques constitue donc l'étape la plus importante dans l'établissement d'une mesure de qualité d'images et pour connu :

- Il faut d'une part que l'image tatouée soit de la même qualité que l'image originale.
- D'autre part les attaques aux quelles le tatouage doit être robuste, doivent conserver la qualité de l'image et la marque.

Les deux plus anciennes méthodes, qui sont malheureusement les plus utilisées, pour mesurer la qualité d'une image sont le PSNR et l'erreur quadratique moyenne (EQM).

4.8 Rapport crête signal sur bruit (PSNR)

Le PSNR est le rapport signal sur bruit (Peak Signal to Noise Ratio) est une mesure de distorsion très utilisée en imagerie numérique et tout particulièrement en compression d'image. Il s'agit de quantifier la performance des codeurs en mesurant la qualité de l'image tatouée par rapport à l'image originale. Il est mesuré en dB à partir de la relation suivante :

$$\mathbf{PSNR} = \mathbf{10} * \boldsymbol{log}_{\mathbf{10}}\left(\frac{\boldsymbol{d}^{\mathbf{2}}}{\boldsymbol{EQM}}\right) \qquad \textbf{(4.1)}$$

où d est la dynamique du signal (la valeur maximum possible pour un pixel). Dans le cas standard d'une image où les composantes d'un pixel sont codées sur 8 bits, d=255.

EQM est l'erreur quadratique moyenne et est définie pour deux images I_0 et I_r de taille M×N.

$$\mathbf{EQM} = \frac{\mathbf{1}}{\boldsymbol{m}*\boldsymbol{n}} \sum_{\boldsymbol{i}=\mathbf{0}}^{\boldsymbol{m}-\mathbf{1}} \sum_{\boldsymbol{j}=\mathbf{0}}^{\boldsymbol{n}-\mathbf{1}} [\boldsymbol{I_o}\,(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{I_r}(\boldsymbol{i},\boldsymbol{j})]^{\mathbf{2}} \qquad \textbf{(4.2)}$$

- I_o : l'image originale.

- I_r: l'image reconstruite.

- M x N : la taille de l'image.

Si le PSNR est utile pour mesurer la proximité de l'image tatouée par rapport à l'originale, il ne prend pas en compte la qualité visuelle de reconstruction et ne peut être considéré comme une mesure objective de la qualité visuelle d'une image.[8]

4.9 Résultats expérimentaux

4.9.1 Application de l'algorithme pour l'authentification et l'intégrité

Nous allons appliquer d'abord l'algorithme décrit dans la figure 4.1 à l'image hôte « Lena » à niveau de gris de taille 256x256 qui est très utilisée en traitement d'image. La figure (4.1) représente l'image hôte (a) et L'image tatouée (b) .

(a) Image originale

(b) Image tatouée

PSNR=74.803412 dB

Figure 4. 4 (a) Image originale et (b) Image tatouée avec l'algorithme utilisant la SVD

A partir de ces deux figures, on peut remarquer qu'il est difficile de différencier entre l'image originale et l'image tatouée, alors la méthode est imperceptible et l'algorithme a réalisé une caractéristique des propriétés de tatouages.

Authenticité et Intégrité	Oui	Non
Image inchangé	X	
Non marquée		X
Compressé		X
Filtrée		X
Recadrée		X

Tableau 4 .1 Résultats d'authentification contre diverses attaques

4.9.2 Application de l'algorithme de la localisation

a) Recadrage:

Nous avons appliqué un recadrage de l'image tatouée pour testé l'efficacité de cet algorithme , est ce qu'il peut détecté la modification ou non, et les résultats et le suivant :

Image tatouée Image recadrage Image extraite

Figure 4.5 Image tatouée après le recadrage et la marque extraite

PSNR= 75.540133 dB

La marque extraite est visiblement différente de celle intégrée à l'image hôte et nous remarquons nettement ou le changement à l'image de Lena a été fait.

l'algorithme réalisé réussit très bien à indiquer en plus de la non-authentification de l'image modifiée par rapport à celle marquée, la localisation du changement apporté à cette dernière.

b) La compression

La compression est classée comme un type d'attaque non intentionnel mais elle influe sur l'image tatouée. la figure 4.7 montre la perte totale de la marque extraite après la compression.

