UNIVERSITE KASDI MARBAH OUARGLA

Faculté des Nouvelles Technologies de l'Information et la Communication

Département de l'informatique et Technologies de l'information

Spécialité : Administrations et sécurité des réseaux

MEMOIRE DE FIN D'ETUDES

Présenté par : BASSIMANE Rihab et HAFOUDA Amira

Thème :

Tatouage numérique aveugle par LSB replacement

Encadré par : KHALDI Amine.

ANNEE UNIVERSITAIRE : 2018/2019

Remercîment

Tout d'abord, nous tenons à remercier "Dieu" le tout puissant, qui nous a donné la force, la patience et la volonté d'accomplir ce modeste travail.

Sans oublie nos parents et nos familles pour leur contribution, leur soutien, leur patience et leurs encouragements,

Nous tenons à remercier ***Mr. KHALDI Amine****, notre encadreur et enseignent au département d'informatique et technologie d'information pour son encadrement, son suivi, sa disponibilité, ses conseils précieux et son encouragement.*

Nos remerciements vont aussi Aux membres de jury d'avoir accepté de juger et d'évaluer ce travail.

Nous tenons à remercier en cette occasion tout le corps professoral et administratif de département d'informatique de l'université Kasdi Merbah de Ouargla pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.

Nous adressons nos plus sincères remerciements à tous nos proches amis, qui nous ont toujours encouragée au cours de la réalisation de ce mémoire.

Enfin, nous tenons également à remercier toute personne qui ont participé de près ou de loin à la réalisation de ce travail.

Résumer

Le tatouage numérique ou « watermarking » a connu, ces dernières années, un essor spectaculaire. Initialement développé pour renforcer la protection des droits d'auteur des documents multimédia (images, son, vidéo). L'utilisation accrue des applications multimédia pose des problèmes concernant la préservation de l'intégrité 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.

L'objectif de notre travail est de réaliser une application du tatouage fragile des images couleurs RGB codée en 24 bits qui vise à insérer et extraire un watermark crypté avec une clé secrète, cette méthode est basée sur l'utilisation de l'algorithme LSB.

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

Abstract:

The digital tattoo or "watermarking" has in recent years a spectacular development.

Initially developed the copyright protection of multimedia documents (images, sounds, videos). The increased use of multimedia applications poses problems in preserving the integrity and authenticity of digital data transmission. In particular the images, must be protected from falsification. The appropriate solution is the use of the fragile tattoo.

The goal of our work is to realize a fragile tattoo application of 24-bit RGB color images that aims to insert and extract an encrypted watermark with a secret key, this method is based of the algorithm LSB. The experimental results provide a good imperceptibility and sensitivity of attacks.

Keywords: fragile tattoo, watermarking, integrity, authentication, LSB.

ملخص

يمكننا أن نلخص محتوى هذا المشروع بأنه يعالج مشكلة يتعرض لها الكثير في ظل تطور التكنولوجيا (الانترنيت) ألا وهي مشكلة حماية الصور الرقمية من التزوير والسرقة.

(إضافة لذا نقترح تطبيق الوشم الرقمي على الصور الرقمية بإضافة علامة معينة للصور المراد حمايتها،وذلك باستعمال طريقة LSBالعلامة في البيتات اقل أهمية في الصورة).وتعد هذه الاخيرة من اهم الطرق لحماية حقوق الملكية للصورة الرقمية.

الكلمات المفتاحية : الوشم الرقمي,LSB , الصور الرقمية

Sommaire

Sommaire

Chapitre II : Tatouage numérique

Sommaire

Sommaire

Liste des figures

Liste des figures

Liste des Tableaux

Liste des Abréviations

Abréviations	Designations
2D	Bidimensionnel
3D	Tridimensionnel
RGB (RVB)	Red- Green- Bleu (Rouge, Vert, Bleu)
CMJN (CMYB)	Cyan Magenta Jaune Noir (Cyan-Magenta-Yellow-Black)
TSL (HSL)	Teinte-Saturation-Luminance (Hue- Luminance-Saturation)
JPEG	Joint Photographic Expert Group
GIF	Graphic Information Format
PNG	Portable Network Graphics
MNG	Multiple-Image Network Graphics
BMP	BitMap
TIFF	Tagged Image Format
PSD	Photoshop Document
PS	PostScript
DXF	Drawing Xchange Format
LZW	Lempel-Ziv-Welch
SVH	Système Visuel Humain
LSB	Least Significant Bits (Bits les moins significatifs)
DFT	Discrete Fourier Transform (Transformée de Fourier discrète)
DCT	Discrete Cosine Transform (Transformée en cosinus discrète)
LL	Low-Low (Basse-Basse)
HL	High-Low (Haute-Basse)
LH	Low-High (Basse-Haute
HH	High-High (Haute-Haute)
PPI (PPP)	Pixels Per Inch (Pixels Par Pouce)
DPI	Dots Per Inch
PSNR	Peak Signal to Noise Ratio (Rapport signal sur bruit de crête)
MSE	Mean Squared Error

INTRODUCTION
GENERALE

Introduction générale

Introduction générale

Le développement des réseaux numériques et l'évolution rapide de la technologie informatique. Qu'il permet de transmettre toute sorte d'information textuelle, sonore 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.

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

En générale, l'authentification d'une image numérique est réalisée en utilisent un tatouage fragile, Avec cette technique, l'information cachée est perdue ou modifiée veut dire 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.

L'objectif de ce mémoire est la réalisation d'une application de tatouage numérique fragile pour les images BMP et PNG basé sur la méthode du dernier bit signification (LSB) pour assurer l'authentification et l'intégrité.

Le premier chapitre présent les concepts de base sur les images numériques ainsi que ses caractéristiques, ses types et ses formats. Nous présentons aussi quelques notions importantes dans le domaine de traitement d'images numériques telles que la numérisation, le codage et le stockage.

Le deuxième chapitre concerne le tatouage numérique, qui contient le principe général de tatouage ainsi que ses contraintes, ses techniques et les attaques existantes, ainsi que les différents domaines d'application ensuite on termine le chapitre par les mesures d'évaluation de qualité des images numériques.

Dans le dernier chapitre nous utilisons l'algorithme LSB pour appliquer le tatouage fragile sur les images codées en 24 bits et nous présentons les résultats expérimentaux obtenus de cette application.

En effet, ces images ont la facilité d'accessibilité pour la falsification et la manipulation malveillante. Pour cette raison il est devenu nécessaire de développer des mécanismes pour assurer l'authentification et vérifié l'intégrité des images numériques.

Chapitre I :
L'image numérique

Chapitre I- L’image numérique

I.1. Introduction :

L'image constitue l'un des moyens les plus intéressants pour communiquer, chacun peut analyser l’image à sa manière, pour en dégager une impression et d’en extraire des informations précises. C'est aussi l'un de moyen le plus utilisé dans tous les domaines, en particulier les domaines scientifiques comme la médecine, l’astronomie, la géologie, la pharmacologie...etc.

De ce fait, le traitement d’images est l’ensemble des méthodes et techniques opérant sur celles-ci, dans le but de rendre cette opération possible, plus simple, plus efficace, d’améliorer l’aspect visuel de l’image et d’en extraire des informations jugées pertinentes.

Dans ce chapitre, nous devons définir et expliquer quelques termes et concepts fondamentaux liés aux images numériques. Nous devons aussi avoir une connaissance approfondie, concernant la représentation des images sur les ordinateurs, et les différentes caractéristiques qui différencient les images les unes des autres ainsi que les différentes manipulations ou traitements possibles qu’on peut exercer sur ces images.

I.2 Définition de L’image :

La définition du terme « image » est : « *Une image est une représentation visuelle, voire mentale, de quelque chose (objet, être vivant et/ou concept). Elle peut être naturelle (ombre, reflet) ou artificielle (peinture, photographie), visuelle ou non, tangible ou conceptuelle (métaphore), elle peut entretenir un rapport de ressemblance directe avec son modèle ou au contraire y être liée par un rapport plus symbolique* ».

Les images analogiques ne peuvent être représentées sur les ordinateurs, que si, est seulement si cette image est numérisée par le processus de discrétisation appelée aussi numérisation. Cette opération consiste à quantifier et échantillonner l’image analogique pour la transformer en image numérique.

Mathématiquement une image est un signal continue 2D (bidimensionnel) ou 3D (tridimensionnel), associée à une fonction continue à 2 variables f (x, y). [1]

I.3 Définition de L’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). Aussi l'image numérique est une matrice à deux dimensions de M x N éléments ou à trois dimensions M x N x L. Chaque cellule de cette matrice correspondante à un pixel de cette image. Le pixel est le plus petit élément constitutif de l’image.

Chaque cellule stocke une valeur numérique codée en binaire. Cette valeur représente la valeur chromatique de ce pixel (noir, blanc, niveau de gris ou couleur). Les valeurs numériques sont souvent réduites à une représentation mathématique compressée. Les bits sont réinterprétés et lus par l'ordinateur afin de délivrer une version analogique de l’image en vue d'être affichée ou imprimée. [2]

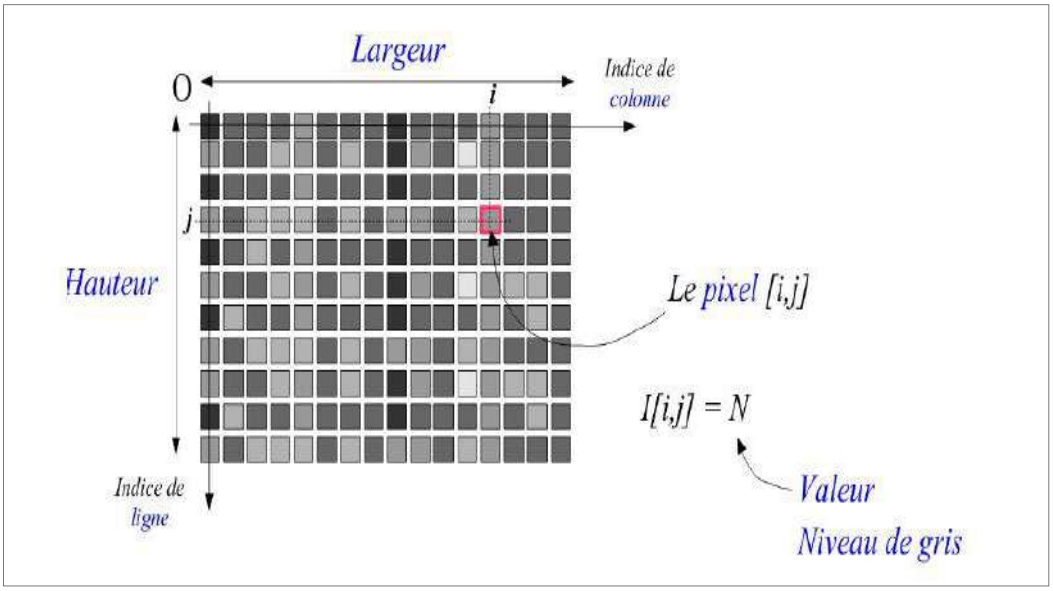


Figure I.1: Représentation d’une image numérique

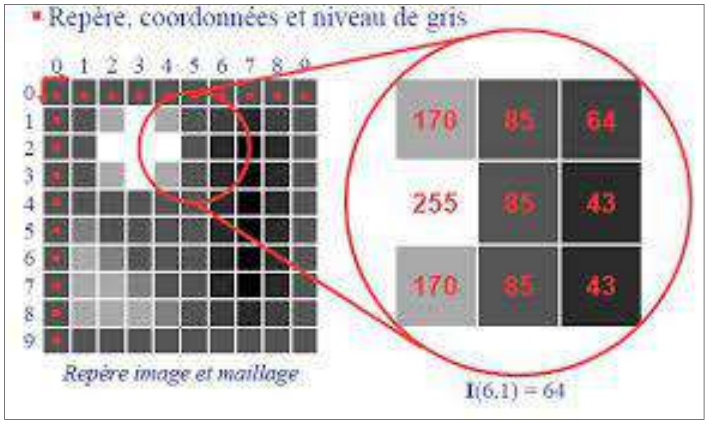


Figure I.2: Valeur d'un pixel

I.3.1 Processus de numérisation :

La représentation informatique d'une image est nécessairement discrète, alors que l'image est de nature continue : le monde est continu, la transformation d'un signal analogique 2D nécessite à la fois une discrétisation de l'espace : c'est l'échantillonnage, et une discrétisation des couleurs : c'est la quantification. [3]

Le processus de numérisation est représenté dans la figure suivante :

Figure I.3:Processus de numérisation d'une image.

Echantillonnage : l'échantillonnage est le procédé de discrétisation spatiale d'une image consistant à associer à chaque pixel R (x, y) une valeur unique I (x, y), (Figure I.4). On parle de sous échantillonnage lorsque l'image est déjà discrétisée et qu'on diminue le nombre de pixels [4].

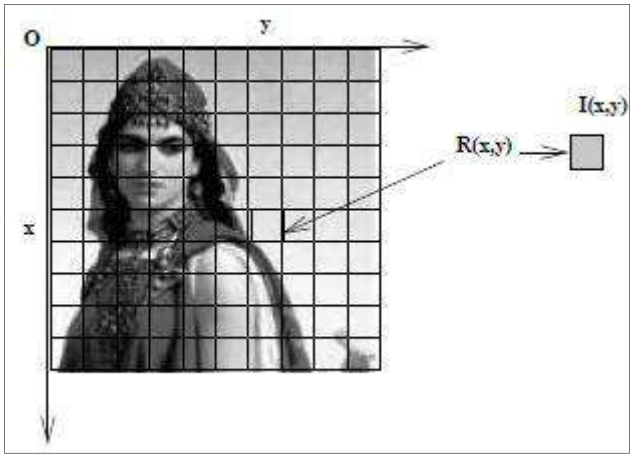


Figure I.4: Echantillonnage, discrétisation spatiale.

- **Quantification :** La quantification consiste à remplacer un nombre infini de valeurs que le I (x, y) peut prendre par un nombre fini (niveau de Quantification) ; elle remplace la valeur exacte de l'image par une valeur approchée. Elle peut également faire apparaitre des distorsions dans les images.

