



REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHÉMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et télécommunication

Par :

BENDJAZIA Fatima
Belgacem Aicha
Sur le thème

Protection des données multimédia dans un réseau non sécurisé avec le tatouage numérique

Soutenu publiquement le 03 / 10 / 2021 à Tiaret devant le jury composé de :

Mme LAARADJ Zohra	Grade Maitre de conférences	Président
Mr SI ABDELHADI Ahmed	Grade Maitre de conférences	Examineur
Mr BENDAOUD Mebarek	Grade Professeur	Co-encadreur
Mr OUAMRI MOKHTAR	Grade Maitre de conférences	Encadreur

2020-2021

Remerciements

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 oublier nos familles pour leur contribution, leur soutien, leur patience et leurs encouragements,

Nous tenons à remercier Mr. Ouamri Mokhetar 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 IBN KHALDOUN de TIARET 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.

Dédicaces

Je dédie ce travail à ma chère maman Bendjazia Zohra, j'espère que vous trouverez ici toute ma gratitude, pour m'avoir Soutenu tout au long de mes études.

A ma chère frère Khaled et toutes mes sœurs surtout ma chère sœur Hanan que dieu les protège

A tous mes collègues de la promo 2017/2018

A tous mes êtres chers.

A tous ceux que j'aime.

Bendjazia Fatima

Je dédie ce travail A mes chers parents, Pour tous leurs sacrifices,

Leurs amours, leur soutien et leurs prières tout au long de mes études.

A mes chers frères et mes sœurs pour leurs encouragements et leur soutien.

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

Je vous dis merci

Belgacem Aicha

Liste des Abréviations

DCT :	Discrete Cosine Transform.
JPEG :	Joint Photographic Experts Group.
PPI :	Pixels Par Pouce.
DPI :	Dots Per Inch.
RGB	(RVB) : Red- Green- Bleu (Rouge, Vert, Bleu)
CMJN	(CMYB) : Cyan Magenta Jaune Noir (Cyan-Magenta-Yellow-Black)
BMP :	Bit Bap
GIF :	Graphical Interchange Format .
TIFF :	Tagged Image File Format.
DWT :	Discrete Wavelet Transform.
DFT :	Discrete Fourier Transform.
MATLAB :	Matrix Laboratory
MSE :	Mean Squared Error
PSNR :	Peak Signal to Noise Ratio (Rapport signal sur bruit de crête)

Résumé

Dans les environnements de réseau non sécurisés, la protection de la propriété des contenus numériques multimedia, tels que les images et videos numeriques, devient une préoccupation croissante. Différentes méthodes de tatouage ont été proposées pour assurer la protection des droits d'auteur et l'authentification de contenus numériques..

La solution préférée est l'utilisation du tatouage fragile. L'objectif de notre travail est d'implémenter une application du tatouage fragile des images codée qui vise à insérer et extraire un watermark avec une clé secrète, cette méthode est basée sur l'utilisation de la transformée en cosinus discrète (DCT).

Mots clés : tatouage numérique, tatouage fragile, authentification DCT

Abstract

In unsecured network environments, protecting the ownership of multimedia digital content, such as digital images and videos, is becoming an increasing concern. Various watermarking methods have been proposed to ensure copyright protection and authentication of digital content.

The preferred solution is the use of fragile watermarking. The objective of our work is to implement an application of the fragile watermarking of coded images that aims to insert and extract a watermark with a secret key, this method is based on the use of the discrete cosine transform (DCT).

Keywords: digital watermarking, fragile watermarking, DCT authentication

الملخص :

في بيئات الشبكات غير الآمنة ، أصبحت حماية ملكية المحتوى الرقمي للوسائط المتعددة ، مثل الصور الرقمية ومقاطع الفيديو ، مصدر قلق متزايد. تم اقتراح طرق مختلفة للعلامات المائية لضمان حماية حقوق التأليف والنشر والمصادقة على المحتوى الرقمي.

الحل المفضل هو استخدام العلامات المائية الهشة. الهدف من عملنا هو تنفيذ تطبيق للعلامات المائية الهشة للصور المشفرة التي تهدف إلى إدخال واستخراج علامة مائية بمفتاح سري ، وتستند هذه الطريقة على استخدام تحويل جيب التمام المنفصل (DCT).

الكلمات الرئيسية: العلامات المائية الرقمية ، العلامات المائية الهشة ، مصادقة

Liste des figures

Figure 1.1 :1839 : Photographie (Louis Jacques Mandé Daguerre) I 1895 : cinématographe. (frères Lumière) I 1885 : rayons X (Röntgen) [4].....	5
Figure 1.2 : Schéma d'un système de traitement d'images [2]	6
Figure 1.3: Représentation d'une image numérique	7
Figure 1.4 : Images matricielles (Bitmap) composées de pixels.[6]	8
Figure 1.5 : Image vectorielle.	8
Figure 1. 6 : Groupe de pixel formant la lettre A.....	9
Figure 1.7 : Représentation d'un pixel.	9
Figure1. 8 : La taille d'image (nombre de pixels) divisé par 4 [5].....	10
Figure 1.9: Résolution d'une image.	10
Figure 1.10 : Les bornes de répartition des niveaux de gris [4].....	11
Figure 1. 11: Deux images différentes avec même histogramme[4].....	11
Figure 1.12: Exemple de luminance	12
Figure 1.13 : Exemple de Contraste [2].....	12
Figure 1. 14 : Exemple image binaire	13
Figure 1.15 : Variation de nombres de niveau de gris pour même image.....	13
Figure 1.16 : image aux niveaux de gris.....	14
Figure 1. 17 :Principe additif des couleurs R.V.B	14
Figure 1.18 : les systèmes de codage des couleurs	15
Figure 1.19 : Synthèse additive des couleurs.....	15
Figure1. 20 : Synthèse soustractive des couleurs.....	16
Figure 1.21 : Différents formats d'image et quand les utiliser	17
Figure 2.1: Modèle générique d'un système du tatouage.....	20
Figure 2.2:Schéma général de l'insertion d'une Marque.....	20
Figure 2.3: Schéma général d'extraction invisible d'une marque	21
Figure 2 .4(a) : Tatouage visible	23
Figure 2.5(b) : Tatouage invisible	23
Figure 2.6: Les Contraintes de tatouage d'image	23
Figure 2.7: Les différentes attaques utilisées en stéganalyse.....	27
Figure 2.8: Application d'un fenêtrage après rotation de l'image	31

Figure 3.1 : Exemple d'une transformée dct d'une matrice de pixels de pixels 8×8.....	34
Figure 3.2: les sous images produites par les coefficients fréquentiels.....	34
Figure 3.3: La bande de coefficients (haute fréquences) visé par le marquage.	35
Figure 3.4: Les entrées/sorties de l'étape d'insertion de la marque	35
Figure 3.5: Découpage en blocs de 8×8 éléments.....	36
Figure 3.6 : Les entrées/sorties de l'étape d'extraction de la marque	37
Figure 3.7: L'organigramme de l'algorithme l'insertion.....	39
Figure 3.8: L'organigramme de l'algorithme l'extraction.....	40
Figure 3.9: L'interface4 d'insertion	41
Figure 3.10: Chargement de l'image original	42
Figure 3.11: Chargement de la marque	42
Figure 3.12: Entremet de paramètres.....	43
Figure 3.13: Resultat finale.....	43
Figure 3.14:L' interface extraction.....	44
Figure 3.15: Charger les paramètres de l'extraction	44
Figure 3.16: Chargement de l'image tatoué.....	45
Figure 3.17: Chargement d'image hôte	45
Figure 3.18: Résultat obtenue la marque extrait	46
Figure 3.19: Images hôtes PNG	47
Figure 3.20: Résultats de t<atouage : image hôte, image tatouée, la marque.....	48
Figure 3.21 : La valeur absolue de différence entre l'image hôte et l'image tatouée	48
Figure 3.22: Résultat de l'extraction après l'attaque de filtre median	52
Figure 3.23 Resultat de l'extraction après l'attaque de bruitage.....	52
Figure 3.24 : Résultat de l'extraction après l'attaque de rotation.	53

Liste des tableaux

Tableau 1 : Qualité des images atouées.....	51
--	----

TABLE DES MATIERES

CHAPITRE –I–

Généralités sur le traitement d'images

Introduction générale	2
1.1 Introduction	5
1.2 Définition de l'image	5
1.2.1 Images numérique	5
1.2.2 Les images matricielles	6
1.2.3 Les images vectorielles	6
1.2.3 La différence entre images matricielles et vectorielles	6
1.4 Système de traitement d'images	6
1.4.1 L'acquisition	7
1.4.2 Le pré traitement	7
1.4.3 L'analyse	8
1.4.4 L'Interprétation	8
1.5 Caractéristiques d'une image numérique	9
1.5.1 le pixel	9
1.5.2 Voisinage de pixels	9
1.5.3 Résolution d'une image	10
1.5.4 Poids d'une image	10
1.5.5 Histogramme	11
1.5.6 Luminance :	11
1.5.7 Contraste :	12
1.6 Les différents types d'images numériques :	12
1.6.1 Les images binaires :	13
1.6.2 Image à niveaux de gris :	13
1.6.3 Image couleur	14
1.6.3.1 Synthèse couleur : le système RGB :	15
1.6.3.2. Synthèse soustractive : les systèmes CMY et CMYK :	16
1.7 Formats d'image numérique :	16
1.7.1 BMP (BitMaP)	16
1.7.2 GIF (Graphical Interchange Format)	16

1.7.3 TIFF (Tagged Image File Format).....	16
1.7.4 JPEG	17
1.8 Conclusion :	17

CHAPITRE –II–

Tatouage des images numériques

2.1 Introduction.....	19
2.2 Présentation du tatouage numérique.....	19
2.3 Définition du tatouage numérique	19
2.4 Différences avec la cryptographie	19
2.5 Schéma général du tatouage numérique des images :	20
2.5.1 Phase d'insertion :	20
2.5.2 Phase d'extraction :	21
2.6 Types de tatouage d'image :	21
2.6.1 Les tatouages robustes :	22
2.6.2 Les tatouages fragiles :.....	22
2.6.3 Les tatouages semi-fragiles :	22
2.7 Les techniques du Tatouage :.....	22
2.7.1 Tatouage visible:.....	22
2.7.2 Tatouage invisible:.....	23
2.8 - Contraintes du tatouage d'image :.....	23
2.8.1 Imperceptibilité:.....	24
2.8.2 Capacité :	24
2.8.3 Robustesse :	24
2.8.4 Sécurité :	25
2.9 Domaine d'insertion :	25
2.9.1 Domaine spatial :	25
2.9.2 Domaine fréquentiel :	25
2.10 Utilisation du tatouage :.....	25
2.10.1 Protection du droit d'auteur :	25
2.10.2 Authentification de documents :.....	26
2.10.3 Protection de Copie :.....	26

2.10.4 Indexation.....	26
2.11 Les Attaques.....	26
2.11.1 Traitements bienveillants	27
2.11.1.1 La compression.....	27
2.11.1.2 Les filtrages	28
2.11.1.3 Les transformations géométriques usuelles : changement d'échelle, fenêtrage et rotation.....	28
2.11.1.4 Les conversions numériques/analogiques	28
2.11.1.5 Les modifications colorimétriques.....	29
2.11.2 Traitements malveillants	29
2.11.2.1 Les attaques simples.....	30
2.11.2.2 Les attaques "anti-détection"	30
2.11.2.3. Les attaques d'ambiguïté.....	31
2.12 Conclusion.....	31

CHAPITRE –III–

Authentification d'images numériques par tatouage fragile

3.1 Introduction :	33
3.2 Méthode DCT :	33
3.3 Schémas de tatouage fragile:.....	35
3.3.1 Approche d'insertion	35
3.3.2 Approche d'extraction	37
3.4 L'organigramme de l'algorithme	39
3.4.1 l'insertion	39
3.4.2 l'extraction	40
3.5 Résultat	40
3.5.1 Les outils de développement	40
3.5.2 Interface graphique implémentée	41
3.5.2.1 Interface d'insertion	41
3.5.2.2: Interface l'extraction.....	44
3.6 Evaluation visuelle de l'approche:	46
3.6.1 MSE : (Mean Square Error) :	48
3.6.2 PSNR :	48
3.6.3 SSIM	49

3.6.4 : Fragilité vis-à-vis les attaques	51
3.6.4.1 : Filtre médian.....	51
3.6.4.2 Bruitage	52
3.6.4.3 Rotation	53
3.7 Conclusion.....	55
Conclusion générale	55
Références bibliographique	57



Introduction générale

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

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

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

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

L'image est un élément qui figurent dans plus documents multimedia visuels comme la video numerique ou les fichiers Portable Document Format (PDF), et est utilisée énormément dans notre vie quotidienne. C'est pour cette raison que nous avons choisi l'image parmi tous les fichiers multimedia.

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

Nous nous intéressons dans ce mémoire au tatouage numérique des images et d'implémenter des méthodes basé sur transformée en cosinus discrète (DCT). Cette transformation a été inventée par N. Ahmed en 1974 dans son article appelé "Traitement d'Image et la transformation cosinus discrète".

la DCT range une grande partie de l'énergies de signal dans les basses fréquences; celles-ci apparaissent dans le coin supérieur- gauche du DCT .

Introduction générale

Le présent mémoire est organisé en trois chapitres :

En premier chapitre, nous allons présenter quelques notions de base d'imageries numériques. Dans le deuxième chapitre, nous allons parler de tatouage numérique sous ses variantes types. Et finalement, nous allons présenter l'approche à implémenter en manifestant en dernier ses résultats expérimentaux.

Chapitre – I -

Généralités sur le traitement d'images

1.1 Introduction

Le traitement d'image représente un certain nombre de méthodes et d'algorithmes et d'outils mathématiques appliqués aux images dans le but d'améliorer leur qualité ou d'en extraire une information. On peut citer par exemple : filtrages, amélioration de la qualité des photos en corrigeant les conditions de prise de vues; la reconnaissance d'éléments graphiques, visages, écritures, l'identification de zones cancéreuses en imagerie médicale, la compression JPEG, etc.

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



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

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

1.2 Définition de l'image :

L'image est un ensemble structuré d'informations qui, après affichage sur l'écran, ont une signification pour l'œil humain.

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

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

Mathématiquement, image est un signal bidimensionnel décrit sous la forme d'une fonction $I(x, y)$, tel que x et y sont les coordonnées spatiales d'un point (pixel) de l'image I [1].

