REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE RECHERCHESCIENTIFIQUE

UNIVERSITE DE KASDI MERBAH OUARGLA

Faculté des Nouvelles Technologies de l'Information et la Communication
Département de l'informatique et Technologies de l'information

N° d'ordre :

N° de série : **Mémoire**

Master Professionnel

Domaine : Math et Informatique

Filière : Informatique

Spécialité : Réseau convergence et sécurité

Présenté par :

- IMENE TRABELSI

-HALIMA MAAMRI

Thème

Tatouage numérique fragile pour l'authentification d'images

Soutenu publiquement

Devant le jury :

Président : SALAH Euschi
Encadreur : Mohamed Khalil MEZGHICHE
Examinateur : CHahrazed Toumi

Année Universitaire : 2015/2016

Je dédie ce travail a :

Je dédie ce travail à mes chers parents

Qu'ils trouvent ici toute ma gratitude pour leur

Soutien tout au long de mes études.

A mes frères et sœurs que dieu les protège

A tout mes collègues promo 2015/2016

A tout mes cousins et ma grande famille

A tout mes amies de cartier et d'enfants

A tous ceux que j'aime.

Remerciements

Tout d'abord, je remercie Allah, le tout puissant, qui m'a donné la force, la patience et la volonté pour accomplir ce modeste travail.

Je tiens à remercier M. **Mohamed Khalil MEZGHICHE** pour son encadrement, sa disponibilité, son suivi, ses conseils précieux et son encouragement.

Je remercie les membres du jury pour m'avoir fait l'honneur d'évaluer mon travail malgré leurs nombreuses responsabilités et occupations.

Je remercie tous les membres de ma famille qui, par leur support et encouragement, m'ont permis de m'investir entièrement dans mes études.

Je tiens à remercier toute personne ayant contribué de près ou de loin à la réalisation de ce travail.

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 est l'utilisation du tatouage fragile. Plusieurs méthodes efficaces de tatouage des images numériques ont en effet été développées. Néanmoins, la plupart des méthodes proposées se sont focalisées sur les images à niveaux de gris.L'objectif de notre travail est de réaliser un nouvel algorithme du tatouage fragile qui vise à insérer un watermark dans les bits LSB d'une image couleur RGB, cette méthode est basée sur l'utilisation de l'opérateur XOR en tant qu'une fonction de hachage pour la vérification 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, XOR.

Abstract

"Watermarking" or tattoo picture has in recent years a spectacular development. The increased use of multimedia applications pose increasing problems concerning the preservation of confidentiality and authenticity of digital data transmission. These data, particularly images must be protected from tampering. The best solution is the use of delicate tattoo. Several effective methods of watermarking digital images have indeed been developed. Nevertheless, most of the proposed methods have focused on images to grayscale. The aim of our work is to achieve a new algorithm fragile tattoo which aims to insert a watermark in the LSB bits of RGB color image, this method is based on using the XOR operator as one a hash function for the image integrity verification. The experimental results showed the feasibility of our proposed algorithm, and that our approach provides a good imperceptibility and sensitivity to various types of attacks.

Keywords: delicate tattoo, digital watermarking, integrity, authentication, LSB, XOR.

Table de matières

Table des figures

Liste des tableaux

Introduction général

L’information visuelle joue un rôle très important dans notre vie quotidienne, plusieurs domaines comme le journalisme, la publicité, l'architecture et la médecine utilisent des applications basées principalement sur l'information visuelle. On dit souvent qu’une image vaut mille mots, mais on sait moins à quel point la communication visuelle est plus puissante. Les images sont comprises par le cerveau en moyenne 60,000 fois plus rapidement que le texte, et
90 % de l’information transmise au cerveau est visuel, les gens retiennent 80% de ce qu’ils voient, 20% de ce qu’ils lisent, et 10% de ce qu’ils entendent.

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.

La révolution numérique a aussi engendré des mécanismes plus efficaces pour le stockage et le traitement des images et le contenu multimédia. Cependant, elle a aussi engendré des moyens plus simples et faciles qui peuvent être utilisés pour la falsification et la manipulation malveillante des images. D’ici, il est devenu nécessaire de développer des mécanismes pour assurer l’authentification et vérifié l'intégrité des images numériques.

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.

Dans ce mémoire, nous avons proposé une nouvelle méthode de tatouage fragile d’images numériques. Cette méthode consiste à remplacer les bits de poids faibles des pixels codant l’image par le résultat de l’opérateur XOR des bits MSB des trois couleurs de chaque pixel.

L'analyse des résultats expérimentaux montre la faisabilité de notre algorithme proposé, et que notre approche permet d'obtenir une bonne imperceptibilité et sensibilité face aux divers types d'attaques, c'est qui représente un bon comportement pour un algorithme de tatouage fragile d'images.

Le travail présenté dans ce mémoire est organisé en quatre chapitres :

Dans le premier chapitre, nous présentons les notions de base du traitement d'images, la notion de l'image numérique, ses types et ses caractéristiques. Nous présentons aussi quelques terminologies et quelques notions importantes dans le domaine de traitement d'images numériques telles que la numérisation, le codage et le stockage.

En deuxième chapitre, nous présentons la technique de tatouage numérique ou (watermarking), ces caractéristiques, les différents concepts et techniques utilisées, les attaques existantes, ainsi que les différents domaines d'application.

Le troisième chapitre est consacré à la présentation de la technique du tatouage fragile des images qui permet d'assurer l'authentification et l'intégrité des images numériques. Enfin, nous présentons quelques algorithmes connus basée sur cette technique.

La présentation du travail réalisé dans ce mémoire, ainsi que l'évaluation expérimentale de la performance de notre algorithme est exposée dans le quatrième chapitre où nous présentons quelques résultats expérimentaux obtenus par notre algorithme de tatouage fragile des images numériques.

Chapitre 1

Concepts de base sur les images numériques

1.1 Introduction

L'image constitue l'un des moyens les plus intéressants qu'utilise l'homme pour communiquer avec son entourage. C'est un moyen de communication universel dont, la richesse du contenu permet aux êtres humains de se comprendre, ce qui a fait des images un des plus importants éléments du flux multimédia.

La manipulation de ce type de documents nécessite des connaissances de base. Permettant de définir l'image, ses caractéristiques et les différents traitements qu'elle peut subir. Le traitement et l'analyse d'images trouvent leurs applications dans des domaines extrêmement varies de l'industrie et de la recherche. Ces méthodes sont utilisées dans de nombreuses disciplines scientifiques, et dans des domaines aussi variés tels que ceux qui ont trait à l'astronomie, l'identification, la pharmacologie [1].

Dans ce chapitre, on va présenter quelques notions de base sur les images numériques qui seront très utiles pour comprendre ce qui viendra tout au long de ce mémoire.

1.2 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 [Picture éléments], 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].

1.3 Image numérique

Contrairement aux images obtenues à l'aide d'un appareil photo, ou dessinées sur du papier, les images manipulées par un ordinateur sont numériques (représentées par une série de bits).L'image numérique est l'image dont la surface est divisée en éléments de taille fixes appelés des pixels, ayant chacun comme caractéristique un niveau de gris ou une couleur.

La numérisation d'une image est la conversion de celle-ci de son état analogique (distribution continue d'intensités lumineuses dans un plan x 0 y) en une image numérique représentée par une matrice bidimensionnelle de valeur numérique f(x, y) ou x, y : son les coordonnées cartésiennes d'un point de l'image[2].

La qualité de l'image compte sur d'une part du nombre de pixels, et d'autre part du nombre de valeurs possibles pour l'intensité [3] [4].

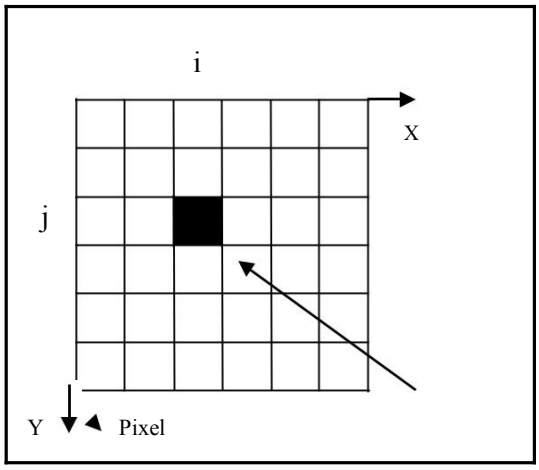


FIG. 1.1 – Représentation d'un Pixel

La localisation spatial d'un pixel est définie par ses cordonnées cartésiennes : i, j.

L'intensité d'un pixel sera définie f (i, j), codée sur 8,16 ou 32 bits.

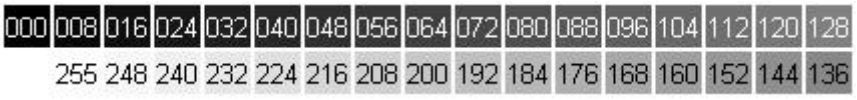


FIG. 1.2 – Représentation Matriciel des couleurs

1.4. Les caractéristiques d'une image numérique

L'image est un ensemble structure d'information donc, ces informations ont des caractéristiques définies par les paramètres suivantes :

1.4.1. Pixel

Le pixel est le plus petit élément que contient une image, et qui peuvent manipuler les matériels et logiciels d'affichage ou d'impression. La dimension, en pixels, détermine le format d'affichage à l'écran (la taille des pixels de l'écran étant fixe) [6].

Le Pixel est l'abréviation de « Picture Elément » La quantité d'information que véhicule chaque pixel donne des nuances entre images monochromes et images couleur. Dans le cas d'une image monochrome, chaque pixel est codé sur un bit. Dans une image couleur (R.V.B.), un pixel peut être représenté sur trois octets : un octet pour chacune de ces couleurs : Rouge, Vert ou Bleu.

1.4.2. La taille de l'image

La taille de l'image présente le nombre de pixels de celle-ci ; donné par le produit du nombre de lignes et le nombre de colonnes de la matrice associée à l'image.

1.4.3. Résolution

La résolution d'une image est définie par le nombre de points image ou "pixels" représentant l'image, par unité de longueur de la structure à numériser (l'image initiale), on exprime cette résolution en points ou pixels par pouce (ppp) ou "dots per inch" (dpi). 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, la définition (dimension de l'image), l'échantillonnage est la qualité de stockage [7].

1.4.4. Luminance (Intensité)

C'est le degré de luminosité des points (Pixels) 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.

FIG. 1.3 – Exemple de Luminance

1.4.5. Contraste

Le contraste est une propriété intrinsèque à une image qui permet de quantifier, la capacité de distinguer deux régions distinctes. Il s'agit dans ce cas de distinguer deux régions suffisamment grandes d'après l'intensité des points présentés par des niveaux de gris.

FIG. 1.4 – Exemple de Contraste

1.4.6. Contours

Les contours représentent la frontière entre les objets de l'image, ou la limite entre deux pixels dont les niveaux de gris ou couleurs représentent une différence significative.