- **Codage des images numériques :**

  - **Codage en noir et blanc :** Pour ce type de codage, chaque pixel est soit noir, soit blanc. Il faut un bit pour coder un pixel (0 pour noir, 1 pour blanc). Ce type de codage peut convenir pour un plan ou un texte mais on voit ses limites lorsqu'il s'agit d'une photographie. (Figure I.5)

Figure I.5: Image codée en noir et blanc.

- **Codage en niveaux de gris :** Chaque pixel codée sur 2 bits donc on aura 4 possibilités (noir, gris foncé, gris clair, blanc). L'image codée sera très peu nuancée. En général, les images en niveaux de gris renferment 256 teintes de gris. Par convention la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur 255 le blanc (intensité lumineuse maximale). Le nombre 256 est lié à la quantification de l'image. En effet chaque entier représentant un niveau de gris est codé sur 8 bits. Il est donc compris entre 0 et $2^8 - 1$ .C'est la quantification la plus courante. On peut coder une image en niveaux de gris sur 16bits ou sur 1 bit : dans ce dernier cas le « niveau de gris » vaut 0 ou 1 : alors il s'agit d'une image binaire (Noir et Blanc) [5].

Figure I.6: Image codée en niveaux de gris.

- **Codage d'une image couleur** : On peut attribuer 3 valeurs à chaque pixel : Rouge (de 0 à 255), Vert (de 0 à 255) et Bleu (de0 à 255). Chaque couleur est codée sur 1 octet = 8 bits. Chaque pixel sur 3 octets c'est à dire 24 bits. On peut obtenir une couleur quelconque par addition de ces trois couleurs primaires en proportions convenables. On obtient ainsi 256 x 256 x 256 = 16777216 (plus de 16 millions de couleurs différentes). (Figure I.7) [6]

Figure I.7 : Image codée en couleurs 24 bits.

I.4 Les caractéristiques d’une image numérique :

L’image est un ensemble structuré d’informations caractérisé par les paramètres suivants :

I.4.1 Pixel :

Le pixel (Picture Element) est le plus petit élément que contient une image. Il possède une valeur qui représenter un niveau de gris ou un vecteur représentant une couleur, ou toute autre chose. C'est aussi l'unité utilisée pour spécifier les définitions d'affichage (largeur × hauteur) [1].

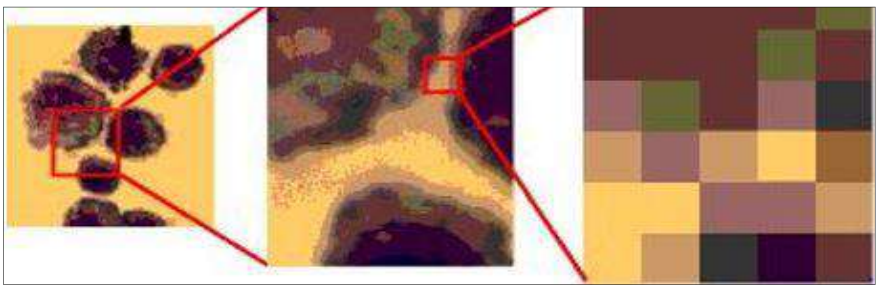


Figure I.8: Représentation d’un pixel.

I.4.2 Dimension :

C’est la taille de l'image, se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multipliée par le nombre de colonnes nous donne le nombre total de pixels dans une image. Une image possédant 640 pixels en largeur et 480 en hauteur aura une dimension de 640 par 480 pixels, notée 640x480. [7]

I.4.3 Résolution :

La résolution d'une image composée de points 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). 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]

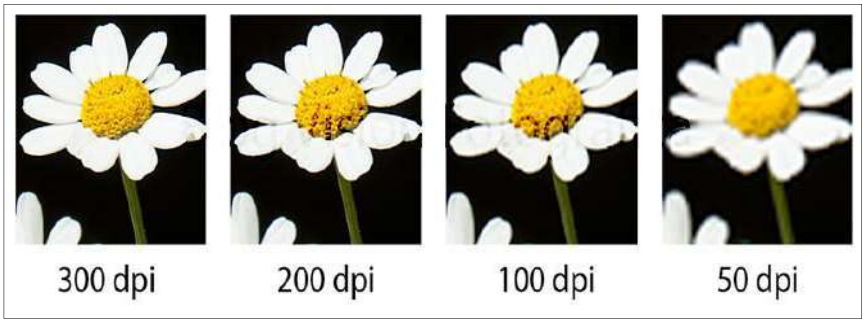


Figure I.9: Résolution d’une image

I.4.4 Taille de stockage :

La taille d’une image change selon le nombre d’octets utilisé dans le codage des couleurs, le format de l’image, ainsi que la résolution de l’image. Plus la résolution est grande plus l’espace de stockage est grand. [1]

I.4.5 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 ou (couleur) dans l'image. Il permet de donner un grand nombre d'informations sur la distribution des niveaux de gris ou (couleur). [1]

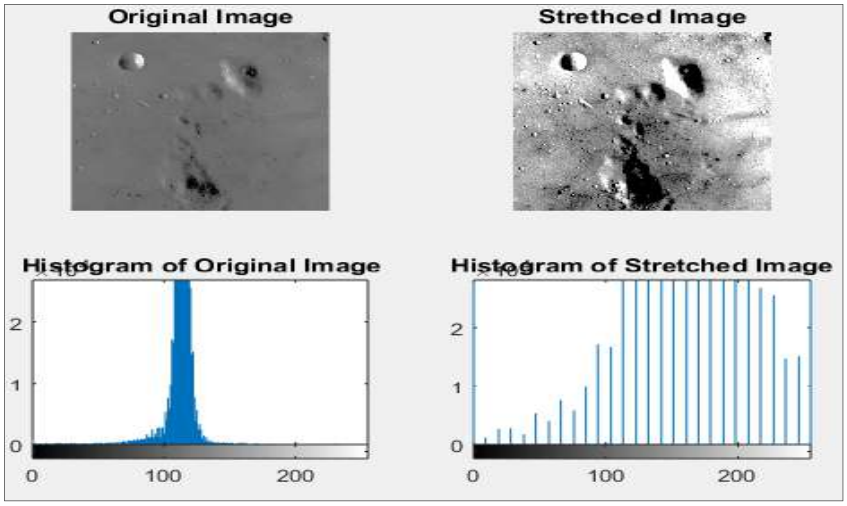


Figure I.10 : Exemple d'histogramme d'une Image

I.4.6 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.[8]

Figure I.11 : Exemple de luminance

I.5 Représentation des couleurs :

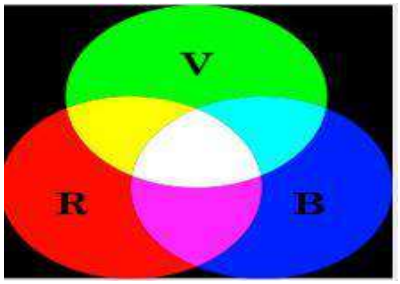
La couleur est une donnée intéressante pour une image. Elle modifie la perception que l'on a de l'image, Il existe plusieurs modes pour représenter les couleurs, le plus utilisé est l'espace colorimétrique rouge, vert et bleu RGB (RVB). Dans ce mode, les différentes couleurs sont obtenues par le mélange des trois couleurs primaires. Ce procédé s'appelle la synthèse additive. Cependant, on trouve aussi d'autres modes de représentation, comme le mode CMJN(CMYB) qui utilise la synthèse soustractive. Les couleurs sont obtenues par mélange des trois couleurs "primaires" : Cyan (C), Magenta (M) et Jaune (J), mais cette fois-ci avec

soustraction des couleurs primaires pour avoir les autres couleurs. La soustraction de toutes les couleurs primaires ensemble donne la couleur noire. [2]

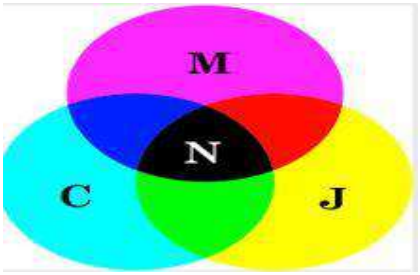
Il existe éventuellement d'autres modes de représentation des couleurs :

- Teinte, saturation, luminance (TSL ou HSL), où la couleur est codée suivant le cercle des couleurs ;
- Base de couleur optimale YUV, Y représentant la luminance, U et V deux chrominances orthogonales.

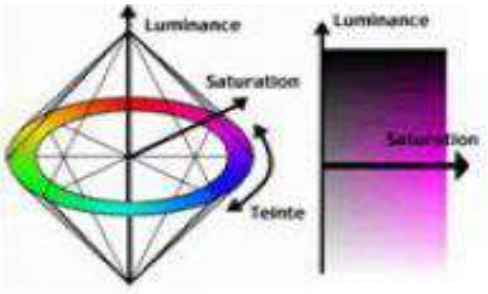
Il faut préciser que ces différents modes de représentation des couleurs sont créés par nécessité de reproduire les couleurs sur différents supports, tels que les écrans, papier...etc. avec une efficacité et une fidélité à l'image originale ou réelle. Par Exemple, le mode RGB est utilisé uniquement dans les écrans PC afin d'afficher les images. Il n'est pas du tout adapté à l'impression offset ou numérique. [2]



Codage RGB
(Rouge-Green-Bleu).



Codage CMYB
(Cyan-Magenta-Yellow-Black)



Codage HLS
(Hue, Luminance, Saturation)

Figure I.12: Composants des modèles de couleur RGB et CMYB et HLS.

I.6 Types d’image numérique :

On distingue deux types d’images à la composition et au comportement différent : les images matricielles et les images vectorielles.

I.6.1 Les Images matricielles (ou images bitmap) :

Elle est composée d’une matrice (tableau) de points à plusieurs dimensions, chaque dimension représentant une (hauteur, largeur), ou autre (niveau de résolution). Dans le cas des images à deux dimensions, les points sont appelés pixels.[9]

Les images matricielles présentent les avantages suivants :

- Le mode de codage des images bitmap (24 bits, codage RGB) les rend adaptées au fonctionnement des principaux périphériques, notamment les contrôleurs d'écran "True Colors" (point allumé ou non, codé sur x bits).
- Elles conviennent fort bien aux images complexes, principalement d'origine analogique, qui ne peuvent être codées qu'en mode point.
- Elles se laissent manipuler et traiter par des opérations techniques "naturelles «pour un graphiste qui retrouve des outils et les manipulations très proches de ceux qui caractérisent son métier et sa pratique professionnelle de type analogique.

Les images matricielles présentent les inconvenants suivants :

- Les images bitmap ont une résolution fixe : aussi la qualité maximale sur un périphérique d'affichage ou d'impression donné rend-elle nécessaire de travailler, dans la majorité des cas, dans la résolution native de ce périphérique. Concrètement cela veut dire qu'une résolution de type écran donnera d'assez mauvais résultats sur un imageur photographique. Les images bitmap sont donc dépendantes du périphérique.
- Elles supportent mal les opérations de redimensionnement, réduction ou agrandissement. Les deux opérations se traduisent par une perte d'information.
  Après une réduction de taille, l'image réduite présentera souvent des effets d’escaliers plus marqués que ceux de l'image source. Un agrandissement se traduira par la multiplication à la taille voulue de chacun des pixels pris séparément : chaque point se voit grossi, mais la résolution demeurante identique, la définition de l'image sera de qualité inférieure.

- Les images bitmap sont "Lourdes » : les fichiers, lorsque l'on traite des images en haute définition, ont des tailles qui varient entre 10 et 30 Mo par image. Elles sont donc encombrantes, difficiles à faire passer sur le réseau, etc.

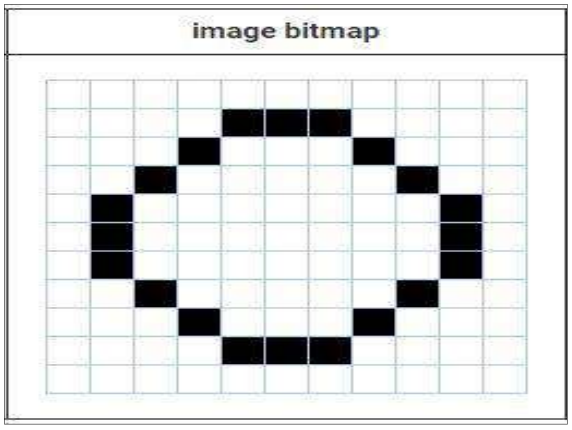


Figure I.13: Cercle créé par la méthode matricielle

I.6.2. Images vectorielles :

Elle est composée de différents objets repérés par leurs coordonnées et comportant différentes attributs (bordure, fond, forme, coordonnées). Leur avantage c’est qu’elles peuvent être facilement redimensionnées. Leur codage dépend directement du logiciel qui a permis de les créer. Elles ne nous concernent pas ce jour consacrer aux traitements d’image bitmap.[10]

Les images vectorielles présentent les avantages suivants :

- L'image numérique doit être calculée avant de pouvoir être affichée par le périphérique (opération qui porte le nom de *rastérisation*). Cette opération peut être faite pour n'importe quelle résolution du périphérique : l'image vectorielle est réellement indépendante du périphérique.
- Toutes les modifications spatiales de l'image (réduction, agrandissement, translation, rotation, etc.) sont aisées et n'occasionnent aucune perte d’information. Il suffit en effet de modifier les coordonnées des points de contrôle qui définissent l'objet. On voit sur l'image ci-contre les points de contrôle de la courbe et, en traits pointillés.

- L’image vectorielle est particulièrement adaptée aux représentations schématiques et stylisés constituées de formes géométriques, uniformément remplies par des à-plats de couleur ou des motifs. [10]

Les images vectorielles présentent les inconvénients suivants :

- Une image vectorielle ne peut coder une image analogique telle qu'une image photographique.
- Le travail sur des objets graphiques isolés qu'il faut ensuite associer ou grouper est peu familier au graphiste ou à l'illustrateur. Il faut donc une certaine habitude et un apprentissage de nouvelles procédures de création.
- Certaines manipulations telles que les modifications de couleurs sont difficiles sur une zone d'un objet, sur un objet simple ou sur un groupe d'objets.