1.2.1 Images numérique

Une image numérique est définie comme un signal bidimensionnel échantillonné et quantifié. Elle est constituée de points (pixels), autrement dit, une image est une matrice $M \times N$ de valeurs entières comprises dans un intervalle borné $[0, N_g]$ où N_g est la valeur maximale du niveau de gris comme l'image suivante. [3]

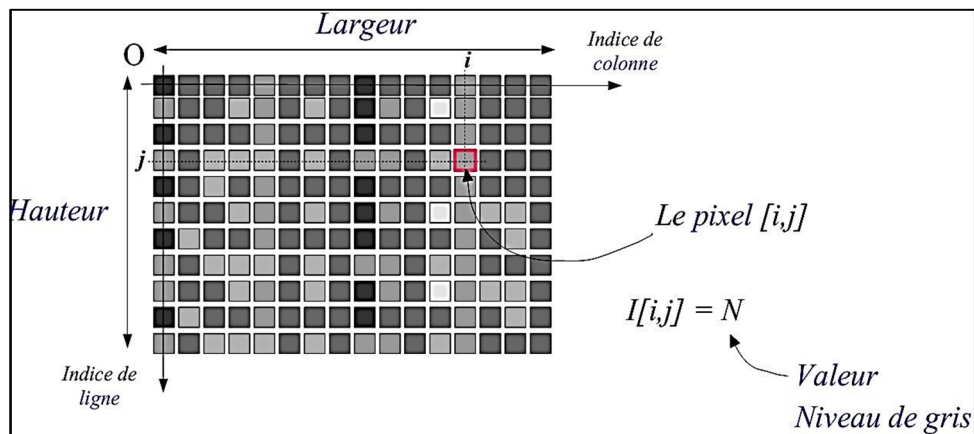


Figure 1.2: Représentation d'une image numérique

Exemples d'images numériques :

- Image "web".
- Image d'un film d'animation.
- Sortie des appareils photos et caméscopes numérique

1.2.2 Les images matricielles :

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

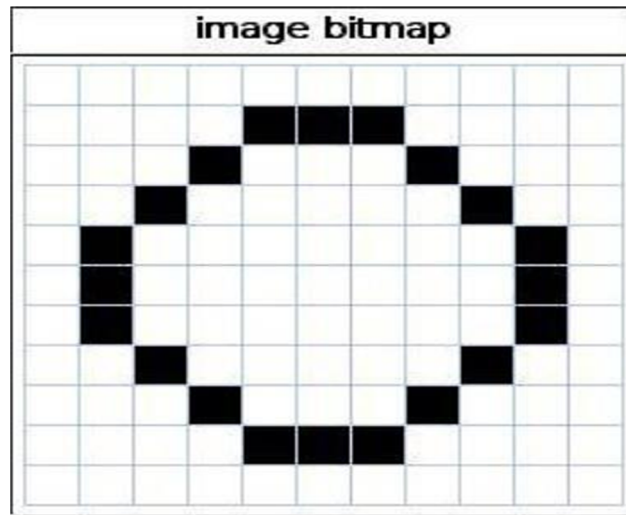


Figure 1.3: images matricielles (Bitmap) composées de pixels.[6]

1.2.3 Les images vectorielles :

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

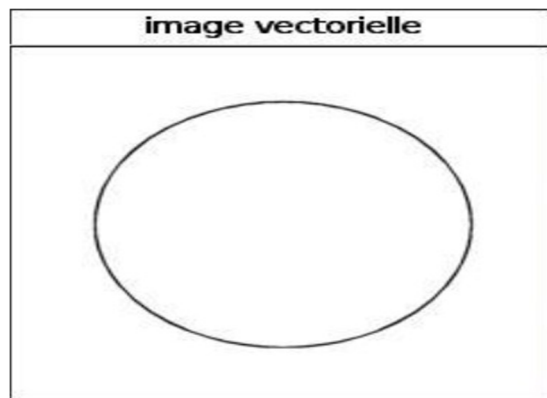


Figure 1. 5: image vectorielle

1.3 La différence entre images matricielles et vectorielles :

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

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

1.4 Système de traitement d'images

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

1.4.1 L'acquisition

L'acquisition est la première étape dans le système de traitement d'images, à partir de laquelle une image numérique est produite, elle consiste en deux étapes l'échantillonnage et le codage. L'échantillonnage correspond au décodage de signal en pixels et le codage correspond à la quantification de l'intensité de chaque pixel en une valeur numérique appelée niveau de gris.

1.4.2 Le pré traitement

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

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

1.4.3 L'analyse

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

1.4.4 L'Interprétation

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



Figure 1.4: Schéma d'un système de traitement d'images [2]

1.5. Caractéristiques d'une image numérique :

1.5.1 le pixel :

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

La lettre A, par exemple, peut être affichée comme un groupe de pixels dans la figure ci-dessous. [2]

Le nombre total de pixels dans une image égale au nombre de pixels d'une colonne multiplié par le nombre de pixels d'une ligne

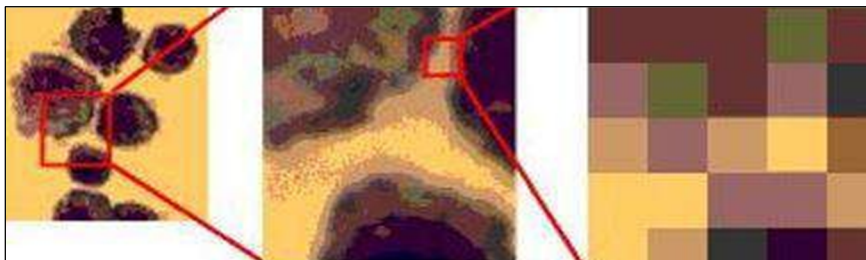


Figure 1.6: Représentation d'un pixel.

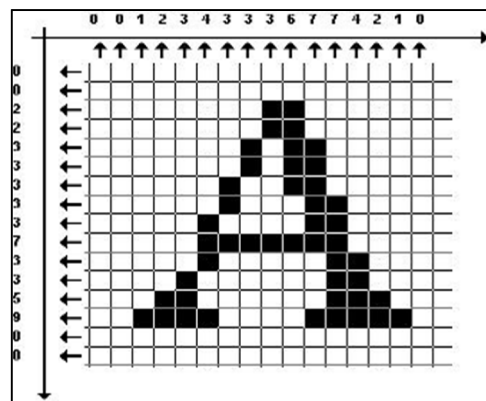


Figure 1.7: groupe de pixel formant la lettre A

1.5.2 Voisinage de pixels :

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

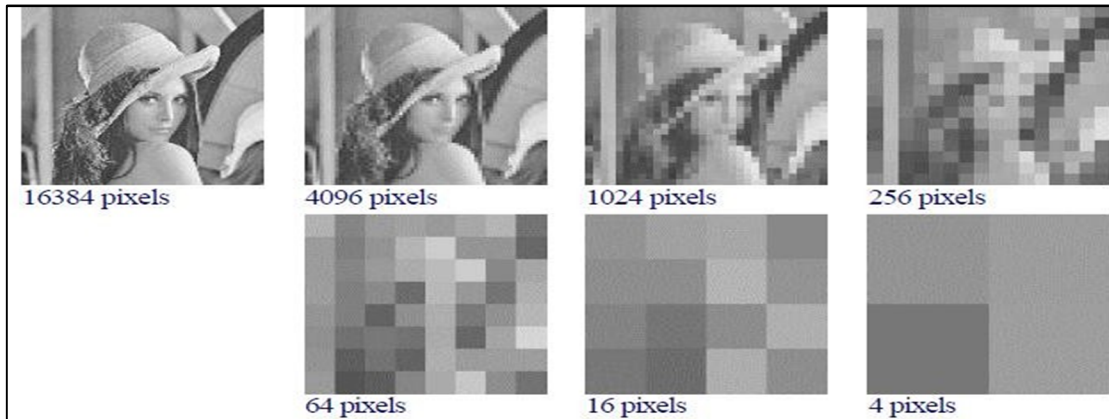


Figure 1.8: la taille d'image (nombre de pixels) divisé par 4 [5]

1.5.3 Résolution d'une image :

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

Les points d'une image ont différents noms dépendant du média. Sur les écrans on parle de pixel, les médias imprimés parlent de points ou dots. Par conséquent la résolution dans le domaine de l'écran est ppi - pixels per inch (PPP en français : pixels par pouce). La résolution dans le domaine des médias imprimés est dpi - dots per inch.

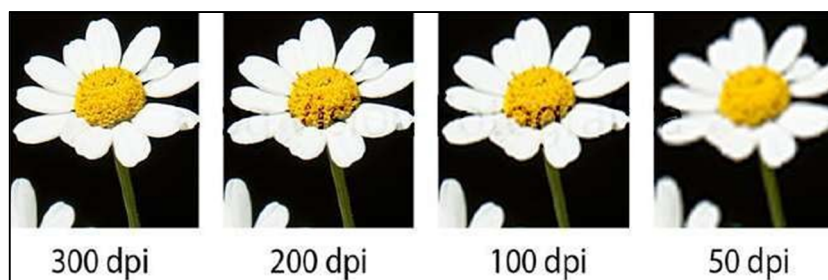


Figure 1.9: Résolution d'une image

1.5.4 Poids d'une image :

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

1.5.5 Histogramme :

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image. Il permet de donner un grand nombre d'information sur la distribution de ces niveaux et de voir entre quelles bornes sont réparties dans le cas d'une image trop claire ou d'une image trop foncée.

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

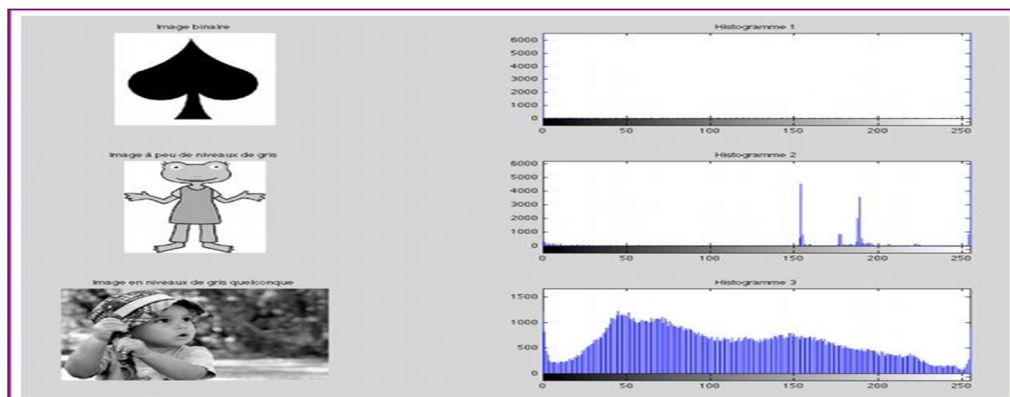


Figure 1.10 : Les bornes de répartition des niveaux de gris [4]

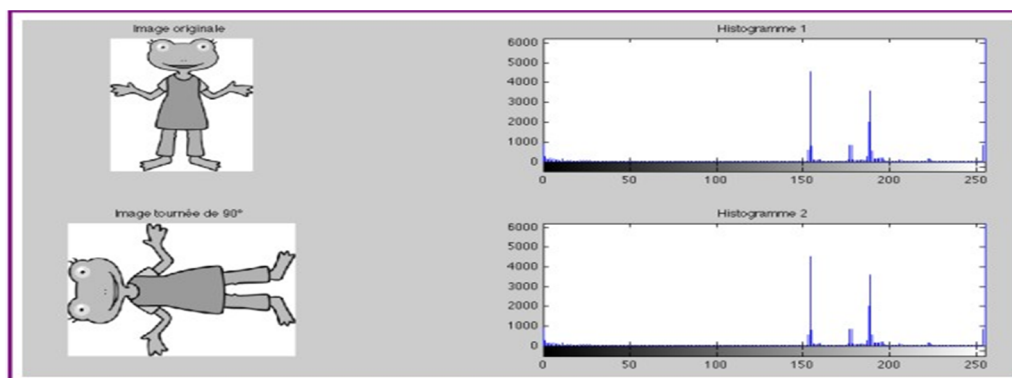


Figure 1.11 : Deux images différentes avec même histogramme[4]

1.5.6 Luminance :

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance.



figure 1.12 : Exemple de luminance

F

1.5.7 Contraste :

C'est l'opposition marquée entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Le contraste est défini en fonction des luminances de deux zones d'images. Si L_1 et L_2 sont les degrés de luminosité respectivement de deux zones voisines A_1 et A_2 d'une image, le contraste C est défini par le rapport : [2]

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



Figure 1.13 : Exemple de Contraste [2]

1.6. Les différents types d'images numériques :

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

1.6.1. Les images binaires :

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

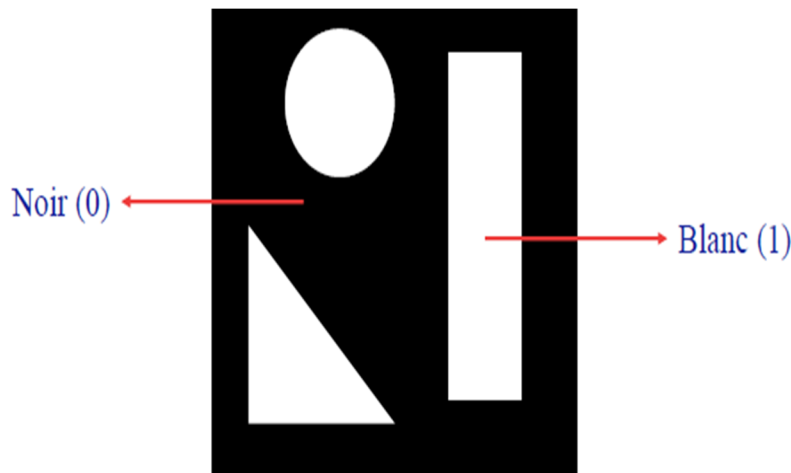


Figure 1.14: Exemple image binaire

1.6.2 Image à niveaux de gris :

Le nombre de niveaux de gris N_g dépend du nombre de bits utilisés pour décrire la valeur de chaque pixel de l'image. Plus ce nombre est important, plus les niveaux possibles sont nombreux $N_g = 2^N$, N est le nombre de bits. Codage sur 8 bits par pixel, correspond à une image de niveaux de gris dont les valeurs sont comprises entre 0 et $2^8 = 256$ possibilités.

Par convention, la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur maximale N_g le blanc (intensité lumineuse maximale).