Image tatouée Image compressé Image extraite

Figure 4.6 Image tatouée après la compression et la marque extraite

PSNR= 75.257566 dB

Remarque : on peut dire que l'algorithme a détecté la modification causée par de compression

c) Modification

Nous avons d'enlever une petite partie de l'image tatouée. cette modification a été détectée par l'algorithme conçu comme le montre la figure 4.7

Image tatouée Image tatouée modifiée Image extraite

Figure 4.7 Image tatouée après le modification et la marque extraite

PSNR= 74.275586 dB

d) Le filtrage

Nous avons appliqué un filtrage passe-bas de l'image tatouée pour tester l'efficacité de notre algorithme , le résultat de l'extraction de la marque nous montre malheureusement que l'algorithme n'a pas pu détecté le filtrage

effectué à notre image tatouée, donc il n'est pas efficace contre le filtrage passe-bas.

Image tatouée Image filtre la marque extraite

Figure 4.8 Image tatouée après le filtrage et la marque extraite

PSNR= 75.122890 dB

4.10 Exemple pour autre image :

a) Modification

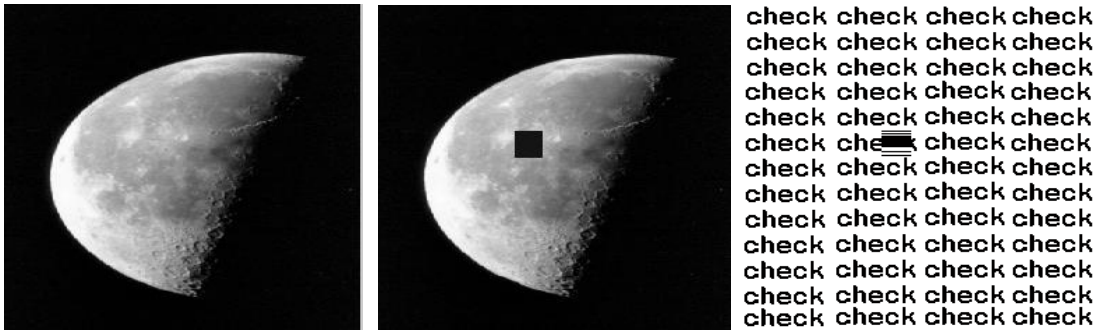

Image tatouée Image modifier Image extraite

b) Compression

Image tatouée Image compressé la marque extraite

c) Filtrage

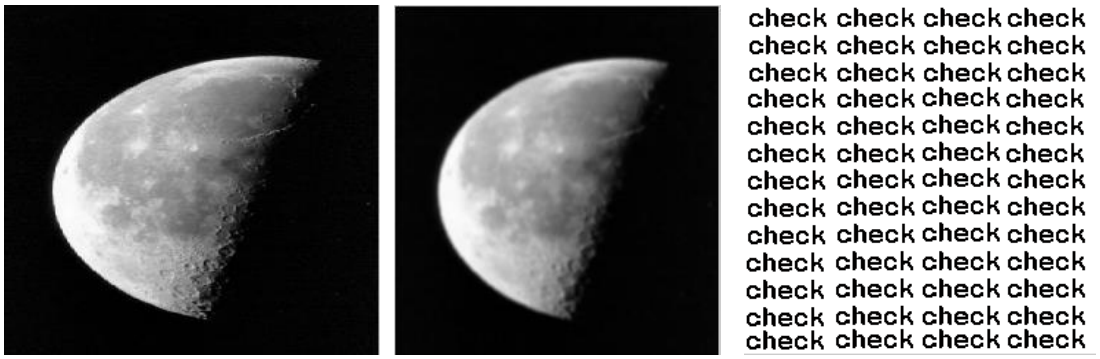

Image tatouée Image filtré la marque extraite

d) Recadrage

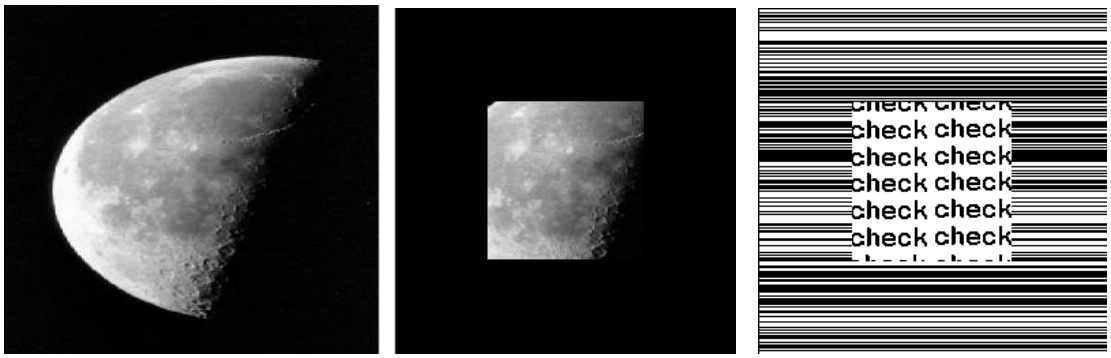

Image tatouée Image recadré la marque extraite

Figure 4.9Image tatouée après (modification, compression ,filtrage , recadrage)et la marque extraite

4.11 Les résultats :

d'après le résultats obtenus on peut dire :

- ✓ pour vérifier l'intégrité des images reçues, nous exploitons les valeurs singulières de SVD de l'images .
- ✓ chaque image peux être représentée avec des valeurs singulières uniques.
- ✓ les données d'authentification, sont très sensibles à toute modification.
- ✓ avec cet algorithme
  i) nous pouvons détecter toute modification de l'image tatouée telle que la compression, le filtrage.

.

iii) la qualité de l'image tatouée est très élevée car seulement les bits LSB de quelques pixels sont changés.

.

- ✓ Dans l'algorithme d'extension réalisé, la marque extraite localise les changements de valeurs de pixels dans l'image originale.

