REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE DE TECHNOLOGIE
DEPARTEMENT D'ELECTRONIQUE
N° : 2017/CI 08/97/482

DOMAINE : SCIENCES ET TECHNOLOGIES
FILIERE : GENIE ELECTRIQUE
OPTION : CONTROLE INDUSTRIEL

Mémoire présenté pour l'obtention
Du diplôme de Master Académique

Par: Seraiche Lemya
Beladjouz Ahlam

Intitulé

Tatouage d'images par la décomposition en valeurs singulières et la transformée en cosinus discrète

Soutenu devant le jury composé de:

Boukhanoufa nabil	Université de M'sila	Président
Hamadouche loubna	Université de M'sila	Rapporteur
Khalfa ali	Université de M'sila	Examinateur

Année universitaire : 2016 /2017

Remerciements

Nous remercions premiérement Allah le tout puissant pour la volante , la santé et la patience, qu'il nous a donné durant toutes ces longues années.

Nous remercions notre encadreur

Madame HAMADOUCHE LOUBNA pour son soutien continuel et son encoragements tant précieux.

Nos remerciements vont aussi à tout le corps enseignant de L'UNIVERSITE DE M'SILA, spécialement les ensignantsde la faculté de technologie et le département d'électronique pour leur apport de connaissance durant les cinq ans d'études.

Nos vives reconnaissances vont également à touts les membres du jury pour avoir accepté d'examiner notre travail.

Nous tenons à les remercier vivement et nous voudronsassocier nos remerciments à toutes les personnes qui ont contribué de prés ou de loin à l'aboutissement de ce travail.

Dédicace

Je dédie ce modeste travail

À ma très cher mère source de tendresse Aucune dédicace ne saurait exprimer mon respect, mon amouréternel et ma considération pour les sacrifices que vous avez consentie pour moninstruction

À mon très cher père, qui m'encourage toujours

À mes chers frères (imed eddine, alaa eddine , badr eddine , sohaib)

À tous mes amis (fatima , ahlam , warda assia , zina ,dalila ,sarah , souhila , wafa amel ,widad , samia hoda)

À mon cher cousine afaf

À tous la famille seraiche

À tous mes amis d'études

Lemya

Dédicace

Je dédie ce modeste travail

Àmes très chers parents(Akila, Nacereddene) sourse de tendresse et de courage

À mes fréres (Zakaria, Ayoub) et ma sœur(Hanane)

À mes amies (lemya, ouarda, assia, souhila, fatima)

Àma tante et mes ancles

Àla grande famille BELADJOUZ

et

Àtous mes amis d'étude.

Ahlam

Sommaire

Chapitre 2 : le tatouage des images numériques

Chapitre 3 : Simulation des algorithmes de tatouage

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Liste des tableaux

Chapitre 1

Chapitre 3

Table des abréviations

2D	bidimensionnel
PAO	Publication assistée par ordinateur
Pixel	Picture élement
BPP	Bit par pixel
RGB	Red, green, bleu
CMNJ	Cyan Magenta Jaune Noir
PPP	Point par pouce
TIFF	Tagged image file format
BMP	Bitmap
GIF	Graphic information format
PNG	portable network graphique
SVH	Systéme visuel humain
LSB	Bit de poids faible
DFT	Transformée de fourrier
DCT	Transformée en cosinus discréte
DWT	Transformée en ondulette discréte
BF	Base fréquence
HF	Haute fréquence
PSNR	Raport de signal sur bruit de créte
EQM	L'erreur quadratique moyenne
NC	Colération normalisée

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.

Pour pallier à ce problème, une nouvelle technique a été introduite. Cette technique, nommée tatouage numérique, en anglais "digital watermarking", a fortement émergé depuis le début des années 1990. Elle consiste à inscrire dans un document numérique une marque afin d'identifier son ayant droit légitime. Ce mécanisme d'insertion de marque devrait respecter au moins deux conditions : la marque doit être imperceptible(l'œil humain ne droit pas pouvoir faire la différence entre une image marquée et celle non marquée) et robuste(le tatouage doit résister à toutes les modifications volontaires ou involontaires). L'idée de base du « watermarking » est de cacher dans un document numérique (image, audio, vidéo) une information subliminale (invisible ou inaudible suivant la nature du document) et robuste.

Dans ce travail, nous nous sommes intéressées au tatouage numérique des images dans le but d'étudier et d'implémenter des méthodes de tatouage d'images basées sur la décomposition en valeurs singulières(SVD) et la transformée en cosinus discrète (DCT). La SVD a été découverte indépendamment par Beltrami en 1873. Elle n'a été employée comme outil informatique que jusqu'aux années 60. Elle est très utilisée dans la compression, le tatouage d'images, le filtrage et d'autres champs de traitement des signaux. Quant à la DCT, elle a été inventée par Nasir Ahmed en 1974 dans son article appelé “Traitement d’image et la transformation cosinus discrète”. Elle a trouvé notamment ces applications dans la compression des images numériques et le tatouage. Précisons que les algorithmes que nous avons développés dans notre travail consistent à utiliser la SVD seule dans le tatouage puis à combiner la SVD avec la DCT. Une étude de performance des deux techniques développées en termes de robustesse, imperceptibilité, et simplicité est réalisée.

Le présent mémoire est organisé en trois chapitres :

- **Le chapitre 1**

Présente une introduction aux images numériques. Plus précisément, nous présenterons quelques terminologies et quelques notions pertinentes dans le domaine des images numériques telles que la numérisation, le codage et le stockage. Nous présenterons aussi quelques aspects du traitement d'images, tels que le filtrage, la compression et le tatouage.

- **Le chapitre2**

Décrit le principe général du tatouage, les domaines d'insertion de la marque, les applications et les classifications des attaques sur le tatouage.

- **Le chapitre 3**

Présent les algorithmes de tatouage étudiés ainsi que les résultats obtenus.

Nous terminerons par une conclusion générale en résumant l'apport et les limites de la méthode de tatouage proposée.

Chapitre 1
Les images numériques

1.1. Introduction

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, de 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 comme les appareils photographiques, caméra, radiographie, scanner, sonar,…etc.

Le traitement et l'analyse d'image trouvent leurs applications dans des domaines extrêmement variés de l'industrie et de la recherche. Ces méthodes sont utilisées dans de nombreuse disciplines scientifiques, citons par exemple :la sécurité (reconnaissance d'empreintes, de visages, de signature), la détection de mouvements, les sciences de la terre la géométrique (la cryptographie et la stéganographie), la robotique (pour le tri et la vérification de pièce électronique) et bien encore des domaines aussi variés tels que l'astronomie l'identification, la pharmacologie etc...

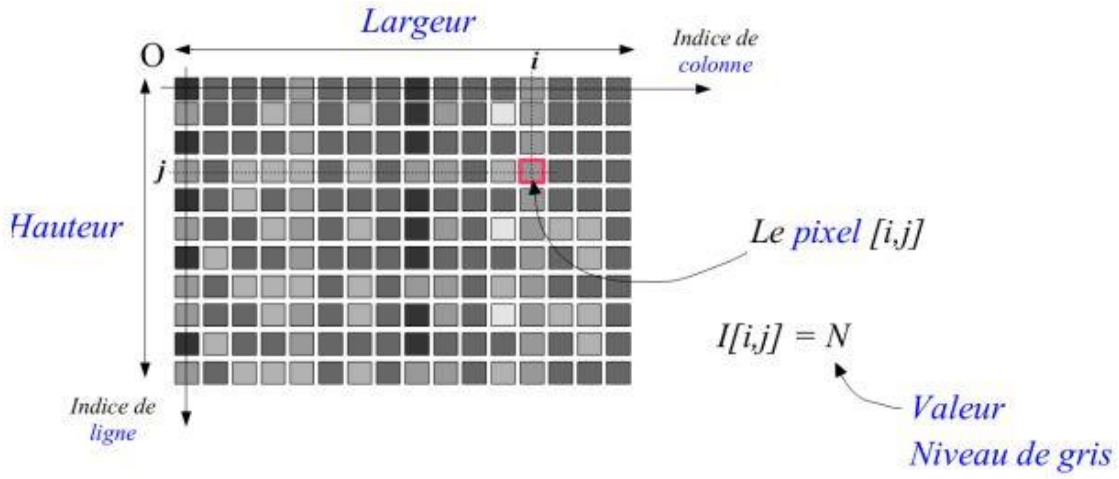
L'objectif de ce chapitre est d'introduire le domaine des images numériques. Nous découvrons ce domaine depuis la phase d'acquisition, numérisation, jusqu'au stockage dans les différents formats possibles.