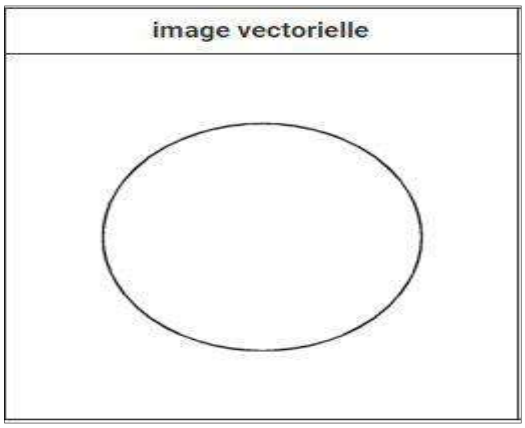


Figure I.14 : Cercle créé par la méthode vectorielle

I.7 Les formats des images numériques :

Les fichiers numériques images se reconnaissent par leur format que l'on identifie grâce à l'extension (en trois caractères) du nom du fichier. Il existe environ 70 formats de fichiers pour les images en mode pixels. Nous citons les plus utilisés.

I.7.1 Formats d'image matricielle :

I.7.1.1 JPEG (Joint Photographic Expert Group) :

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 comité 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'oeil humain. Le JPEG2000 est la norme internationale (ISO 15444-1). Elle apporte quelques améliorations au JPEG classique et notamment permet un réglage autorisant une compression sans perte ou encore la résistance aux erreurs de transmission. JPEG 2000 est relative à la compression d'images qui s'appuie sur un mécanisme de compression par ondelettes. [11]

I.7.1.2 GIF (Graphics Interchange Format) :

Le format GIF pour *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 a permis une compression sans perte (algorithme LZW). Quelques problèmes juridiques avec la société Unisys détenant un brevet sur le LZW et donc revendiquant des royalties sur le GIF ont favorises le développement de nouveau format a l'instar du PNG. Ces brevets ont aujourd'hui expiré faisant tomber le GIF dans le domaine public. Ce format fonctionne sur la base d'une palette de 256 couleurs indexées (8 bits), le GIF est de fait limité à seulement 256 couleurs. 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 [12, 11].

I.7.1.3 PNG (Portable Network Graphic):

Le PNG pour Portable Network Graphic (ISO 15948) a été développé par le W3C pour remplacer le GIF. Il surpasse ce dernier en ce qu'il n'est notamment pas limité à 256 couleurs.

De même, le format est ouvert et permet une bonne compression sans perte. Son utilisation est recommandée à l'instar du GIF pour les petits logos. Coté photo, s'il permet une compression sans perte, le poids de la photo n'est pas compétitif avec les formats JPEG.

Précisons que le PNG ne gère pas l'animation mais un format dérivé, le MNG, y est destiné.[13]

I.7.1.4 BMP (BitMaP) :

Le BMP est un des formats les plus simples développés 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. En BMP la couleur est codée en RGB (synthèse additive), le format lui-même supportant la palette 256 couleurs que le « True Color » [8]

I.7.1.5 TIFF (Tagged Image File Format):

C'est un format d'images non compressées qui peut être comprimé. Il est conçu pour être une norme, il est complètement paramétrable. Il existe plusieurs variations de ce format. Il permet la sauvegarde en noir et blanc, en niveaux de gris et en couleur. Les images TIFF peuvent être de 1, 4, 8 ou 24 bits par pixel. Les fichiers TIFF peuvent enregistrer les informations des modes de couleur RVB, CMJN et Lab, True Colors. [7]

I.7.1.6 PSD (Photoshop document) :

Le format PSD pour *Photoshop document* (Adobe) est pour sa part très complet mais la taille Des fichiers produits rend son utilisation en ligne difficile. Il est donc limité à la retouche d'images et au développement. Il est reconnu par plusieurs logiciels de traitement d'images, du fait de la grande diffusion des produits Adobe dans le domaine d'images numériques. Ce format peut coder la couleur sur 2, 8, 16, 24 et 32 bits, utilisant le mode RGB ou CMJN [11]

	Type	Compression des données	Nombre de couleurs supportées	Affichage Progressif	Animation	Transparence
JPEG	Matriciel	Oui, réglable (Avec perte)	16 millions	Oui	Non	Non
JPEG2000	Matriciel	Oui, Avec ou sans perte	4 milliards	Oui	Oui	Oui
GIF	Matriciel	Oui, Sans perte	256 maxi (Palette)	Oui	Oui	Oui
PNG	Matriciel	Oui, Sans perte	Palettisé (256 couleurs ou moins) ou 16 millions	Non	Non	Oui (couche Alpha)
TIFF	Matriciel	Compression ou pas avec ou sans pertes	De monochrome à 16 millions	Non	Non	Oui (couche Alpha)

Tableau I.1: Comparatif des différents formats matricielle.

I.7.2 Formats d'image vectorielle :

I.7.2.1 PICT(Picture*) :*

PICT pour *Picture* de Apple est obsolète comparé aux autres formats disponibles. Le format PICT est le format standard d'images du monde Macintosh, toutes les applications de dessin sous cet environnement sont généralement capables d'exporter des images dans ce format. Les fichiers PICT peuvent provenir directement du Macintosh, ou encore être génères par des applications de dessin Windows comme Photoshop ou Corel Raw. L'utilisation du format PICT à l'intérieur de la base de données permet de visualiser ces images à la fois sur Macintosh et sur PC. L'extension des fichiers PICT sous Windows peut être soit PIC, soit PCT, suivant le logiciel ayant génère l'image. Les fichiers PICT sont compressés ou non par QuickTime.[14]

I.7.2.2 PS (PostScript) :

PS pour *PostScript* utilisé avec la majorité des applications d'aujourd'hui, autant les logiciels de mise en pages, de traitement de textes et autres, il est possible d'exporter un document en format PS (PostScript) lequel pourra être acheminé vers un périphérique d'impression. Ce

format est également une façon sûre de rendre disponible un document seulement pour impression sans droit de modification. Il s'agit toutefois d'un format très lourd à éviter lorsqu'il doit être transfère par Internet sur des liens à basse vitesse.[14]

I.7.2.3 DXF :

Le format DXF est un format crée par la compagnie AutoDesk pour son logiciel de CAOAUTOCAD. Bien qu'étant un format très répandu dans le monde de la conception et du dessin assisté par ordinateur, le format DXF est très peu répandu en d'autres domaines.[14]

I.7.2.4 WPG :

Le format WPG est un format utilisé par les logiciels de la gamme de WordPerfect (WordPerfect, DrawPerfect, WP Présentations et autres) sous DOS, Windows ou Macintosh. Ce format donne un résultat acceptable lors de l'impression, mais qui doit surtout être utilisé en tant que format de travail. D'autant plus que ce n'est pas un format qui est reconnu par tous les logiciels [12, 11].

I.8 Aspects du traitement d'images :

Dans cette section, nous présentons les trois aspects du traitement d'images qui nous intéressent : filtrage, compression et tatouage.

I.8.1 Filtrage :

Pour améliore la qualité visuelle de l'image, on doit éliminer les effets des bruits (parasites)en lui faisant subir un traitement appelé filtrage. Le filtrage consiste à appliquer une transformation (appelée filtre) à tout ou à une partie d'une image numérique en appliquant un opérateur.[6]

I.8.1.1 Filtre passe-bas (lissage) :

Un filtre passe-bas accentue les éléments qui ont une basse fréquence spatiale tout en atténuant les éléments à haute fréquence spatiale (pixels foncés). Il en résulte une image qui apparait plus homogène (un peu floue) particulièrement en présence d'arêtes. Ce type de filtrage est généralement utilise pour atténuer le bruit de l'image, c'est la raison pour laquelle on parle habituellement de lissage.[6]

I.8.1.2 Filtre passe-haut (accentuation) :

Les filtres passe-haut atténuent les composantes de basse fréquence de l’image et permettent notamment d’accentuer les détails et le contraste, c’est la raison pour laquelle le terme de « filtre d’accentuation » est parfois utilisé. Ce filtre n’affecte pas les composantes de haute fréquence d’un signal, mais doit atténuer les composantes de basse fréquence. Un filtre passe haut favorise les hautes fréquences spatiales, comme les détails, et de ce fait, il améliore le contraste. [6]

I.8.1.3 Filtre passe-bande (différentiation) :

Cette opération est une dérivée du filtre passe-bas. Elle consiste à éliminer la redondance d’information entre l’image originale et l’image obtenue par filtrage passe-bas. Seule la différence entre l’image source et l’image traitée est conservée. Les filtres différentiels permettent de mettre en évidence certaines variations spatiales de l’image. Ils sont utilisés comme traitements de base dans de nombreuses opérations comme le rehaussement de contraste ou la détection de contours.[6]

I.8.2 La compression :

La compression de données consiste à obtenir des fichiers plus légers, afin d'améliorera vitesse de transfert sur internet ou limiter l'espace de stockage utilisé sur un disque dur. Il existe deux principaux types de compression :

I.8.2.1 La compression sans perte :

Appelée aussi « compactage ». Cette solution consiste simplement à coder les données binaires de manière plus concise dans un fichier. Elle permet ainsi de retrouver la totalité désinformations après une procédure de décompactage.

I.8.2.2 La compression avec perte :

Concernant essentiellement les fichiers de média (image, son, vidéo), elle consiste en une « réduction » de l'information basée sur notre propre limite humaine à percevoir ces médias. Puisque l'oeil ne perçoit pas nécessairement tous les détails d'une image, il est possible de réduire la quantité de données de telle sorte que le résultat soit ressemblant à l'original, voire identique, pour l'oeil humain. [6]

I.8.3 Le tatouage :

L’idée de base du tatouage numérique est de cacher dans un document numérique une information subliminale (i.e. invisible ou inaudible suivant la nature du document) permettant d’assurer un service de sécurité (copyright, intégrité, traçabilité, non répudiation, etc.) ou à but d’information [15].

Le principe et les notions liées ce traitement sont bien détailles dans le chapitre suivant.

I.9 Conclusion :

Dans ce chapitre, nous avons présenté les différents concepts concernant les images numériques, en donnant quelques définitions élémentaires portant sur ce sujet, et qui seront sûrement des points essentiels dans la suite de notre travail. Nous avons également présenté quelques aspects du traitement d’image, tels que le filtrage, la compression et le tatouage.

Chapitre II :
Tatouage numérique

Chapitre II : Tatouage numérique

II.1 Introduction :

Les différentes multimédias (image, vidéo et audio) sont devenues des outils très importants dans différentes domaines (imagerie médicales, satellitaire... etc.) ou leur transmission est très facile à travers les réseaux. En effet les documents multimédias peuvent être dupliqués, modifiés et falsifiés. Dans ce contexte il est nécessaire de mettre en œuvre des systèmes adaptés aux nouvelles technologies qui permet de respecter le droit d'auteur et de vérifier l'intégrité et de garantir l'authentification.

Pour répondre à ces besoins il existe plusieurs techniques qui sont utilisées pour plusieurs buts ainsi que la protection de droit d'auteur. Une solution possible consiste à insérer une certaine information invisible dans les images où l'information peut être intégrée ou extraite à des fins différentes. Le tatouage numérique est un processus visant à insérer une certaine information appelé la marque dans différents types de médias appelé image hôte.

Dans ce chapitre nous présenterons le concept général du tatouage d'images, ensuite nous présenterons les domaines d'application, les techniques de tatouage et les attaques.

II.2 Historique du tatouage numérique :

Les tatouages du papier sont apparus dans l'art de la fabrication du papier il y a presque 700ans. 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 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 puise 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. [16] en 1990 et par Tirkel et al. **[17]** 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. [18]

La Figure II.1 montre le nombre de publications avec le mot clé "watermarking" sur la base de données bibliographiques INSPEC.

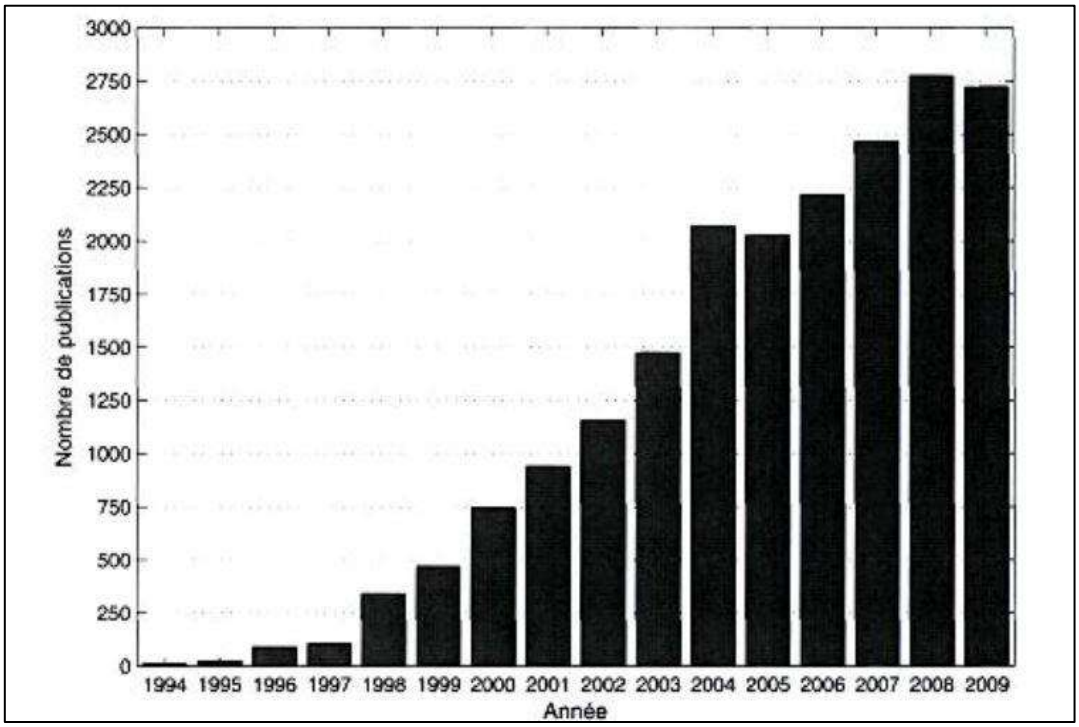


Figure II.1 : Nombre de publications sur le tatouage numérique (INSPEC - juin 2010).