les résultats obtenus nous permettent de déduire que la méthode du tatouage fragile proposée est efficace du point de vue qualité de l'image tatouée et aussi efficacité de dé détection des anomalies dans l'image tatouée. [1]

4.12 Conclusion

. Dans ce chapitre, nous avons présenté notre algorithme de tatouage fragile d'images à niveaux de gris , dans l'objectif est de vérifier l'authentification et l'intégrité des images numériques.

Cette méthode est efficace en termes d'imperceptibilité et fragilité par rapport aux divers types d'attaques standards et conventionnelles. Les résultats expérimentaux obtenus sont très prometteurs et montrent la faisabilité de cette méthode, qui permet de maintenir une haute qualité d'images tatouées, et en même temps d'être très sensible contre plusieurs types d'attaques conventionnelles.

Conclusion générale :

Nous avons introduit ce travail en présentant et en définissant les objectifs du tatouage d'images numériques. Le tatouage numérique a été introduit comme une technique alternative à la cryptographie et efficace pour la protection des images et la vérification de l'intégrité des données. Initialement développé pour renforcer la protection des droits d’auteur des documents multimédia, il tend de plus en plus à être utilisé pour remplir d’autres fonctions de sécurité, notamment des fonctions d’intégrité et d’authentification des données, le tatouage numérique doit être fragile et avec une bonne imperceptibilité.

Au cours de ce mémoire, nous avons présenté les notions de bases liées au domaine de

l'image numérique et de son traitement, en donnant quelques définitions élémentaires important sur ce sujet. Nous avons aussi présenté les différents types d'attaques sur les images numériques. Enfin, nous avons abordé le tatouage fragile d’images, quelques algorithmes connus, ainsi que les domaines d'applications.

Dans ce mémoire, nous avons proposé une méthode de tatouage fragile d’images numériques basée sur la SVD. Cette méthode utilise les bits LSB. Les résultats expérimentaux ont montré la faisabilité de l' algorithme proposé, et que cette approche permet d’obtenir une haute qualité d’images tatouées et en même temps, elle est très sensible contre plusieurs types d'attaques conventionnelles.

Bibliographie

[1] Hetatache Karima, Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformées discrètes,Mémoire de Magister université ferhat abbas-setif UFAS (ALGERIE),2014.