1.2. Définition d'une image réelle

Une image réelle est obtenue à partir d'un signal contenu bidimensionnel comme par exemple un appareil photo ou une caméra... Sur un ordinateur, on ne pas représenter de signaux continus, on travaille donc sur des valeurs discrètes [1].

1.3. Définition d'une image numérique

Une image numérique est définie comme un signal fini bidimensionnel échantillonné à valeurs quantifiées dans un certain espace de couleurs. Elle est constituée de points (pixel).Autrement dit, une image est une matrice MxN de valeurs entières sur un intervalle borné [0,Ng] où Ng est la valeur maximale du niveau de gris [2].



Figue1.1. Image numérique *I [2]*

1.3.1. Image en niveaux de gris

Une image en niveaux de gris autorise un dégradé de gris entre le noire et le blanc. En générale, on code le niveau de gris sur un octet (8 bits) soit 256 nuance de dégradé. L'expression de la valeur du niveau de gris avec Ng=256devient : p (i, j) ϵ [0,255].

1.3.2. Image couleur

Une image en couleur correspond à la synthèse additive de trois images, rouge, vert et bleu. Chaque pixel est donc codé sur 3×*N* bits. La couleur finale est obtenue par synthèse additive de ces trois composantes [3].

1.4. Processus de numérisation

La représentation informatique d'une image est nécessairement discrète, alors que l'image est de nature continue. 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 [4].

Le processus de numérisation est représenté dans la figure suivante :

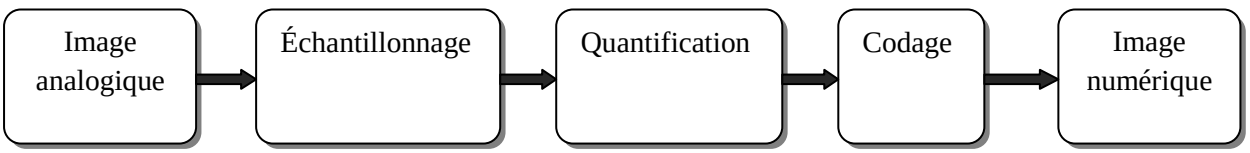


Figure 1.2. Processus de numérisation d'une image

1.4.1. 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).

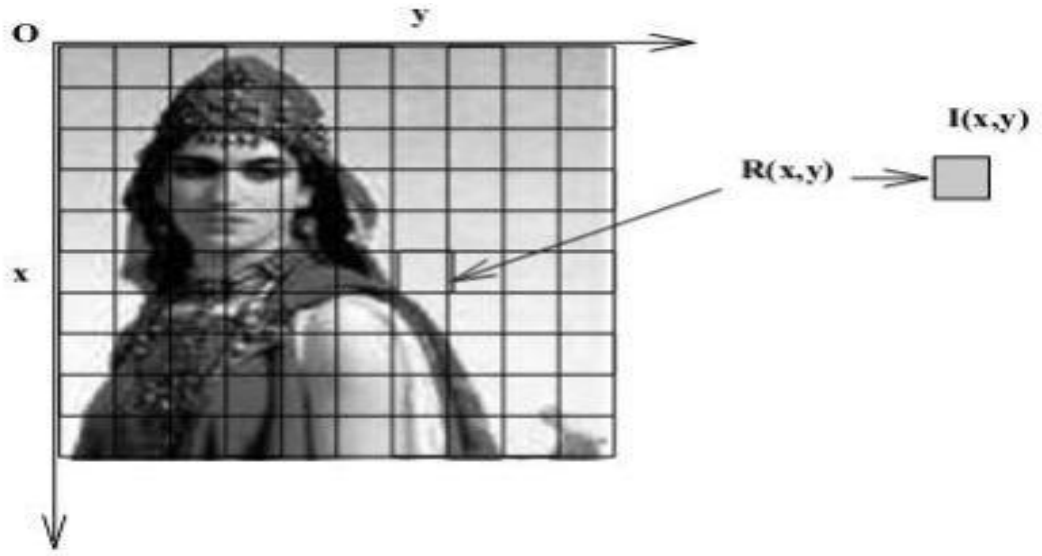


Figure 1.3. Echantillonnage discrétisation spatiale

1.4.2. La 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.

1.4.3. Codage des images numériques

1.4.3.1. 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.

1.4.3.2. Codage en niveaux de gris

Si on code chaque pixel sur 2 bit on aura 4 possibilités (noir, gris foncé, gris clair, blanc). L'image codée sera très peut 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 255le 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 bit. Il est donc compris entre 0 et 2^8-1. C'est la quantification la plus courante. On peut coder une image en niveau de gris sur 16 bit ou sur 1 bit : dans ce dernier cas « le niveau de gris » vaut 0 ou 1 : il s'agit alors d'une image binaire (monochrome)[5].

1.4.3.3. Codage d'une image couleur

On peut attribuer trois valeurs à chaque pixel : rouge (de 0 à 255), vert (de 0 à 255) et bleu (0 à 255). Chaque couleur est codée sur 1 octet = 8 bit. Chaque pixel est codée sur 3 octet c'est-à-dire 24 bit. On peut obtenir une couleur quelconque par addition de ces trois couleurs primaires en proportions convenables. On obtient ainsi 256x256x256 = 16777216 (plus de 16 millions de couleurs différentes).

1.5. Les type d'images numériques

Il existe deux sortes d'image numériques : les images vectorielles et les images matricielles.

1.5.1.L'image vectorielle

Les données sont représentées par des formes géométriques simples qui sont décrites d'un point de vue mathématique. Par exemple, un cercle est décrit par une information du type (cercle, position du centre, rayon). Ces images sont essentiellement utilisées pour réaliser des schémas ou des plans. Les logiciels de dessin industriel fonctionnent suivant ce principe. Les principaux logiciels de traitement de texte ou de PAO (publication assistée par ordinateur) proposant également de tel outil.

Ces images présentent deux avantages :

- Elles occupent peu de place en mémoire.
- Elles peuvent être redimensionnées sans perte d'information et sans effet d'escalier.

1.5.2.L'image matricielle

L'image matricielle (ou « image en mode point », ou en anglais un « bitmap») est une image numérique dont les donnée sont stockées dans une matrice de point appelés « pixel ». Les images matricielles sont créées par les imprimantes, scanners, appareils photographiques et certains logiciels d'infographique comme Photoshop [6].

Ces images présentent des avantages :

- Les images bitmap autorisent la qualité photographique.
- Des normes se sont imposées qui sont libres de droits d'auteur (ex. JPEG).
- Elles sont directement affichables par l'ordinateur qui affiche des 'points'.

Les inconvénients des bitmap :

- Leur taille est encombrante.
- L'agrandissement provoque un effet de distorsion : l'apparition des pixels [pixellisation].

1.6. Les caractéristiques d'une image numérique

Une image matricielle est caractérisée par :

- Sa définition.
- Sa résolution.
- Son codage ou profondeur de couleur exprimé en bit par pixel (bpp).
- Son mode colorimétrique (RGB ou CMNJ), composition des multiples couches.

1.6.1.Définition d'une image

La définition de l'image est le nombre fixe de pixels qui est utilisé pour représenter l'image dans ses deux dimensions. Pour une image analogique donnée, plus la définition est grande, plus la précision des détails sera élevée. Ce nombre de pixels détermine directement la taille des informations nécessaire au stockage de l'image. La dimension, en pixels, détermine le format d'affichage à l'écran (la taille des pixels de l'écran étant fixe).

1.6.2. Résolution

Il existe deux types de résolution dans une image. La résolution "spatiale" et la résolution "tonale".

- **Résolution spatiale**

C'est le nombre de point contenue dans une surface précise (en pouce). Elle est exprimée en point par pouce (PPP, en anglais : DPI pourDots Per Inch). Un pouce mesure 2.54 cm.

600*400 pixels/pouce 150*100pixels/pouce 38*25 pixels/pouce 10*7 pixels/pouce

Figure 1.4. Résolution spatiale

- **Résolution tonale (de tons de gris)**

La résolution "tonale" est le nombre de possibilité de nuances de couleur par pixel exprimée le plus souvent en nombre de couleurs ou en nombre de bits par pixel.

Figure 1.5. Résolution tonale

Règles mathématiques de calcul de résolution "tonale" :

2 puissance (nombre de bits) = nombre de couleurs possibles par pixel.