Sachant que l'œil humain perçoit en moyenne 200 niveaux d'intensité, une échelle de gris de 256 valeurs (8 bits par pixel), suffit à représenter un dégradé qui semblera uniforme, selon l'image suivant. [4]



Figure1.15 : Variation de nombres de niveau de gris pour même image

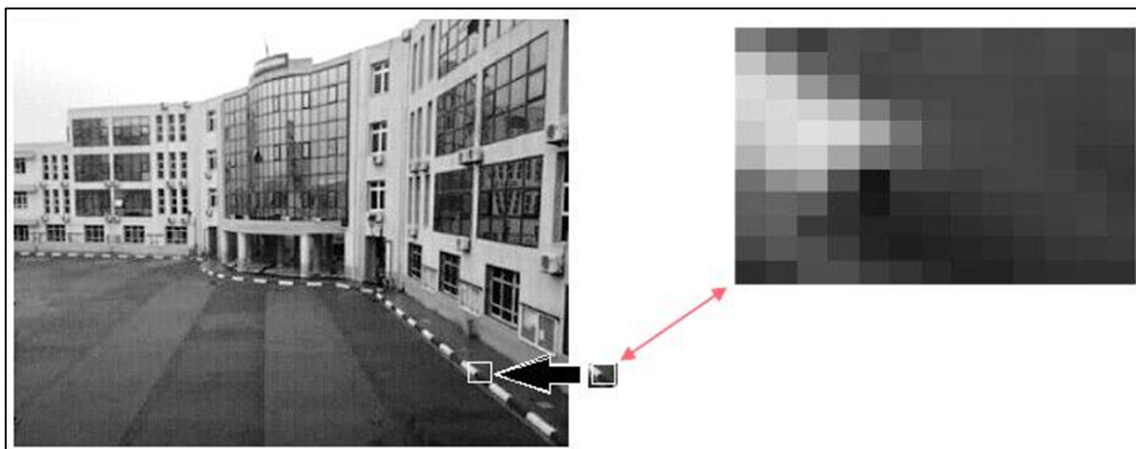


Figure1.16 : image aux niveaux de gris.

1.6.3 Image couleur

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

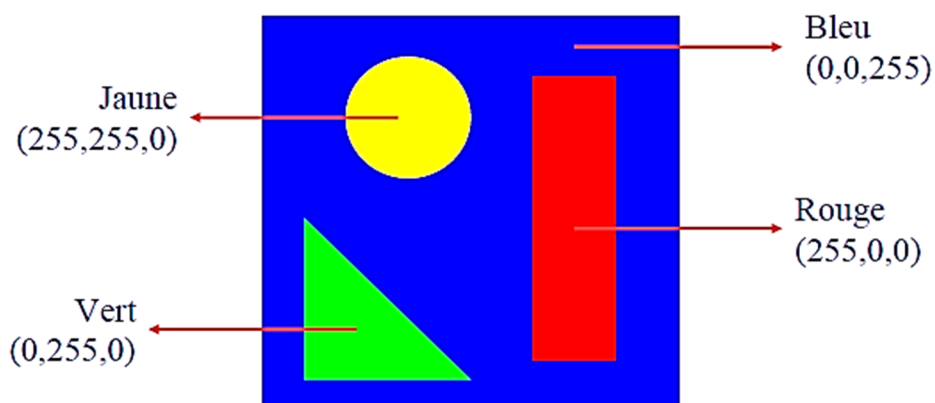


Figure 1.17 : Principe additif des couleurs R.V.B

On peut classer les codes de couleurs dans deux catégories : les codes couleurs destinées

à l'impression selon le mode soustractif (CMJN et PMS) et les couleurs destinées aux écrans selon le mode additif (RVB et HEX). Comme le montre la figure (1.18)

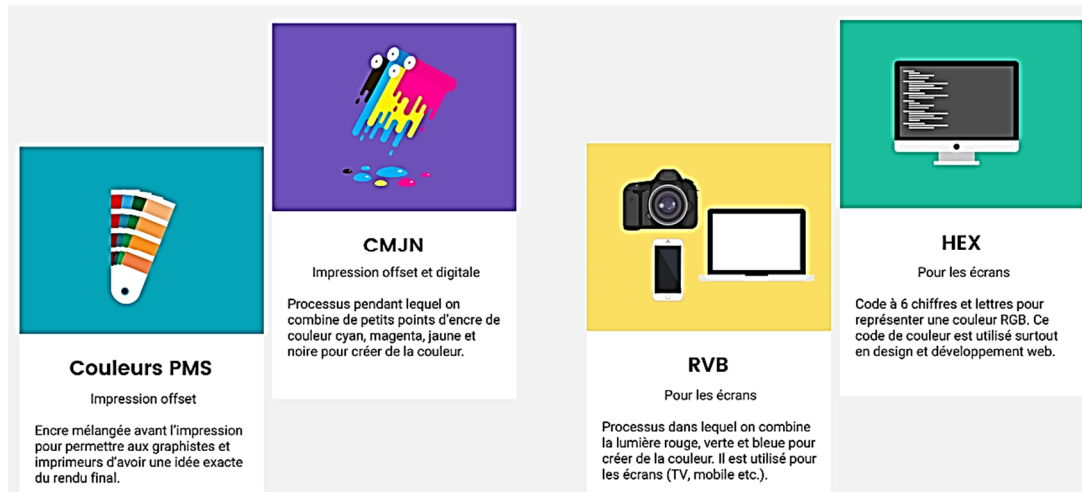


Figure 1.18 : les systèmes de codage des couleurs

Les deux codages couleur, les plus connus du grand public est le système RGB et CMYK

- CMYK pour faire référence au CMJN français.
- RGB qui correspond à RVB en français

1.6.3.1 Synthèse couleur : le système RGB :

Le système de couleurs RGB est un mélange de couleurs additif. Il est utilisé pour les systèmes à lumières émettrices, par exemple les téléviseurs, écrans ou appareils numériques se traduit par (figure 1.19). [7]

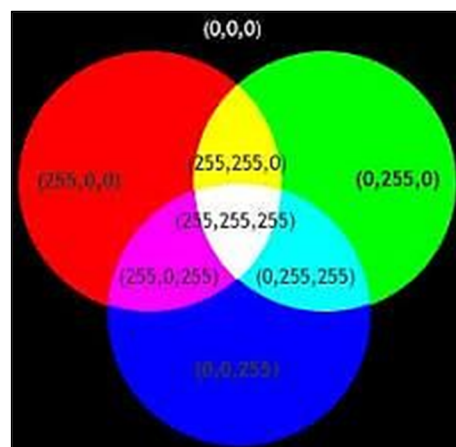


Figure 1.19 : Synthèse additive des couleurs

1.6.3.2 Synthèse soustractive : les systèmes CMY et CMYK :

Les couleurs CMYK comprennent le cyan (C), le magenta (M) et le jaune (Yellow : Y). Le K représente le noir. Le spectre CMY est un mélange de couleur soustractif. Le noir est ajouté afin d'obtenir une meilleure profondeur lumineuse et de meilleurs contrastes. Les couleurs CMYK, connues également sous le nom d'échelle des couleurs ou Euro-échelle, sont utilisées pour la reproduction des couleurs dans l'impression. comme montre La figure ci-dessous.



Figure 1.20 : Synthèse soustractive des couleurs.

1.7 Formats d'image numérique :

1.7.1 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.

1.7.2 GIF (Graphical Interchange Format) :

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

1.7.3 TIFF (Tagged Image File Format) :

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

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

1.7.4 JPEG :

Ce format est l'un des plus complexes, son étude complète nécessite de solides bases mathématiques, cependant malgré une certaine dégradation, il offre des taux de compressions plus qu'intéressants. JPEG est la norme internationale (ISO 10918-1) relative à la compression d'images fixes, notamment aux images photographiques. La méthode de compression est "avec pertes" et s'appuie sur l'algorithme de transformée en cosinus discrète DCT. Un mode "sans perte" a ensuite été développé mais n'a jamais été vraiment utilisé. Cette norme de compression a été développée par le 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'œil humain[28]

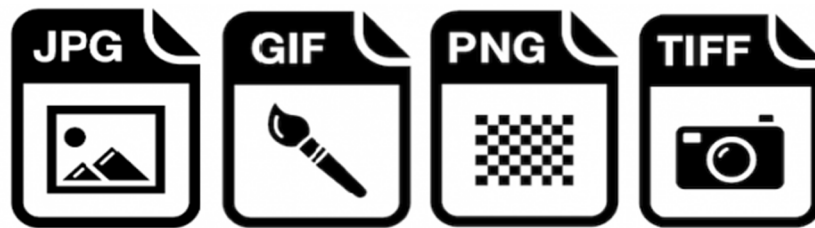


Figure 1.21 : Différents formats d'image et quand les utiliser.

1.8 Conclusion :

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

Chapitre – II -

Tatouage des images numérique

2.1 Introduction :

Les médias numériques sont aujourd'hui le besoin des gens en remplaçant les médias papier. Comme la technologie s'est développée, les numériques ont besoin d'être protégés lors de leur transfert sur Internet ou sur d'autres supports. Les techniques de tatouage ont été développées pour répondre à cette exigence. Ce chapitre vise à fournir une étude bibliographique de toutes les techniques de tatouage.

Nous présenterons les différentes applications possibles du tatouage numérique pour les images à la fin de ce chapitre et nous présenterons brièvement l'évaluation en termes d'imperceptibilité et de robustesse des schémas de tatouage numérique des images.

2.2 Présentation du tatouage numérique :

Le tatouage numérique (digital watermarking) est une technique qui consiste à insérer des informations numériques appelé marque ou signature (watermark) de manière imperceptible et inaltérable dans le même corps d'un autre document numérique.

Le tatouage numérique est considéré depuis quelques années comme une solution pour de nombreuses applications telles que la protection des droits d'auteur, l'intégrité des données multimédias, la prévention de la redistribution non autorisée, l'indexation et le renforcement du contenu.

2.3 Définition du tatouage numérique :

Le tatouage numérique ou watermarking est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. [28]

Le message inclus dans le signal hôte, généralement appelé marque ou bien simplement message, est un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant du créateur, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le signal hôte. [28]

2.4 Différences avec la cryptographie :

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

La stéganographie se définit comme l'art de cacher une information dans un support. Deux types d'approches sont envisageables. La première consiste à cacher l'information à protéger à l'intérieur d'un autre document par approches nommées Data hiding. La seconde

méthode d'utilisation de la stéganographie est d'intégrer la marque dans le document traité. Cette dernière est appelée Tatouage ou Watermarking.

2.5 Schéma général du tatouage numérique des images :

Le tatouage comporte deux phases fondamentales :

- Phase d'insertion.
- Phase d'extraction

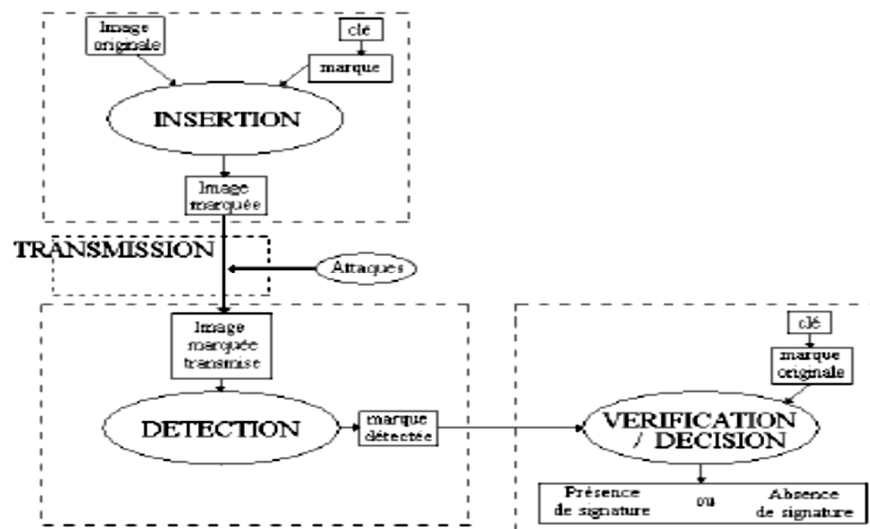


Figure 2.1 : Modèle générique d'un système du tatouage. [5]

2.5.1 Phase d'insertion :

Les entrées de l'insertion de tatouage sont la marque, l'image hôte et des paramètres de tatouages qui vont former la clé. La marque peut prendre la forme d'une séquence de nombres/caractères, une suite 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 réduites à l'image tatouée. [28]

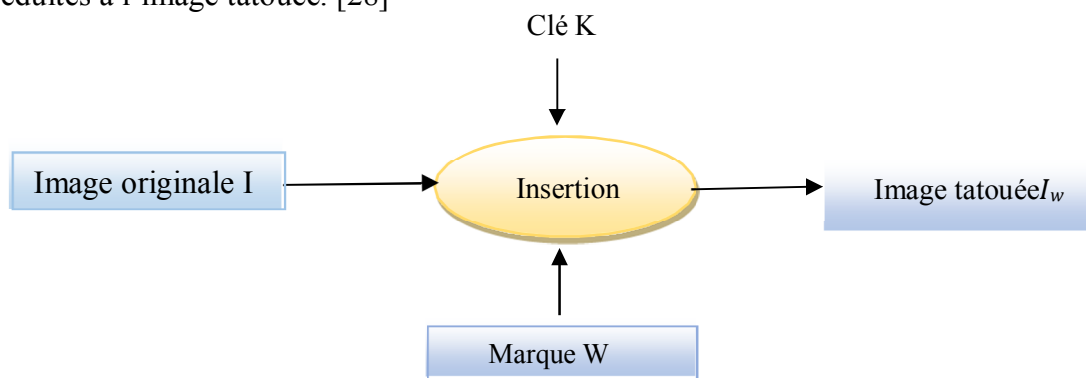


Figure 2.2 : Schéma général de l'insertion d'une marque.

La figure 2.2 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 .

2.5.2 Phase d'extraction :

Quant à l'étape de l'extraction de la marque, les entrées sont l'image tatouée, les paramètres de l'extraction et l'image hôte et la marque originale selon l'approche optée. Aussi, il existe des schémas l'extracteur n'exige pas la disponibilité de la copie originale comme le cas de tatouage invisible.

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 l'image ou non en utilisant une fonction de corrélation ou une autre règle d'identification. 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/ou l'authentification.

La marque est considérée comme robuste si elle est intégrée de manière que la marque peut rester robuste et stable même si les données tatouées passé par différentes modifications. La procédure de l'extraction est indiquée par la formule comme suit :

$$W' = \text{extraction}(I_w^*, K)$$

La marque W' doit être détectée à partir de I^* avec/ou sans la connaissance de l'image originale I . Si I_w n'est pas modifiée (attaquée), alors W' correspond exactement à W . La figure 2.3 présentent le schéma général de l'extraction de la marque. [28]

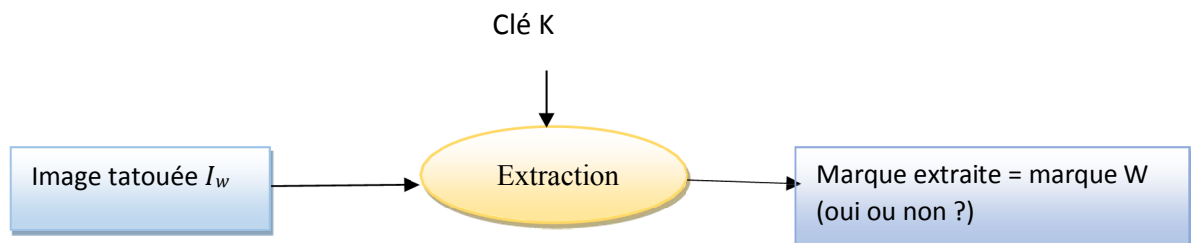


Figure 2.3 : Schéma général d'extraction invisible d'une marque.