[2] Imen Trabelsi, Halima Maamri, Tatouage numérique fragile pour l'authentification d'images, Mémoire de Master université de Biskra, 2016.

[3] Boukhlouf Djemaa, *Résolution de problèmes par écosystèmes : Application au traitement d'images.* Masters thesis, Université Mohamed Khider - Biskra. (2005)

[4] Nicolas Thome,Bases du traitement des images Introduction et fondement Ni,2016.

[4] www. master-ivi.univ-lille1.fr/fichiers/Cours/seance8_wmk.pdf

[6] Jean-Bernard CAMBIER, Introduction aux images numériques ,haute école condorcet,

[7] Cédric Piovano & Julien Pugliesiimages, Le Tatouage Ou WATERMARKING", 2014.

[8] Maache Mohcin, Tatouage D'images Numériques Dans Le Domaine Fréquentiel **,** mémoire de Master, Universtié Mohamed Boudhiaf,2015.

[9] Nour El-Houda Golea, Tatouage numérique des images couleurs RGB. université Hadj lakhdar Batna .

[10] Rabia Riad, Tatouage robuste d'images imprimées, l'université d'Orléans

et de l'université Ibn Zohr,2015

[11] Walton S., "Information Authentication for a Slippery New Age", *Dr. Dobbs Journal,* vol. 20, no. 4, pp. 18–26, April, 1995.

[12] R. Wolfgang, I. Podilchuk, and E. Delp. Perceptual Watermarks for Digital Images and Video. *IEEE*, 87(7):1108–1126, 1999.

[13] M. Swanson, B. Zhu, and A. Tewfik. Transparent Robust Image Watermarking. In *IEEE* International Conference on Image Processing *(ICIP'96)*, volume 3, pages 211–214, 1996.

[14] Baaziz N., "Adaptive watermarking schemes based on a redundant contourlet transform", *Accepted paper in IEEE International Conference on Image Processing, ICIP-05*. Genoa, Italy, 2005.

[15] Bouzidi A. and Baaziz N., "Contourlet domain feature extraction for image authentication", *IEEE International Workshop on Multimedia Signal Processing*, Victoria, Canada, October 2006.

[16] J. Seitz. *Digital Watermarking for Digital Media*. Information Science Publishing, 2004.

[17] F. Mintzer, G. Braudaway, and M. Yeung. Effective and Ineffective Digital Watermarks. In *IEEE International Conference on Image Processing (ICIP'97)*, volume 3, pages 9–12, 1997.

[18] A. Tirkel, G. Rankin, R. Schyndel, W. Ho, N. Mee, and C. Osborne. ElectronicWatermark.In*DICTA 1993*, pages 666–672, 1993.

[19] S. Bhattacharjee and M. Kutter. Compression Tolerant Image Authentication. *IEEE International Conf. on Image Processing (ICIP'98)*, Chicago, USA, Oct. 1998

[20] J.-L. Dugelay. Procédé de dissimulation d'informations dans une image

Numérique.Brevet *INPI FR 98-04083 (EURECOM 09-FR)*, March 1998.

[21] Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the

DiscreteWavelets Transform and Singular Value Decomposition, European Journal

Of Scientific Research.

[22] Arnold, M. 2000. Audio watermarking: Features, applications and algorithms,

Proceeding of the IEEE International Conference on Multimedia and Expo,

[23] J. Fridrich. Robust Bit Extraction from Images. In *IEEE International Conference on Multimedia Computing and Systems ICMCS'99*, volume 2, pages 536–540, 1999.

[24] Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography incolor and grayscale images. Proceedings of the 2001 workshop on Multimedia and security new challenges - MM&Sec '01, 27. New York, New York, USA: ACM Press.

[25] Gonzalez, Rafael C., and Paul A. Wintz. "Image Compression Standards." Digital Image Processing. 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002. 492-510.

[26] Sung-Cheal Byun, Sang-Kwang Lee, Ahmed H. Tewfik, and Byung-Ha Ahn, "A SVD-Based Fragile Watermarking Scheme for Image Authentication", Springer-Verlag Berlin Heidelberg, pp. 170–178, 2003.

[27] Mohamed KOUBAA,robuste de vidéo basé sur la notion de régions d'intérêt ,université de BORDEAUX 1, 2010.