1.6.3. Profondeur de couleur

Une image numérique utilise plus ou moins de mémoire selon le codage des informations de couleur qu'elle possède. C'est que l'on nomme le codage de couleur ou profondeur des couleurs, exprimé en bit par pixel (bpp) : 1, 4, 8,16 bits… En connaissant le nombre de pixels d'une image et la mémoire nécessaire à l'affichage d'un pixel, il est possible de définir

exactement le poids que va utiliser le fichier image sur le disque dur (ou l'espace mémoire requis en RAM pour réaliser un calcul sur cette image).

Poids (octet) = nombre de pixel total * codage couleur (octet)

1.7. Format des images sur disque

Un format d'image est une représentation informatique de l'image associée à des informations sur la façon dont l'image est codée, et fournissant éventuellement des indications sur la manière de la décoder et de la manipuler.
Voici quelque format :

1.7.1. Principaux formes de fichiers non compressés

Ces formats de fichiers utilisent en général beaucoup de mémoire. De par leur poids élevé, ils ne sont pas adaptés pour le web mais doivent être utilisés lorsqu'on a besoin de préserver la totalité des informations d'une image pour retravailler dessus par exemple.

- **TIFF**

Le TIFF pour (tagged image file format) été mis au point en 1987.

Le format TIFF est un ancien format graphique, permettant de stocker des images bitmap de taille importante (plus de 4 Go compressées). Le format TIFF permets de stocker des images en noir et blanc, en couleurs réelles (jusqu'à 32 bit par pixels), ainsi que des images indexées faisant usage d'une palette de couleurs.

- **BMP**

Le BMP est un des formats les plus simples développé conjointement par Microsoft et IBM, ce qui explique qu'il soit particulièrement répandu sur les plates-formes Windows et OS/2. C'est un format ouvert non compressé. Sa taille rédhibitoire rend son utilisation en ligne difficile, mais sa grande compatibilité en fait un format de travail efficace. En BMP, la couleur est codé en RGB, le format lui-même supporte la palette 256 couleurs que le « truecolor» [7].

1.7.2. Principaux formats de fichier compressés

Ce sont les formats de fichiers qui permettent, selon un algorithme particulier, de gagner plus ou moins de mémoire en supprimant certaines informations peu ou non perceptibles par

l'œil humain. Ils sont particulièrement adaptés à l'internet. On les utilisera donc pour exporter des images destinées à la visualisation sur internet ou à l'archivage.

- **JPEG**

Ce format est l'un des plus complexes, son étude complète nécessite de solides bases

mathématiques. Cependant malgré une certaine dégradation de l'image, 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 perte" et s'appuie sur l'algorithme de transformée en cosinus discret DCT. Un mode "sans perte" a ensuite été développé mais n'a jamais été vraiment utilisé. Cette norme de compression a été développé par le comité JPEG (joint photographique experts group) et normalisée par I'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.

Le JPEG 2000 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'image qui s'appuie sur un mécanisme de compression par ondelettes.

- **GIF**

GIF (graphic information format) : c'est un format léger qui peut également contenir des animations. Une image GIF ne peut contenir que 2, 4, 8, 18, 32, 64, 128 ou 256 couleurs parmi 16.8 millions dans sa palette en mode RGB. Elle supporte également une couleur de transparence.

- **PNG et MNG**

Le PNG pour portable network graphique (ISO 15948) a été développé par le W3C pour remplacer le GIF. Il surpasse ce dernier car 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 petit logos. Coté photo, s'il permet une compression sans perte, le poids de la photo n'est pas compétitif avec les formats JPEG. Le PNG ne gère pas l'animation mais un format dérivé, le MNG, y est destiné[8].

1.8.Aspects du traitement d'images

Dans cette section, nous présentons trois aspects du traitement d'image : le filtrage la compression et le tatouage.

1.8.1. Filtrage

Pour améliorer 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.

1.8.1.1.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 utilisé pour atténuer le bruit de l'image, c'est la raison pour laquelle on parle habituellement de lissage.

1.8.1.2. Filtre passe-haut (accentuation)

Le filtre passe-haut atténue les composantes de basse fréquence de l'image et permet 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.

1.8.1.3.Filtre passe-bande (différentiation)

Cette opération est une dérivée du filtre passe-bas et filtre passe-haut. 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.

1.8.2.La compression

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

1.8.2.1.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 des informations après une procédure de décompactage.

1.8.2.2.La compression avec perte

Concerne essentiellement les fichiers média (image, son, vidéo), elle consiste en une « réduction » de l'information basé sur notre propre limite humaine à percevoir ces médias. Puisque l'œil 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 très ressemblant à l'original voire identique, pour l'œil humain.

1.8.3. Le tatouage

Le tatouage numérique consiste à insérer une marque invisible (dans certain cas visible) appelée aussi signature, (ou tatouage) dans une image ou dans d'autres documents numériques pour divers buts tel que la lutte contre la fraude, le piratage informatique et la protection des droits d'auteur. La marque insérée est essentiellement une séquence aléatoire, un logo binaire ou une image à niveaux de gris : elle doit être connue uniquement par le propriétaire ou par le diffuseur [10].

1.9. Les pixels

Contraction de l'expression anglaise « Picture éléments » : éléments d'image, le pixel est le petit point de l'image ; c'est une unité calculable qui peut recevoir une structure et une quantification. Le pixel est le plus petit élément que peuvent manipuler les matériels et logiciels d'affichage ou d'impression.

Les pixels sont approximativement rectangulaires, parfois carrées. Leur dimension peut être changée en réglant l'écran ou la carte graphique. Habituellement, on indique la taille de l'écran en donnant la longueur de la diagonale, en pouce le matériel informatique.

Voici quelques exemples :

	Taille écran			
	14 soit 35,56 cm (28,8cm x21,6cm)	17 soit 43,18 cm (34,4cm x25 cm)	19 soit 48,26 cm (38,4cm x28,8cm)	21 soit 53,3 cm (42,4cm x 31cm)
Définition de l'écran	**Taille de pixel (mm x mm)**			
VGA (640 x 480 px)	0,45 x 0,45	0,54 x 0,54	0,60 x 0,60	0,66 x 0,66
XGA (1024 x 768 px)	0,28 x 0,28	0,34 x 0,34	0,37 x 0,37	0,41x 0,41
SXGA (1280 x 1024 px)	0,225 x 0,211	0,269 x 0,252	0,300 x 0,281	0,331 x 0,311
UXGA (1600 x 1200 px)	0,180 x 0,180	0,215 x 0,215	0,240 x 0,240	0,265 x 0,265

Tableau1.1.Exemple sur les pixels

1.9.1. Occupation mémoire d'un pixel

Pour l'informatique, un pixel est codé sur un ou plusieurs bits :

- Noir et blanc : un bit.
- 16 couleurs (standard VGA) :4 bit
- 256 couleurs (ou 256 niveaux de gris, ce qui revient au même en termes d'occupation mémoire) : 8 bits (1 octet).
- 65536 couleurs (milliers de couleur) : 16 bits.
- 16777216 couleurs (16,7 millions de couleur) : 24 bits.

La place mémoire réelle utilisée peut être plus importante. Par exemple, en mode 16 millions de couleurs, le pixel occupe parfois 32 bits (4octets), l'octet supplémentaire étant inutilisé pour coder la transparence. Les appareils photographiques professionnels enregistrent jusqu'à 16 bits par couleur, soit 48 bits.

1.10. Conclusion

Dans ce chapitre, nous avons présenté les images numériques d'une manière générale. Nous nous sommes intéressés aux terminologies et aux notions pertinentes dans le domaine des images numériques telles que la numérisation le codage et le stockage. Nous avons également présenté quelques aspects du traitement d'image, tels que le filtrage, la compression et le tatouage.

Chapitre 2
Le tatouage des images numériques

2.1. Introduction

Le tatouage numérique est un domaine scientifique assez récent apparu au début des années 90 et il présente de multiples intérêts. Dans ce chapitre, on présentera le principe du tatouage numérique des images. Après avoir donné un aperçu historique sur cette technique et sur les techniques de dissimulation de l'information, nous présenterons le tatouage numérique et ses différentes étapes qui conduisent à l'insertion de la marque. Nous présenterons ensuite les différentes applications possibles du tatouage numérique pour les images. A la fin de ce chapitre nous présenterons brièvement l'évaluation en termes d'imperceptibilité et de robustesse des schémas de tatouage numérique des images.