2.6 Types de tatouage d'image :

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.

2.6.1 Les tatouages robustes :

Le tatouage robuste permet de rendre possible de déceler la marque du propriétaire de l'image malgré les différentes attaques possibles. Cependant, si le contenu de l'image n'est plus exploitable après un traitement, il n'est plus nécessaire que la marque soit détectée.

2.6.2 Les tatouage 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. [14]

2.6.3 Les tatouage 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. [14]

2.7 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.

La classification selon la visibilité se base sur le fait que la marque insérée doit être vue par l'œil humain ou non.

2.7.1 Tatouage visible

Le tatouage visible est très simple. Il est équivalent à l'estampage d'un watermark sur le papier, et pour cette raison il est appelé parfois estampage numérique.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watermark est visible, alors elle peut être facilement attaquée.

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.



Figure 2.4 : Tatouage visible

2.7.2 Tatouage invisible

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. [15,16]



Figure 2.5 : Tatouage invisible.

2.8 Contraintes du tatouage d'image :

Les performances d'un marquage sont appréciées sous les trois critères suivants : Imperceptibilité, Robustesse, Capacité [17].

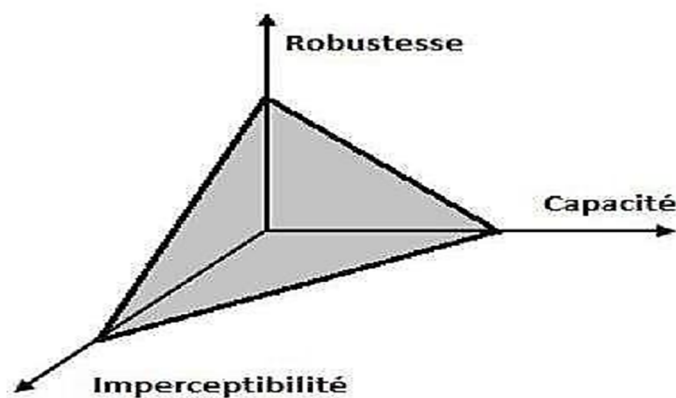


Figure 2.6 : Les Contraintes de tatouage d'image

Il est clair de voir que ces trois critères sont opposés, c'est-à-dire il est impossible d'inventer un système de tatouage numérique qui assure 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 .[18]
- **Coût d'algorithme** : le temps de calcul passe par l'algorithme pour permettre une implémentation en temps réel. [18]

2.8.1 Imperceptibilité :

La notion d'imperceptibilité est liée à la perception visuelle ou auditive des distorsions résultant à l'insertion de la marque dans un document. Le tatouage doit être invisible pour un observateur humain. De plus, la marque insérée ne devrait pas affecter la qualité du document. [17]

L'évaluation de la qualité visuelle ou auditive des documents après le tatouage devient un critère important pour la validation des algorithmes de tatouage. En ce qui concerne les images, une telle évaluation nécessite une analyse du système visuel humain (HVS). Plusieurs mesures objectives ont été proposées dans la littérature pour mesurer la qualité visuelle d'un document tatoué. Une description détaillée des mesures objectives peut être trouvée dans [Nguyen 2011].[17]

2.8.2 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.

2.8.3. Robustesse :

Ce critère représente la résistance ou non de la marque après des modifications subies par les attaques. Aussi Cox et Miller 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. [19]

2.8.4 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 [20].

2.9 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.

2.9.1 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 coûteuses 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. [14]

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. [14]

2.9.2 Domaine fréquentiel :

Les techniques de tatouage numérique qui travaillent dans le domaine fréquentiel sont largement utilisées à cause de leurs robustes face aux divers attaques et leurs complexités. Pour insérer 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). [18]

2.10 Utilisation du tatouage :

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

2.10.1 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).[21]

2.10.2 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. [21]

2.10.3 Protection de Copie :

La protection contre les copies consiste à intégrer au document une marque "intelligente", ou plus précisément un environnement matériel et/ou logiciel capable de communiquer avec la marque. 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. [21]

2.10.4 Indexation :

La marque intégrée au document dépend du contenu de celui-ci. L'algorithme utilisé devra permettre d'intégrer une marque de grande capacité. Par exemple, dans le cadre de la vidéo, la marque pourrait contenir la date d'enregistrement, le titre de la séquence, les noms des personnages ou objets principaux, etc. La marque devra être de grande capacité et invisible. La robustesse est à définir selon l'application mais n'est à priori qu'un problème secondaire. [21]

2.11 Les attaque :

Nous avons vu les différentes possibilités de protection de données, à travers la cryptographie, la stéganalyse et en particulier le tatouage. Une science s'oppose à ces techniques : la stéganalyse. Elle concerne l'étude des attaques. Dans ce paragraphe, nous allons expliquer les différents types d'attaques que nous connaissons et quelques techniques d'applications de celles-ci.

D'un point de vue général, il existe deux types d'attaques :

✓ Les traitements bienveillants ou innocents, parfois considérés aussi comme des attaques de coïncidence, qui sont relatives à de simples traitements de données. Par exemple, pour des images, les opérations de lissage et de compression n'ont pour but que de corriger l'aspect de

l'image ou de la rendre plus facile à transmettre.

✓ Les traitements malveillants ou attaques (en anglais, nous pouvons trouver les termes de "hostile" ou "malicious attacks"), qui peuvent avoir trois actions :

- Effacement de la signature.
- Désynchronisation de la signature.
- Utilisation des faiblesses de l'algorithme de marquage.

En figure 2.7, nous proposons une classification des attaques les plus courantes en tatouage, suivant celle proposée par Voloshynovskiy et al. [4]. Dans les paragraphes suivants, nous allons détailler ces différentes techniques.

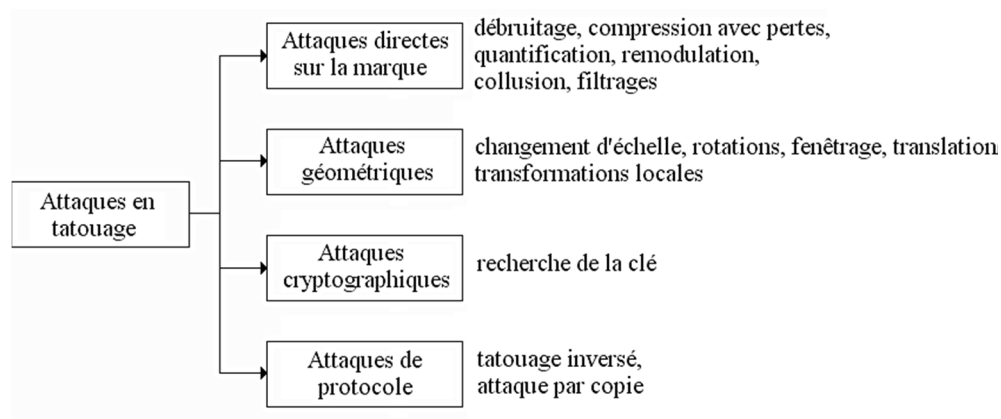


Figure 2.7 : Les différentes attaques utilisées en stéganalyse.

2.11.1 Traitements bienveillants :

Dans ce paragraphe, nous allons étudier les principaux traitements qui pourraient malencontreusement altérer la marque intégrée à des données.

2.11.1.1 La compression :

Il est très classique de compresser une image pour pouvoir faciliter son transfert. Toutefois, la compression JPEG provoque une perte de détails et une apparition de la géométrie des blocs pour des taux de compression élevés. Ce type d'attaque est non linéaire et ne peut pas se modéliser très facilement. Cependant, la perte de petits détails (composantes haute-fréquences de l'image) résultant de la compression et la conservation des informations prépondérantes nous permettent d'assimiler la compression à un filtrage passe-bas. Donc, pour contrer l'attaque compression, la marque doit posséder, en général, une composante basse-fréquence qui pourra être conservée après le processus de compression.

2.11.1.2 Les filtrages :

L'application de filtres dans le cadre du traitement d'images sert en général à améliorer l'aspect de l'image. Par exemple, l'augmentation des composantes hautes fréquences de l'image (le rehaussement) augmente le contraste car les détails sont mis en valeur.

Un autre exemple est celui du lissage. Cette fois-ci, les composantes hautes fréquences sont atténuées. L'image apparaît alors plus floue mais cela permet d'atténuer le bruit contenu dans l'image. Dans tous les cas, ces opérations sont linéaires et l'influence sur le tatouage est facilement prévisible. Des traitements plus complexes, comme le filtrage médian ou certains algorithmes de débruitage, vont utiliser des opérations non linéaires et vont donc être plus difficilement caractérisables par rapport à leur influence sur le tatouage. Toutefois, comme pour la compression, en analysant leur effet, nous pouvons essayer d'approximer l'influence de l'attaque par une opération linéaire.

2.11.1.3 Les transformations géométriques usuelles : changement d'échelle, fenêtrage et rotation :

Il existe plusieurs transformations géométriques dont certaines sont utilisées couramment dans le traitement d'images. Le but est par exemple de pouvoir isoler une partie de l'image, de faire un agrandissement ou une réduction. Dans le cas du fenêtrage, deux effets sont possibles : la désynchronisation, c'est-à-dire l'impossibilité de localiser la marque, ou le découpage de celle-ci, provoquant une perte d'information, empêchant ainsi l'identification de la marque ou diminuant l'exactitude de celle-ci.

Le cas d'un changement d'échelle est différent car compenser cet effet ne nécessite pas seulement de connaître le facteur d'échelle. En effet, l'application successive d'une dilatation et d'une contraction de l'image à partir du même facteur ne permet pas d'obtenir l'image initiale (par exemple simplement la taille peut déjà être différente). En général, l'opération de changement d'échelle fonctionne par interpolation et n'est donc pas inversible.

De plus, lors de la détection, après attaque, nous ne connaissons pas l'algorithme utilisé pour effectuer le changement d'échelle. Les problèmes sont similaires dans le cadre d'une attaque par rotation. Nous sommes en présence d'opération mal définie dans le domaine numérique et donc qui ne peuvent pas se résumer à un processus bien précis. C'est pourquoi ce type d'attaque peut être difficile à contrer.

2.11.1.4 Les conversions numériques/analogiques :

Lorsque des images numériques sont imprimées, elles sont transformées en support analogique. Pour faire une détection de marque, il est alors nécessaire de ré-numériser ce support. Cette conversion peut provoquer une diminution de la qualité de l'image (ajout de

bruit et apparition d'une trame) et introduire de légères déformations géométriques. Notons aussi que différents effets sont alors observables, tels que le changement d'échelle ou des couleurs de l'image, la perte d'information au niveau des textures les plus fines, etc. Pour pouvoir compenser cette attaque, il faut ainsi tenir compte de nombreuses opérations.

Toutes ces manifestations peuvent altérer la marque. Ce type d'attaque reste un problème très complexe du fait du non conservation d'une expression numérique de l'information.

Dans le cadre de la protection contre les copies, il est aussi envisagé un tatouage qui est révélé à la copie. Par exemple, dans le cas de billets de banque, la photocopie fait apparaître des modifications de couleurs, des "taches", sur les reproductions. Le document obtenu apparaît alors comme dégradé par rapport à l'original, permettant ainsi de dénoncer la fraude.

2.11.1.5 Les modifications colorimétriques :

Divers opérations liées à la couleur peuvent détruire une marque.

Le premier type d'attaque est lié à la modification de la représentation de la couleur. L'image couleur peut-être quantifiée suivant une table de couleur. Un autre exemple est celui de l'extraction de la composante luminance, afin d'obtenir une image en niveaux de gris. Afin d'améliorer le contraste d'une image, il est possible de modifier la correction gamma (liée aux paramètres d'acquisition d'une image), ou d'appliquer une égalisation d'histogramme.

De nombreux traitements classiques peuvent altérer la marque de façon involontaire. En revanche, certaines attaques ont directement pour but de court-circuiter l'opération de tatouage. Nous allons donc étudier ces différentes attaques malveillantes.

2.11.2 Traitements malveillants :

D'une façon générale, l'objectif d'une attaque malveillante est de gêner l'étape de détection de la marque. Dans ce paragraphe, nous allons étudier différentes techniques qui ont pour but de supprimer, de détériorer la marque, et celles liées à des méthodes de tatouage.

Les attaques peuvent être classées en quatre catégories d'après Meerwald [5] :

- les attaques simples,
- les attaques "anti-détection",
- les attaques d'ambiguïté,
- les attaques de séparation de la marque.

2.11.2.1 Les attaques simples :

L'objectif de ces attaques est d'ajouter des distorsions au support afin de rendre la marque indétectable ou illisible. L'attaque simple est réussie si la marque ne peut plus être détectée et si le support n'a pas été dégradé vis-à-vis d'une application prévue. Les opérations possibles pour réaliser ce type d'attaques sont la compression avec perte, l'ajout de bruit (Gaussien par exemple), le filtrage médian, et le ré-échantillonnage suivi d'une remise à l'échelle.

2.11.2.2 Les attaques "anti-détection" :

L'objectif de ces attaques est de réduire la corrélation entre la marque initiale et la marque détectée. Dans le cas d'une image, cela peut être réalisé par "brassage" des pixels. Les valeurs des pixels résultant de l'attaque et de l'image originale sont semblables, mais leur localisation a pourtant changé.

Trois attaques composent principalement cette catégorie :

- Les attaques géométriques font subir des translations, des rotations, des changements d'échelles à l'image. Notons en particulier le cas de la rotation où, comme illustrée sur la figure 1.8, une rotation est automatiquement suivie d'un fenêtrage pour camoufler l'application de cette rotation, et en particulier l'apparition de "triangles" dans les coins de l'image.
- Les attaques "jittering" ou de synchronisation ont pour but de délocaliser la marque, par exemple en supprimant ou en insérant des lignes ou des colonnes dans l'image.
- Le programme StirMark propose ces différents types d'attaques. L'une de ses opérations consiste à intégrer des déformations géométriques locales. A ce jour, seules les techniques de tatouage non aveugle (utilisation de l'image originale lors de la détection) peuvent être robustes à ce type d'attaque.