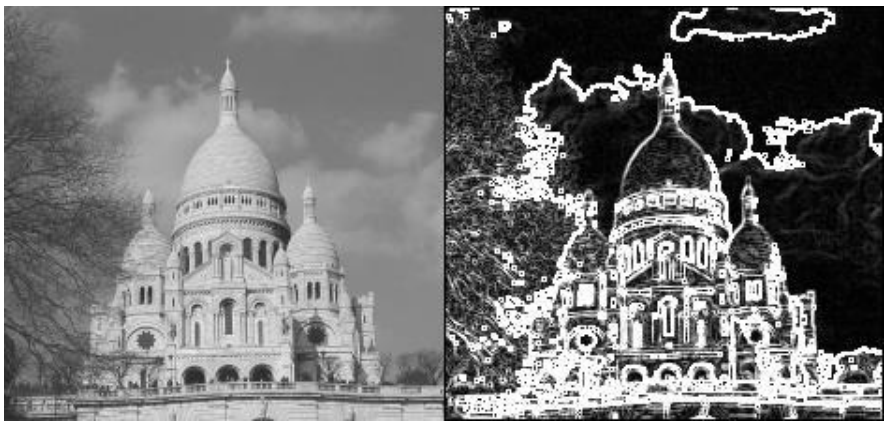


FIG. 1.5– Exemple de Contour

1.4.7. Texture

Les textures décrivent la structure de l'image. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différentes [5].

La texture est modélisée comme une structure spatiale constituée de l'organisation de primitives ayant chacune un aspect aléatoire ou définie comme une microstructure de la surface. Une texture peut avoir un aspect périodique ou bien aléatoire.

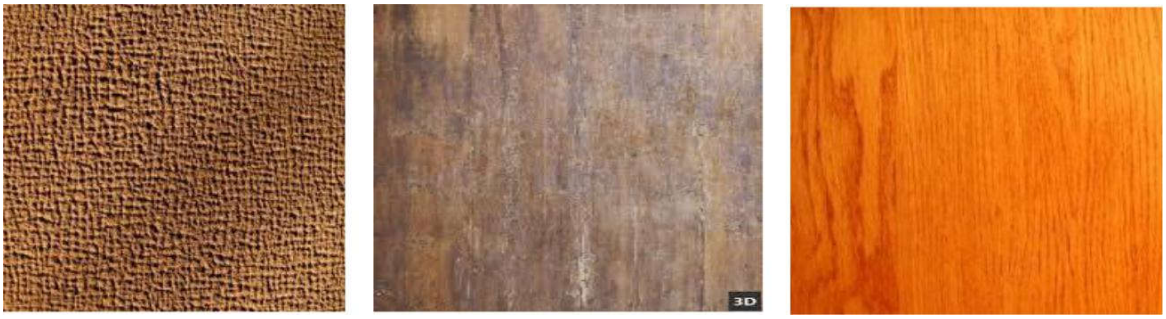


FIG. 1.6 – Exemple de Texture

1.4.8. La couleur

La couleur est un des premiers descripteurs qui sont employés pour la recherche d'images. La couleur forme une partie significative de vision humaine, sans elle beaucoup de tâches journalières prouveraient très difficile. Nous pouvons distinguer efficacement les objets basés sur seule la couleur. Deux espaces de couleur le plus utilisée sont le RGB et HVS. La forme la plus simple de descripteur de couleur est l'histogramme de couleur [3].

1.4.9. La forme

Au même titre que les caractéristiques de texture, les attributs de forme sont complémentaires de la description couleur. Les caractéristiques de forme sont extraites à partir des régions dans les images (contours), Nous distinguons deux catégories de descripteurs de formes [2]:

- ✓ Les descripteurs bases régions.
- ✓ Les descripteurs bases frontières.

1.4.10. Bruit

C'est un signal qui lors de l'acquisition ou la transmission vient s'ajoutera l'image, Il se matérialise par la présence dans une région homogène des valeurs plus ou moins éloignées de l'intensité de la région. Le bruit est le résultat de certains défauts électroniques du capteur et de la qualité de numérisation [8].

FIG. 1.7 – Exemple de Bruit

1.4.11. L'histogramme

L'histogramme des niveaux de gris ou de 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'informations sur la distribution des niveaux de gris ou des couleurs.

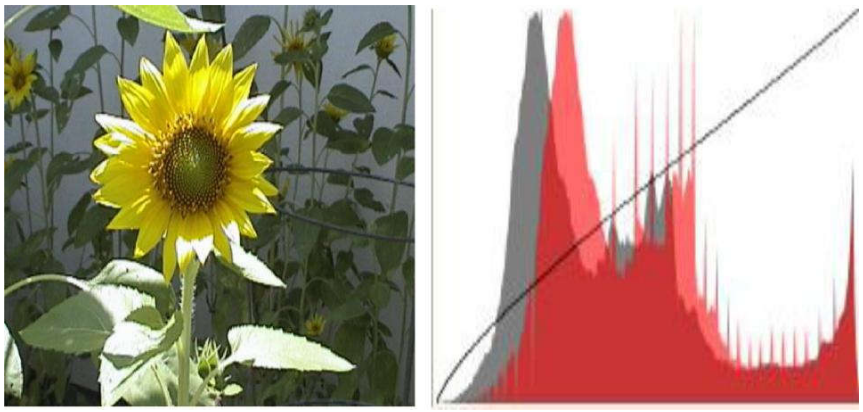


FIG. 1.8 – Exemple d'Histogramme d'Image (RGB, NdG)

1.5 Les différents types d'images

Il existe différentes catégories d'image selon le nombre de bits sur lequel est codée la valeur de chaque pixel.

1.5.1 Image noir et blanc

Le mode le plus simple, chaque pixel y est soit allumé [Blanc] soit éteint [Noir], l'image obtenue n'est pas très nuancée. Alors, pour convertir une image couleur en mode noir et blanc il faut d'abord passer par le mode niveaux de gris.

FIG. 1.9 – Image en Mode Monochrome

1.5.2 L'image en niveaux de gris

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur de pixel prend des valeurs allant de noir au blanc en passent par un nombre fini de niveaux intermédiaires. Les valeurs peuvent être comprises entre 0 et 255 ; les pixels sont alors codés non pas sur un bit mais sur un octet.

FIG. 1.10 – Images en Niveau de Gris

1.5.3 Images en couleurs

Peut-être codée elle aussi sur 4 bits (image en 16 couleurs), 8 bits (image en 256 couleurs) ou davantage : 24 bits pour une image en 16 millions de couleurs (16777216= 2^{24}) On obtient ainsi 256 x 256 x 256 = 16777216 (plus de 16 millions de couleurs différentes) [5].

FIG. 1.11 – Images en Couleur

1.6. Formats d'image

1.6.1. Les images Bitmap

Les images affichées sur l'écran d'un PC sont des images matricielles, encore appelées bitmap, chaque image est en réalité une matrice de pixels.

1.6.1. Les images vectorielles

L'image vectorielle est définie par une fonction mathématique. Pour définir par exemple la silhouette de la lettre « d » ou dira à l'ordinateur de dessiner un anneau, à la droite de laquelle est accolé un rectangle vertical et allongé de même couleur, positionné de manière spécifique par rapport à l'anneau [10], Mais pour afficher à l'écran ou imprimer, Ces images vectorielles sont en fait automatiques traduites en images bitmap, car c'est le seul format directement affichable par ordinateur.

1.7. Amélioration et prétraitement d'images

Les images brutes permettent rarement de parvenir à une extraction directe des objets à analyser. Avant d'extraire les objets et d'analyser une image, il va donc être nécessaire d'améliorer l'image.

1.7.1. Amélioration d'images

❖ **En améliorant le rapport signal sur bruit :** Le transfert de l'image d'un objet jusqu'à l'ordinateur se produit avec un certain bruit. Le bruit est dû en particulier aux imperfections de la source qui génère l'image.

On améliorera la qualité de l'image en modifiant le rapport signal sur bruit. La méthode la plus simple consiste à effectuer plusieurs acquisitions de l'image, plusieurs sommations du signal. Le bruit n'apparaissant statistiquement jamais au même point, il sera uniformément réparti, alors que le signal, apparaissant toujours au même endroit, sera amplifié.

❖ **Par filtrage :** L'amélioration du rapport signal sur bruit, bien qu'intéressante, ne suffit pas toujours pour obtenir de bonnes images. L'amélioration de l'image est essentiellement obtenue par ce que l'on appelle une opération de "filtrage". Un filtre est une transformation mathématique permettant, pour chaque pixel de la zone à laquelle il s'applique, de modifier sa valeur en fonction des valeurs des pixels avoisinants, affectées de coefficients [11].

1.7.2. Pré traitement d'une image

❖ **Segmentation d'image :** est une opération de traitement des images [12]. C'est une des étapes critiques de l'analyse d'images qui conditionne la qualité de la mesure ultérieurement effectuée. Elle permet d'isoler dans l'image les objets sur lesquels doit porter l'analyse.

FIG. 1.12 – Image Segmentée

1.8. Système de traitement d'images

Un système de traitement d'images est une chaîne séquentielle d'étapes allant de l'étape d'acquisition jusqu'à l'interprétation, il est représenté comme suit :

1.8.1. 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.

1.8.2. 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 [13].
- **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.

1.8.3. 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.

1.8.4. 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).

1.9. Domaine d'application de traitement d'image

Le traitement d'image possède l'aspect multidisciplinaire, on trouve ces applications dans des domaines très variés tels que :

- **Imagerie aérienne et spatiale :** Dans laquelle les traitements concernent l'étude des images satellites, l'analyse des ressources terrestres, la cartographie automatique, les analyses météorologiques.

- **L'imagerie médicale :** On trouve des utilisations de cette technique dans l'échographie, la résonance magnétique nucléaire, ainsi que dans le domaine de la reconnaissance automatique des cellules ou de chromosomes [14].

- **La Robotique :** Qui connaît actuellement le plus grand développement et dont les tâches usant de l'imagerie sont principalement l'assemblage (pièce mécanique, composants électroniques,...), le contrôle de la qualité, ainsi que la robotique mobile.

1.10. Conclusion

Dans ce chapitre, on a 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.

Nous présenterons dans le chapitre suivant une introduction au tatouage numérique et les différentes techniques et les méthodes existantes dans ce domaine.

Chapitre 2

Introduction au tatouage numérique

1. **Introduction**
2. **Définition du tatouage numérique**
3. **Caractéristiques d'un marquage numérique**
4. **Le processus du tatouage numérique**
5. **Classification de marquages**
6. **Les attaques**
7. **Applications**
8. **Conclusion**

2.1 Introduction

L'apparition de la révolution numérique et l'accessibilité des nouvelles technologies de l'information au grand public ont entraîné un volume d'échange de documents multimédias de plus en plus grandissant. Des milliards des fichiers électroniques se trouvent dans l'internet, qui a ouvert le champ à la copie et à la distribution illégale. Les premiers à en souffrir sont les artistes, l'économie et l'emploi de façon générale.