2.2.Historique et terminologie

2.2.1.Historique

Les tatouages du papier sont apparus dans l'art de la fabrication du papier il y a presque 700 ans. Le plus ancien document tatoué trouvé dans les archives remonte à 1292 et à son origine dans la ville de Fabriano en Italie qui a joué un rôle important dans l'évolution de l'industrie papetière. A la fin du troisième siècle, environ 40 fabricants du papier partageaient le marché du papier.

La concurrence entre ces fabricants était très élevée et il était difficile que n'importe quelle partie maintienne une trace de la provenance du papier et ainsi que son format et sa qualité. L'introduction des tatouages était la méthode parfaite pour éviter n'importe quelle possibilité de confusion. Après leur invention, les tatouages se sont rapidement étendus en Italie et puis en Europe et bien qu'au commencement ont été 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 numérique sont été publié par Tanaka et al [2]. En 1990 et par Tirkel et al [3]. En 1993.

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 d'avantage de recherches des méthodes de travail et des systèmes pratiques ont été développés [11].

La figure 2.1 montre le nombre de publications avec le mot clé "watermarking" sur la base de données bibliographique INSPEC[12].

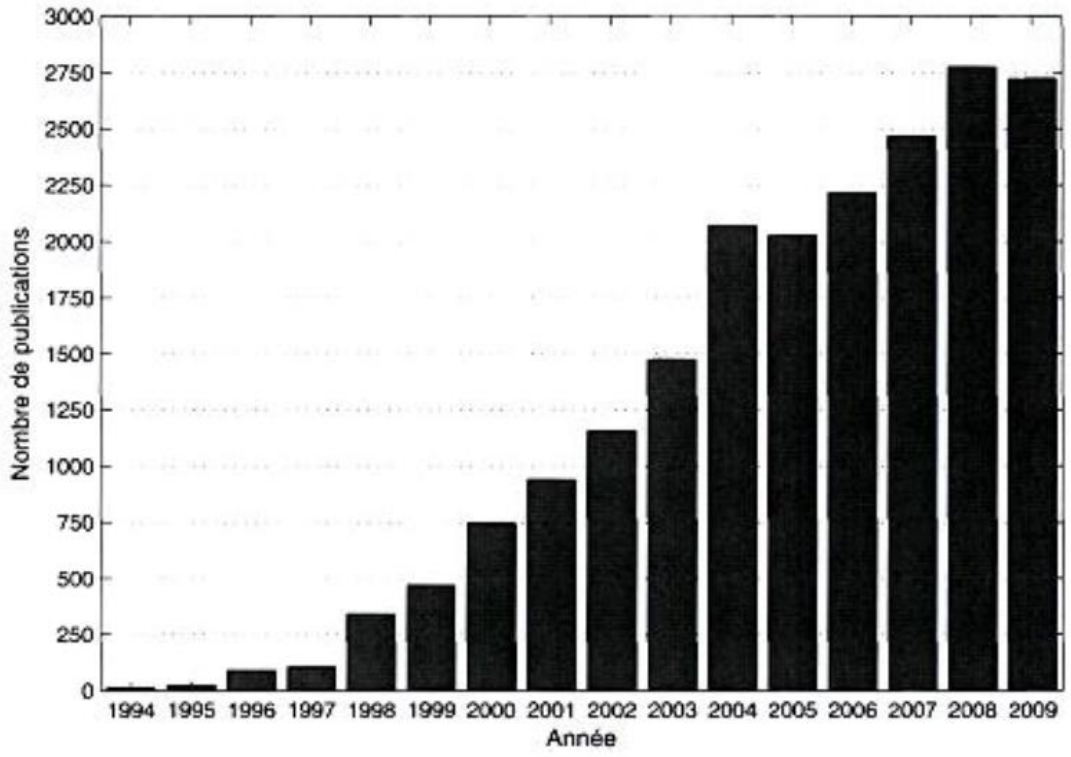


Figure 2.1. Nombre de publications sur le tatouage numérique (INSPEC - juin 2010)

2.2.2. Terminologies

- **Tatouage visible et invisible**

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

a) Tatouage visible

Le tatouage visible est très simple. Il est équivalent à l'estampage d'un watermark sur le papier, et pour cette raison il est appelé parfois estampage numérique. Le tatouage visible altère le signal ou le fichier (par exemple : ajout d'une image pour en marquer une autre). Il est fréquent que les agences de photo ajoutent un watermark visible en forme de copyright (©) aux versions

de pré-visualisation (basse résolution) de leurs photos. Ceci à fin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

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

Figure 2.2. Exemple d'un tatouage visible

b) Tatouage invisible

En revanche, le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le signal d'une manière imperceptible par l'utilisateur final. Pour reprendre l'exemple de l'agence de photo, les photos hautes résolutions vendues par l'agence possèdent au contraire un watermark invisible, qui ne dégrade pas le contenu visuel de ces images et permet de détecter l'éventuelle source d'un vol. Le message caché par le tatouage peut être un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur [13].

Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs [14]. La majorité des techniques concernant la protection de propriété intellectuelle suit la branche du tatouage invisible.

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

a) Image originale b) Image tatouée

Figure 2.3. Exemple d'un tatouage invisible

2.3. Définition du tatouage numérique

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc..). Une des particularités du tatouage numérique, 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 détecté ou extrait même si le document a subi des modifications ou s'il est incomplet [15].

2.4. Modèle générique du tatouage

Le système typique du tatouage numérique comprend deux sous-systèmes : le sous-système d'insertion du watermark (appelé aussi la phase de codage) et le sous-système de détection/extraction(appelé aussi la phase de décodage).

Le sous-système d'insertion (embedding) comprend en entrée un watermark *W* un document hôte (porteur) *I* et une clé secrété *K* spécifique au tatouage. Cette dernière est utilisée pour renforcer la sécurité de tout le système

La phase d'insertion génère en sortie un document tatoué *Iw,* cette phase est modélisée par la fonction suivante :

$$Iw=\mathbf{E}\ (\mathbf{I, W, K}).$$

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

La phase de détection/extraction prend en entrée le document tatoué et éventuellement attaqué*Iw**, la clé *K* et éventuellement (dépend de la méthode utilisée), le document original *I* et /ou le watermark original *W*.

La phase de détection consiste à prouver la présence du watermark en utilisant une mesure de confidentialité ρ. Elle est modélisée par la fonction:

$$\rho=\mathbf{D}\ (Iw*, K)$$

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

$$W' =\mathbf{D}(I*w,K)$$

I et *W* sont des paramètres optionnels pour la fonction D. [**1], [9]**

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

- Le watremark W' doit être détecté à partir de *Iw*avec/ou sans la connaissance explicite de *I*.
- Si *Iw*n'est pas modifié (attaqué), alorsW' correspond exactement à W.

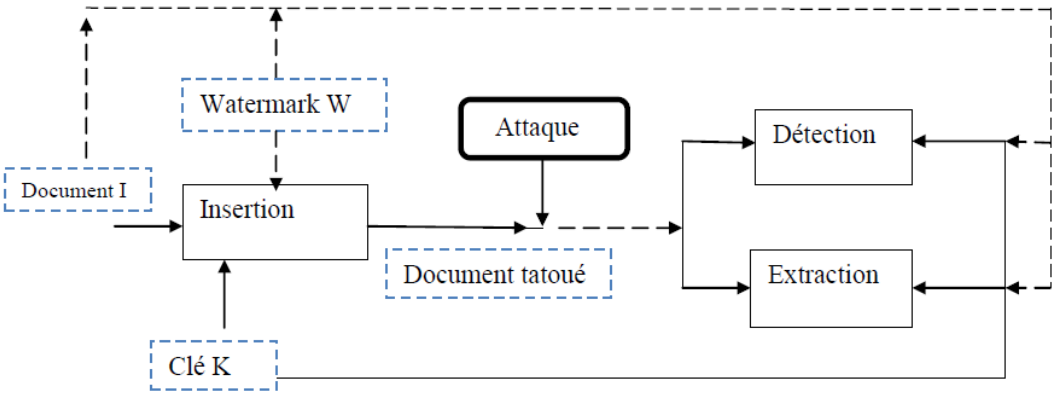


Figure 2.4. Modèle générique d'un système du tatouage

2.5. Conditions requises pour les techniques du tatouage d'images numériques

Les méthodes du tatouage requiérent différent propriétés selon leurs domaines d'application et leurs finalités. Le watermark caché dans une image doit remplir certaines conditions essentielles :

- **Imperceptibilité**

Le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée.

Le watermark inséré 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.