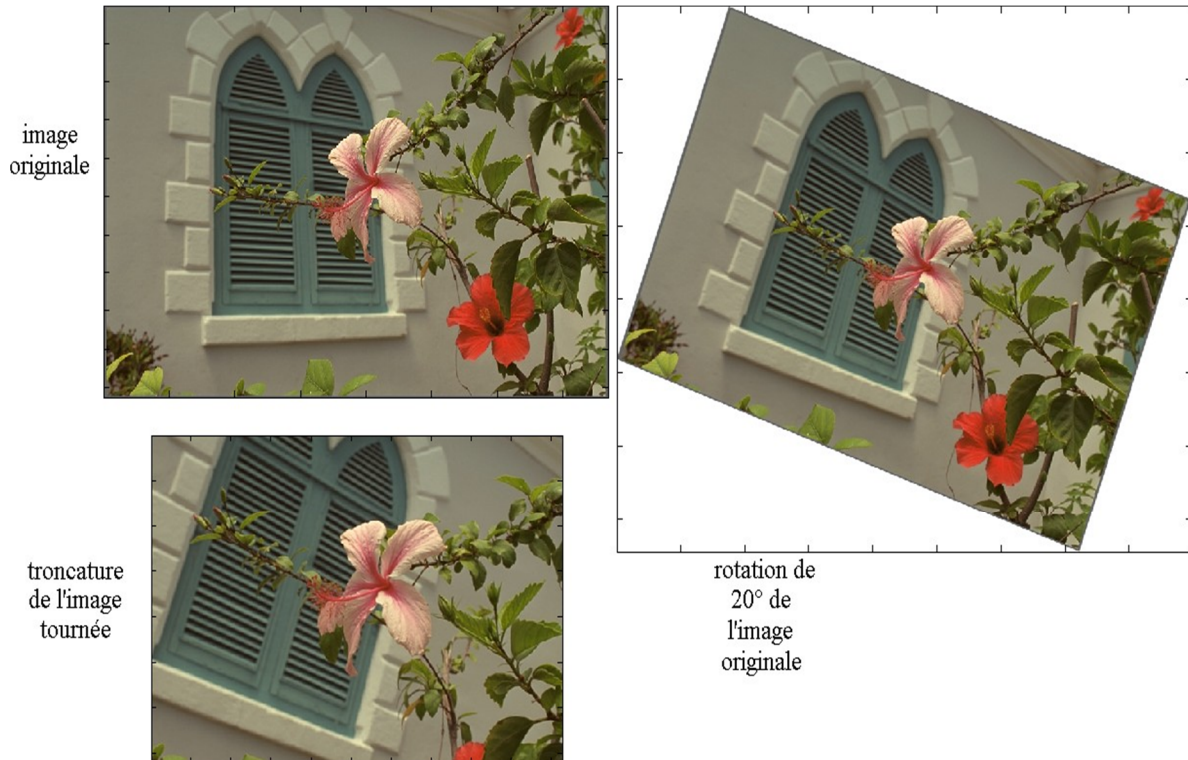


Figure 2.8 : Application d'un fenêtrage après rotation de l'image

2.11.2.3 Les attaques d'ambiguïté

Les attaques d'ambiguïté, aussi appelées attaques "bloquantes", ont pour but de discréditer l'autorité de la marque. Il suffit par exemple de rajouter sa propre marque sur le support pour dis- créditer la marque initiale. C'est le cas de l'inter blocage, présenté dans le paragraphe concernant le droit d'auteur.

2.12 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 -

Authentification d'images numériques par tatouage fragile

3.1 Introduction :

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

Dans ce chapitre, nous allons présenter une approche de tatouage fragile d'images numérique permettant ainsi l'authentification et la vérification de l'intégrité de l'image. La marque est insérée dans le domaine fréquentiel en appliquant la transformée en cosinus discrète. En premier nous allons la transformé fréquentiel dct puis nous allons décrire tous les étapes d'insertion et d'extraction de la marque. Et on termine le chapitre par évaluer l'approche par des métriques d'évaluation visuelle et sa fragilité vis-à-vis de l'attaque potentielle.

3.2 Méthode DCT:

La transformée en cosinus discrète DCT (discrete cosine transform) a été proposée pour la première fois par Ahmed et al. en 1974. La dct est parfaitement utilisée dans le domaine de codage et sécurité de l'information visuelle images et vidéo numériques car elle permet de donner des coefficients fréquentiels réels indépendants statiquement (décorrelés).

Mathématiquement, la dct d'une fonction bidimensionnelle $Img(x,y)$ est définie comme suit :

$$[1] F(u, v) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Img(x, y) \cdot \cos\left[\frac{\pi}{N} u \left(x + \frac{1}{2}\right)\right] \cdot \cos\left[\frac{\pi}{N} v \left(y + \frac{1}{2}\right)\right]$$

L'écriture de DCT est normalisée :

$$[2] F(u, v) = \frac{2}{N} c(u) \cdot c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Img(x, y) \cdot \cos\left[\frac{\pi}{N} u \left(x + \frac{1}{2}\right)\right] \cos\left[\frac{\pi}{N} v \left(y + \frac{1}{2}\right)\right]$$

La transformation inverse est donnée par :

$$[3] Img(x, y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u) \cdot c(v) \cdot F(u, v) \cdot \cos\left[\frac{\pi}{N} u \left(x + \frac{1}{2}\right)\right] \cdot \cos\left[\frac{\pi}{N} v \left(y + \frac{1}{2}\right)\right]$$

$$O \left\{ \begin{array}{l} c(0) = (2)^{-1/2} \\ c(w) = 1 \text{ pour } w = 1, 2, \dots, N-1 \end{array} \right\}_u$$

Matrice de pixels d'entrée							
140	144	147	140	140	155	170	175
144	152	140	147	140	148	167	170
152	155	136	167	163	162	152	172
168	145	156	160	152	155	136	160
162	148	156	148	140	136	147	162
147	167	140	155	155	140	136	162
136	156	123	167	162	144	140	147
148	155	136	155	152	147	147	136
Matrice DCT							
1210	-18	15	-9	23	-9	-14	-19
21	-34	26	-9	-11	11	14	7
-10	-24	-2	6	-18	3	-20	-1
-8	-5	14	-15	-8	-3	-3	8
-3	10	8	1	-11	18	18	15
4	-2	-18	8	8	-4	1	-7
9	1	-3	4	-1	-7	-1	-2
0	-8	-2	2	1	4	-6	0

Figure 3.1 : Exemple d'une transformée dct d'une matrice de pixels de pixels 8×8.

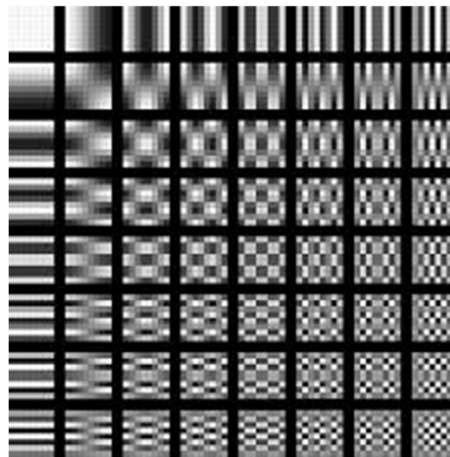


Figure 3.2: Les sous images produites par les coefficients fréquentiels.

La figure 3.1 montre un simple calcul de dct appliqué à une matrice de 8 × 8 éléments.

La figure 3.2 suivante présente les sous images que chaque coefficient peut représenter : $F(0,0)$ représente l'énergie (l'information globale) de l'image et est appelé *DC* contrairement

aux autres coefficients nommés *ACs* et ils sont classés sous bande de basse, moyenne et haute fréquences .

3.3 Schémas de tatouage fragile

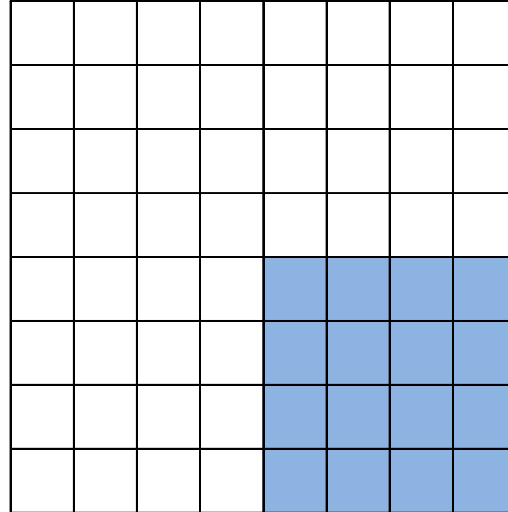


Figure 3.3: la bande de coefficients (haute fréquences) visé par le marquage.

L'approche choisie [27] pour le tatouage fragile est fréquentielle c.-à-d. la marque est insérée dans le domaine fréquentiel de l'image hôte. Parmi les avantages de ce choix est de maintenir l'invisibilité de la marque dans l'image tatouée.

3.3.1 Approche d'insertion :

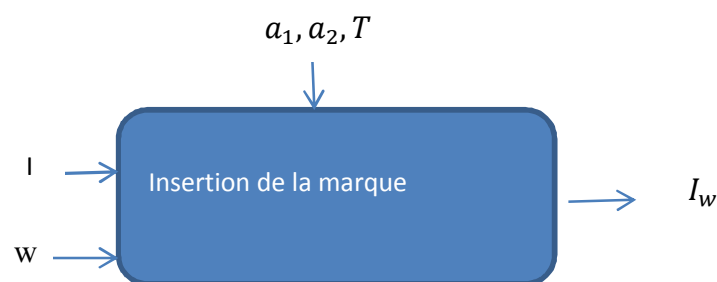


Figure 3.4: Les entrées/sorties de l'étape d'insertion de la marque

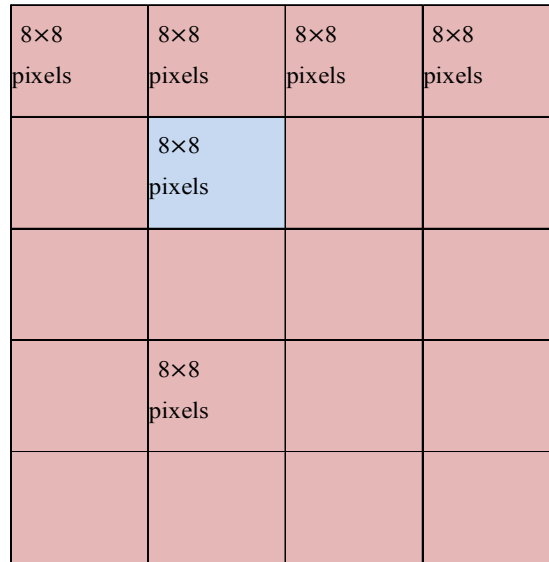


Figure 3.5: découpage en blocs de 8×8 éléments.

L'étape d'insertion consiste (voir figure 3.4) à insérer la marque w dans l'image hôte I et de produire comme résultat une image tatouée I_w à travers de paramètres de tatouage a_1, a_2, T . La marque $w = \{w(n), n = 1, 2, \dots, N\}$ est une séquence binaire de longueur N . Premièrement, l'image hôte est considérée dans cette approche en niveaux de gris. Elle est découpée en bloc de 8×8 pixels (la figure 37 montre un exemple de découpage appliqué à une matrice de 40×40 pixels). Après, chaque bloc est soumis à une transformation fréquentielle dct.

Pour chaque bloc fréquentiel B , quatre éléments binaire de la marque vont être insérer dans les coefficients de haute fréquences. Ces coefficients sont désignés en bleu dans la figure 3.3.

L'insertion de la marque $w(n)$ dans le coefficient $B(i, j)$ est appliquée selon la règle suivante :

Si $|B(i, j)| > T$ alors

$$|B'(i, j)| = |B(i, j)| + \frac{\alpha_1 w(n)}{D}$$

Sinon

$$|B'(i, j)| = |B(i, j)| + \frac{\alpha_2 w(n)}{D}$$

Fsi

Où T est un seuil, $\alpha_1, \alpha_2 \in]0, T[$ et $D=256$. Aussi, il est clair que la condition d'arrêt de processus d'insertion est que quand la séquence w est totalement insérée.

Après avoir insérer la marque, on va appliquer la transformé inverse en cosinus discrète à tous les blocs pour reconstituer l'image tatouée I_w , l'algorithme ci-dessous résume l'étape d'insertion :

Données d'entrées : $I, w, T, \alpha_1, \alpha_2$

Données de sortie : I_w

Debut

1- Décomposer I en blocs de 8×8 frequences

2- Appliquer la transformée dct à l'image I

$$I' = dct(I, [8 \ 8])$$

3- Pour chaque bloc fréquentiel B

Pour i de 4 à 8

Pour j de 4 à 8

Si $|B(i, j)| > T$ alors

$$|B'(i, j)| = |B(i, j)| + \frac{\alpha_1 w(n)}{D}$$

Sinon

$$|B'(i, j)| = |B(i, j)| + \frac{\alpha_2 w(n)}{D}$$

Fsi

Fpour

Fpour

4- Appliquer la transformée inverse à I' : $I_w = idct(I')$

Fin

3.3.2 Approche d'extraction :

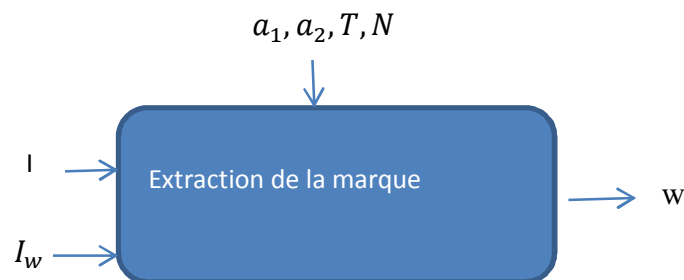


Figure 3.6 : les entrées/sorties de l'étape d'extraction de la marque

L'étape d'extraction (figure 3.6) consiste à trouver la marque à partir de l'image hôte et l'image tatouée I_w en utilisant les mêmes paramètres employés pour l'insertion α_1, α_2 , et T en plus de la dimension ou la longueur N de la marque w . L'algorithme ci-dessous décrit la procédure d'extraction :

Données d'entrées : $I, I_w, T, \alpha_1, \alpha_2, dimension(w)$

Données de sortie : w

Debut

1- Appliquer la transformée dct à l'image I

$$I' = dct(I, [8\ 8])$$

2- Décomposer I' en blocs de 8×8 frequences

3- Appliquer la transformée dct à l'image I_w

$$I'_w = dct(I_w)$$

4- Décomposer I'_w en blocs de 8×8 frequences

$n \leftarrow 0$

5- Pour chaque bloc fréquentiel B de I'