L'impact économique et juridique de violation de la propriété intellectuelle a mené à un certain nombre d'initiatives, plusieurs techniques ont été proposées. Parmi ces techniques, on trouve la technique de tatouage numérique qui permet de suivre précisément l'utilisation ou de crypter un contenu afin d'en limiter les utilisations futures.

Dans ce chapitre, nous présentons la technique de tatouage numérique ou (watermarking), ces caractéristiques, les différents concepts et techniques utilisées, les attaques existantes, ainsi que les différents domaines d'application.

2.2 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, qui consiste à insérer une marque invisible dans un support numérique. S'il a été envisagé pour la première fois au cours des années 70, il a réellement trouvé ses applications lors de l'explosion de l'utilisation du support numérique [17].

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. Le nom de cette technique provient du marquage des documents papier et des billets [18].

Le tatouage numérique permet d'insérer des informations (une signature) dans un document informatique. L'ajout de cette signature doit être imperceptible et indécelable par tout système

ignorant son mode d'insertion. En particulier, il faut qu'il soit totalement invisible pour l'oeil humain. Cette méthode est différente de la cryptographie qui permet de cacher un message en le rendant illisible.

Une image numérique tatouée est regardable et utilisable comme n'importe quelle image. Le tatouage est possible avec deux programmes différents. Le premier permet l'insertion d'une signature dans un document numérique (on signe son oeuvre). Le second sert à vérifier l'existence ou non d'un tatouage dans un document numérique [19] (on expertise la signature).

Le marquage des données numériques fait partie du domaine de «information hiding ». Information hiding consiste à dissimuler des informations dans un document formé de données numériques.

La cryptographie : Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité [20].

La stéganographie : Le mot stéganographie vient du grec 'steganos' (caché ou secret) et 'graphy' (écriture ou dessin) et signifie, littéralement, 'écriture cachée'. C'est une Technique qui consiste à dissimuler un message, que l'on désire transmettre confidentiellement, dans un ensemble de données d'apparence anodine, de façon à ce que sa présence soit imperceptible [5].

2.3 Caractéristiques d'un marquage numérique

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

2.3.1 Imperceptibilité

Appelée aussi la distorsion d'insertion, Il s'agit de faire en sorte que l'impact visuel du marquage soit le plus faible possible afin que l'image tatouée soit visuellement équivalente à l'image originale [21].

Le tatouage doit être invisible à l'œil humain. Prenons un exemple très simple pour souligner son importance. Imaginons une image en niveau de gris avec une large zone uniforme. Si l'on rajoute un peu de bruit, ceci va immédiatement se voir dans cette zone. Il faut plutôt mettre le tatouage dans des zones de fort gradient (contour de formes, zones fortement texturées,…) où l'œil est moins sensible.

FIG 2. 1. Image original

FIG 2.2. Image marquée

2.3.2 Robustesse

On pourrait séparer cette rubrique en deux parties : la *robustesse* et la *sécurité*. Ces deux caractéristiques sont souvent confondues surtout dans le cas du marquage. On parle de robustesse pour définir la résistance du tatouage face à des transformations de l'image tatouée. Ces transformations peuvent être de type géométrique (rotation, zoom, découpage …). Elles peuvent modifier certaines caractéristiques de l'image (histogramme des couleurs, saturation…). Il peut aussi s'agir de tous les types de dégradations fréquentielles de l'image (compression avec pertes, filtres passe haut ou passe bas, passage analogique numérique, impression de l'image, etc.…).
Ces attaques sont dénommées « attaques aveugles », car le pirate agit sans réellement savoir ce qu'il fait. Il espère ainsi laver l'image [22].

La sécurité caractérise la façon dont le marquage va résister à des attaques «malicieuses ». On peut faire des parallèles avec la cryptanalyse. Le pirate va chercher à laver l'image de façon

intelligente. Il est sensé connaître l'algorithme et va, en général, chercher la clef qui lit le tatouage. Cela demande souvent une analyse approfondie de la technique de marquage employée.

2.3.3 Complexité

Dans la pratique, la plupart des opérations de tatouage doivent pouvoir s'effectuer en temps réel (surtout la détection, pour des films par exemple). Ceci implique une contrainte supplémentaire sur la complexité des opérations utilisées pour le marquage et pour la détection.[23]

2.3.4 Capacité

La capacité d'un système de tatouage numérique désigne le rapport : « nombre de données » à dissimuler sur « taille du document hôte ». Dans le cas du marquage, et comme nous l'avons vu précédemment, la capacité se limite souvent à 1 bit. De façon générale, plus la capacité est faible, plus la robustesse et l'imperceptibilité sont fortes. [24]

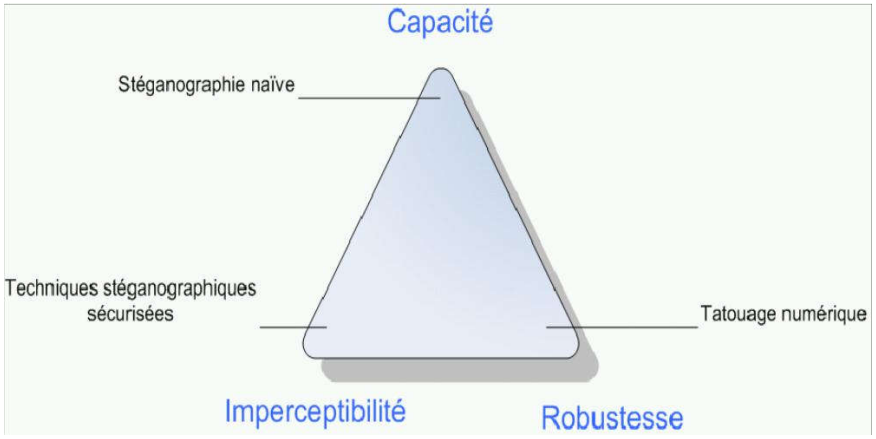


FIG 2.3. Caractéristiques de marquage

2.4 Le processus du tatouage numérique

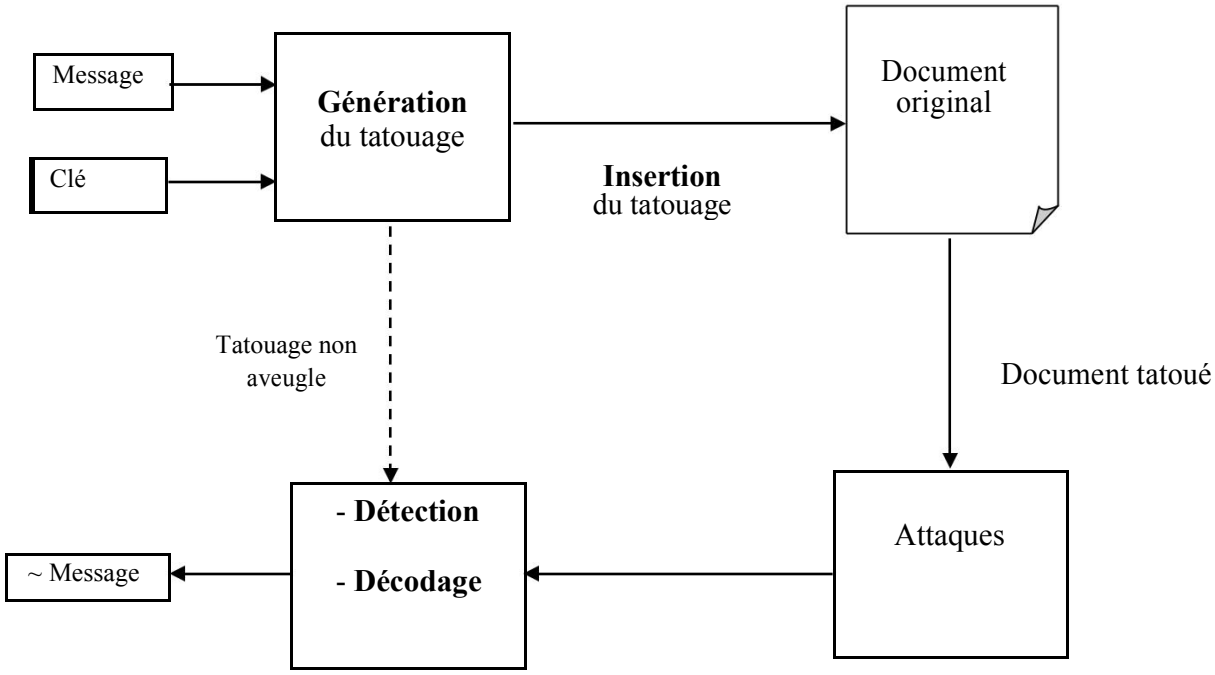


FIG 2.4. Le schéma du tatouage numérique

un message contenant L bits d'information est transformé selon une clé en un tatouage par le générateur, qui est ensuite inséré dans le document (aussi appelé "hôte") pour donner un document tatoué.

la phase d'insertion. Ici, le tatouage est exprimé sous la forme d'un bruit qui est ajouté au document, la déformation dépendant de la puissance du bruit est secrète et spécifique au tatoueur.

le document est ensuite copié et attaqué, ce qui est modélisé par la transmission dans un canal soumis à du bruit.

La réception d'un document consiste en deux parties : d'une part, la détection du tatouage et d'autre part, s'il est présent, son décodage.

La phase de détection consiste à prouver la présence d'un tatouage dans le document grâce au clé.

la phase de décodage consiste à calculer une estimation de message original. Si la taille du message inséré L est suffisamment grand et contient une information intelligible (par exemple, des caractères ASCII) [25], certains auteurs considèrent que la détection devient inutile puisqu'on peut appliquer un simple décodage. Si la chaîne décodée est inintelligible (par exemple, non ASCII), on considère qu'il n'y a pas de tatouage.

Si le document original n'est pas utilisé à la réception, l'algorithme de tatouage est qualifié d'aveugle. Dans le cas inverse (beaucoup moins intéressant en pratique), l'algorithme est qualifié de non aveugle ou à décodeur informé. Si le document original est utilisé dans la construction de tatouage, on parlera de tatouage informé. Lorsque plusieurs tatouages sont insérés (correspondant souvent à plusieurs utilisateurs), on parle de tatouage multiple [26].

2.5 Classification de marquages

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

- **Le marquage faible (ou fragile)** : Dans ce cas particulier, on demande au tatouage d'avoir une très grande imperceptibilité et une faible robustesse. Ainsi, la marque ne supportera quasiment aucun traitement. On pourra ainsi certifier ou non l'intégrité de l'image [27].

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

- **Le marquage symétrique (ou privé) :** Le parallèle avec la cryptographie prend ici tout son importance. Le marquage symétrique signifie que l'on utilise la même clef pour insérer et détecter le tatouage [28].