- **Robustesse et fragilité**

La robustesse est le pouvoir de récupérer la marque insérée même si l'image tatouée a été manipulée par des attaques. Il est nécessaire de distinguer plusieurs types d'attaques selon qu'elles sont considérées comme étant bienveillantes ou malveillantes. Les attaques bienveillantes sont les manipulations effectuées de bonne foi par un utilisateur. On retrouve dans cette catégorie : la compression JPEG, certaines transformations géométrique, le filtrage spatial et fréquentiel, l'ajout de bruit, l'impression et la numérisation, la correction gamma et l'égalisation d'histogramme.

Il est néanmoins intéressant de remarquer qu'il peut être utile, dans certain cas de favoriser une fragilité plutôt qu'une robustesse. Pour s'assurer par exemple l'intégrité d'un document, le fait de tatouer avec un algorithme fragile permettra, par la suite de vérifier si l'information tatouée est toujours présente, ce qui sous entends donc qu'elle n'a subit aucune modification malveillante [16].

- **Sécurité**

La sécurité constitue une troisième contrainte indépendante des deux premières. Elle concerne par exemple la génération de la clé secrète, ainsi que le protocole d'échange général. La méthode du tatouage doit également respecter le principe suivant énoncé par Kirchhoff:" L'algorithme lui-même doit pouvoir être rendu public. La sécurité ne dépend 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 ne savent pas le processus du tatouage.

- **Capacité à transférer les informations**

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

2.6. Applications du tatouage numérique des images

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

- **Protection du droit d'auteur**

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

- **Authentification du contenu d'une image**

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

- **Contrôle du nombre de copies**

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

❖ **Autres applications**

Il existe d'autres applications telles que l'indexation et contrôle d'accès, etc.

2.7. Classification des algorithmes de tatouage numérique

Au cours des deux dernières décennies, plusieurs schémas du tatouage numérique des images ont été développés pour diverses applications. A première vue ces schémas semblent très différents les uns des autres. Dans cette section, nous présentons une classification des algorithmes de tatouage numérique des images. Cette classification peut se faire selon différents critères tel que : le domaine d'insertion, la robustesse, la technique d'insertion utilisée le mode d'extraction, la perception de la marque et préservation de l'image originale. La figure 2.5 présente un organigramme de cette classification [8].

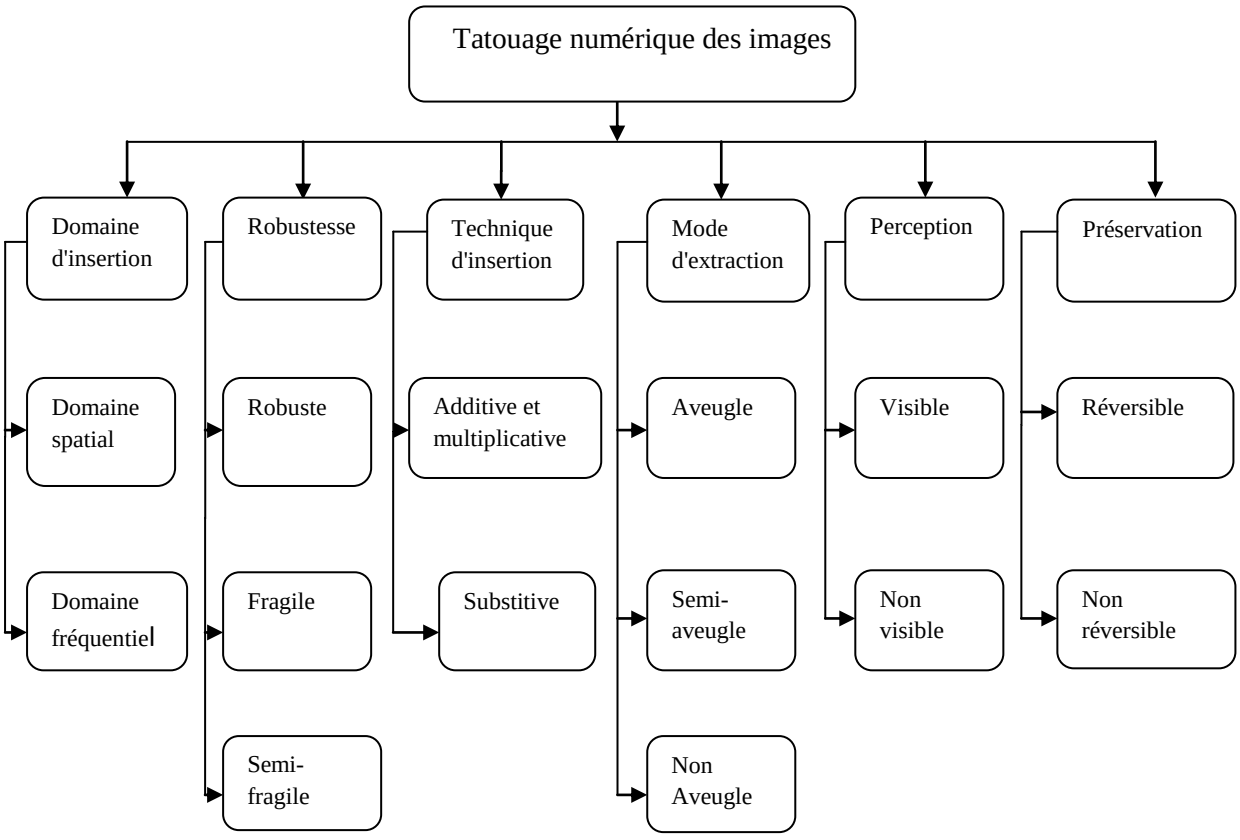


Figure 2.5. Organigramme de classification des algorithmes de tatouage numérique

2.7.1. L'algorithme de détection : Aveugle, Semi-aveugle et Non aveugle

Le tatouage aveugle est la plus forme ancienne du tatouage. Il n'oblige pas l'extracteur d'avoir connaissance de l'image originale, ni du watermark. Seule l'image tatouée et la clé secrète

doivent être disponibles au moment de l'extraction. La fonction d'extraction est modélisée comme suite :

$$W' = \mathbf{D}\ (I^{*}w, \mathbf{K})$$

Dans le cadre d'un système semi-aveugle, nous avons besoin d'informations supplémentaires pour aider la détection ou l'extraction. Cette demande est due à la perte de synchronisation à cause du canal bruité ou de la technique d'insertion. La phase d'extraction requière le watermark ou l'image tatouée (l'image originale juste après l'incrustation du watermark) [17].

La fonction d'extraction est modélisée comme suit :

$$W' = \mathbf{D}\ (I^{*}w, \mathbf{K}, \mathbf{W},)$$

Au contraire du tatouage aveugle, les algorithmes de marquage non-aveugle nécessitent toujours l'image originale. En se basant sur le modèle générique présenté dans la section précédente la fonction d'extraction est modélisée comme suit :

$$W' = \mathbf{D}\ (I^{*}w, \mathbf{K}, \mathbf{I})$$

Le nombre d'algorithmes non-aveugle n'est pas important par rapport aux nombreux algorithmes semi-aveugles et aveugles. Ceci est dû au fait que la disponibilité des données originales au moment de l'extraction du watermark, ne peut être toujours garantie.

Les termes tatouage aveugle, semi-aveugle et non-aveugle peuvent être désignés respectivement par tatouage publique, semi-privé et privé dans certains articles [18].

2.7.2. La robustesse de l'algorithme : Fragile, Semi-fragile et Robuste

Dans le tatouage fragile, le watermark est fortement sensible aux modifications de l'image tatouée. Cette approche sert à prouver l'authenticité et l'intégrité d'un fichier tatoué.

Le tatouage semi-fragile a pour objectif de reconnaitre les perturbations malintentionnées et se rester robuste à certaines classes de dégradations légères de l'image, comme la compression avec pertes par exemple.

Le tatouage robuste dispose d'un large champ de théories et de résultats. Celui-ci cherche à préserver les données cachées face aux attaques. Le watermark doit donc être suffisamment résistant aux attaques afin de rester identifiable [12].

2.7.3. La préservation de l'image originale : Inversible et Non-inversible

Le tatouage inversible permet de récupérer toutes les propriétés originales de l'image hôte après l'extraction du watermark.

Dans le tatouage non-inversible, l'image originale est définitivement altérée par le mécanisme d'insertion du watermark. La matrice originale de pixels est irrécupérable. La plupart des méthodes citées jusqu'ici sont non-inversibles.

2.7.4. La technique d'insertion : Additif et Substitutif

Dans le tatouage additif, le message à ajouter n'est pas corrélé à l'image hôte. La plupart des techniques du tatouage aveugle sont basées sur une insertion additive.