Pour chaque bloc fréquentiel C de I'_w

Pour i de 4 à 8

Pour j de 4 à 8

$n \leftarrow n+1$

Si ($n > dimension(w)$) alors

Arrêt

Fsi

Si $|B(i, j)| > T$ alors

$$w(n) = D \times (|B(i, j)| - |C(i, j)|) / \alpha_1$$

Sinon

$$w(n) = D \times (|B(i, j)| - |C(i, j)|) / \alpha_2$$

Fsi

Fpour

Fpour

Fpour

Fpour

Fin

3.4 L'organigramme de l'algorithme :

3.4.1 l'insertion :

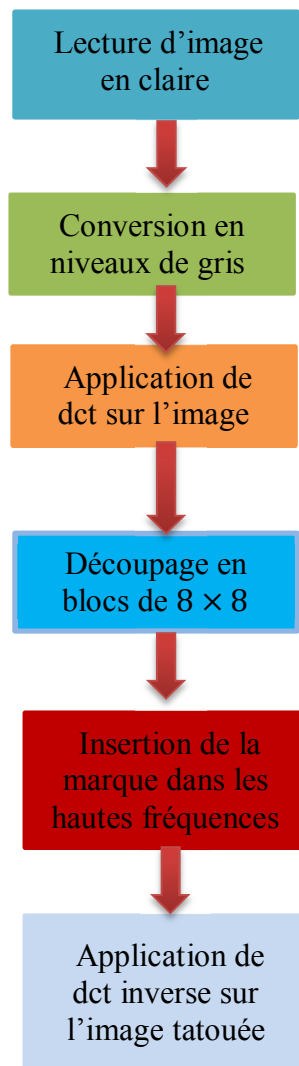


Figure 3.7: L'organigramme de l'algorithme l'insertion

3.4.2 l'extraction :

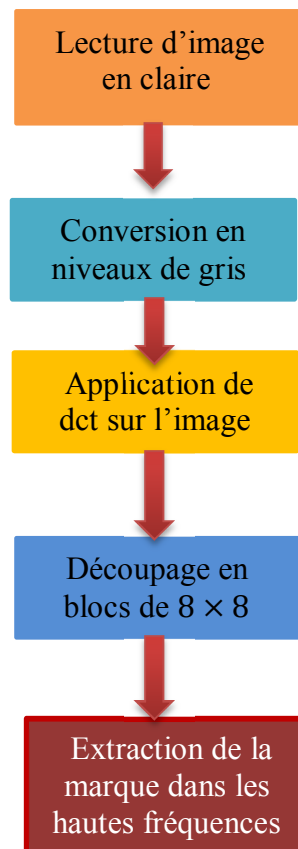


Figure 3.8 : L'organigramme de l'algorithme l'extraction

3.5 Résultat :

3.5.1 Les outils de développement :

La plate-forme MATLAB (abréviation de matrix laboratory) est optimisée pour résoudre les problèmes scientifiques et techniques. Le langage MATLAB, basé sur les matrices, est le moyen le plus naturel au monde pour exprimer les mathématiques computationnelles. Les graphiques intégrés permettent de visualiser facilement les données afin d'en dégager des informations. Grâce à la vaste bibliothèque de boîtes à outils prédéfinies, vous pouvez commencer directement par les algorithmes essentiels à votre domaine. L'environnement bureau encourage l'expérimentation, l'exploration et la découverte. Les outils et les fonctionnalités MATLAB sont tous testés rigoureusement. Ils sont conçus pour fonctionner conjointement.

3.5.2 Interface graphique implémentée:

Nous avons implémenté l'approche choisie par matlab 2017 où nous avons conçu deux interfaces graphiques : une pour l'insertion de la marque dans l'image hôte, et une autre pour extraire la marque de l'image tatouée.

3.5.2.1.Interface d'insertion :

- L'interface d'entrée pour l'insertion est présentée ci-dessous :

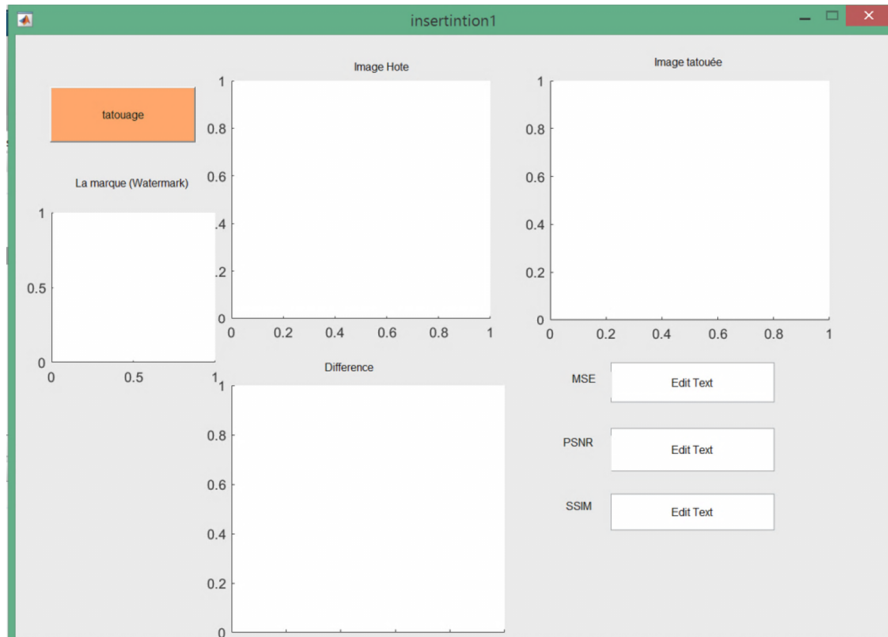


Figure 3.9: l'interface d'insertion

- Après l'appui sur le bouton tatouage, nous devons choisir l'image hôte (voir figure 3.9)

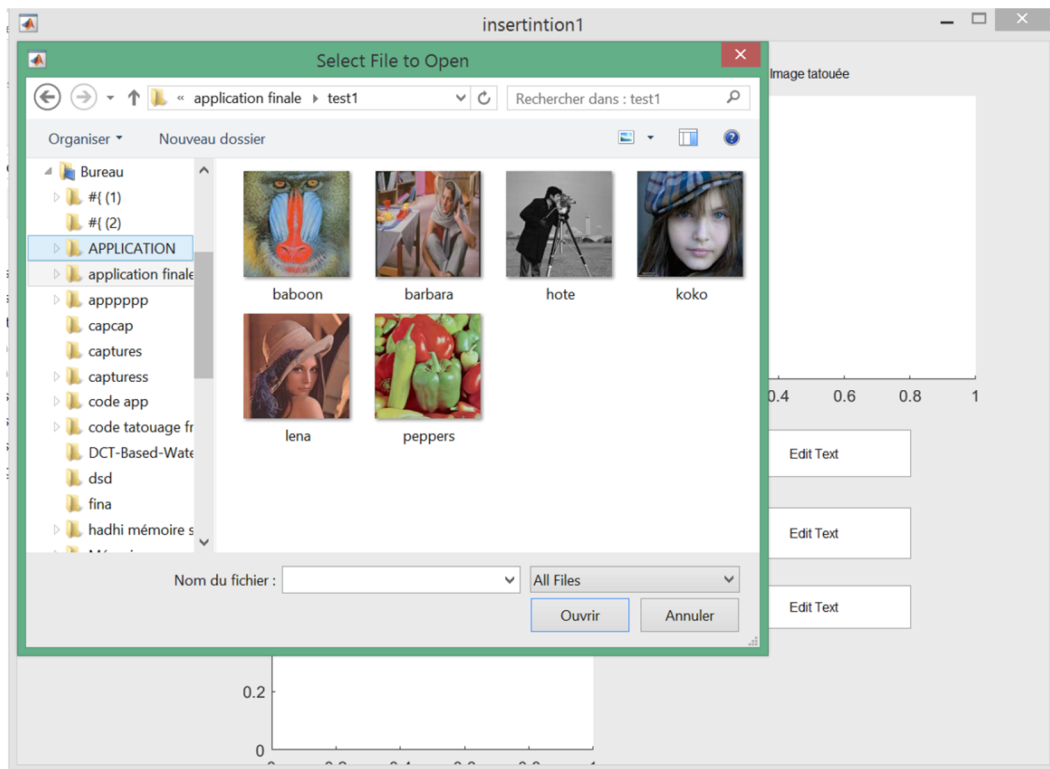


Figure 3.10: chargement de l'image original

- Ensuite nous devons choisir la marque (voir la figure 3.10)

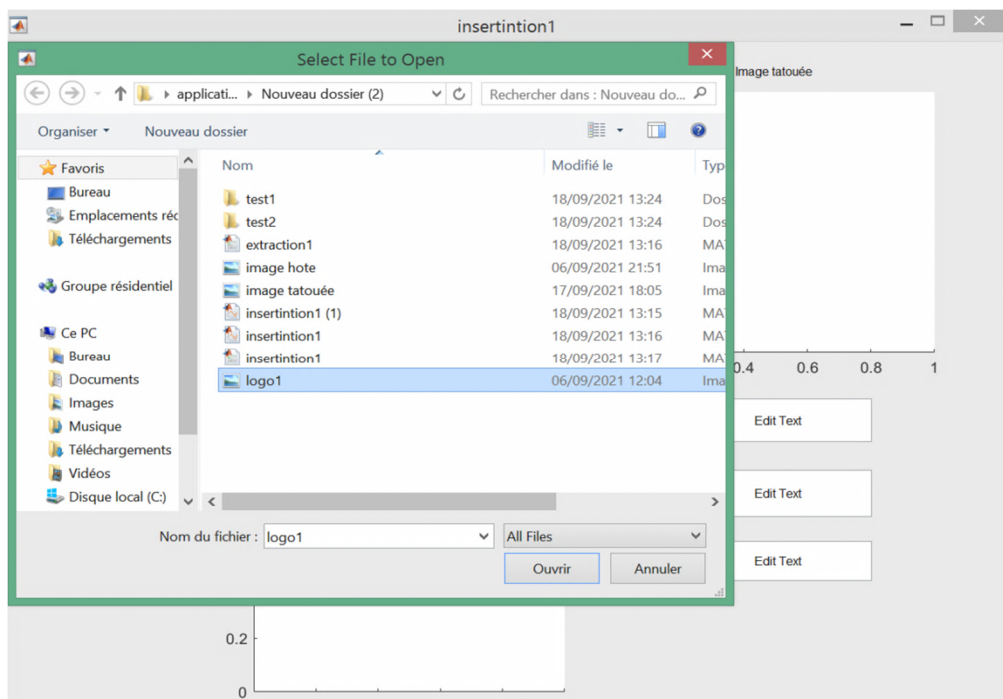


Figure 3.11: chargement de la marque

- Après, nous allons saisir les paramètres de tatouage (voir la figure 3.12)

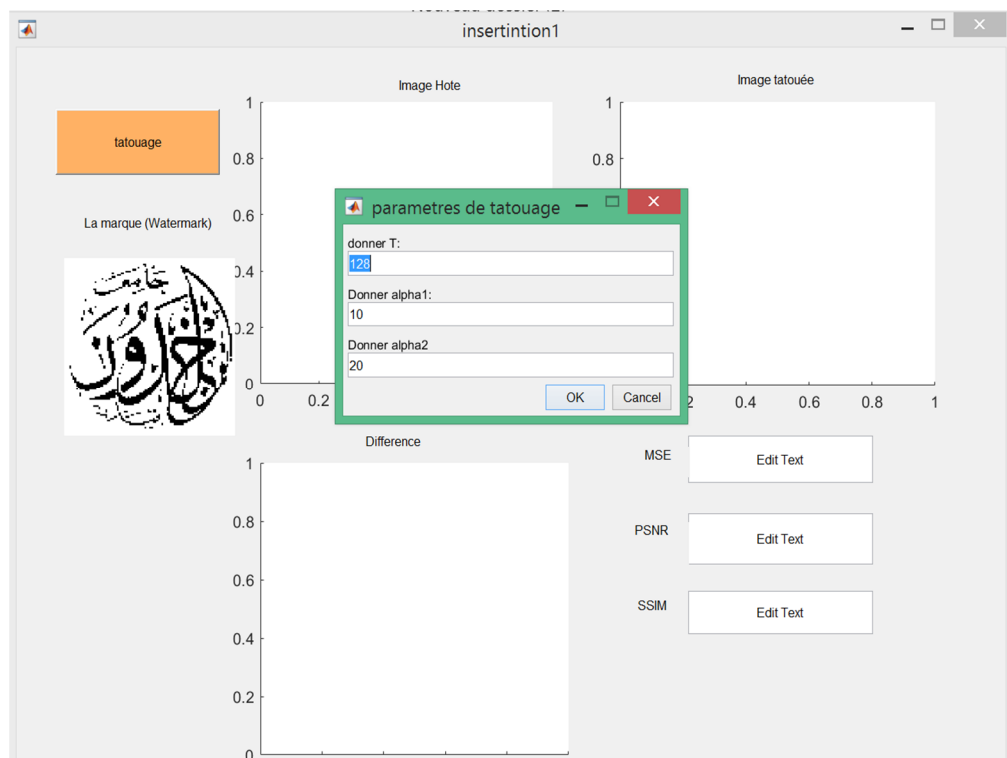


Figure 3.12: entremet de paramètres

- Finalement, nous allons obtenir les resultats visuels et les valeurs de metriques visuelles associées.

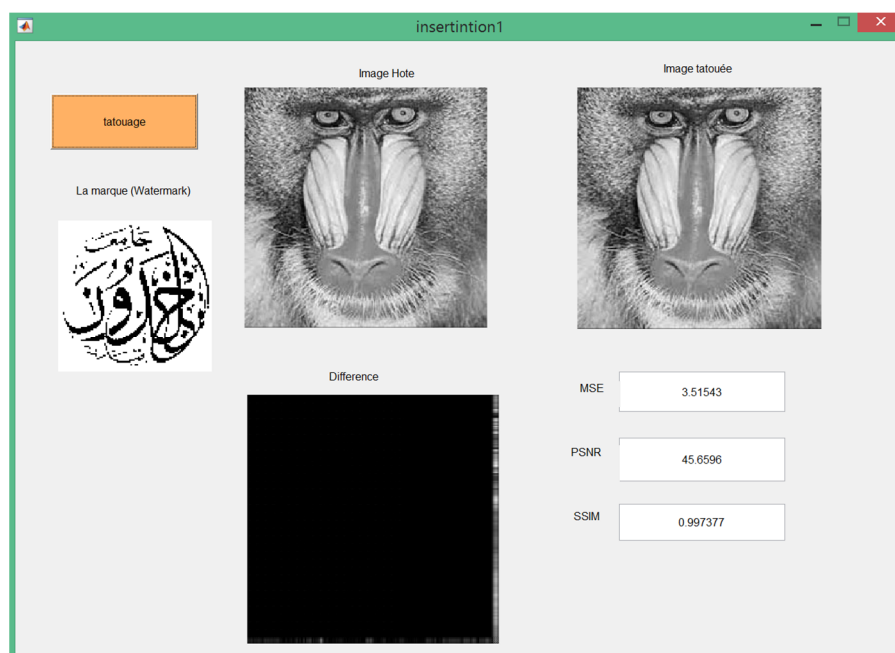


Figure 3.13: résultat finale

3.5.2.2. Interface d'extraction :

- L'interface d'entrée pour l'extraction de la marque est présentée dans la figure 3.14.