II.3 Définitions :

II.3.1 Le tatouage numérique :

En raison de l'absence d'une définition normalisée de terme « tatouage numérique », nous présentons quelques définitions parmi plusieurs, proposées par différents auteurs du domaine informatique, électronique ou autre.

Chapitre II : Tatouage numérique

Définition Miller et Cox 1997

Le tatouage numérique signifie l'incorporation d'une information numérique dans un contenu multimédia, comme une vidéo, un audio ou une image de telle manière que l'information insérée doit être imperceptible pour un observateur humain, puis à tenter de la récupérer après que le document tatoué ait éventuellement subi des manipulations de nature variée [19].

Définition Kundur et Hatzinakos 1998

Le processus du tatouage numérique implique la modification des données multimédia originales pour insérer un watremark contenant des informations clés telles que les codes d'authentification ou de droit d'auteur. La méthode d'insertion doit conserver les données originales visuellement inchangés, mais d'imposer des modifications qui peuvent être détectés à l'aide d'un algorithme d'extraction. Les types de signaux à tatouer sont des images, le son vidéo et le texte [20].

Définition Petitcolas, Anderson et Kuhn 1999

Le tatouage numérique signifie l'intégration d'une information dans un document numérique de façon à ce que cette information soit imperceptible pour un observateur humain, mais facilement détectée par l'ordinateur. Le watermark est une information transparente, invisible qui est insère dans un document source en utilisant un algorithme informatique [21].

Définition Christian REY et Jean-Luc DUGELAY 2001

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (i. e, invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc.) ou à but d'information. Une des particularités du tatouage numérique par rapport à d'autres techniques, comme par exemple un stockage simple de l'information dans l'en-tête du fichier, est que le watermark est lié de manière intime et résistante aux données. De ce fait, le tatouage est théoriquement indépendant du format de fichier et il peut être détecte ou extrait même si le document a subi des modifications ou s'il est incomplet [15].

Chapitre II : Tatouage numérique

Définition Chun-Shien Lu 2004

Le tatouage numérique est un signal intégré de façon permanente dans des données numériques (audio, image, vidéo et texte) qui peut être détecte ou extrait plus tard par l'exécution d'un algorithme informatique afin de faire des affirmations sur les données. Le tatouage est caché dans le document hôte de telle manière qu'il est inséparable des données et qu'il est résistant à de nombreuses opérations, sans dégrader la qualité du document hôte. Ainsi, par le biais du tatouage, le travail est encore accessible, mais définitivement marqué [22]. Quel que soit la manière d'exprimer la définition de la technique du tatouage, son principe et ses exigences restent les mêmes. Dans les sections suivantes, nous présentons ce principe (à travers un modèle générique) et les exigences d'une technique du tatouage invisible.

II.3.2 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 [23].

II.3.3 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 [24].

II.4 Schéma général du tatouage numérique des images :

Le tatouage comporte deux phases fondamentales :

- Phase d'insertion.
- Phase d'extraction.

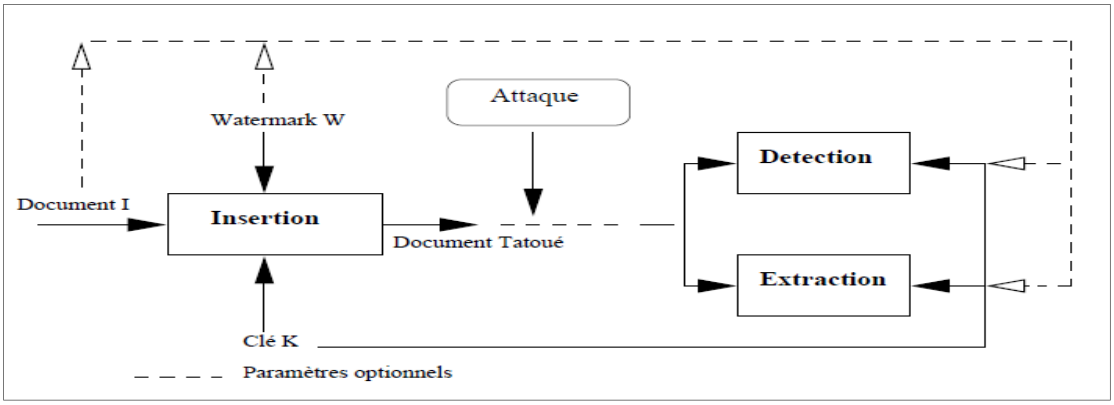


Figure II.2 : Modèle générique d'un système du tatouage.

II.4.1 Phase d'insertion :

Les entrées de l'insertion de tatouage sont la marque, les données originales et. La marque qui peut être une séquence de nombres, une séquence de bits binaire ou peut être une image. La clé est utilisée pour améliorer la sécurité du système de tatouage. Les sorties de processus de l'insertion sont des données tatouées.

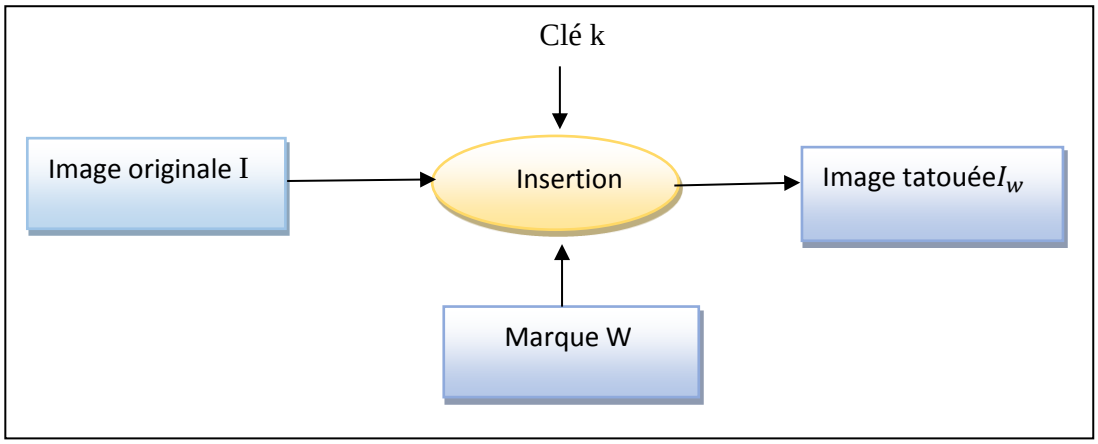


Figure II.3: Schéma général de l'insertion d'une marque.

La figure II.*3* présente le schéma général de l'insertion de la marque W à l'aide d'une clé K. L'image originale I est tatouée de la marque W par la propriétaire possède de la clé K. L'image marquée $I_w$est visuellement équivalente à I.

II.4.2 Phase d'extraction :

Dans le processus de l'extraction les entrées sont les données tatouées, la clé de sécurité et les données originales et la marque originale en fonction de la technique utilisée, si l'extracteur ne nécessite pas la disponibilité de la copie originale, le schéma de tatouage est appelé « tatouage aveugle »(voir la figureII.6), si l'extracteur nécessite l'image originale, il est appelé « tatouage non aveugle » (voir la figure II.4).Dans le schéma semi aveugle la connaissance de l'image originale et la marque ne sont pas nécessaires mais quelques informations supplémentaires de celle-ci (voir figure II.5).

Ensuite, l'étape suivante consiste habituellement à la comparaison de la marque extraite avec la marque originale et le résultat pourrait être comme une sorte de mesure qui représente la possibilité de la présence de la marque originale dans le document ou non utilisant une fonction de corrélation. Pour certains algorithmes de tatouage, la marque extraite peut être encore décodé pour obtenir le message incorporé à des diverses buts telles que la protection du droit d'auteur et l'authentification. La marque est considérée comme robuste si elle est incorporée de manière que la marque peut rester robuste et stable même si les données tatouées passé par différents traitements. La procédure de l'extraction est indiquée par la formule comme suit :

$$W' = D(I_w^*, K)$$

La marque W′ doit être détectée à partir de I_w^* avec/ou sans la connaissance de l'image originale *I*. Si I_w n'est pas modifiée (attaquée), alors W′ correspond exactement à W. Les figures II.4, II.5 et II.6 présentent le schéma général de l'extraction de la marque.

On peut classifier le schéma de l'extraction selon la nécessité de l'utilisation de l'image originale *I* et la clé K en trois classes :

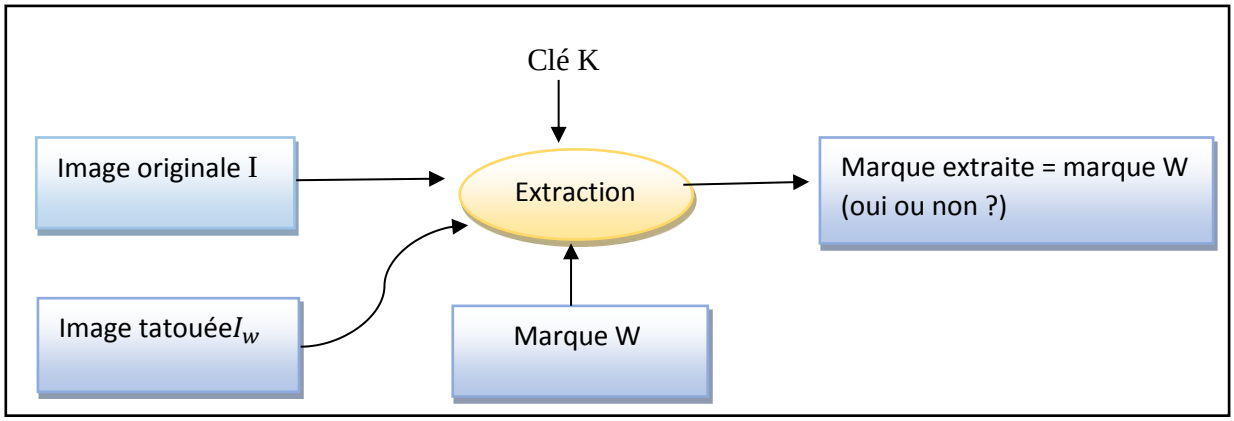


Figure II.4: Schéma général d'extraction non aveugle d'une marque.

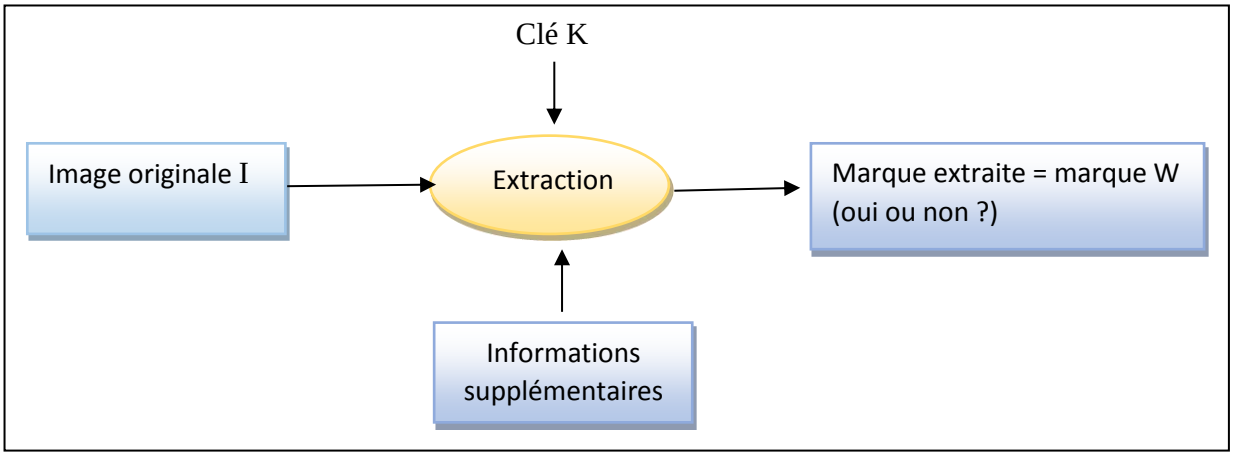


Figure II.5: Schéma général d'extraction semi aveugle d'une marque.

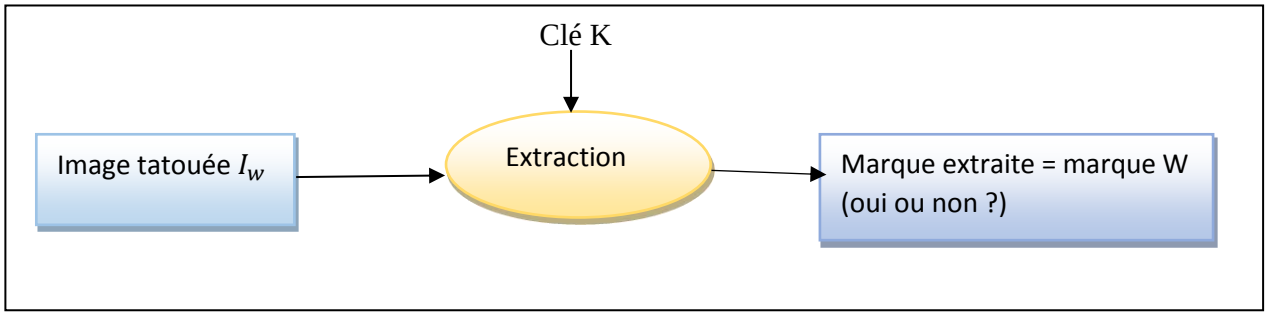


Figure II.6: Schéma général d'extraction aveugle d'une marque.