Le tatouage substitutif modifie les bits de l'image hôte afin de les faire correspondre au watermark. Ce type de marquage est connu comme tatouage par contrainte, parce qu'il force l'image hôte à respecter certaines propriétés qui déterminent le watermark [19].

2.7.5. Classification selon le domaine d'insertion

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

2.7.5.1. 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. La plus part des techniques spatiales sont basées sur l'addition d'une séquence pseudo-bruit(PN) d'amplitude fixe.

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 continues dans les bits LSB sont visuellement insignifiantes en utilisant la connaissance de la séquence PN (et peut être la connaissance d'une clé secrète, Le watermark est généralement inséré, comme la location du watermark) [20].

2.7.5.2. Domaine Fréquentiel

Les algorithmes travaillant dans le domaine fréquentiel incluent le watermark non pas directement dans l'image mais dans une transformée de cette image. Ce type de tatouage est plus robuste, et permet en plus de choisir les pixels qui seront plus résistants à certain type d'attaques.

Plusieurs schémas du tatouage peuvent effectuer l'insertion du watermark dans des espaces transformés. Un espace transformé est obtenu après l'emploi d'une transformée comme: la DFT (transformée de fourrier rapide),DCT(transformée en Cosinus Discrète) DWT(transformée en ondelette discrète)etc... Cette stratégie rend le watermark plus robuste face à la compression, puisqu'elle utilise le même espace qui sert au codage de l'image. Contrairement au domaine spatial, le watermark inséré dans le domaine fréquentielles très sensible aux transformations géométriques parce que ce genre de transformations modifie considérablement les valeurs des coefficients transformés [21].

2.7.5.2.1. Transformée en Cosinus Discrète (DCT)

Cette transformation a été inventé par Nasir Ahmed en 1974 dans son article appelé “traitement d'image et la transformation cosinus discrète". La norme de compression connue JPEG l’utilise dans son implémentation.

Cette méthode de transformation permet de séparer les basses fréquences des hautes fréquences comme il est indiqué sur la Figure (2.6).

L’intégralité de l’information de l’image se trouve dans les basses fréquences. Par contre les détails de l’image se localisent en hautes fréquences. Si la marque est insérée dans les BF le tatouage sera robuste mais la marque sera visible. Si la marque est insérée dans les HF, elle sera invisible mais le tatouage ne sera plus robuste à cause des opérations de compressions. Donc pour trouver un compromis entre la visibilité et la robustesse, la marque est insérée dans les moyennes fréquences.

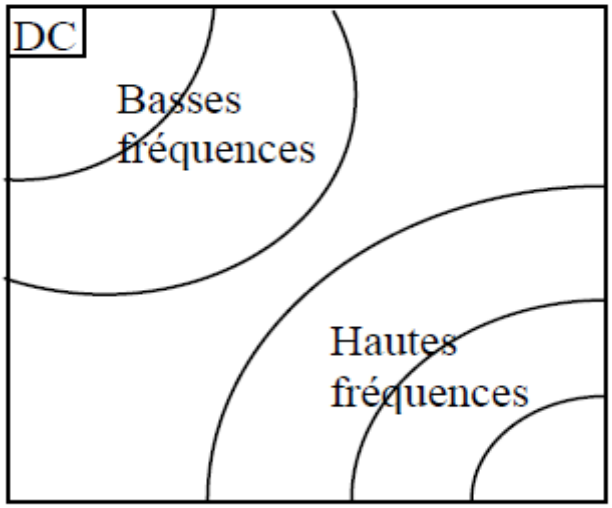


Figure 2.6. Répartition des fréquences

La transformation en cosinus discrète de l'image MxN est définie comme suit:

$$F = (u, v) = \left(\frac{2}{N}\right)^{1/2} \left(\frac{2}{M}\right)^{1/2} A(u).A(v) \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} I(i,j).\cos\left[\frac{\pi.u}{2.N}(2i+1)\right].\cos\left[\frac{\pi.v}{2.M}(2j+1)\right]$$

Et la transformation inversée IDCT est définie comme suit :

$$I(i,j) = \left(\frac{2}{N}\right)^{1/2} \left(\frac{2}{M}\right)^{1/2} \sum_{u=0}^{N-1} \sum_{v=0}^{M-1} A(u).A(v).F(u,v) \cos\left[\frac{\pi.u}{2.N}(2i+1)\right].\cos\left[\frac{\pi.v}{2.M}(2j+1)\right]$$

A cause de ces caractéristiques, la DCT est souvent utilisée dans les algorithmes de tatouage numérique des images, et la plupart des algorithmes basés sur cette transformée cache le message secret dans les moyennes fréquences. Les auteurs de ces méthodes espèrent ainsi anticiper et prévenir au moins les attaques liées à une compression JPEG.

Dans la plupart de cas, on divise l'image en blocs 8x8 et on applique cette transformation sur l'image. Donc, la transformation est 0comme suivante :

$$I(i,j) = \frac{1}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} A(u).A(v).F(u,v).\cos\left[\frac{\pi.u}{16}(2i+1)\right].\cos\left[\frac{\pi.v}{16}(2j+1)\right]$$

$$A(i) = \begin{cases} \frac{1}{\sqrt{2}} \; si \; \varepsilon = 0 \\ 0 \; viceversa \end{cases}$$

N,M: dimensions de l'image.

I(i,j): intensité du pixel dans la ligne i et colonne j.

F(u,v):le coefficient DCT dans la ligne u et colonne v.

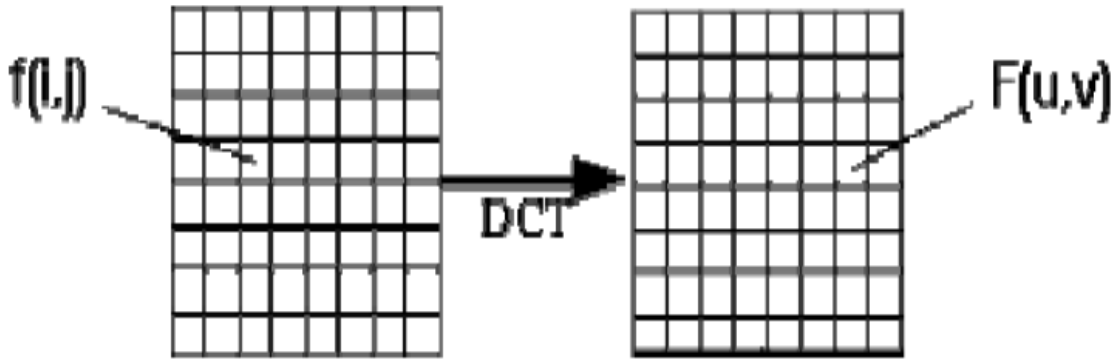


Figure 2.7.Application de la DCT sur un bloc 8x8

2.7.5.2.2. Décomposition en valeurs singulières(SVD)

La théorie de la décomposition en valeurs singulières a été établie pour les matrices réelles carrées dans les années 1870 par Beltrani et Joadan et pour les matrices complexes par Autonne en 1902. Récemment, la décomposition en valeurs singulières a été utilisée dans différents applications du traitement d'image telle que la compression, la dissimulation de l'information et la réduction du bruit.

- **Principe**

Soit **A**une matrice quelconque de taille m*n de rang r (le rang de la matrice A est le nombre de valeurs singulières non nulles). Alors il existe une matrice orthogonale **U** d'ordre m*m une matrice orthogonale **V** d'ordre n*n et une matrice "pseudo-diagonale" **S** de dimension que **A** telles que :

$$\mathbf{A=U*S*V^T}$$

$$\begin{cases} U * U^T = I(m) \\ V * V^T = I(n) \\ s(m,n) = \begin{bmatrix} S1 & 0 & 0 \\ 0 & S2 & 0 \\ 0 & 0 & Sn \end{bmatrix} \end{cases}$$

S1, S2…..Sn sont les valeurs singulières de A.

Ce sont des nombres réels et nom négatifs et qui respectent la condition : S1>S2>S3>…..>Sn

- **L'intérêt de la SVD pour le traitement d'images**

Le principal intérêt de cette méthode vient de fait que :

- Les valeurs singulières représentent l'énergie de l'image, c'est-à-dire que la SVD range le maximum d'énergie de l'image dans un minimum de valeurs singulières.
- Les valeurs singulières d'une image ont une très bonne stabilité, c'est-à-dire que quand une petite perturbation (par exemple une marque) est ajoutée à une image, les valeurs singulières ne changent pas significativement.
- En plus, la factorisation en SVD est unique.