- **Le marquage asymétrique (ou publique) :** La clef de marquage et celle de détection sont différentes Outre l'intérêt immédiat (n'importe qui peut lire la signature sans pour autant pouvoir l'enlever ou la modifier), ces techniques récentes sont plus sécurisées Elles portent officieusement le nom de « marquage de seconde génération » [29].

2.6 Les attaques

Nous allons aborder la question des attaques que peut subir un tatouage numérique. La sensibilité d'un marquage vis à vis des attaques est très importante. Elle influe sur deux des caractéristiques du marquage : la robustesse et la sécurité. Nous parlerons dans un premier temps des attaques dites « aveugles » (ou « blind ») qui mettent à l'épreuve la robustesse du tatouage. Ensuite, nous aborderons la sécurité des marquages face aux attaques « malicieuses » (ou « malicious »).

2.6.1 Les attaques aveugles

Le pirate sait que l'image est tatouée. Il cherche à laver l'image du marquage. Mais, le pirate a peu de connaissances sur l'algorithme de tatouage employé. Il cherche à mettre en défaut le détecteur de marquage en appliquant des transformations à l'image. Il espère que celles-ci seront suffisantes pour que l'on ne puisse plus détecter le marquage. Comme dans le cas d'un vrai tatouage, celui-ci doit être résistant à toutes les formes de nettoyages et son extraction de façon « brute » doit laisser une cicatrice suffisamment importante pour rendre le document quasiment inexploitable. Le pirate a, à sa disposition, toute une palette d'attaques que l'on peut séparer en deux groupes [30].

2.6.1.1 Les transformations géométriques

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

FIG 2.6. Symétrie vertical

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

FIG 2.7. Rotation

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

FIG 2.8. Le recadrement

❖ **Changement d'échelle :** Ce genre de transformations peuvent être séparées en deux groupes :

les transformations uniformes (pour lesquelles on conserve les proportions, l'échelle en X varie comme l'échelle en Y)

les transformations non uniformes (où l'échelle en X ne varie pas comme l'échelle Y).

❖ **Attaque par Mosaïque :** Il s'agit ici d'utiliser le "crop" d'une façon beaucoup plus violente et qui se prête assez bien aux pages HTML. Il suffit de découper l'image en autant de morceaux que l'on désire (plus il y a de morceaux plus l'attaque à des chances d'aboutir), puis de recoller cette image au moment de l'affichage en créant par exemple en HTML un tableau dont chacune des cellules contiendra un morceau de l'image. Cette attaque est très peu applicable en pratique, et heureusement car elle est d'une rare efficacité si l'on se donne les moyens de bien découper l'image [31].

FIG 2.9. Attaque par Mosaïque

2.6.1.2. Les transformations fréquentielles

Les attaques ne sont pas toujours réalisées par des pirates mais parfois inconsciemment. Ainsi, la compression MPEG2 d'un film, va attaquer de façon relativement importante l'image. La quantification va modifier les coefficients de la DCT (surtout pour les hautes fréquences). Ainsi, toutes les compressions avec pertes vont endommager l'image et altérer la détection du tatouage.

L'utilisation de compressions MPEG4, par l'intermédiaire d'un codec tel que DivX, entraîne souvent une altération très importante du tatouage. Il est indispensable que les nouveaux marqueurs en tiennent compte. A coté de cela, le pirate dispose de nombreux filtres (passe haut, passe bas, ou même passe bande) qui vont lui permettre de rechercher le meilleur compromis entre la disparition du tatouage et une faible dégradation de la qualité de l'image.

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

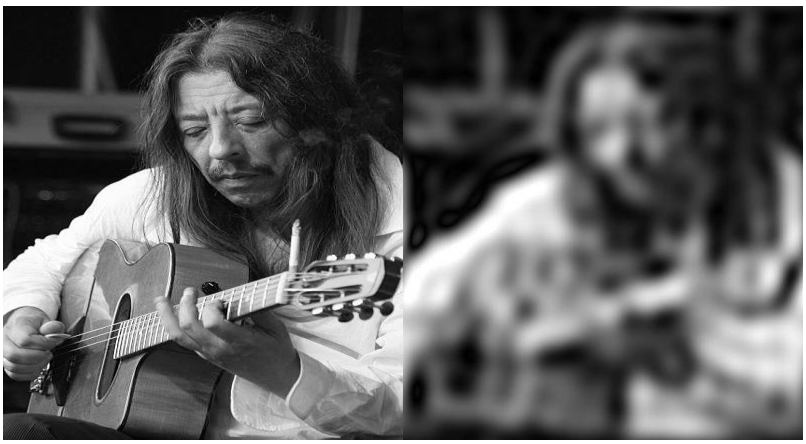


FIG 2.10. Filtres passe-bas

- **Accentuation des contours :** Ou encore appelé filtre "passe-haut" (car il supprime les basses fréquences), ou "Sharpen". Il s'agit de l'inverse du filtre passe-bas (encore appelé "Blur"). L'intérêt d'une telle attaque est assez faible, sachant que l'on conserve le bruit (et

les forts gradients de l'image), et que c'est souvent à ce niveau-là que se situe le tatouage (car c'est dans ces zones ou l'on cache de préférence de l'information).

FIG 2.11. Filtre passe-haut

2.6.2 Les attaques malicieuses

Ce type d'attaques est beaucoup plus intéressant car il demande des connaissances en traitement du signal ainsi qu'une analyse sérieuse du marquage. Les attaques malicieuses sont différentes des attaques aveugles car le pirate va s'attacher à trouver la faiblesse du système qui utilise le marquage. Selon cette faiblesse, il ciblera son attaque.

Par bien des aspects, cela se rapproche beaucoup de la cryptanalyse (l'art de briser les systèmes de chiffrement en cryptologie).

2.6.2.1. Exemple d'attaque sur le copyright

Comme nous l'avons vu, une des utilisations du marquage peut être la protection des droits d'auteur (« copyright »). Par exemple, le document va être tatoué avec en paramètres le nom de l'auteur, l'identification du contenu, un secret etc. Seul l'auteur connaît ces paramètres. Cette version marquée sera mise à disposition sur Internet. La version originale ne sera pas divulguée. L'auteur est le seul à pouvoir détecter le marquage pour prouver que ce document lui appartient.

Dans ce cas précis, le pirate va chercher à semer le trouble sur l'origine de l'image. En effet, il ne sert à rien d'ajouter une autre marque au contenu divulgué sur Internet. L'auteur a toujours à sa

disposition la version originale. Le pirate essaie plutôt de recréer une image originale (c'est à dire sans marquage) en soustrayant un faux marquage.

2.7 Applications

Les applications du marquage numérique d'images sont différentes selon les objectifs de sécurité poursuivis. Parmi ces applications nous trouvons : la gestion numérique des droits d'auteurs et leur protection, la prévention de la copie illégale et de la redistribution non autorisée d'images,

L'authentification de la source du document image, la vérification de l'intégrité des données du document (tamper-proofing) et la protection du contenu sémantique du document image [32].

2.7.1. La protection des droits d'auteur

La protection des droits d'auteurs constitue une des premières applications du marquage. Ce type d'application requiert l'insertion d'une marque identificatrice de l'auteur ou du propriétaire légal du document image. Ainsi, en cas de conflit, la preuve de propriété peut être démontrée en détectant la marque. La robustesse de la marque est dans ce cas requise afin de protéger la marque contre toutes tentatives visant à l'effacer (attaque destructive), à faire échouer sa détection (attaque géométrique) ou à créer une ambiguïté dans la décision (attaque de protocole).

2.7.2. La prévention de la copie illégale ou « fingerprinting »

Dans ce type d'application, la marque insérée dans le document est identificatrice de l'entité à laquelle cet objet est légalement destiné (receveur). Sachant qu'un document image est ainsi marqué, toute personne ayant l'intention de faire des copies (illégales) et de les redistribuer sera dissuadée de peur d'être identifiée. Ce type d'application requiert une marque robuste à toutes les tentatives visant à détruire la marque, à faire échouer sa détection ou à créer une ambiguïté de décision (collision au sein d'une coalition de personnes).

2.7.3. L'authentification

Le but de cette application est d'insérer dans un document 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. Ce type d'application est très demandé pour les images médicales. Mais dans d'autres cas, on voudrait assurer une authentification du contenu.

2.8 Conclusion

Nous avons présenté de manière plus ou moins approfondie la technique de tatouage numérique, le watermarking a été annoncés comme un outil de protection des droits de l'auteur, imposaient une identification des producteurs et autres exploitants économiques de l'œuvre, et d'autre part que le watermarking garantissait avant tout l'authenticité de l'œuvre, le watermarking et l'un des technique de protection de droit d'auteur les plus utilisées a de cause son efficacité et sa facilité d'implantation.

Nous avons présenté le processus de son implantation, et les différents types d'attaques sur les documents tatoués, ainsi que la manière d'extraction de l'information de tatouage et en fin, on a abordé les domaines d'applications de marquage.

Chapitre 3

Tatouage fragile des images numériques

1. **Introduction**
2. **Principe**
3. **Définitions**
4. **Schéma générique d'un système d'authentification d'image**
5. **Modèle générique d'une technique de tatouage fragile**
6. **Caractéristiques d'un système de tatouage fragile**
7. **Types d'attaques**
8. **Algorithmes de tatouage fragile**
9. **Conclusion**

3.1 Introduction

Le tatouage d'images numériques a connu un grand progrès ces dernières années, au début développé 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 d'images. Nous présentons aussi les différentes techniques utilisées dans ce domaine, ainsi que quelques algorithmes de tatouage fragile les plus populaires.

3.2 Principe

Parmi les premières méthodes proposées pour assurer un service d'intégrité étaient 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 [33]) dans l'image d'origine de telle manière que les moindres modifications apportées à l'image se répercutent également sur la marque insérée (figure 3.1). Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence de cette marque (figure 3.2).