II.5 Contraintes du tatouage d'image :

Pour qu'en puisse quantifier la performance d'une technique de tatouage ou pour concevoir un algorithme de tatouage performant, L'algorithme de tatouage doit respecter quelques facteurs essentiels, ces facteurs sont : l'imperceptibilité, robustesse, et la capacité. Qui sont détail en au-dessous. Ces facteurs sont représentés schématiquement dans la figure suivante :

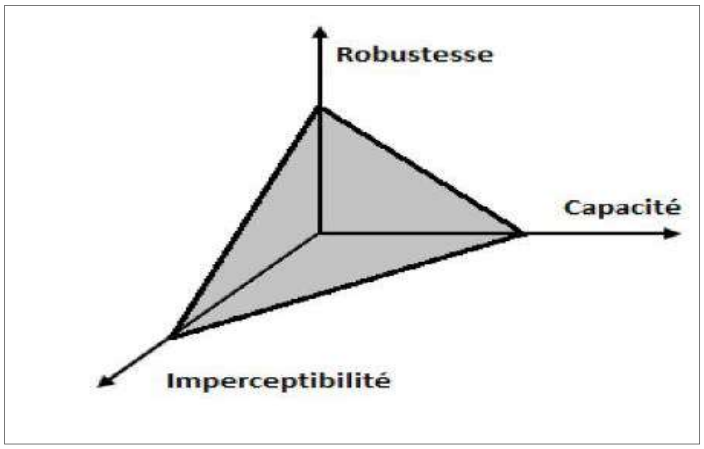


Figure II. 7: Les Contraintes de tatouage d'image

Il est clair de voire que ces trois critères sont opposés, c'est-à-dire il est impossible d'inventer un système de tatouage numérique qui assurer toutes ces facteurs en même temps, si on veut améliorer un facteur parmi ces facteurs-là, on aura en contrepartie un effet indésirable sur les autres facteurs. Il est donc nécessaire de trouver le meilleur arrangement possible entre ces trois facteurs en fonction de l'application envisagée.

En plus des contraintes précédentes Il y'a d'autre contrainte, qu'ont peuvent les considérer aussi :

- **Fausse Alarme :** la détection d'une marque dans une image alors que l'image n'a pas été tatouée ou bien qu'elle ait été tatouée avec une autre marque [25].
- **Coût d'algorithme :** le temps de calcule passe par l'algorithme pour permettre une implémentation en temps réel [25].

II.5.1 Imperceptibilité :

Le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée. [26] définissent l'imperceptibilité en tant que similitude visuelle entre la version

originale et les versions tatouées. Le watermark insère doit être entièrement invisible par le système visuel humain (SVH). L'opération d'insertion ne doit pas détériorer l'image hôte de façon perceptible, c'est à dire l'image tatouée doit être visuellement équivalente à l'image originale. Non seulement, il ne faut pas dénaturer l'image, mais en plus si le watermark est visible, il pourrait être facilement éliminé.

II.5.2 Capacité :

Signifié la quantité des informations ou de la marque que l'on peut insérer dans l'image, plus la taille de la marque est grande plus la dégradation est grande.

II.5.3 Robustesse :

Ce critère représente la résistance ou non de la marque après des modifications subis par les attaques. Aussi Cox et Miller **[27]** définissent la robustesse comme capacité de détecter le watermark après des opérations de modifications (traitements), par exemple plus la qualité d'information dans l'image augmente, plus la signature sera visible ou perceptible et donc la robustesse diminue.

II.5.4 Sécurité :

La sécurité constitue une contrainte indépendante des trois 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 [28].

II.6 Types de tatouage d'image :

En plus de classer les schémas de tatouage en fonction du type d'algorithmes utilisés, on définit aussi le type de tatouage en fonction de sa résistance aux attaques. Il existe trois types de schéma de tatouage en fonction de leur résistance.

II.6.1 Les tatouages robustes :

Les tatouages robustes sont conçus dans le but de protéger des documents. 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. Ce système doit résister aux opérations licites effectuées sur le document numérique (compression, conversion analogique-numérique, filtrage, etc.) et celles illicites (attaques malveillantes des pirates). [8]

II.6.2 Les tatouages semi-fragiles :

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. Les tatouages semi-fragiles doivent résister à une compression JPEG avec un haut niveau de qualité et à quelques attaques. Leurs applications sont surtout réservées à l'authentification d'images. [8]

II.6.3 Les tatouages fragiles :

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. [8]

II.7 Les techniques du Tatouage :

Vue le nombre important des techniques de tatouage numériques qui existe à cette époque-là, Nous allons les classer en trois grandes catégories selon que le tatouage soit visible ou invisible, le types d'algorithmes utilisés dans l'insertion et l'extraction de la marque et le domaine d'insertion.

II.7.1 Tatouage visible et invisible :

La classification selon la visibilité ce base sur le fait que la marque insérée doit être vu par l'oeil humain ou non.

Dans les techniques de tatouage visible, il existe au moins deux inconvénients :

- La marque insérée est facilement enlevée par un simple découpage.
- La visibilité de la marque insérée dégrade la qualité visuelle de l'image l'hôte.

Dans la technique de tatouage invisible, l'image originale est très similaire à l'image tatouée, il n'est pas donc facile de faire la distinction. Ainsi, il est difficile d'enlever ou détruire la marque insérée sans avoir une dégradation de la qualité visuelle de l'image tatouée de manière significative. [29,30]

Figure II. 8 : Tatouage visible.

Figure II. 9 : Tatouage invisible.

II.7.2 Type de l'algorithme :

II.7.2.1 Types d'insertion :

L'insertion de la marque peut se faire principalement selon deux règles : par Multiplication ou par substitution. Selon la technique d'insertion, les schémas de tatouage numérique peuvent être classifies en deux groupes : les algorithmes multiplicatifs, et les algorithmes substitutifs.

a) Insertion par multiplication :

L'insertion selon la règle multiplicative est très robuste face aux attaques mais sa capacité d'insertion est très limitée. Dans cette catégorie on peut citer plusieurs approches d'insertion :

- L'approche perceptuelle additive pour insérer une information secrète dans l'image en utilisant les transformées DCT et DWT.

- Les schémas multiplicatifs d'étalement du spectre dans le domaine fréquentiel. Basée sur la détection statistique et la DCT.

b) Insertion par substitution :

Avec l'insertion par substitution, la marque à insérer n'est pas ajoutée mais plutôt substituée à des composantes de l'image originale I [25]. L'ajout de la marque par substitution peut se faire selon plusieurs méthodes, telles que la substitution des bits les moins significatifs (LSB), la substitution d'histogramme, la substitution des caractéristiques géométriques et la substitution par quantification.

L'avantage de l'insertion par substitution est résidé dans sa grande capacité. Par contre, sa robustesse est limitée. Il est nécessaire pour avoir plus de robustesse, d'effectuer une sélection intelligente des coefficients en plus de rajouter des dispositifs comme les codes correcteurs d'erreurs [25].

II.7.2.2 Types d'extraction :

Les schémas de tatouages peuvent être classés en trois catégories Selon les éléments nécessaires pour l'extraction de la marque [31] [25].

- **Algorithmes informés ou non aveugles :** celles qui ont besoin de l'image originale lors de l'extraction.
- **Algorithmes non informés ou aveugles :** Les algorithmes qui n'utilisent pas l'image originale.
- **Algorithmes semi-aveugle :** Dans ce type on n'utilise pas l'image originale, mais on se sert uniquement de la marque et dans le cas échéant d'une clé qui a été utilisée lors de la phase d'insertion

II.7.3. Robustesses d'algorithme :

On peut distinguer dans cette classification trois catégories de tatouage numérique : robuste, fragile et semi-fragile [25][31].

- **Tatouage robuste** : cherche à préserver la marque insérée face aux attaques bienveillantes ou malveillantes. La marque ne doit pas pouvoir être éliminée sans endommager l'image tatouée.

- **Tatouage fragile :** la marque doit être très sensible à toutes modifications quel que soit sa nature.
- **Tatouage semi-fragile** combine les caractéristiques du tatouage robuste et fragile pour détecter les manipulations malveillantes tout en demeurant robuste face aux attaques bienveillantes.

II.7.4 Domaine d'insertion :

Les techniques de tatouage courantes décrites dans la littérature peuvent être regroupées selon leurs domaines d'insertion en deux classes, techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

II.7.4.1 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. [8]

II.7.4.2 Domaine fréquentiel :

Les techniques de tatouage numérique qui travailler dans le domaine fréquentiel sont largement utilisées à cause de leurs robustes face aux dévers attaques et leurs complexités.

Pour insérée La marque les coefficients de la transformée fréquentielle utilisée doit être modulée. Parmi les transformées utilisées dans les algorithmes du tatouage numérique des images on peut citer : la transformée en cosinus discrète (DCT), la transformée en ondelettes discrète (DWT), la transformée de Fourier discrète (DFT) [25].

a) Domaine de la DFT :

Depuis l'apparition du tatouage numérique, la transformée de Fourier a largement été utilisée. La transformée de Fourier d'une image est généralement de nature complexe. Elle peut être représentée par deux composantes, à savoir une amplitude et une phase.

Plusieurs techniques de tatouage exploitent la modulation d'amplitude de la DFT. L'invariance du spectre en translations ou décalages a motivé certains auteurs à tatouer l'amplitude du spectre de Fourier. Quand le tatouage change l'amplitude du coefficient il doit préserver la symétrie positive [25,32].

La modulation de la phase de la DFT pour l'insertion d'une marque est exploitée dans plusieurs articles, la phase contient les composantes les plus importantes de l'image, en modulants la phase en permet d'accroître la robustesse du schéma, Une attaque opérant dans la phase du spectre dégraderait rapidement la qualité de l'image [32].

Une seconde raison justifiant le tatouage de la phase du spectre provient de la théorie de la communication ou la modulation de la phase possède une meilleure immunité au bruit que la modulation d'amplitude [32,25].

b) Domaine de la DWT :

La transformer en ondelettes discrète (DWT) est une description multi-résolution qui consiste à décomposer le signal en plusieurs bandes de fréquences (basse-fréquence et haute-fréquence). En utilisant respectivement des filtres passe-bas et passe-haut qui doivent être orthogonaux.

La décomposition de niveau simple de l'image donne quatre représentations de fréquence. Ces quatre représentations s'appellent les sous-bandes LL (approximation), LH (vertical), HL (horizontal), et HH (diagonal) Pour reconstruire le signal, il faut rassembler ces diverses bandes [32][33][25]. Plusieurs recherches ont même été faites pour combiner la DWT avec d'autres transformées.

LL	HL
LH	HH

Figure II.10: Un niveau de décomposition en utilisant la DWT.

d) La Décomposition en Valeurs Singulières (SVD) :

La SVD est un outil mathématique très utilisé dans le traitement numérique d'images. Récemment, cette transformée est utilisée pour le tatouage numérique à cause de ses propriétés algébriques.

II.8 Utilisation du tatouage :

Les systèmes de tatouage numérique sont développés en fonction de différents domaines d'applications parmi celle-ci on peut citer :

II.8.1 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. 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).[43]

II.8.2 Authentification de documents :

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.[43]

II.8.3 Protection de Copie :

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.[43]

II.8.4 Indexation et les liens descriptifs :

Le tatouage permet d'insérer une signature dans l'image pour rendre l'indexation plus simple. La signature générée par un créateur est une collection d'informations avec un sommaire ou un descripteur ou un lien vers une autre information pour faciliter le classement et la recherche rapide dans une base de données [45] [44] [46].

La marque peut contenir des informations descriptives sur l'image hôte telles que l'étiquetage et le sous-titrage. Pour ce type d'application, la capacité de la marque devrait être relativement grande.

II.9 Les attaques des images tatouées :

Une attaque est tout traitement qui peut empêcher la détection de la marque lors de son extraction. Les données tatouées traitée est alors sont appelées des données tatouées attaquées.

Selon S. Voloshynovskiy et al. [37] Les attaques sont regroupées en quatre classes principales : les attaques d'effacement ou de suppression, les attaques géométriques, les attaques cryptographiques et les attaques de protocole.

Selon les auteurs Cox et al [26] les attaques sont classées en deux types : les attaques sur la robustesse et les attaques sur la sécurité.