2.8. Attaque sur les images tatouées

Un des critères fondamentaux à prendre en compte lors la conception d'un algorithme de tatouage numérique est la marque. En effet, la marque doit résister aux différentes attaquesNous proposons dans la Figure une classification en trois catégories :

- Les attaques d'effacement.
- Les attaques géométriques.
- Les attaques de sécurité.

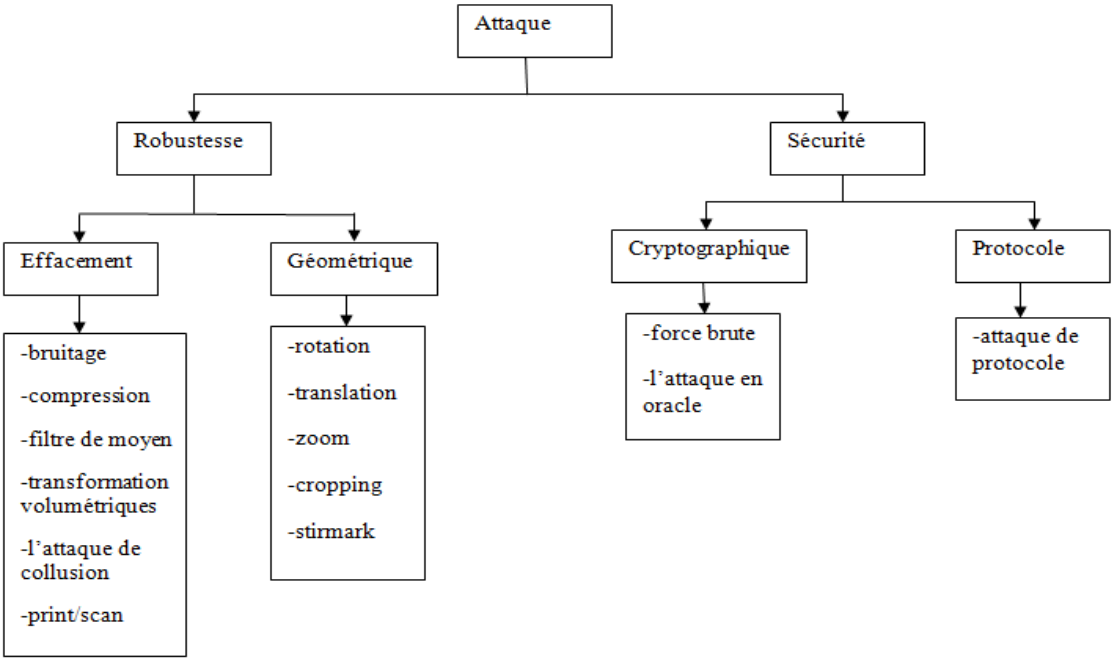


Figure 2.8.La classification des attaques que peut subir un document tatoué

2.8.1. Attaque d'effacement

Ce sont des attaques liés à l'image (ou au signale de watermark), dont le but est de faire disparaitre le watermark masqué dans l'image. Cela se résume à des transformations plus ou moins violentes. Ces transformations ont pour but de rendre illisible le marquage. Il est intéressant de remarquer néanmoins que ces attaques ne sont pas forcément volontaires. En effet sans le savoir, l'image peut être dégradée suffisamment pour que le tatouage soit effacé. Un algorithme de marquage robuste est sensé résister de manière efficace à ce type de transformations, ou du moins tant que l'image reste utilisable. Nous citons par exemple:

- **Attaque par filtrage**

Le filtrage correspond à l'augmentation (resp. la diminution) des composantes hautes fréquences. En effet, l'ajout d'un bruit blanc gaussien ou un filtre moyen permet de désynchroniser la phase de l'insertion et la détection. Un exemple simple, si le marquage est effectué en modifiant la luminance de certains pixels. Il suffit alors d'effectuer un filtre passe-bas sur l'image afin d'avoir alors la quasi-certitude de détruire complètement le tatouage.

- **Attaque par mosaiques**

Ce type d'attaque a comme principe de découper l'image en plusieurs morceaux, qui sont ensuite juxtaposés. On peut donc la regarder sans s'apercevoir de la munipulation, mais le tatouage est totalement désynchronisé si sa détection est automatisée. Cette attaque vise les moteurs de recherche automatique (crawlers) des marques dans les images sur internet.

- **Transformations volumétriques**

Le principe de ce type d'attaque est de changer 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.

- **Compression**

La compression avec perte cherche à simplifier le codage du document, en supprimant l'information peu significative ; comme le tatouage est imperceptible, il est naturellement considéré comme peu significatif. En fait, les algorithmes dans le domaine spatial souffrent des attaques par compression. Dans le but d'augmenter la robustesse face à la compression l'une des techniques de tatouage consiste à mettre en évidence la simulation d'un processus de

compression dans la mise ou point d'un algorithme de tatouage, d'autre technique consistent à concevoir des algorithmes de tatouage adaptés au contenue des images dans le domaine DCT ou DWT.

- **Conversion analogique-numérique**

La conversion analogique-numérique entraine en générale une désynchronisation du signal de tatouage, ainsi que de petites distorsions. Par exemple, le processus d'impression suivie d'un scan (print/scan) d'une image, l'enregistrement d'un film à l'aide d'un caméscope dans une salle de cinéma ou le réenregistrement de la musique.

2.8.2. Attaque géométriques

Ce genre de transformation a pour effet de désynchroniser le signal de tatouage, ce qui empêche la détection de la marque, c'est-à-dire la difficulté de localiser la marque en empêchant ou diminuant l'exactitude de celle-ci. Il existe plusieurs transformations géométriques. Certaines sont utilisées couramment dans le traitement d'image, nous citons les plus usuelles :

Rotation : des petite angles de rotation, n'ont pas l'habitude de changer la valeur commerciale de l'image, mais peuvent le watermark non détectable.

Scaling(modification des dimensions) : ce type d'opération est appliqué quand une image imprimée est scannée ou quand une image numérique de haute résolution est utilisée pour des applications électroniques, telles que la publication Web.

Cropping(rognage) : supprimer ou couper une partie d'une image qui s'étend au-delà d'une certaine limite, le borne de la fenêtre, par exemple. Certains programmes graphiques autorisent aussi le rognage comme moyen de tout masquer, sauf un objet donné, afin que les outils de dessin s'appliquent à l'objet seul.

Stirmark : consiste à appliquer une succession de distorsions géométriques aléatoires appliquées globalement et localement à plusieurs endroit dans l'image [22]

L'image originale

Figure 2.9. La distorsion géométrique locale appliquée par Stirmark

Bien que plusieurs méthodes de tatouage soient plus robustes à plusieurs attaques d'effacement, souvent elles ne sont pas robustes aux attaques géométriques. Une solution consiste à utiliser en parallèle des techniques de synchronisation spéciales pour résister à ces attaques. Ces techniques reposent souvent sur l'utilisation soit d'un domaine d'une transformation invariante (Fourier-Mellin), l'ajout d'un pattern de synchronisation (insertion d'un template) [23],[24] ou des marques périodiques[25]. Cependant, en exploitant la connaissance préalable du système de synchronisation utilisé, l'attaque peu concevoir des attaques dédiées pour introduire une désynchronisation entre la phase d'insertion et celle de la détection.

2.8.3. Attaque sur la sécurité

La plupart des algorithmes de tatouage sont publiques, alors si on suppose qu'un pirate connait l'algorithme mais il n'a aucune information le secret (comme par exemple des porteuses ou des clefs secrètes). Il lui suffit d'avoir plusieurs documents tatoués puis observer la réponse des documents modifiés à la zone de détection et de choisir celui qu'est proche d'un documents modifiés à la zone de détection et de choisir celui qu'est proche d'un document tatoué sans modification mais en hors de la zone de détection. Parmi les attaques sur la sécurité nous citons :

- **L'attaque de cryptographie**

Le principe consiste à rendre un système de tatouage inutilisable en exploitant des failles dans la gestion des clés (déchiffrer la clé) et ensuite de faire disparaitre de la marque de tatouage, d'accéder aux informations confidentielles, ou de tatouer un document en s'appropriant illégalement une identité. On distingue généralement deux types : l'attaque par force brute qui consiste à tester toutes les clés possibles. L'autre est l'attaque en oracle

imaginée par Linnartz et al [26]. Dans cette attaque le pirate insère des contenus en entrée au décodeur puis observe en sortie les messages décodés afin d'estimer la forme de la frontière entre les documents tatoués et les documents non tatoués [27].