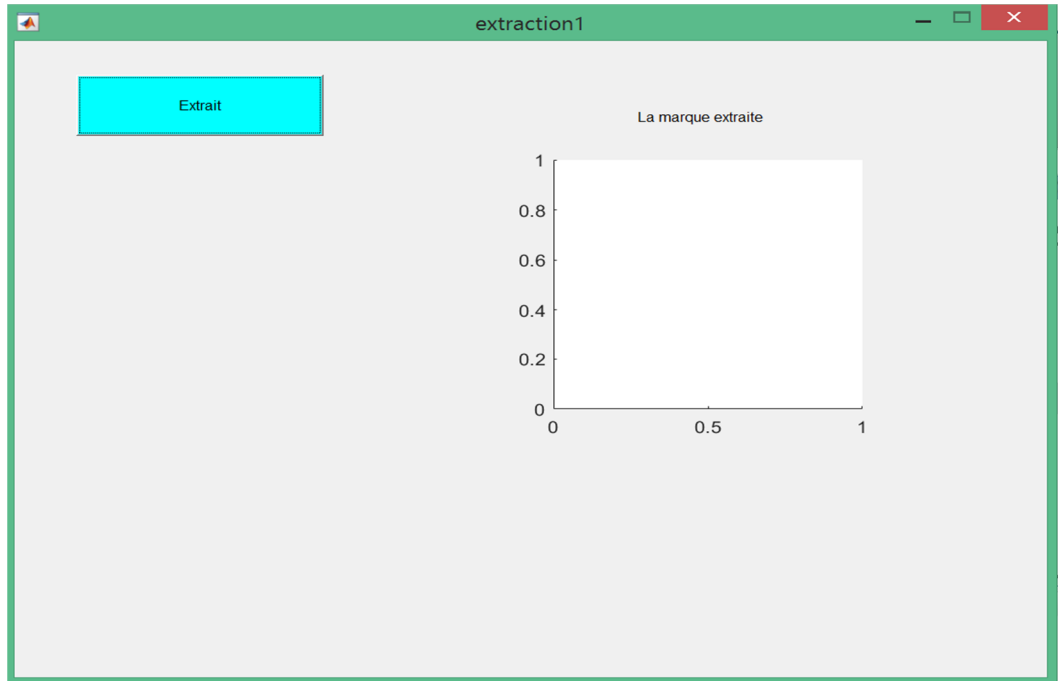


Figure 3.14: L' interface extraction

- Après l'appui sur le bouton extraction, nous devons saisir les paramètres de l'extraction comme la montre figure 3.15

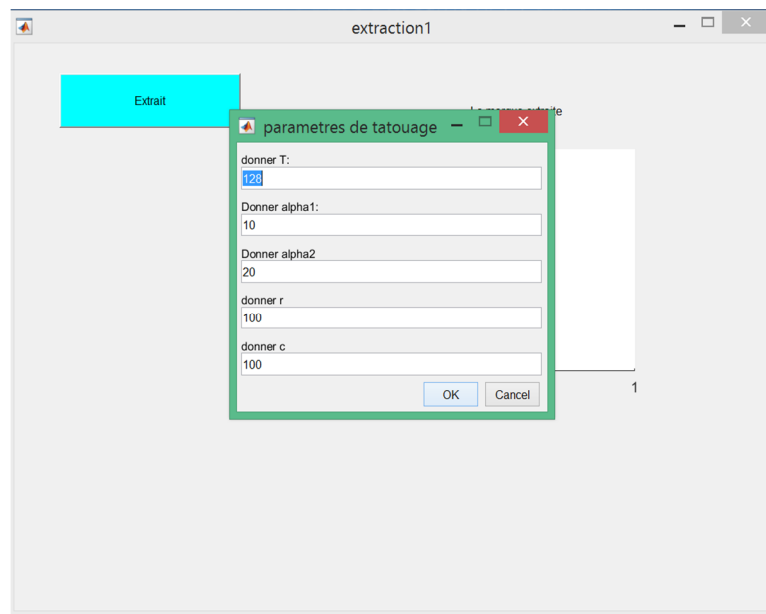


Figure 3.15: charger les paramètres de l'extraction

- Ensuite, il est venu l'étape de chargement de l'image tatouée (voir figure 3.16)

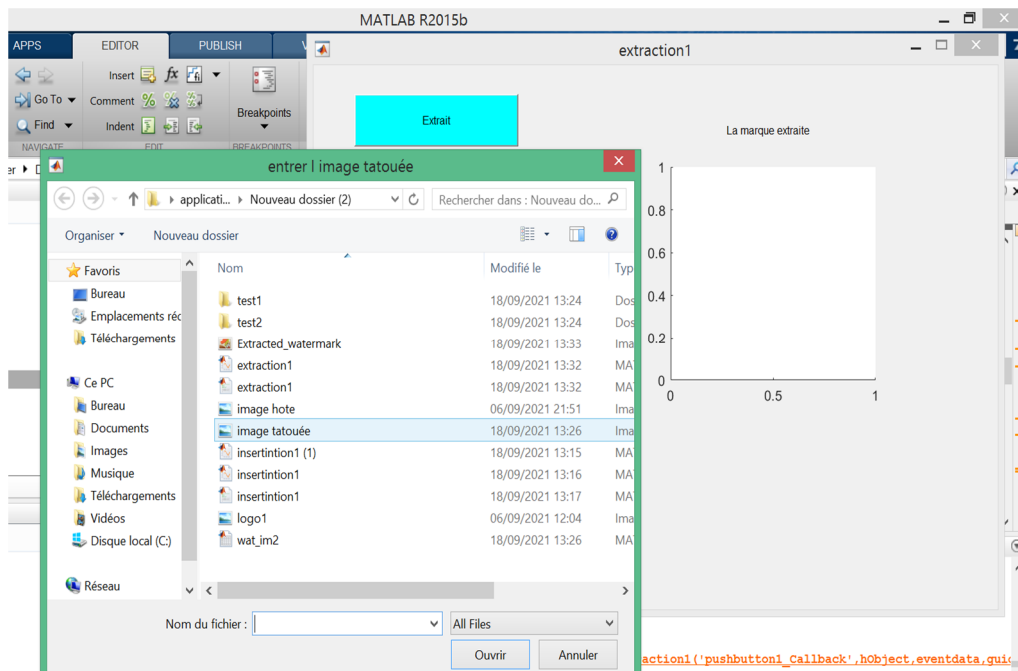


Figure 3.16: Chargement de l'image tatouée

- Ensuite l'image hôte sera chargée (voir figure 3.17).

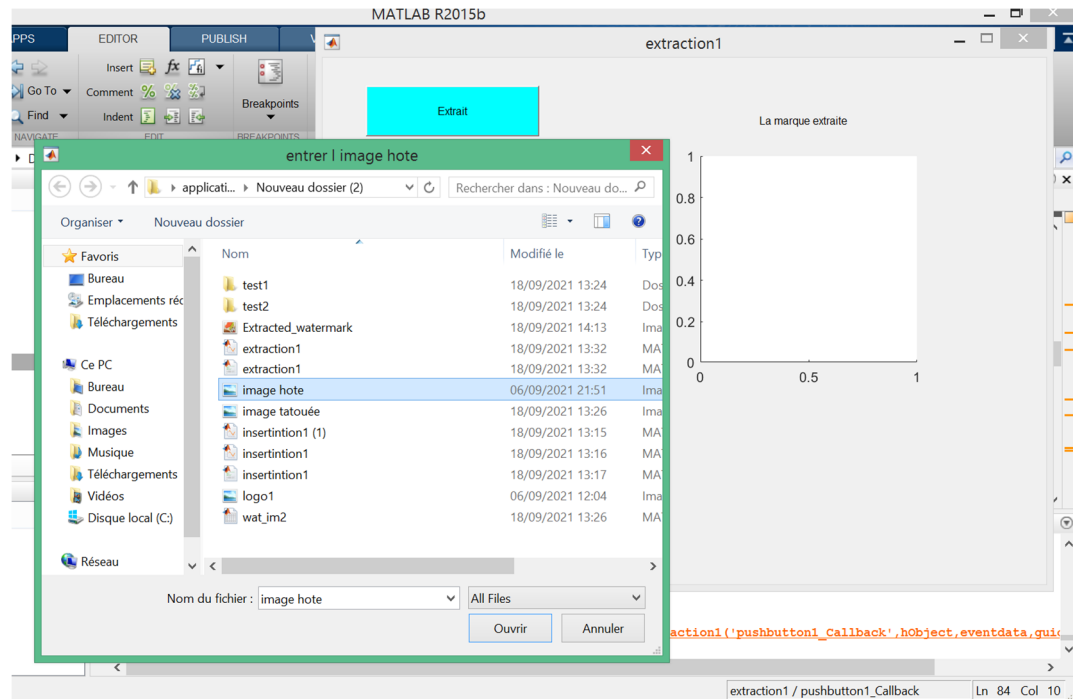


Figure 3.17: Chargement d'image hôte

- En fin, nous avons obtenu la marque extraite



Figure 3.18: résultat obtenue la marque extrait

3.6 Evaluation visuelle de l'approche:

Nous avons expérimenté pour le test de notre approches deux ensembles d'images : la première contient cinq images qui représente différentes formes et textures et de format JPEG, et la deuxième qui contient des images à différents taille (de 250×250 jusqu'à 1000×1000). La marque que nous avons choisie pour le tatouage est le logo de notre université comme le montre la figure



La marque

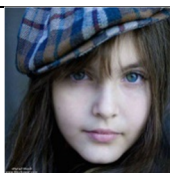
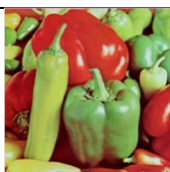
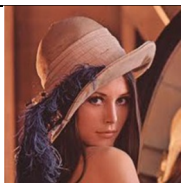
L'intitulé	L'image	La taille
Image 1		255 × 255
Image 2		255 × 255
Image 3		255 × 255
Image 4		255 × 255
Image 5		255 × 255

Figure 3.19

Premièrement, nous avons appliqué le tatouage avec $\alpha_1 = 10$, $\alpha_2 = 10$, et $T = 128$. La figure montre une image hôte (image 4) sélectionnée pour le tatouage, l'image tatouée, et la marque. Les images hôte et sa version tatouée sont traitées en niveaux de gris alors que la marque est convertie en niveaux de gris. Il est bien évident que la marque est invisible et le rendu visuelle hôte dans l'image tatouée n'est pas altéré. La figure montre la valeur absolue de différence entre l'image hôte et l'image tatouée.

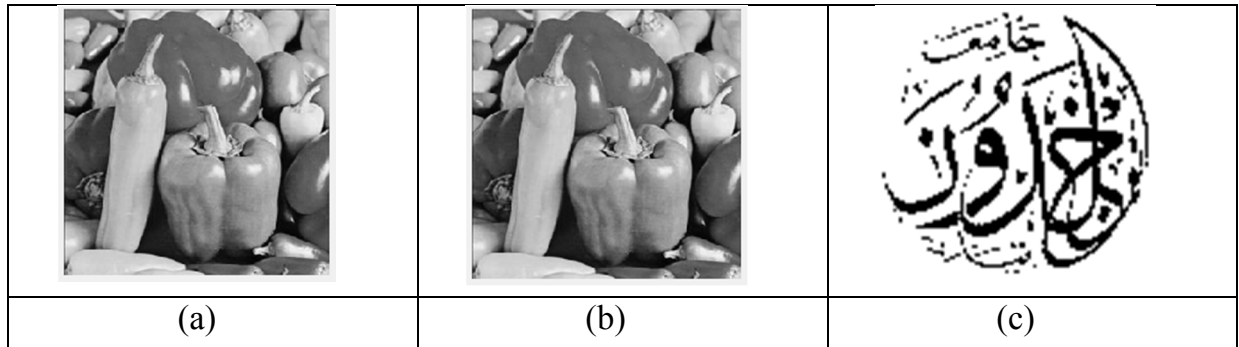


Figure 3.20 : résultats de tatouage : image hôte, image tatouée, la marque.



Figure 3.21: la valeur absolue de différence entre l'image hôte et l'image tatouée.

3.6.1 l'erreur quadratique moyenne (MSE)

L'image dégradée $\hat{I}$ est toujours comparée à l'originale I pour déterminer son rapport de ressemblance. Ce critère est le plus utilisé se basant sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et dégradés [3]:

$$MSE = \frac{1}{M \times N} \sum_{m=1}^M \sum_{n=1}^N \left(\hat{I}(m,n) - I(m,n) \right)^2$$

Où $(M \times N)$ est la taille de l'image, et $I(m,n)$ et $\hat{I}(m,n)$ sont respectivement les amplitudes de pixel sur les images originale et dégradée. Il est vraisemblable que l'œil tienne beaucoup plus compte des erreurs à grandes amplitudes, ce qui favorise la mesure quadratique.

3.6.2 Le rapport crête signal sur bruit (PSNR) :

Au lieu de mesurer la distorsion, cette valeur (Peak Signal to Noise Ratio, PSNR) [3] mesure la fidélité, puisqu'elle est proportionnelle à la qualité. Tout de même, elle est une

fonction de MSE ; sa définition et son utilisation proviennent du domaine du traitement de signal:

$$PSNR = 10 \log_{10} \left(\frac{Imax^2}{MSE} \right)$$

Pour une image à niveau de gris, I max désigne la luminance maximale possible. Une valeur de PSNR infinie correspond à une image non dégradée, et cette valeur décroît en fonction de la dégradation. Le PSNR lie donc le MSE à l'énergie maximale de l'image.

3.6.3 L'index de similarité structurelle (SSIM) :

SSIM [5] est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image déformée, par rapport à l'image originale. L'idée de SSIM est de mesurer la similarité de structure entre les deux images, plutôt qu'une différence pixel à pixel comme le fait par exemple le PSNR. L'hypothèse sous-jacente est que l'œil humain est plus sensible aux changements dans la structure de l'image (voir Fig.1).