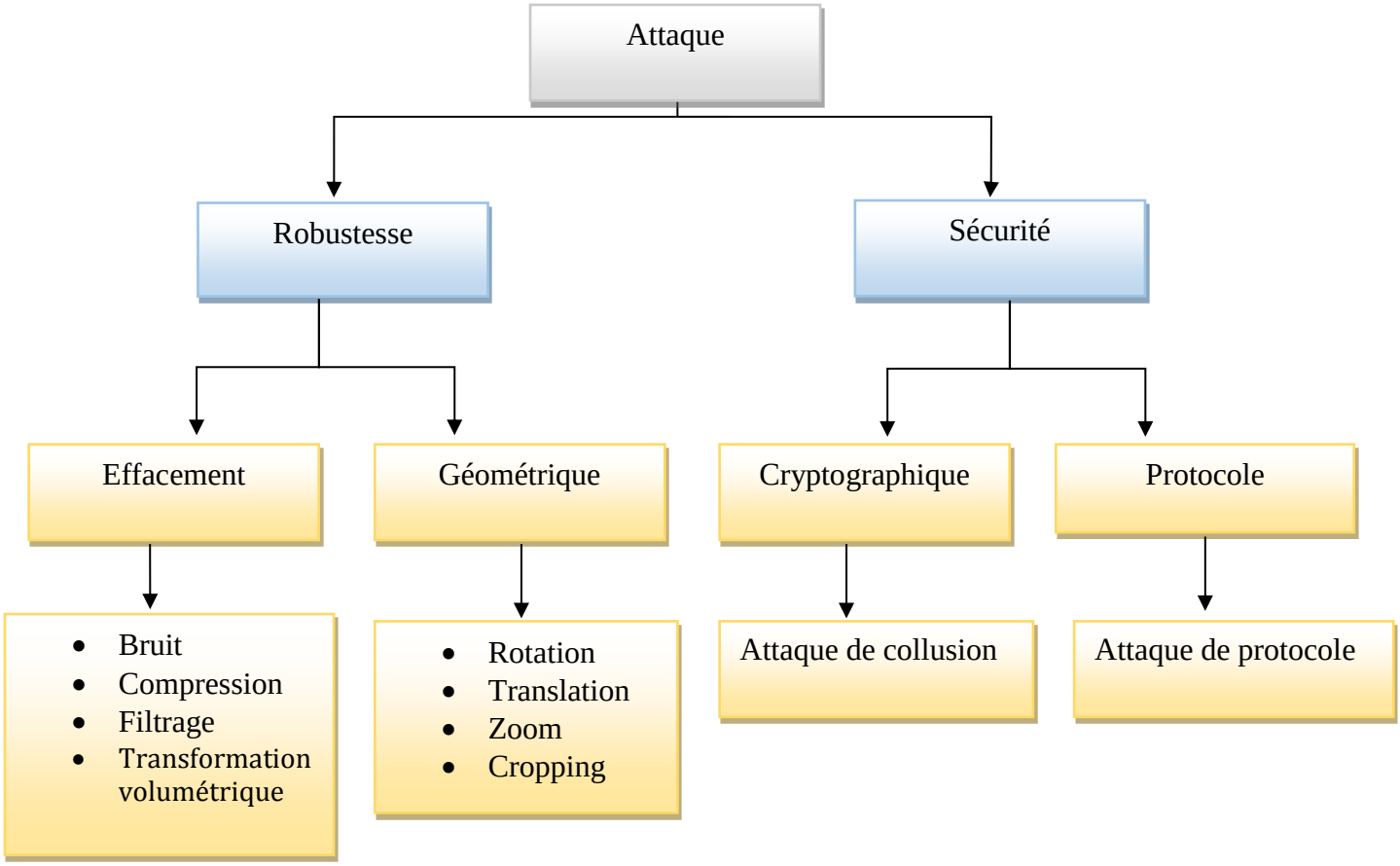


Figure II. 11: Classification des attaques

II.9.1 Les attaque d'effacements :

Permet de supprimer la marque et elles s'inspirent du domaine de traitement d'image qui tente d'évaluer ou d'estimer l'image originale à partir de l'image tatouée en appliquant plusieurs traitements (compression, lissage, conversion analogique numérique, addition de bruit et le filtrage…). Parmi les attaques de suppression on cite [34] :

a) Attaque de bruitage :

Permet de trouver la forme approchée de watremark pour pouvoir le supprimer.

b) Compression avec perte JPEG :

Qui permet de diminuer la taille de l'image par la suppression des données redondantes dans l'image et les données les moins significatifs. L'invisibilité de la marque est considérée comme moins significatif ce qui rend la suppression facile de la marque invisible.

c) Filtrage et le lissage :

Permet d'augmenter les entités de haute fréquence, les filtre les plus utilisés sont : le médian, le gaussien, la placien et le filtre moyen, tel que le lissage est une opération inverse qui permet d'atténuer les composantes de haute fréquence.

Figure II.12: Filtres passe-bas

Figure II.13 : Filtres passe-haut

d) Transformations volumétriques :

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

II.9.2 Les attaques géométriques :

Permettent de déformer ou déplacer l'image tatouée pour empêcher la détection de watermark telle que la translation, la rotation, l'agrandissement, la réduction, contrairement aux attaques de suppression, les attaques géométriques ne fait pas enlever le watermark

inséré, mais tentent de déformer la synchronisation de l'extracteur de la marque insérée. Les informations de watermark insérées peuvent être récupérées si la synchronisation parfaite est retrouvée. Les attaques géométriques permettent de déformer ou déplacer l'image tatouée ce qui rend la détection de watermark ou la signature difficile, parmi les transformations géométriques les plus usuelles : la translation, la rotation, l'agrandissement, la réduction...

a) Rotation :

C'est une transformation qui est très utilisée après avoir scanné une image.

Elle sert à réaligner des images et peut être fatale à certains types de marquages (Des petits angles de rotation appliqués, peuvent rendre le watremark non détectable).

Figure II.14 : Rotation

b) 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). [35]

c) Le recadrement (Cropping) :

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.

Sert à supprimer ou couper une partie d'une image. [35]

Figure II.15: Le recadrement

d) 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 [36].

Figure II.16:Attaque par mosaïque

II.9.3 Les attaques sur la sécurité :

Parmi les attaques sur la sécurité nous citons [35] :

a) Les attaques cryptographiques :

Elles relèvent du domaine de la cryptographie telle que la collusion (deux textes différents donnant une même signature).

b) Les attaques de protocole :

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

Craver et al[37] ont mentionnés une attaque, comme l'attaque d'inversion de watremark ou l'attaque IBM, qui produit un faux schéma de tatouage qui peut être appliqué sur une image tatouée qui permet à créer un doute sur ce qui a été inséré en premier ,l'attaque de copier est un autre type d'attaque de protocole, dans ce cas, la marque est prédite en utilisant un ensemble de données tatouées, ce watremark prévu est inséré dans une autre donnée en adaptant les caractéristiques locales pour satisfaire son imperceptibilité.

II.10 Mesures d'évaluations visuelles de la qualité des images :

Pour pouvoir mesurer efficacement la distorsion introduite par les techniques de tatouage afin d'assurer le respect du facteur de l'imperceptibles, il est nécessaire d'introduire un critère perceptuel basé sur une modélisation de la perception des signaux multimédia.

En général, la métrique qui peut être utilisées pour évaluer l'imperceptibilité, c'est la métrique basée sur les pixels, Ces mesures sont basées sur le calcul de la différence (mesures de distances) entre l'image originale et l'image tatouée (attaquée ou non attaquée).

La mesure habituellement utilisée pour quantifier la distorsion entre un signal original x et un signal modifié y est le $PSNR$ (Peak Signal-to-Noise Ratio). Elle est basée sur l'erreur quadratique moyenne MSE (Mean Square Error), définie par [38, 25,33] :

$$\mathrm{MSE} = \frac{1}{\mathrm{n}}\sum_{\mathrm{i}=1}^{\mathrm{n}}(\mathrm{xi}-\mathrm{yi})^2$$

Où n est la dimension commune aux deux vecteurs considérés. Quant au $PSNR$, il est calculé par [38, 25 ,33] :

$$\mathrm{PSNR} = 10.\log_{10}[\frac{(\max(\mathrm{x}))^2}{\mathrm{MSE}}]$$

On considère généralement en tatouage d'images qu'un tatouage est imperceptible pour un $PSNR$ supérieur à 36 dB, et plus il est élevé, moins la distorsion est importante.

Les métriques de corrélation (par exemple corrélation normalisée NC) sont légèrement plus complexes, elles permettent de calculer la corrélation entre les deux images. De telles métriques ne mesurent plus la différence entre deux images, mais plutôt la ressemblance des images [25,38].

$$\mathrm{NC} = \sum_{\mathrm{i,j}}^{\mathrm{MN}} (\mathrm{x(i,j).\,y(i,j)}) \Big/ \sum_{\mathrm{i,j}}^{\mathrm{MN}} \mathrm{x(i,j)}^2$$

Dans le même conteste en trouve le MAE (Mean Absolute Error) qui mesure la déférence entre une marque original et la marque extraite correspondante, la valeur la plus petite de MAE signifier une ressemblance proche des deux marques [39].

$$\mathrm{MAE} = \sum \|(\mathrm{w(i,j)} - \widehat{\mathrm{w}}\ \mathrm{(i,j)}\|\mathrm{MN_{i,j}} / \|\mathrm{w}\|$$

Si ces métriques représentent grossièrement une mesure de dégradation des images, elles ne sont cependant pas adaptées au système visuel humain.

II.11 Conclusion :

Le watermarking et l'un des techniques de protection de droit d'auteur les plus utilisées à cause de son efficacité et sa facilité d'implantation.

Dans ce chapitre, nous avons présenté quelques notions de base du tatouage numérique d'images ainsi que les exigences de ce domaine, nous avons aussi présenté les critères de classification des techniques du tatouage, les différentes attaques et comment mesurer les techniques de tatouage.

Chapitre III :

Conception et implémentation d'un tatouage fragile par LSB replacement

Chapitre III Conception et implémentation d'un tatouage fragile par LSB replacement

III .1 Introduction :

Le tatouage numérique fragile, se présente comme solution alternative pour résoudre les problèmes de sécurisation des documents numériques.

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 la conception, la mise en œuvre de notre application et les algorithmes du tatouage fragile d'images numériques qui vise à insérer un watermark dans les bits poids faible (méthode LSB) d'une image couleur RGB, pour assurer l'authenticité des images numériques. Ensuite, on a fait une étude comparative de qualité entre les formats des images visant à évaluer la performance de notre algorithme du tatouage fragile.

III .2 Conception :

Notre application est composée de deux phases :

- Phase d'insertion : Insertion la marque dans l'image hôte par la méthode LSB (Bit de poids faible).
- Phase d'extraction : L'extraction de la marque de l'image tatouée par la méthode LSB inverse.

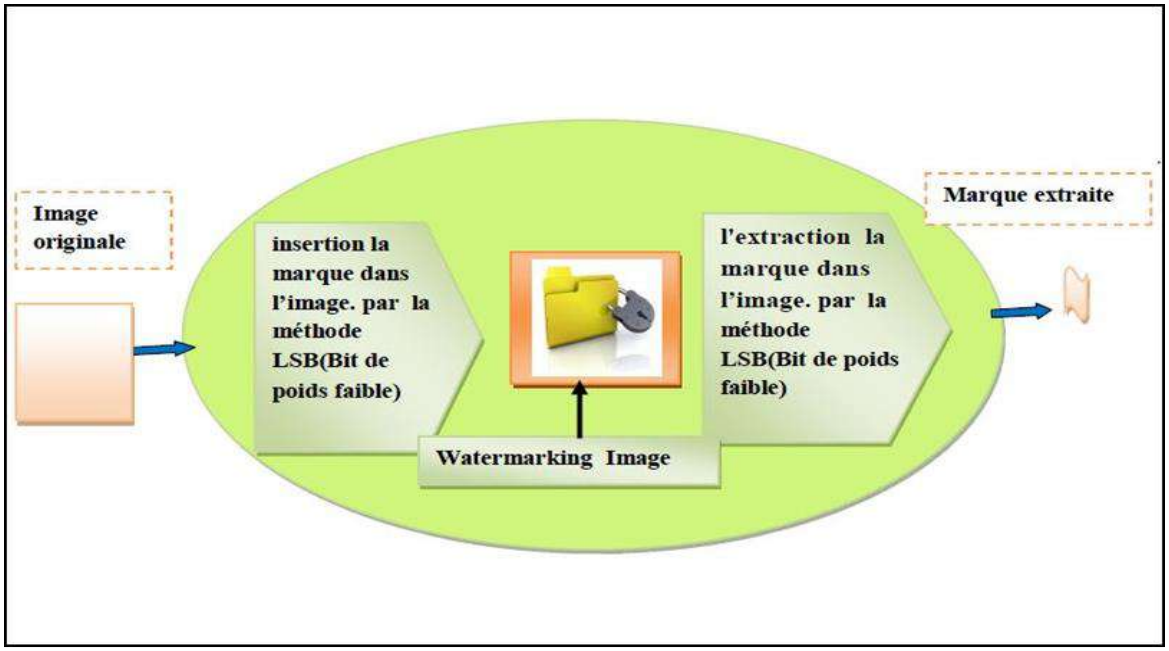


Figure III.1:Schémas général de l'application.

III.3 les outils de développement :

III.3.1 Langage Java :

Pour réaliser notre travail nous avons opté le langage de programmation Java sous l'environnement NetBeans. C'est un langage orienté objet simplifie le processus de développement quelle que soit la machine sur laquelle on programme, ce langage capable de s'exécuter sur n'importe quelle plateforme.

Le langage java peut effectuer à l'instar des autres langages, toutes les tâches (bureautiques, graphiques, bases de données, etc.). Le point fort de Java, qui le démarque des autres langages, est sa portabilité de ses bibliothèques de classes indépendantes de la plate-forme, ce qui est le point essentiel de la programmation sur Internet où plusieurs machines dissemblables sont interconnectées. [47]

III.3.2 NetBeans :

NetBeans est un environnement de développement intégré (EDI), placé en Open Source par « Sun ». En plus de Java, NetBeans permet également de supporter différents autres langages,

comme C, C++, JavaScript, PHP, HTML … Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi langage, éditeur graphique d'interfaces et de pages Web, …). Conçu en Java, NetBeans est disponible sous Windows, Linux, Solaris, Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java Développent Kit (JDK) est requis pour les développements en Java.