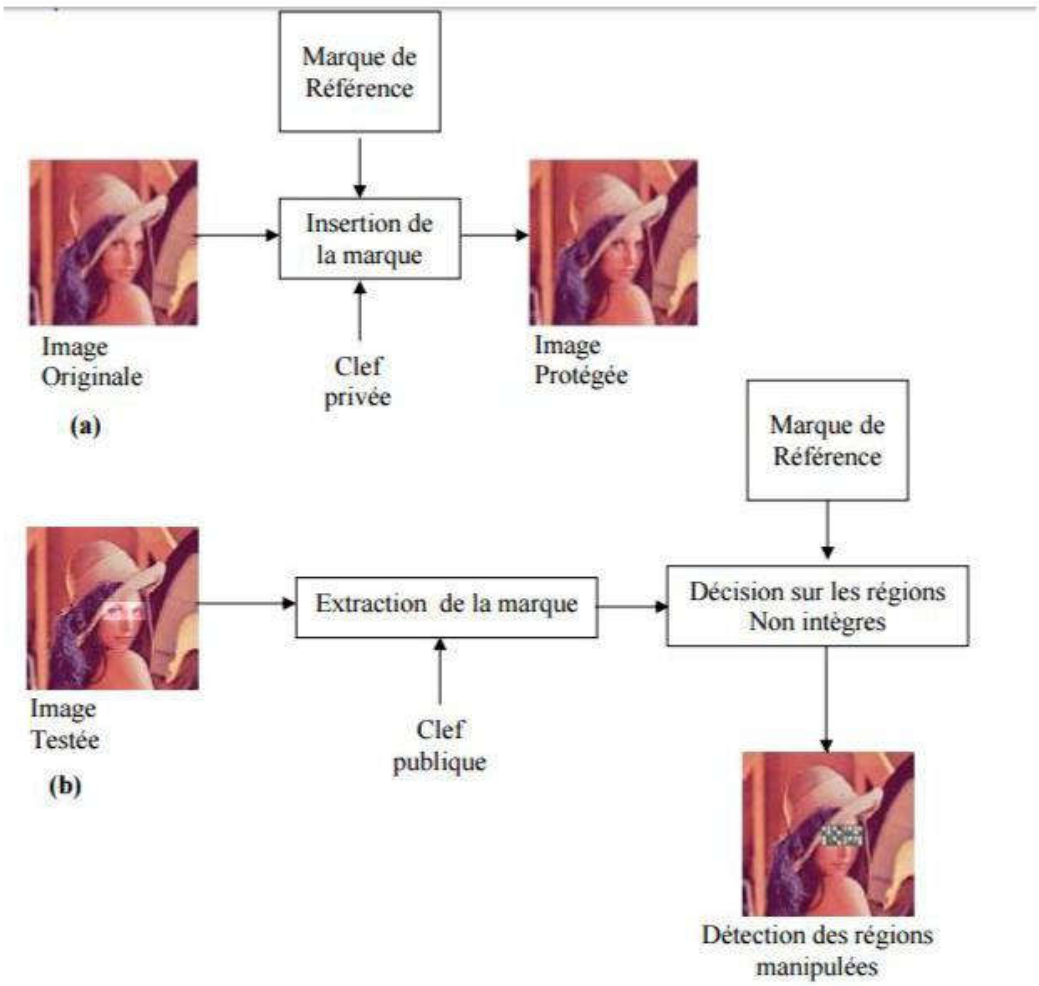


Fig. 3.1 Schéma général d'un système d'intégrité basé sur un tatouage fragile.

3.3 Définition d'un tatouage fragile

Il est intéressant de remarquer qu'il peut être utile, dans certain cas, de favoriser une fragilité plutôt que une robustesse. Le principe de ce type d'algorithmes est d'exploitée la fragilité du tatouage afin d'authentifier (prouver l'intégralité) des images.

De ce fait, si la marque est altérée, l'image n'est plus considérée comme authentifiée. Nous citons, par exemples, les techniques reposant sur la substitution de plan LSB4 de l'image par la différence entre l'image et sa forme chaotique [34] ou par la carte des conteurs et les moments invariants [35]

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

3.3. 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 [36].

3.3. 2 La sécurité

Il s'agit de protéger les informations insérées par des méthodes de cryptographie afin d'éviter qu'elles soient falsifiées ou manipulées. Le schéma de tatouage doit résister aux attaques visant à décrypter la clé. La méthode du tatouage doit également respecter le principe de Kerckhoff : « *La sécurité d'un algorithme doit résider dans le secret de la clé. Les algorithmes utilisés doivent pouvoir être rendus publics*» [37].

3.3. 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 [38].

3.3. 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 [39].

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.).

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

Les auteurs proposent un schéma générique d'un système d'authentification d'images. Ce dernier doit satisfaire les critères suivants :

- **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 ou 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 sépare, 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 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).

3.5 Modèle générique d'une technique de tatouage fragile

Cette section traite les techniques de tatouage pour assurer un service d'authentification. Le modèle général d'un système d'authentification base sur le tatouage numérique est illustré dans la Figure3.2.

Généralement, une clé secrète K connue par l'émetteur et le récepteur est utilisé pour générer un watermark W qui sera insère dans l'image hôte f. L'image tatouée fw est ensuite délivrée par le canal de communication (par exemple, Internet, satellite, etc.) ou stockée dans une base de données. Pour authentifier l'image reçue f w, la même clé secrète est utilisée pour générer le watermark original W. Ce dernier est utilisé pour extraire et comparer la version intégrée W [40].

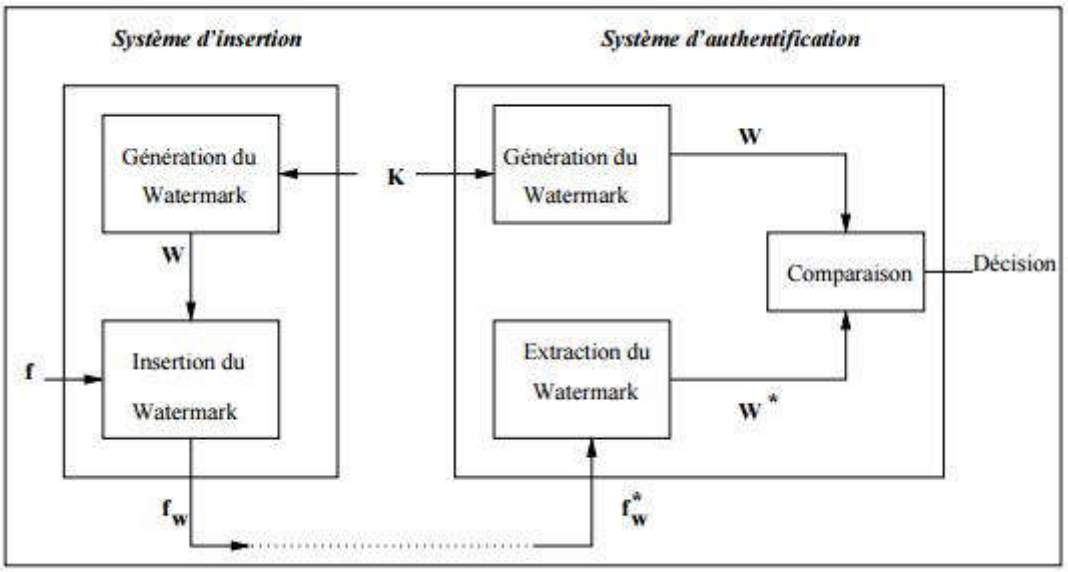


Fig. 3.2.Le modèle général d'un système d'authentification base sur le tatouage fragile.

3.6 Caractéristiques d'un système de tatouage fragile

3.6.1 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.

3.6.2 Imperceptibilité

Le watermark inséré ne doit pas être visible par l'observateur [41]. Dans la plupart des cas il s'agit de préserver la qualité visuelle de l'image tatouée.

3.6.3 La phase de détection ne doit pas requérir l'image originale

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).

3.6.4 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.

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

Une attaque particulière mentionnée qui consiste en la suppression du watermark d'une image tatouée, et l'insertion de ce dernier dans une autre image. Pour cette raison l'insertion du watermark par des personnes non autorisées doit être difficile.

3.7 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 [42].

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 affectes par la manipulation, on a toutes les chances pour que le watermark soit dégrade 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.

3.7.1 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 réinsère dans l'image [43].

3.7.2 Collge attack

Dans le même esprit, l'attaque « Collage-Attack » [44], 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 a 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.

3.7.3 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 [43]. Un attaquant peut être intéresse par la suppression totale du watermark. Pour ce faire, un attaquant peut ajouter un bruit aléatoire a 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.

3.7.4 Brute Force Attack

Une autre attaque classique consiste à essayer de trouver la clé secrète utilisée pour générer le watermark. Ce type d'attaque, 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.

3.7.5 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).

3.8 Algorithmes de tatouage fragile

Le marquage fragile des images est utilisé pour l'authentification stricte des données de ces images. En d'autres mots, ce type de marquage vise à prouver l'intégrité des données de l'image. Les techniques de marquage fragile utilisent la cryptographie qui se résume dans les fonctions de hachage, la signature numérique, et les systèmes à clés privées/publiques. Ces techniques agissent soit sur l'image entière, ou bien sur des blocs, des lignes ou des colonnes.

3.8.1 Utilisation des bits de poids faible (LSB)

L'utilisation des LSB (Low State Binary ou bits de poids faible) [45] 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.

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

3.8.2 L'algorithme de Walton

1) Choix d'un nombre entier suffisamment grand *N*;

2) Diviser l'image en blocs de 8x8 pixels;

3) 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 la somme (*check-sum*) à l'aide de :

$$S = \sum^{64}_{=1}(aj \,.\, g(pj)) \bmod N.$$

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

5) 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, la *check-sum* calculée à partir de l'image testée avec la *check-sum* extraite 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 [46].

3.8.3 Algorithme de Fridrich et Goljan

Fridrich et Goljan [47] proposent 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 déceler d'éventuelles manipulations, mais surtout de permettre une reconstruction partielle des blocs altères.

Le principe de base consiste à découper l'image en blocs de taille 8×8 pixels, et on calcule les coefficients DCT en ne tenant compte que des MSB. Ces coefficients DCT sont ensuite quantifies 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 éloigne afin d'éviter qu'une modification locale de l'image n'altère à la fois l'image et les données de reconstruction.

3.8.4 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 [48].

3.9 Conclusion

Dans ce chapitre, nous avons présenté un panorama des méthodes de marquage fragile des images numériques, qui permettant d'assurer un service d'intégrité adapté aux images. Contrairement aux techniques classiquement employées en sécurité pour assurer cette fonction.

Chapitre 4

Algorithme de tatouage fragile pour l'authentification d'images

1. **Introduction**
2. **Utilisation des bits LSB**
3. **Algorithme proposé**
4. **Evaluation de l'algorithme proposé**
5. **Conclusion**

4.1 Introduction

Aujourd'hui, et avec la prolifération des documents numériques, le tatouage numérique fragile, se présente comme solution alternative ou complémentaire aux techniques précédentes pour résoudre les problèmes de sécurisation de ces documents.

La principale application du tatouage fragile est l'authentification des données. En effet, la perte ou l'altération du watermark sera prise comme une preuve que les données ont été falsifiées, alors que la récupération de l'information du watermark contenue dans les données est utilisée pour certifier l'intégrité du document.

Dans ce chapitre, nous présentons notre algorithme du tatouage fragile d'images numériques qui vise à insérer un watermark dans les bits LSB d'une image couleur RGB, pour assurer l'authenticité des images numériques. Ensuite, nous présentons une étude expérimentale visant à évaluer la performance de notre algorithme du tatouage fragile.