La métrique SSIM est calculée sur plusieurs fenêtres d'une image de taille NxN. On dénote x et y les vecteurs de l'image originale et déformée respectivement. La similarité compare la luminance, le contraste et structure entre chaque couple de vecteurs. La luminance est estimée par la mesure de l'intensité moyenne de chaque faisceau spatial:

$$\mu_x = \frac{1}{N} \sum_{i=1}^N x_i$$

Le contraste de chaque faisceau est mesuré par:

$$\sigma_x = \left(\frac{1}{N-1} \sum_{i=1}^N (x_i - \mu_i)^2 \right)^{1/2}$$

La similarité est déterminée par la perte de corrélation entre les deux vecteurs:

$$\sigma_{xy} = \frac{1}{N-1}$$

La fonction de comparaison de luminance notée par l(x, y) est une fonction de x et y. Le contraste entre deux faisceaux spatiaux noté par c(x, y), comparent les variances de x et y. La troisième fonction compare les structures des deux vecteurs spatiaux donnés par la fonction s(x, y) en fonction de deux vecteur normalisés. Finalement la fonction mesurant la similarité, est une fonction de l(x, y), c(x, y) et de s(x, y). Elle est de la forme :

$$S(x, y) = f(l(x, y), c(x, y), s(x, y))$$

Une propriété intéressante est que les trois composants de la fonction $f(.)$ sont relativement indépendants. Aussi, la fonction $s(x, y)$ doit satisfaire les conditions suivantes :

1. $S(x, y) = S(y, x)$
2. $S(x, y) \leq 1$
3. $S(x, y) = 1$ si et seulement si $x = y$

Wang et Al ont proposé dans [5] une fonction de comparaison de luminance de la forme :

$$l(x, y) = \frac{2\mu_x\mu_y + (K_1L)^2}{\mu_x^2 + \mu_y^2 + (K_1L)^2}$$

K_1 est une constante de très faible valeur. La constante $(K_1L)^2$ évite l'instabilité de la fonction de comparaison lorsque $\mu_x^2 + \mu_y^2$ sont très proches de zéro. Dans le cas des images à niveau de gris, la constante est $L = 255$.

On remarque que l'équation est conforme à la loi de Weber, largement utilisée pour la modélisation de l'adaptation à la lumière dans le SVH (système visuel humain). Selon la loi de weber la variation de luminance est proportionnelle à la luminance de fond. En d'autres termes, le SVH est sensible aux variations relatives de luminance entre les deux signaux ou encore entre les deux images. La fonction de comparaison de contraste prend une forme similaire :

$$c(x, y) = \frac{2\sigma_x\sigma_y + (K_2L)^2}{\sigma_x^2 + \sigma_y^2 + (K_2L)^2}$$

Où K_2 est une constante de très faible valeur. La comparaison de structure est réalisée par la corrélation entre les deux vecteurs après soustraction de la luminance et normalisation par la variance. Notons que la corrélation entre les deux vecteurs est une mesure simple et effective de la similarité structurelle. Alors la fonction de comparaison structurelle est donnée par :

$$s(x, y) = \frac{2\alpha_{xy} + (K_2L)^2}{2\sigma_x\sigma_y + (K_2L)^2}$$

Finalement, la mesure de similarité résultante des trois comparaisons est donnée par une expression simplifiée de l'index de similarité structurelle entre x et y :

$$SSIM(x, y) = l(x, y) \cdot c(x, y) \cdot s(x, y)$$

où encore sous une forme simplifiée:

$$SSIM(x, y) = \frac{2\mu_x\mu_y + (K_1L)^2}{\mu_x^2 + \mu_y^2 + (K_1L)^2} \frac{2\sigma_x\sigma_y + (K_2L)^2}{\sigma_x^2 + \sigma_y^2 + (K_2L)^2}$$

L'index de similarité est exploité pour un choix approprié des constantes K_1 et K_2 pour généraliser l'évaluation à toute l'image.

- On suppose les paramètres de tatouages est :
- $T : 128$ $\alpha_1 : 1$ $\alpha_2 : 2$

Image PNG	PSNR	MSE	SSIM
Image1	81.79	0,4443	0,9997
Image2	83.21	1,9419	0,9997
Image3	82.10	1,0665	0,9995
Image4	81.67	0,8618	0,9986

Tableau 3.1 : Qualité des images tatouées.

Nous avons examiné la qualité visuelle d'images tatouées en calculant des métriques visuelles à savoir PSNR, MSE et SSIM respectivement. Le tableau 1 nous montre que les valeurs de PSNR sont élevées et supérieures à 40 avec des valeurs de SSIM proches de 1, ce qui signifie qu'une forte qualité d'images tatouées ont été atteinte.

3.6.4 Fragilité vis-à-vis les attaques :

Dans cette expérience, nous avons subi l'image tatouée à quelques attaques géométriques en testant ainsi sa fragilité. Et pour chaque attaque, nous avons vérifié si la marque est changée ou pas à la suite des modifications affectée par l'attaque associée. Pour atteindre cet objectif, nous avons calculé le PSNR et SSIM respectivement : Si la marque n'est pas modifiée, les valeurs de PSNR et de SSIM sont infini et 1 respectivement.

3.6.4.1 Filtre médian

Le filtre médian est un filtre d'image numérique qui permet d'améliorer la qualité d'image où la valeur de chaque pixel est remplacée par la médiane (et non la moyenne) de son voisinage.

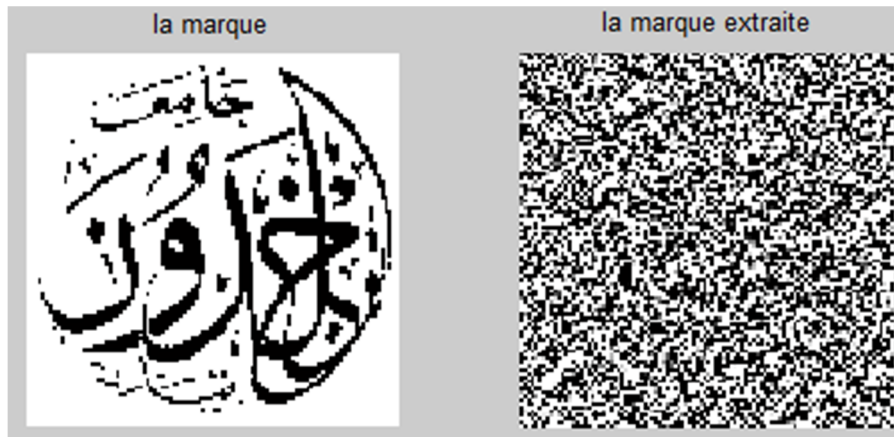


Figure 3.22 : résultat de l'extraction après l'attaque de filtre median .

3.6.4.2 Bruitage:

Nous avons appliqué un bruit gaussien blanc à la vidéo tatoué de variance égal à 0.01, nous avons trouvé que la marque est modifiée comme le montre la figure 2.23.

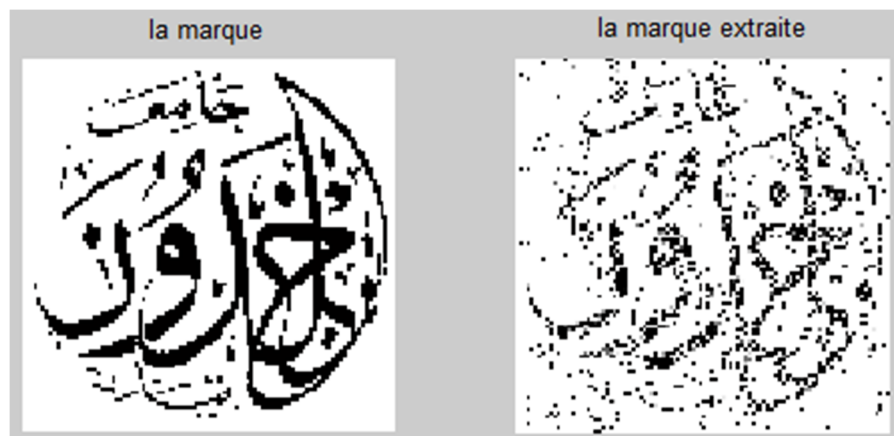


Figure 3.23 : résultat de l'extraction après l'attaque de bruitage.

3.6.4.3 Rotation :

L'image tatouée a été subie à une rotation de 3 degrés, nous avons trouvé que la marque a été modifiée et changé carrément.

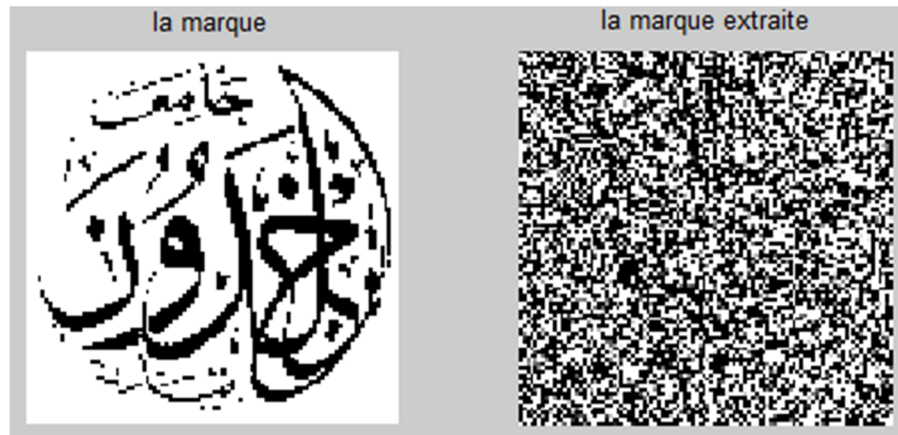


Figure 3.24 : résultat de l'extraction après l'attaque de rotation.

3.7.Conclusion :

Dans ce chapitre, 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 fragilité. Elle est aussi efficace car elle peut extraire facilement le watermark en utilisant seulement l'image tatouée sans nécessité de la marque 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, et aussi elle permet d'insérer une grande capacité de la marque sans altérer le contenu visuel de l'image.



Conclusion générale

A cause des utilisations illicites des documents numériques. Le tatouage numérique a été introduit comme une solution alternative à la cryptographie et efficace pour la protection des données multimédia 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 l'objectif de vérifier l'authentification et l'intégrité des images numériques, nous avons implémenté une approche de tatouage fragile d'images numériques basée sur l'insertion d'une marque binaire dans les hautes fréquences où la transformée employée est la DCT.

Les résultats expérimentaux montrent l'invisibilité de la marque dans l'image tatouée surtout où nous avons travaillé avec des images compressées de type JPEG. La capacité d'insertion pour l'approche choisie est aussi importante et peut s'appliquer au quart de l'image hôte.

L'image est un élément figurant dans plusieurs fichiers multimédia visuels à savoir la vidéo numérique, les fichiers PDF,...etc. Pour cela, il est bien évident que l'approche implémentée peut être appliqué à tous les trames (frame) de la vidéo numérique, ou aux pages extraites de document PDF.

:



Bibliographie



- [1] Hetatache Karima, Développement d'algorithmes de tatouage d'images basés sur la DCT et les transformées discrètes, Mémoire de Magister université ferhat abbas-setif UFAS (ALGERIE), 2014.
- [2] Imen Trabelsi, Halima Maamri, Tatouage numérique fragile pour l'authentification d'images, Mémoire de Master université de Biskra, 2016.
- [3] K. Tanaka, Y. Nakamura, K. Matsui. " Embedding Secret Information into a Dithered Multilevel Image ". In 1990 IEEE Military Communications Conference, pages 216–220, 1990.
- [4] E. Incerti, "Compression d'images, algorithmes et standards", Edition Vuibert, pp. 14, Paris, 2003.
- [5] [www. master-ivi.univ-lille1.fr/fichiers/Cours/seance8_wmk.pdf](http://www.master-ivi.univ-lille1.fr/fichiers/Cours/seance8_wmk.pdf)
- [6] Jean-Bernard CAMBIER, Introduction aux images numériques ,haute école condorcet,
- [7] T. Mohamed ,D. Djafar, "la découverte des concepts sémantiques cachés avec plusieurs niveaux d'abstraction pour la recherche d'images", Université Kasdi Merbah Ouargla, 2013
- [8] **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.
- [9] **F. Petitcolas, R. Anderson, and M. Kuhn**. Information Hiding Terminology: A Survey. *IEEE Signal Processing*, 78(7) :1062–1078, 1999.
- [10] **Chun-Shien Lu**. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, 2005.
- [11] Le Marquage Et La Propriété Intellectuelle, **Michel Blanchard**, 2003.
- [12] **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.
- [13] **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.
- [14] **I. Cox, M. Miller, and J. Bloom**. Digital Watermarking: Principles & Practices. Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.
- [15] **I. Cox and M. Miller**. The first 50 years of electronic watermarking. *EURASIP Journal on Applied Signal Processing*, 2002(2):126–132, 2002.
- [16] [www. master-ivi.univ-lille1.fr/fichiers/Cours/seance8_wmk.pdf](http://www.master-ivi.univ-lille1.fr/fichiers/Cours/seance8_wmk.pdf).

- [17] <http://www.crdp.ac-grenoble.fr/image/general/general.htm>.
- [18] **R. ISDANT**, « Traitement numérique de l'image », 2009.
- [19] **P. Singh, R.S. Chadha**, “A Survey of Digital Watermarking Techniques, Applications and Attacks, “IJEIT, Volume 2, Issue 9, March 2013.
- [20] **P. LIPiński**, “On domain selection for additive, blind image watermarking,” Institute of Information Technology, University of Lodz, Pologne, 2012.
- [21] **E. Muharemagic, B. Furht**, “Survey of Watermarking Techniques and Applications,” Department of Computer Science and Engineering, Florida Atlantic University, USA, 2010.
- [22] **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
- [23] Tatouage d'images par la décomposition en valeurs singulières et la transformée en cosinus discrète, dans UNIVERSITE MOHAMED BOUDIAF - M'SILA, 2017.
- [24] **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, January 2012.
- [25] **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
- [26] **I. Cox, M. Miller, and J. Bloom**. Digital Watermarking: Principles & Practices. Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.
- [27] **S. Al-Shehhi, M. Al-Muhairi, D. Abuoeida, H. Al-Ahmed, N. Werghi and A. Kunhu**, "Robust and Fragile Watermarking Scheme Based on DCT and Hash Function for Color Satellite Images," 2013 Sixth International Conference on Developments in eSystems Engineering, 2013, pp. 253-258, doi: 10.1109/DeSE.2013.53.
- [28] Mémoire de magister en 2014 dans université dr Belabes