III.3.3 PSNR :

(Sigle de Peak Signal to Noise Ratio) c'est une mesure de similarité utilisée en image numérique. Il s'agit de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image tatouée par rapport à l'image originale. [42]

Il est mesuré en dB à partir de la relation suivante :

$$\mathrm{PSNR} = 10.\log_{10}[\frac{(\max(x))^2}{\mathrm{MSE}}]$$

- x : est le signal original.
- y : est le signal modifié.
- n : est la dimension commune aux deux vecteurs considérés.
- MSE (Mean Square Error) : est l'erreur quadratique moyenne calculé par cette formule :

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(xi - yi)^2$$

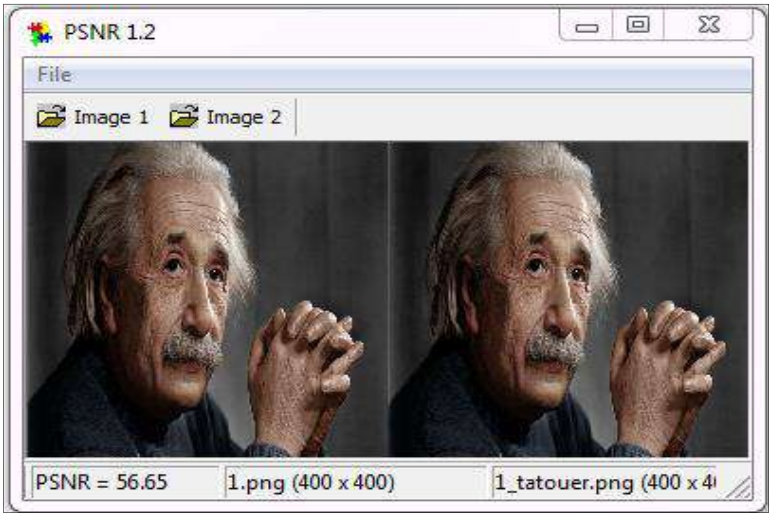


Figure III. 2: Fenêtre PSNR

Chapitre III Conception et implémentation d'un tatouage fragile par LSB replacement

III.4 L'organigramme de l'algorithme :

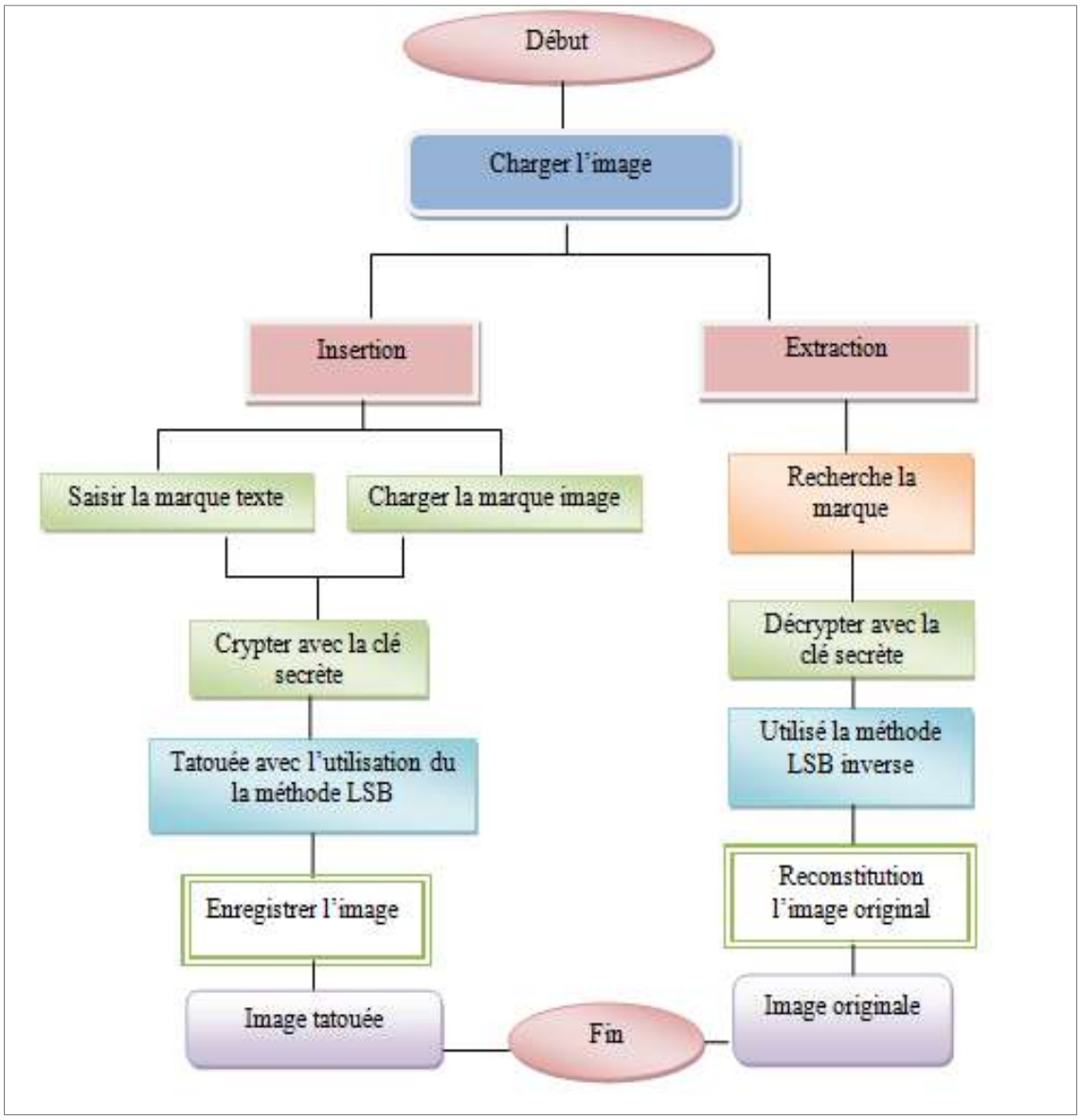


Figure III. 3 : Fonctionnement générale de l'algorithme

III.5 Méthode 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. [40]

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.

[41]

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^{eme} 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. [17]

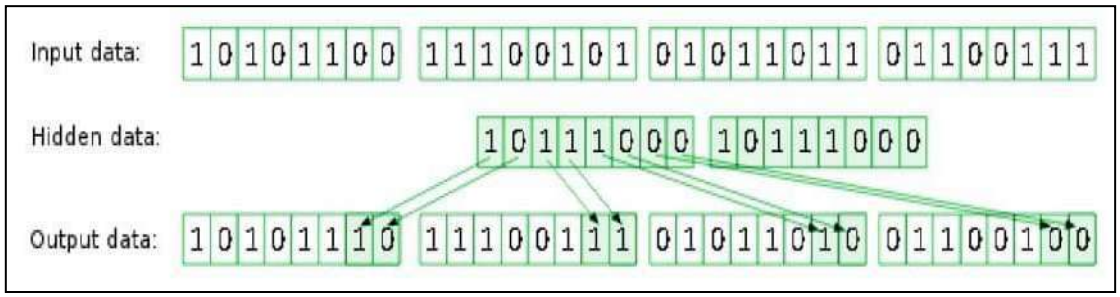


Figure III. 4: Méthode LSB

III.5.1 L'objectif de l'utilisation de la méthode LSB dans le tatouage fragile :

- Méthode basée sur le bit de poids faible.
- Simple à implémenter.
- Ne modifie pas la taille de l'image.
- Modifications invisibles à l'oeil 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.

III.6 Algorithme d'insertion :

Entrées :

F= image couleur RGB de taille m × m.

W =marque de taille n × m.

En cas la marque texte :

- Convertir la marque en binaire.
- Crypter la marque avec une clé secrète (chaque octet de watermark fait un XOR avec la clé secrète).
- Insérer la marquer dans l'image F (appliquer la méthode LSB).

En cas la marque image :

- Crypter la marque avec une clé secrète (chaque octet de watermark fait un XOR avec la clé secrète).
- Convertir la marque en binaire.
- Insérer la marque dans l'image F (appliquer la méthode LSB).

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

- Remplacer le bit de poids faible de R (i, j) par le premier bit de W (i, j).
- Remplacer le bit de poids faible de G (i, j) par le deuxième bit de W (i, j).
- Remplacer le bit de poids faible de B (i, j) par le troisième bit de W (i, j).

Sortie :

F_W: Image tatouée de taille m × m

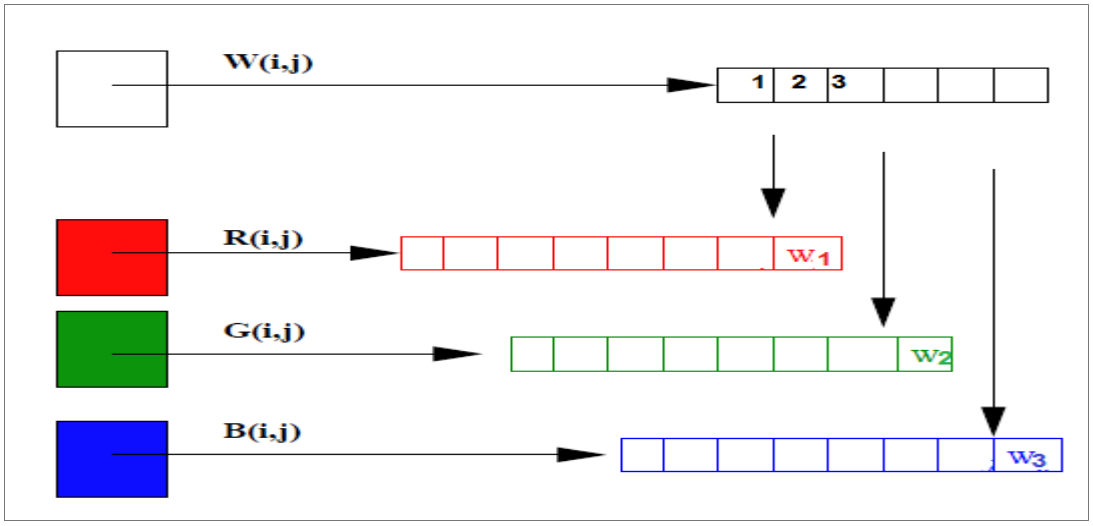


Figure III. 5: Algorithme d'insertion

III.7 Algorithme d'extraction :

Entrées :

F_W: Image tatouée (image couleur RGB de taille m × m).

Sortie :

W : la marque (watermark).

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

En cas la marque texte :

- Appliquer la méthode LSB inverse.
- Décrypter la marque avec la même clé secrète.
- Afficher la marque.

En cas la marque image :

- Appliquer la méthode LSB inverse.
- Décrypter la marque avec la même clé secrète.
- Convertir la marque en binaire.
- Afficher la marque.

III.8 Déroulement de L'application :

Pour le cas de l'insertion, l'utilisateur sélectionne l'image qui veut être tatouée par cliquer sur le bouton « Charger votre image ».

Puis ajouter la marque (texte ou image) par saisir le texte dans la zone texte ou charger l'image par cliquer sur le bouton « Charger votre marque ».

Ensuite, pour appliquer la méthode LSB, l'utilisateur cliquer sur le bouton « Tatouer » pour insérer la marque. Après il Enregistre l'image tatouée.

Pour le cas de l'extraction, l'utilisateur charge l'image tatouée lorsqu'il clique sur le bouton « Charger l'image tatouée ». Puis cliquer sur le bouton « Extrait » pour faire l'extraction de la marque insérée et reconstituera l'image originale avec l'utilisation de la méthode LSB inverse.

III.9 Résultat :

Pour évaluer notre application, nous présentons l'exécution de cet exemple :

III.9.1 Phase d'insertion :

L'algorithme d'insertion génère l'mage tatouée en utilisent l'image hôte f et le watermark w.

Il est modalisé par la fonction d'insertion E suivante :

$$f_w = \mathrm{E}(f, w)$$

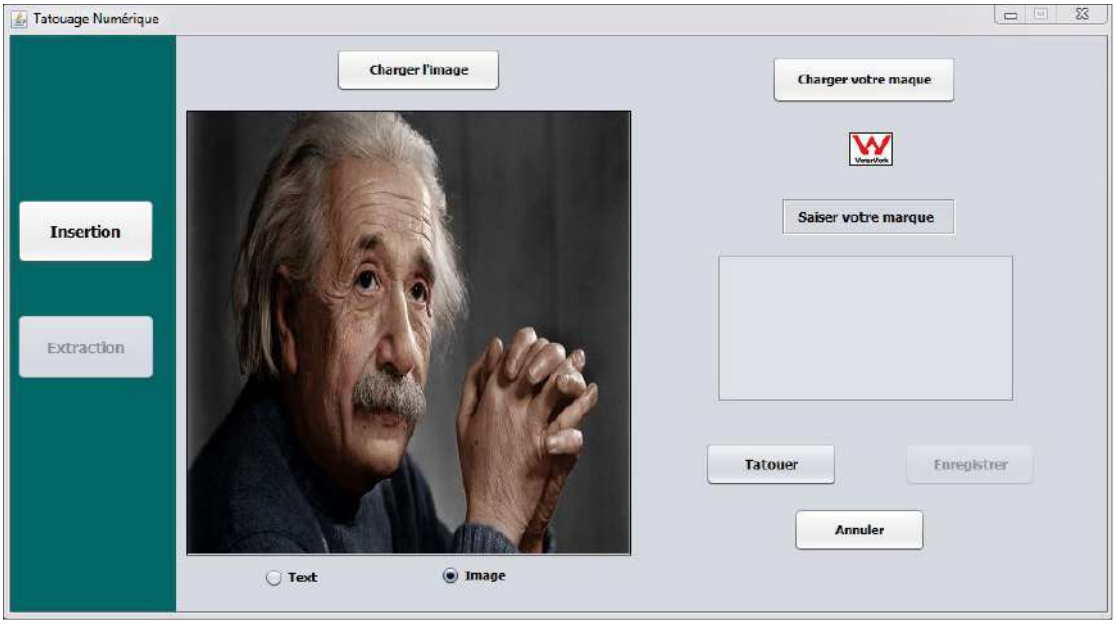


Figure III.6 : Chargement de l'image original et la marque.

Pour insérer la marque dans l'image hôte, on cliquer sur le bouton « Tatouer ». Le résultat obtenu c'est l'image tatouée. (Voir la Figure III.7*)*

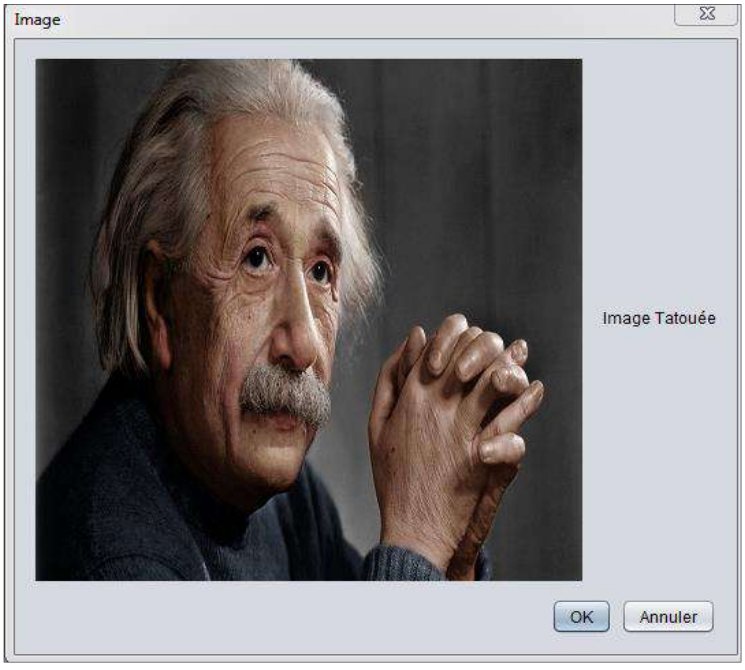


Figure III.7 : Image tatouée.