4.2 Utilisation des bits LSB

Le bit de poids faible (en anglais Least Significant Bit, ou LSB) est pour un nombre binaire le bit ayant dans une représentation donnée la moindre valeur (celui de droite dans la représentation positionnelle habituelle).La substitution est le processus consistant à ajuster les pixels les moins significatifs de bits de l'image porteuse. Elle représente une approche simple pour intégrer un message dans l'image. [49]

L'utilisation de bit LSB minimise la variation des couleurs que la substitution crée. Par exemple, l'intégration dans le bit le moins significatif modifie la valeur de la couleur par un.
L'incorporation dans le deuxième plan de bits peut changer la valeur de couleur par 2. [50]

L'insertion LSB varie en fonction du nombre de bits dans une image. Pour une image de 8 bits, le bit le moins significatif à savoir le 8^{e} bit de chaque octet de l'image est modifié au bit de message secret. Pour une image 24 bits, les couleurs de chaque composant comme RVB (rouge, vert et bleu) sont modifiés. [42]

L'objectif de l'utilisation de la méthode LSB dans le tatouage fragile :

Méthode basée sur le bit de poids faible en utilisant des ensembles d'entiers pour la sélection.

Simple à implémenter.

Ne modifie pas la taille de l'image.

Modifications invisible à l'œil nu.

Les bits de poids faibles sont sensibles à la moindre modification. Une petite modification peut changer toute l'image, quand le tatouage est fragile, on a choisi cette méthode.

4.3 Algorithme proposé

Notre algorithme de tatouage fragile d'images numériques est inspiré de [33], il repose sur l'utilisation de la méthode LSB. Cette méthode consiste à modifier les bits de poids faibles des pixels codant l'image, (une image numérique est une suite de pixels dont on code la couleur à l'aide de 3 octets).

L'idée est de remplacer les 2 bits LSB de chaque couleur par le résultat de l'opérateur XOR entre les 6 bits MSB des couleurs de pixel choisi. L'opérateur XOR représente une fonction du hachage qui permet de calculer une empreinte servant à identifier les données initiales.

Le résultat obtenu est une image très peu différente de l'image d'origine, l'œil humain ne pourra pas faire la différence entre l'image d'origine de départ et l'image finale contenant le message dissimulé.

L'algorithme d'insertion comprend en entrée un watermark W, une image hôte f. Cette phase d'insertion génère en sortie une image tatouée fw. L'image tatouée pourrait ensuite être copiée et attaquée. L'image reçue par la destination est f w.

4.3.1 Algorithme de génération du watermark

Cette phase génère un watermark de taille 6 bits qui dépend des 6 bits MSB de chaque couleur de pixel choisi (voir Figure 4.1). Le détail de cet algorithme est présenté ci-dessous.

Entrées :

– f : Image hôte (une image couleur RGB de taille n × m).

Sortie :

– W : matrice de taille n × m, ou chaque élément W(i, j) est une séquence binaire de taille 6bits {W1, …,W6}.

Etapes : – Pour chaque pixel R(i, j), G(i, j) et B(i, j) faire :

1. Prendre les 6 bits MSB à partir des trois couleurs R(i, j), G(i, j) et B(i, j) du pixel (i,j).
2. Le watermark obtenu W(i, j) est le résultat de l'opérateur XOR de 6 bits MSB de chaque couleur.

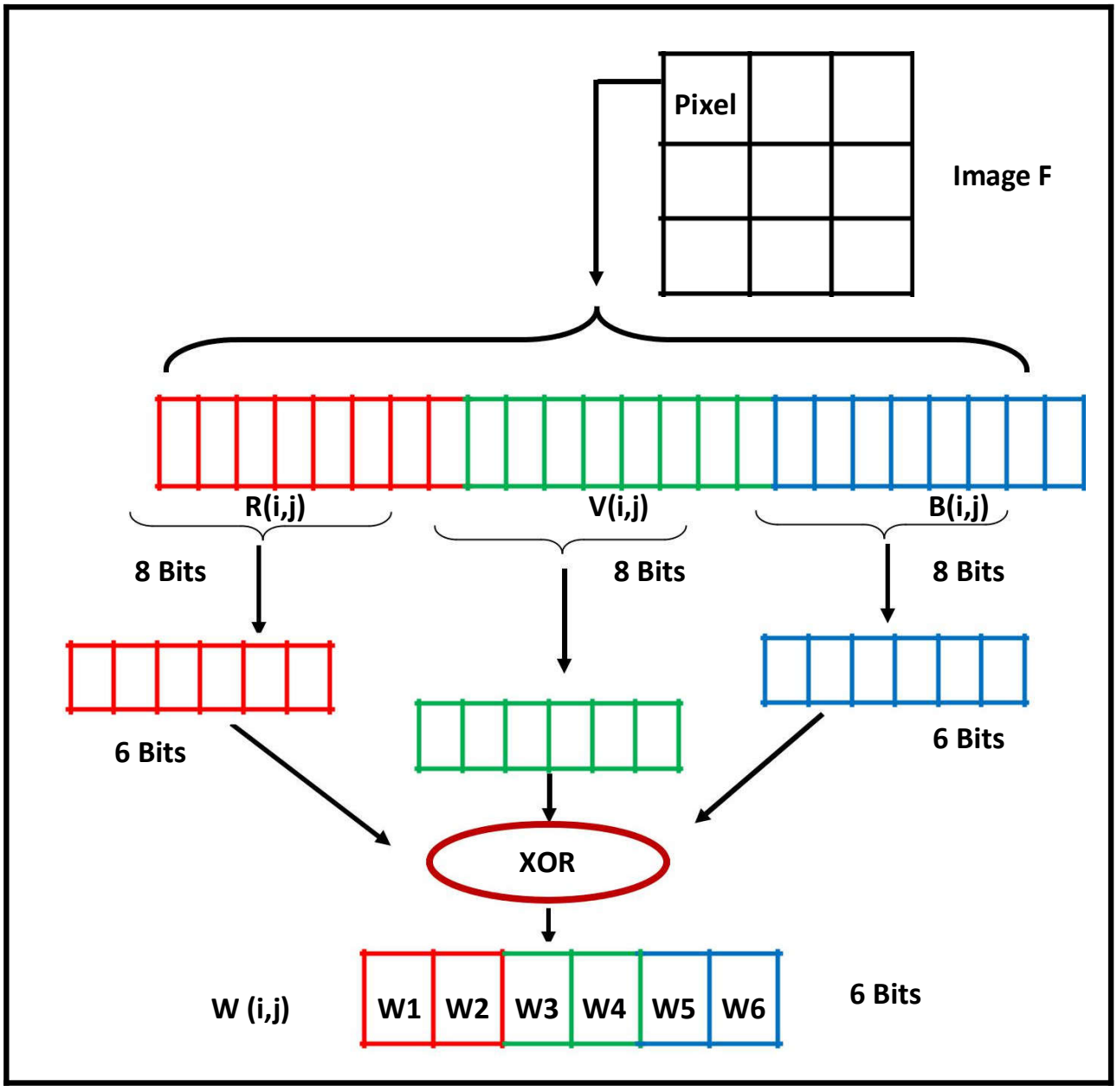


FIG. 4.1 – Algorithme de générations du watermark.

4.3.2 Algorithme d'insertion

Dans cet algorithme le watermark généré précédemment est inséré dans les deux bits LSB des trois couleurs R, G et B correspondants (voir Figure 4.2). Le principe de cet algorithme est présenté ci-dessous.

Entrées :

– f : Image hôte : image couleur RGB de taille n × m.

– W : watermark de taille n × m.

Sortie :

– fw: image tatouée de taille n × m.

Etapes :– Pour chaque pixel R(i, j), G(i, j) et B(i, j) faire :

1. Remplacer les deux bits LSB de R(i, j) par les deux premiers bits de W(i, j).
2. Remplacer les deux bits LSB de G(i, j) par le troisième et le quatrième bits de W(i, j).
3. Remplacer les deux bits LSB de B(i, j) par les cinquième et le sixième bits de W(i, j).

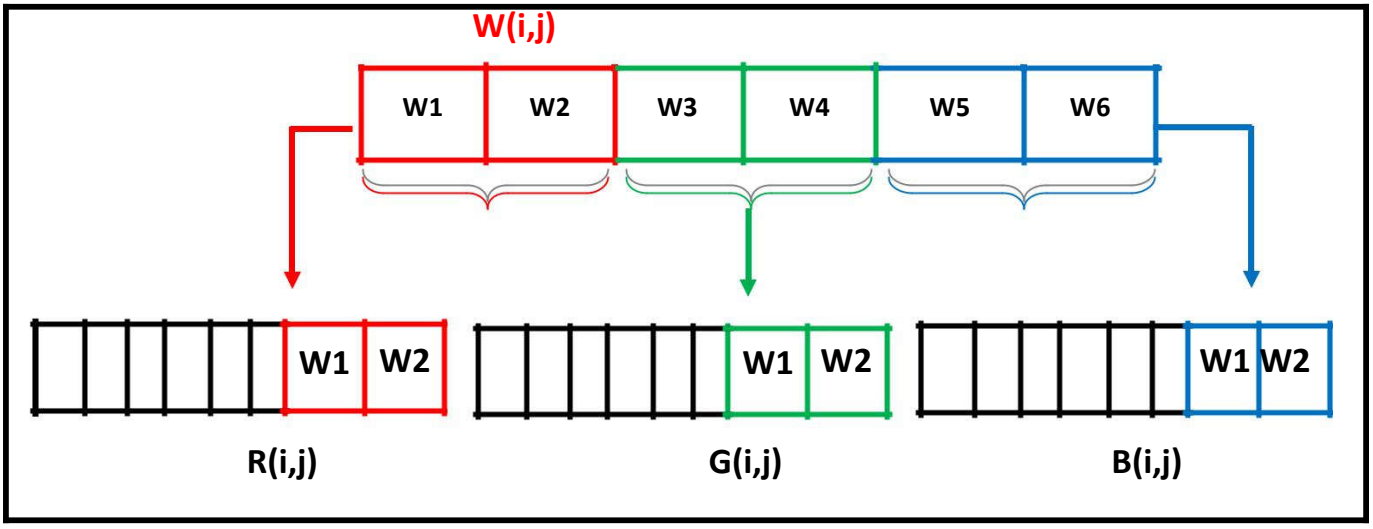


FIG. 4.2 – Algorithme d'insertion.

4.3.3 Algorithme de détection

Dans cet algorithme, le résultat de l'opérateur XOR de 6 bits MSB des trois couleurs R, G et B est comparé avec le watermark W contenu dans les 2 bits LSB. Si les deux valeurs sont identiques alors le pixel n'est pas attaqué, sinon il est attaqué (voir Figure 4.3). Le principe de cet algorithme est présenté ci-dessous.

Entrées :

– fw: Image tatouée (image couleur RGB de taille n × m).

Sortie :

S : image binaire (de taille n × m).

Etapes :– Pour chaque pixel R(i, j), G(i, j) et B(i, j) faire :

1. Calculer le résultat de l'opérateur XOR de 6 bits MSB des trois couleurs R, G et B de pixel (i,j).

2. Extraction du watermark W(i, j) : obtenu par la concaténation des 2 bits LSB des trois couleurs du pixel (i,j).

3. Comparaison entre le résultat de l'opérateur XOR et W(i, j)

   Si les deux valeurs sont identiques alors le pixel n'est pas attaqué : S(i,j) = 0

   Sinon il est attaqué : S(i,j) = 1

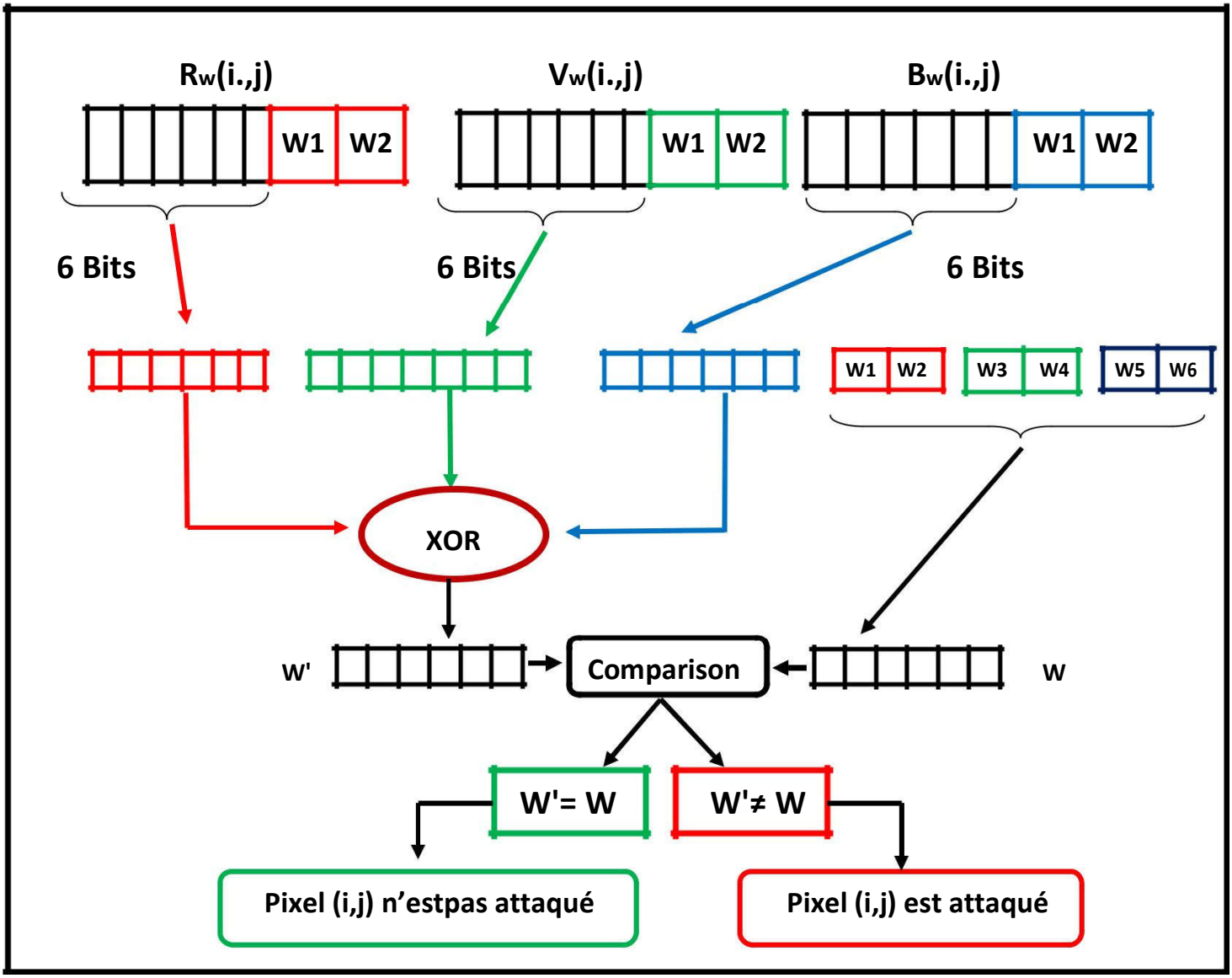


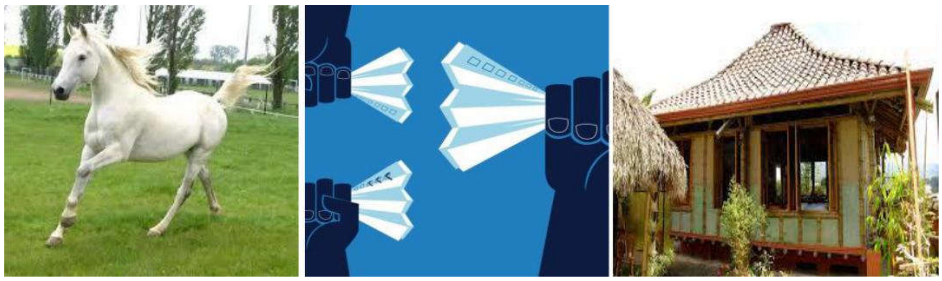
FIG. 4.3 – Algorithme de détection

4.4 Evaluation de l'algorithme proposé

Dans cette section, nous avons évalué l'efficacité de notre algorithme en terme de degré de dégradation de l'image tatouée, la sensibilité et l'aptitude de détecter toute transformation dans l'image. Pour ceci, nous avons séparé les tests en deux parties : la première est d'analyser la propriété d'imperceptibilité et la deuxième est l'évaluation de la propriété de fragilité par rapport aux attaques.

4.4.1. Propriété d'imperceptibilité

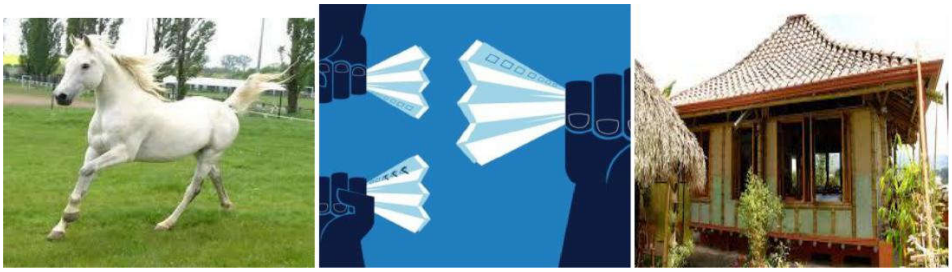
Nous avons appliqué notre méthode sur 6 images afin de s'assurer des résultats obtenus. Les images hôtes utilisées pour tester l'imperceptibilité de notre algorithme (FIG 4.4) et les images tatouées sont illustrées dans (FIG 4.5).



Cheval Peoplel Maison

Poivrons Papillon Taj Mahal

FIG 4.4 – Images hôtes.



Cheval Peoplel Maison

Taj Mahal Poivrons Papillon

FIG. 4.5 – Images tatouées.

PSNR : (sigle de Peak Signal to Noise Ratio) est une mesure de distorsion utilisée en image numérique, tout particulièrement en compression d'image. Il s'agit de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale. [32]

A partir de ces figures, on peut voir que la dégradation des images tatouées est imperceptible par l'observateur. Nous avons jugé utile de présenter aussi le PSNR des images tatouées afin de déterminer le degré de dégradation de l'image tatouée. Le tableau 1 présente les valeurs de PSNR. D'après le tableau 1, il est claire que les valeurs de PSNR sont très bonnes, ce qui signifie que notre méthode de tatouage maintien une haute qualité d'images tatouées.

Images hôtes	**PSNR**
Poivrons	44.4665
Cheval	44.3993
Papillon	44.0484
Maison	44.6087
Taj Mahal	44.0800
Peoplel	42.9658

Tableau 1 – Qualité des images tatouées.

4.4.2. Propriété de fragilité

La validité de toute technique de tatouage ne peut prendre de l'importance que si elle résiste à différents types d'attaques. Pour ceci, nous avons choisi de faire subir à chaque image tatouée un ensemble d'attaques et de vérifier la sensibilité de son tatouage et son aptitude de détecter toute transformation dans l'image. Si la matrice résultat est égale à 0 donc l'image n'est pas modifiée, sinon elle est modifiée.

Filtrage : Le principe du filtrage est de modifier la valeur des pixels d'une image, généralement dans le but d'améliorer son apparence. En pratique, il s'agit de créer une nouvelle image en se servant des valeurs des pixels de l'image d'origine. Nous présentons dans cette par divers types de filtres.

❖ **Attaque wiener**

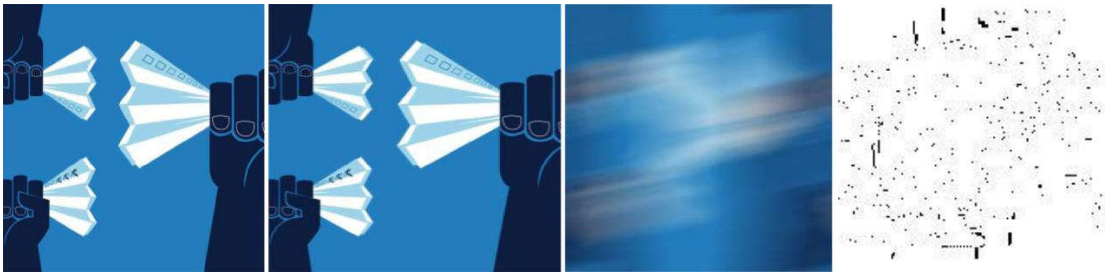


Image original Image tatouée Filtre Wiener Détection de modification (98.18 %)

FIG. 4.6 – Performances contre l'attaque wiener

❖ **Attaque laplacian**

Image original Image tatouée Filtre Laplacian Détection de modification (74.09 %)

FIG. 4.7 – Performances contre l'attaque laplacian

❖ **Attaque Sharpene**

Image originale Image tatouée Filtre Sharpen Détection de modification (98.41 %)

FIG. 4.8 – Performances contre l'attaque sharpene

❖ **Attaque Gaussain**

Image originale Image tatouée Filtre Gaussian Détection de modification (98.51 %)

FIG. 4.9 – Performances contre l'attaque Gaussain

❖ **Attaque average**

Image originale Image tatouée Filtre average Détection de modification (89.31 %)

FIG. 4.10 – Performances contre l'attaque average

Attaques géométriques :

❖ **Rotation**

Image originale Image tatoué rotation Détection de modification (0%)

FIG. 4.11 – Performances contre la rotation.