III.9.2 Phase d'extraction :

Pour vérifier que l'image tatouée est attaquée (Modifiée) ou non, on charger l'image tatouée et extrait la marque insérée

Figure III.8: chargement l'image tatouée.

Si on clique sur le bouton « Extrait » donc notre programme extrait la marque cachée dans l'image tatouée. (Figure III.9)

Figure III.9: Extraire la marque.

Donc la récupération de la marque(watermark) montre que l'image tatouée n'est pas attaquée.

III.10 Evaluation de l'algorithme :

Dans cette partie, nous avons évalué l'efficacité de notre algorithme à la sensibilité de la modification. Pour ceci, nous avons analysé la propriété d'imperceptibilité.

III.10.1 L'imperceptibilité :

Nous avons appliqué notre méthode sur 2 images de type (PNG)et (BMP) de taille 400×400 afin de s'assurer des résultats obtenus. Les images hôtes utilisées pour tester l'imperceptibilité de notre algorithme (Figure III.10) et (Figure III.12) et les images tatouées sont illustrées dans (Figure III.11) et (Figure III.13).

(1) (2)

Figure III.10: Images hôtes PNG

(1_tatouée) (2_tatouée)

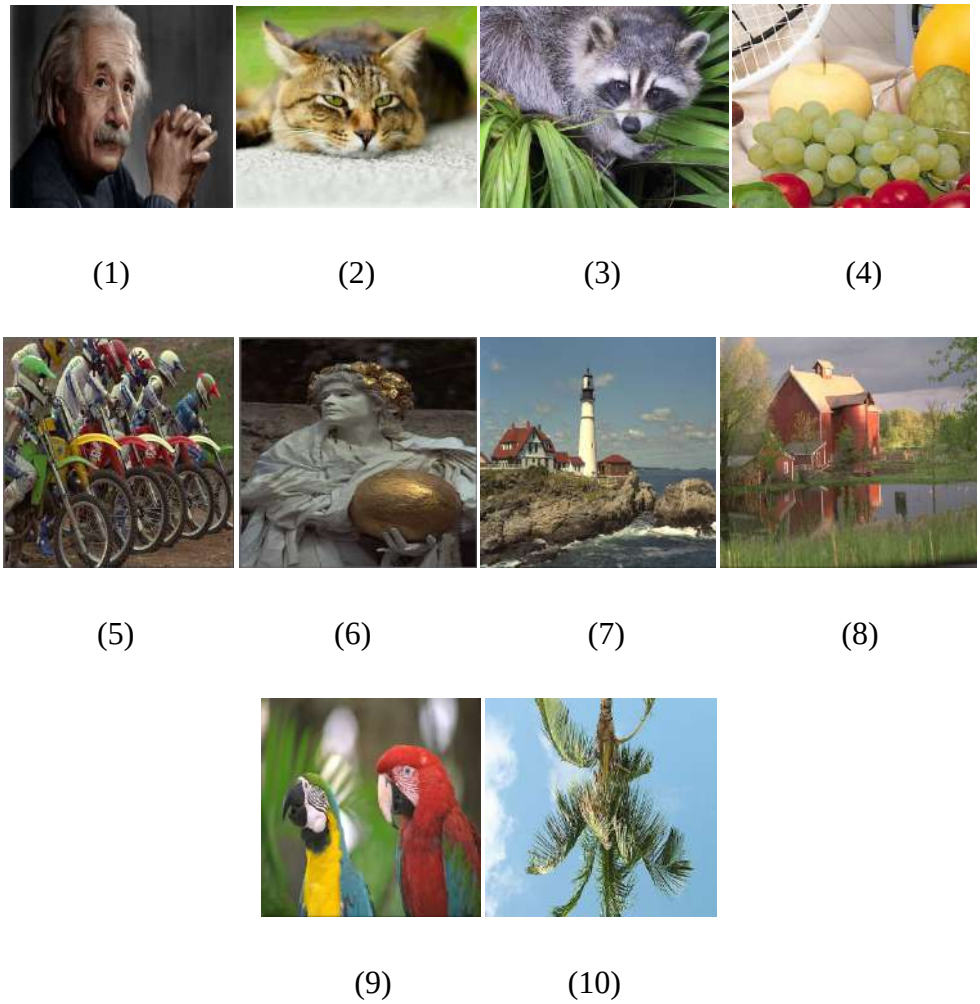
Figure III.11 : Images tatouée PNG

(i) (b)

Figure III.12: Images hôtes BMP

(i_ tatouée) (b _tatouée)

Figure III.13: Images tatouée BMP



(1) (2) (3) (4)

(5) (6) (7) (8)

(9) (10)

Figure III. 14 : Résultats de tatouage pour les images PNG

(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j)

Figure III.15 : Résultats de tatouage pour les images BMP

A partir de dix figures tatouée (dix images PNG, dix images BMP) on peut voir que la dégradation des images tatouées est imperceptible par l'observateur. Le Tableau III.1 présente les valeurs de PSNR.

Image PNG	PSNR(PNG)		Image BMP	PSNR(BMP)	
	Texte	Image		Texte	Image
Image 1	80.50	56.65	Image a	86.96	56.89
Image 2	82.49	56.80	Image b	87.41	56.98
Image 3	82.05	56.92	Image c	86.90	56.96
Image 4	82.33	56.88	Image d	87.07	56.96
Image 5	81.79	56.93	Image e	88.12	56.93
Image 6	83.21	56.97	Image f	86.52	56.96
Image 7	82.10	56.89	Image g	87.49	57.01
Image 8	81.67	56.92	Image h	87.17	56.96
Image 9	82.08	56.97	Image i	88.03	56.93
Image 10	82.38	56.93	Image j	87.53	56.97

Tableau III. 1 : Qualité des images tatouées.

En plus le tableau PSNR aussi clarifier que les valeurs très bonnes, ce qui signifie que notre méthode de tatouage fragile garantir une haute qualité d'images tatouées.

III.10.2 Discussion :

D'après les résultats obtenus on peut dire que :

- Les données d'authentification, sont très sensibles à tout modification.
- La qualité de l'image tatouée est très élevée car seulement les bits LSB de quelques pixels sont changée.
- La perte de la marque sera prise comme une preuve que les données falsifient.

Les résultats obtenus nous permettent de déduire que la méthode du tatouage fragile appliquée est efficace du point de vue à la qualité d'image tatouée.

III.11 Conclusion

Dans ce projet nous avons présenté notre algorithme de tatouage fragile d'images à niveaux de couleur RGB, dans l'objectif est de vérifier l'authentification et l'intégrité des images numériques. Nous concluons que Cette méthodes est performante en termes d'imperceptibilité et de robustesse. Elle est aussi efficace car elle peut extraire facilement le watermark en utilisant seulement l'image tatouée sans nécessité de l'image originale. Les résultats expérimentaux 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.

Conclusion
Générale

Conclusion générale :

A cause des utilisations illicites des documents numériques. Le tatouage numérique a été introduit comme une technique alternative à la cryptographie et efficace pour la protection des images et la vérification de l'intégrité des données. 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 importantes sur ce sujet. Nous avons aussi présenté le tatouage numérique ses contraintes, ses caractéristiques, le processus de l'insertion et celui de l'extraction, et les différents types d'attaques sur les images numériques.

Dans ce mémoire, nous avons appliqué les algorithmes de tatouage fragile d'images à niveaux de couleur basée sur l'utilisation de la méthode LSB, dans l'objectif de vérifier l'authentification et l'intégrité des images numériques.

Les résultats expérimentaux montrent la faisabilité de notre algorithme proposé, et que cette méthode (LSB) 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] **YAOVI GAGOU**, " Cours traitement d'image," dans Université de Picardie Jules Verne, 2008.

[2] Application des Ondelettes pour le Tatouage Numérique des Images, dans UNIVERSITE FERHAT ABBAS DE SETIF - 01, 2015.

[3**] S. Mohanty, N. Ranganathan,** and **K. Namballa**. « VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design ». In17th International Conference on VLSI Design, pages 1063–1068, 2004.

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

[5] **Y. Hu, J. Huang, S. Kwong**, and **Y. Chan**. « Image Fusion Based Visible Watermarking
Using Dual-Tree Complex Wavelet Transform ». InIWDW'2003, pages 86–100, 2003.

[6] Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformées discrètes, UNIVERSITE FERHAT ABBAS-SETIF, 2014.

[7**] Danielle CH AN TEGREL**, " *Traitement numérique de l'image,* " Académie de Poitiers, 2004.

[8] TATOUAGE FRAGILE DES IMAGES NUMERIQUES, dans UNIVERSITE MOHAMED BOUDIAF-M'SILA, 2017.

[9] « http://membres.lycos.fr/compressions/menua.html », Octobre 2002.

[10] Tatouage numérique robuste (watermarking) par LSB (Least Significant Bit), dans Université de Kasdi Merbah Ouargla, 2015.

[11] http://www.eclairement.com/Image-numerique-quel format.2007.

[12] D. Lingrand. *Introduction au traitement d'images*. Vuibert, 2008.

[13] **D. Zheng, Y. Liu, J. Zhoa,** and **A. Saddik**. « A survey of RST Invariant Image Watermarking Algorithms. »ACM Computing Surveys, 39(2), 2007.

[14] Tatouage numérique des images couleurs RGB. Dans UNIVERSITE ELHADJ LAKHDER – BATNA.

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

[16] **K. Tanaka, Y. Nakamura,** and **K. Matsui**. « Embedding Secret Information into a Dithered »Multilevel Image ». In1990 IEEE Military Communications Conference, pages 216–220, 1990.

Bibliographie

[17] A. **Tirkel, G. Rankin, R. Schyndel, W. Ho, N. Mee,** and **C. Osborne**. « Electronic Watermark ». In DICTA 1993, pages 666–672, 1993.

[18] Jean **Luc Le Luron**. « Les images numériques, généralités ». 2003.

[19] **I. Cox** and **M Miller**. A Review of Watermarking and the Importance of Perceptual Modeling. In *Electronic Imaging'97*, 1997.

[20**] D. Kundur** and **D. Hatzinakos**. Digital Watermarking Using Multiresolution Wavelet Decomposition. In *IEEE International Conference on Acoustics, Speech and Signal Processing, Seattle, Washington*, volume 5, pages 2969–2972, 1998.

[21] F. **Petitcolas, R. Anderson,** and **M. Kuhn**. Information Hiding Terminology: A Survey. *IEEE Signal Processing*, 78(7) :1062–1078, 1999.

[22] Chun-**Shien Lu**. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, 2005.

[23] Le Marquage Et La Propriété Intellectuelle, **Michel Blanchard**, 2003.

[24] 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.

[25] **K. LOUKHAOUKHA** "Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective, " mémoire de doctorat, Faculté des études supérieures, Université Laval, QUÉBEC, 2010.

[26] I. **Cox, M. Miller,** and **J. Bloom**. Digital Watermarking: Principles & Practices. Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.

[27] I. **Cox and M. Miller**. The first 50 years of electronic watermarking. EURASIP Journal on Applied Signal Processing, 2002(2):126–132, 2002.

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

[29] http://www.crdp.ac-grenoble.fr/image/general/general.htm.

[30] R**. ISDANT**, « Traitement numérique de l'image », 2009.

[31] P. **Singh, R.S. Chadha**, "A Survey of Digital Watermarking Techniques, Applications and Attacks, "IJEIT, Volume 2, Issue 9, March 2013.

[32] P. **LIPIŃSKI**, "On domain selection for additive, blind image watermarking," Institute of Information Technology, University of Lodz, Pologne, 2012.

[33] E. **Muharemagic, B. Furht**, "Survey of Watermarking Techniques and Applications," Department of Computer Science and Engineering, Florida Atlantic University, USA, 2010.

Bibliographie

[34] Etude et implémentation des techniques de tatouage numérique, UNIVERSITE DJILLALI LIABES, 2017.

[35] Tatouage numérique fragile pour l'authentification d'images, UNIVERSITE DE KASDI MERBAH OUARGLA ,2015.

[36] 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.

[37] S**. Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, and J. Su**. Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks. IEEE CommunMag, 39(9) :118–126, 2001.

[38] Mr. **F. ZEHDA,** " Tatouage d'images basé sur des transformées discrètes entières," thèse magister, département d'électroniques, université Sétif, Algérie, 2014.

[39] **T. Chai R. et R. Draxler**," Root mean square error (RMSE) or mean absolute error (MAE)? –Arguments against avoiding RMSE in the literature," in Geosci, 2014.

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

[41] 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.

[42] **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.

[43] Tatouage d'images par la décomposition en valeurs singulières et la transformée en cosinus discrète, dans UNIVERSITE MOHAMED BOUDIAF - M'SILA,2017.

[44] **A.M. Alattar**, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. Image Process., vol.13, no. 8, pp. 1147–1156, Aug. 2004.

[45] **D. Coltuc and A. Tremeau, E. J. Delp** and **P. W. Wong, Eds**., Simple reversible watermarking schemes, in Proc. SPIE: Security, Steganography, Watermarking Multimedia Contents VII, pp.561–568,2005.

[46] **S. Bekkouche, A. Chouarfia**. Mammography Image Authentication: A Comparison of Combined Watermarking Techniques Based on Reversible Watermarking and CDMA in Frequency Domain, International Journal of Network and Mobile Technologies, Volume 3, Issue 1, Hong Kong, January2012.

[47] **HugusBersini**, La programmation orientée objet Cours et exercices en UML 2, avec Java 5, C# 2, C++, Python, PHP 5 et LINQ.