❖ **Zooming**

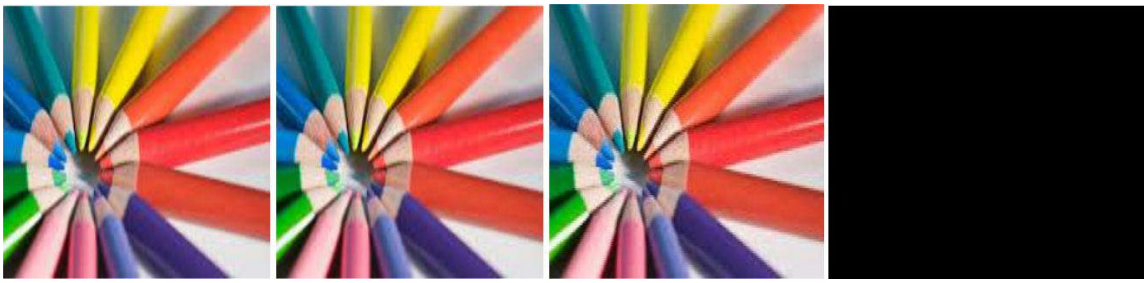


Image originale Image tatoué zooming Détection de modification (0%)

FIG. 4.12– Performances contre le zooming.

❖ **Compression JPEG:**

Image originale PNG Image tatouée Compression JPEG Détection de modification (47.21 %)

FIG. 4.13– Performances contre la compression JPE

Débruitage

❖ **Salt &pepper**

Image originale | Image tatoué | Salt &pepper | Détection de modification (96.98 %)

FIG. 4.14– Performances contre le Salt &pepper

Discussion : 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 d´détection des anomalies dans l'image tatouée. Le point faible de cette méthode est dans le cas où les pixels ne sont pas modifiés, mais la position des pixels est changée (rotation, zooming), dans ce cas notre algorithme est incapable de détecter la modification.

4.5 Conclusion

Dans ce chapitre, nous avons présenté notre algorithme de tatouage fragile d'images couleurs RGB, dans l'objectif est l'authentification d'images numériques. L'idée est de remplacer les bits LSB par le résultat de l'opérateur XOR des bits MSB, cet opérateur est utilisé comme une fonction du hachage pour identifier les données.

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 notre méthode, qui permet de maintenir une haute qualité d'images tatouées, et en même temps d'être très sensible contre plusieurs types d'attaques conventionne.

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 portant sur ce sujet. Ensuite, nous avons présenté le tatouage numérique et les différentes techniques et les méthodes existantes dans ce domaine. Nous avons aussi présenté le processus de son implantation et les différents algorithmes de marquage utilisés. On a 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 nouvelle méthode de tatouage fragile d'images numériques. Cette méthode est basée sur l'utilisation des bits LSB, elle consiste à remplacer les bits de poids faibles des pixels codant l'image par le résultat de l'opérateur XOR des bits MSB des trois couleurs de chaque pixel. L'opérateur XOR est utilisé comme une fonction de hachage qui permet d'identifier les données d'une manière unique.

Les résultats expérimentaux montrent la faisabilité de notre algorithme proposé, et que notre approche permet d'obtenir une haute qualité d'images tatouées et en même temps, elle est très sensible contre plusieurs types d'attaques conventionnelles.

A partir du travail réalisé dans le cadre de ce mémoire, quelques perspectives peuvent être dégagées :

- Notre contribution se place dans le cadre de proposer des nouveaux schémas de tatouage d'images couleurs RGB. Nous avons voulu améliorer notre travailler sur différents critères : robuste/fragile, domaine spatial/domaine transforme.

- Etendre notre algorithme de tatouage d'images proposé pour l'utilisation à la vidéo.

- S'orienter vers d'autres applications, en dehors du contexte sécuritaire du watermarking, telles que l'augmentation ou l'enrichissement des contenus (indexation multimédia, canal caché), la création de méta-documents,….etc.

- Nous pouvons envisager à la correction des erreurs en utilisant des codes correcteurs d'erreurs tels que les turbo-codes.

- Nous nous sommes bases dans l'étude expérimentale sur l'utilisation des métriques baséespixels. Dans le future, nous essayerons d'utiliser des métriques psycho-visuelles telles que JNCD Nous essayerons aussi d´élaborer un mécanisme pour assurer la contrainte de sécurité.

Bibliographie:

[1] M . Nixon and A. Aguado. *Feature Extraction and Image Processing*. British Library Cataloguing in Publication Data, 2002.

[2] M. Bergounioux. Quelques méthodes mathématiques pour le traitement d'image. In *Cours MASTER, chapter 1*, 2009.

[3] Y. Hu, J. Huang, S. Kwong, and Y. Chan. Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform. In IWDW'2003, pages 86–100, 2003.

[4] S. Perreira, J. J. K. O Ruanaidh, F. Deguillaume, G. Csurka, T. Pun:

Template Based Recovery of Fourier-Based Watermarks Using Log-polar

[5] C. Lou, J. Liu, and T. Li. Digital Signature-based Image Authentication. Idea Group Publishing, 2004. [66] Chun-Shien Land Log-log Maps, *IEEE int. Conf on Multimedia Computing and Systems (ICSMS'99)*, Florence, Italy, June 1999.

[6] C. Rey, J.-L. Dugelay: Blind Detection of Malicious Alterations On Still

Images Using Robust Watermarks, *IEEE Secure Images and Image Authentication colloquium*, London, UK, 2000.

[7] K. Maeno, Q. Sun, S. Chang, and M. Suto. New Semi-fragile Image Authentication Watermarking Techniques Using Random Bias ND Non Uniform Quantization. IEEE Transactions on Multimedia, 8(1) :32–45, 2006

[8] F. Autrusseau, A. Saadane, and D. Barba. Psychovisual approach for watermarking. SPIE Electronic Imaging, January 2001.

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

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

[11] G. Coatrieux, B. Sankur, and H. Maıtre. Strict Integrity Control of Biomedical Images. In *Security and Watermarking of Multimedia Contents III*, volume 4314, 2001.

[12] C. L. Tan and B. Yuan. Document text segmentation using multi-band disc model. Document Recognition and Retrieval VIII, 4307 :212–222, 2000. (Cité page 39.)

[13] D. Lingrand. *Introduction aux traitement d'images*. Vuibert, 2008.

[14] S. Bhattacharjee and Kutter. M. Compression Tolerant Image Authentication. In *IEEEInternational Conference on Image Processing (ICIP98), Chicago, USA*, 1998.

[15] La Propriété Intellectuelle Guide De Association Canadienne Pour Les Études Supérieures.

[16] Techniques And Applications Of Digital Watermarking And Content Protection ,Michael Arnold ,Martin Schmucker , Stephen D. Wolthusen , 2003 .

[17] Contribution Des Filtres Lptv Et Des Techniques D'interpolation Au Tatouage Numérique , Vincent Martin , 2006 .

[18] Lee S.,Yoo C.D. and Kalker T., "Reversible Image Watermarking Based on Integer-to Integer Wavelet Transform", *IEEE transaction on Information Forensics and Security*, Vol.2, No.3.pp.321-330, September 2007**.**

[19] F.A.P. Petitcolas, R.J. Anderson, *Evaluation of copyright marking systems*, IEEE Multimedia Systems (ICMCS'99), 1999, p. 574-579

[20] Le Marquage Et La ProprieteIntellectuelle , Michel Blanchard, 2003.

[21] Développement De Techniques De Marquage D'authentification Pour La Protection De Données Multimédias , Ali JabeurBouzidi , 2009.

[22] Bartolini F., Barni M., Tefas A. and Pitas I., "Image authentication techniques for surveillance applications", *Proceedings of the IEEE*, vol. 89, no. 10, pp. 1403–1418, October, 2001.

[23] Deguillaume F., Voloshynovskiy S. and Pun T., "Hybrid robust watermarking resistant against copy attack", *In Proceedings of the European Signal Processing Conference (EUSIPCO2002),* Toulouse, France, September, 2002

[24] Dugelay, J.-L., Rey C., "A Survey Of Watermarking Algorithms For Image Authentication", Eurasip Journal On Applied Signal Processing, 2002.

[25] Petitcolas, F.A., Anderson R. J., and Kuhn M. G., "Attacks on copyright marking systems". *In Proceedings of the second workshop on information hiding,* vol.1525, pp. 218-238, 1998.

[26] Sun Q.-B., Chang S.-F., Kurato M. and Suto M., "A new semi-fragile image authentication framework combining ECC and PKI infrastructure", *ISCAS02*, Phoenix, USA, May, 2002.

[27] F.A.P. Petitcolas, R.J. Anderson, *Evaluation of copyright marking systems*, IEEE Multimedia Systems (ICMCS'99), 1999, p. 574-579

[28] G. Coatrieux, B. Sankur, and H. Maıtre. Strict Integrity Control of Biomedical Images. In *Security and Watermarking of Multimedia Contents III*, volume 4314, 2001.

[29] M.M. Yeung and F. Mintzer. An Invisible Watermarking Technique for Image Verification. *IEEE International Conf. on Image Processing*, Santa Barbara, USA, Oct. 1997.

[30] D. Caragata, A. L. Radu, S. El Assad: Fragile Watermarking using Chaotic

Sequences, *International Journal for Information Security Research (IJISR)*, Vol. 1(1), March 2011

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

[32] M.M.Yeung, F.Mintzer. An Invisible Watermarking Technique for Image Verification. In Proceedings of IEEE International Conference on Image Processing, Santa Barbara, USA, Vol 2, No 26–29, pages 680 – 683, Oct. 1997.

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

[34] Dugelay, J.-L., Rey C., "A Survey of Watermarking Algorithms for Image Authentication", *EURASIP Journal on Applied Signal Processing,* pp. 613-621, March, 2002

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

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

[37] A.Watson. DCT QuantizationMatrices Visually Optimized for Individual Images. In *SPIE*,volume 1913, pages 202–216, 1993

[38] 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.

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

[40] Lee S.,Yoo C.D. and Kalker T., "Reversible Image Watermarking Based on Integer-to Integer Wavelet Transform", *IEEE transaction on Information Forensics and Security*, Vol.2, No.3.pp.321-330, September 2007.

[41] J.-L. Dugelay& S. Roche. Process for marking a multimedia document, such an image, by generating a mark. *Pending patent EP 99480075.3 (EURECOM 11/12 EP)*, July 1999.

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

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

[44] J.-L. Dugelay. Procédé de dissimulation d'informations dans une image numérique.*Brevet INPI FR 98-04083 (EURECOM 09-FR)*, March 1998.

[45] Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the DiscreteWavelets Transform and Singular Value Decomposition,European Journal Of Scientific Research

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

Proceeding of the IEEE International Conference on Multimedia and Expo,

[47] Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color 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.

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

[49] NourEl-Houda GOLEA, Tatouage numérique des images couleurs RGB, Mémoire de Magister.

[50] Shree K Nayar, Sammeer A Nene, and Hiroshi Murase. Columbia object image library (coil 100). Department of Comp. Science, Columbia University, Tech.Rep. CUCS-00696,1996