- **Attaques de protocoles**

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

- **L'attaque de collusion**

Dans ce type d'attaque suppose que le pirate dispose de plusieurs versions d'un document sans tatouage. Une modélisation par la théorie des jeux [28] consiste à formaliser la rivalité naturelle entre le tatoueur et l'attaquant et d'établir une stratégie optimale de tatouage.

2.9. Conclusion

Dans ce chapitre, nous avons présenté la technique du tatouage numérique d'une manière générale. Nous nous sommes intéressés aux terminologies et notions liées aux tatouages invisibles des images numériques. Nous avons présenté aussi les techniques du tatouage selon différents critères, les types d'algorithmes, les champs d'application et les domaines d'insertion.

Chapitre 3
Simulation des algorithmes de tatouage

3.1. Introduction

Dans ce chapitre, nous allons présenter les algorithmes et les différents résultats pratiques obtenus du tatouage numérique des images. Le tatouage est réalisé d'abord en utilisant la SVD (décompositions en valeurs singulières) seule puis en combinant la SVD avec la DCT. Nous allons évaluer les performances de ces techniques en termes d'invisibilité de la marque et de robustesse face aux diverses attaques telles que la compression, le filtrage, l'ajout de bruit le recadrage. En conséquence, pour construire un algorithme de tatouage efficace il faudra dans le meilleur des cas trouver un compromis entre les trois aspects (invisibilité capacité et robustesse).Tous les programmes sont réalisés avec Matlab 2013.

3.2. Mesure de qualité

La notion de qualité intervient deux fois dans le cahier de charge d'un processus de tatouage parce que :

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

3.2.1. Le PSNR

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

$$\text{PSNR}=10 * log_{10}(\frac{d^2}{EQM})$$

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

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

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

- I_o : l'image originale.

- I_r: l'image reconstruite.

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

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

3.2.2. Le coefficient de corrélation normalisé

Le coefficient de corrélation simple est un indice de mesure de l'intensité d'un lien qui peut exister entre deux variables. Le coefficient de corrélation peut prendre une valeur comprise entre -1 et +1. S'il est égal à 0, cela signifie qu'il n'existe aucun lien entre ces deux variables. Il est généralement utilisé dans le cadre de l'analyse de variables quantitatives.

- **Aspects mathématiques**

Le coefficient de corrélation simple est égal à la division entre la covariance entre X et Y et le produit des écarts-types :

$$\text{Cor}(X,Y)=\frac{\boldsymbol{Cov(X,Y)}}{\boldsymbol{\sigma_X \sigma_Y}}$$

- **Cas pratique**

Dans le cadre d'un échantillon de taille n :

$$r = \frac{\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} (\boldsymbol{X_i - \bar{X}})(\boldsymbol{Y_i - \bar{Y}})}{\sqrt{\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} (\boldsymbol{X_i - \bar{X}})^2 \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} (\boldsymbol{Y_i - \bar{Y}})^2}}$$

r est donc un estimateur dit le coefficient de corrélation d'échantillonnage. Pour le tatouage la valeur optimale de $|r| = 1$, lorsque r est proche de 1 on a de bons résultats.

3.3. Algorithmes de tatouage en utilisant la SVD seulement

Dans cette section, nous allons présenter les algorithmes de tatouages d'images en niveaux de gris basées sur la SVD. La marque est insérée dans la matrice U, puis dans la matrice S. Une étude comparative entre les deux algorithmes est réalisée dans ce qui suit. Notons que le principe de la décomposition SVD d'une matrice est déjà expliqué dans le deuxième chapitre.

3.3.1. Algorithme utilisant la matrice U

Dans cet algorithme la marque est insérée dans la matrice U.

3.3.1.1. Algorithme d'insertion

L'algorithme d'insertion est expliqué par le schéma synoptique suivant la Figure 3.1. Le résultat dépend de la constante α. Elle est choisie expérimentalement et elle peut être vue comme une clé privée.

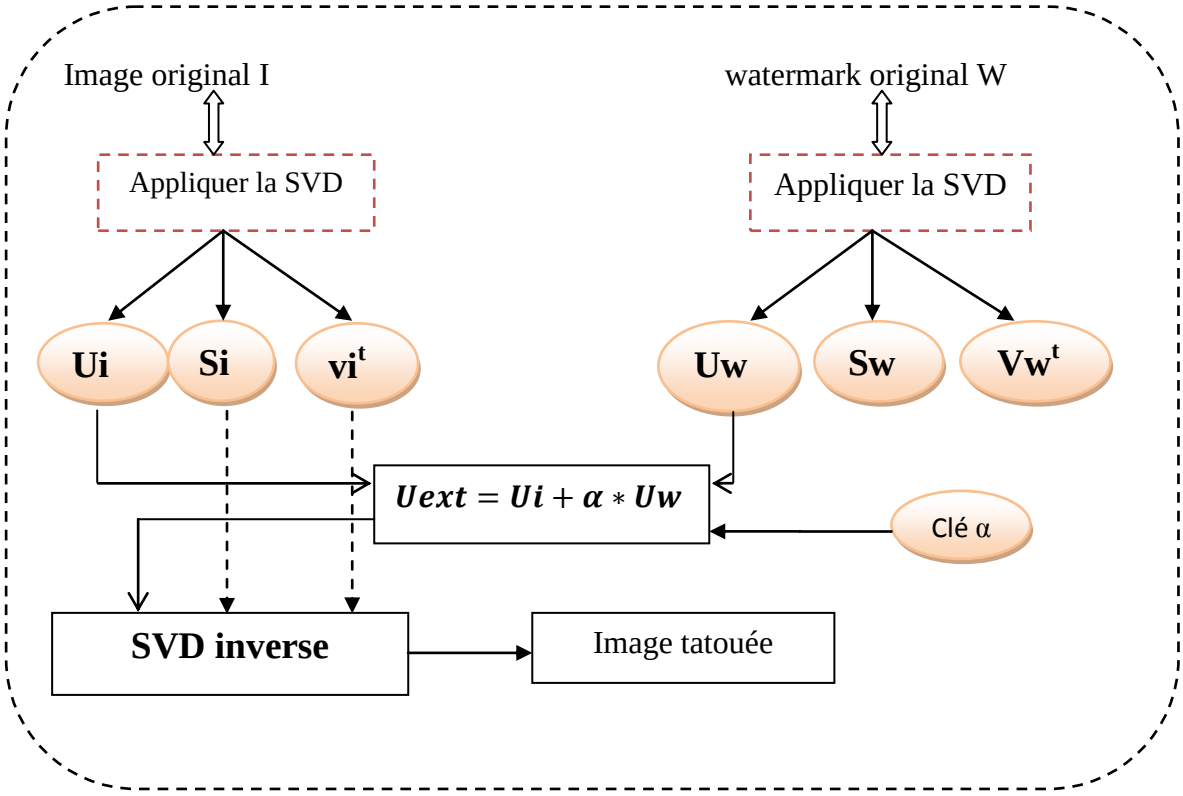


Figure 3.1.Algorithmed'insertion du watermark dans la matrice U

Exemple d'application de l'algorithme d'insertion

Nous appliquons l'algorithme décrit précédemment à l'image hôte « cameraman » qui est très utilisée en traitement d'image. L'image tatouée représentée sur la Figure 3.2.

Image hôte

Watermark original

Figure 3.2. Images tatouées pour différentes valeurs de la force du tatouage α

α	**3**	**2**	**1**	**0.3**	**0.2**	**0.1**	**0.03**	**0.02**	**0.01**
PSNR	-4.0284	-0.506	5.5140	15.9716	19.4994	25.5140	35.9716	39.4934	45.5140
NC	0.2781	0.3777	0.9991	0.9243	0.9636	0.9904	0.9991	0.9996	0.9999

Tableau 3.1.PSNR et coefficient de corrélation normalisée pour déférents valeurs de α

Le Tableau 3.1 montre les effets des diverses valeurs de la force du tatouage α sur l'image tatouée. On peut voir que le choix d'un poids élevé provoque une déformation

significative sur l'image tatouée, par contre quand la force du tatouage est trop petite, la marque devient irrécupérable. Alors il faut choisir une force du tatouage optimale qui permet une imperceptibilité de la marque. La valeur de α = 0.03 nous a donné le meilleur résultat. Par la suite, l'image tatouée sera traitée en utilisant cette valeur, qui représente en même temps la clé du tatouage et devra être gardée secrète.

3.3.1.2. Algorithme extraction

Dans cette section nous présentons le schéma synoptique de l'algorithme d'extraction.

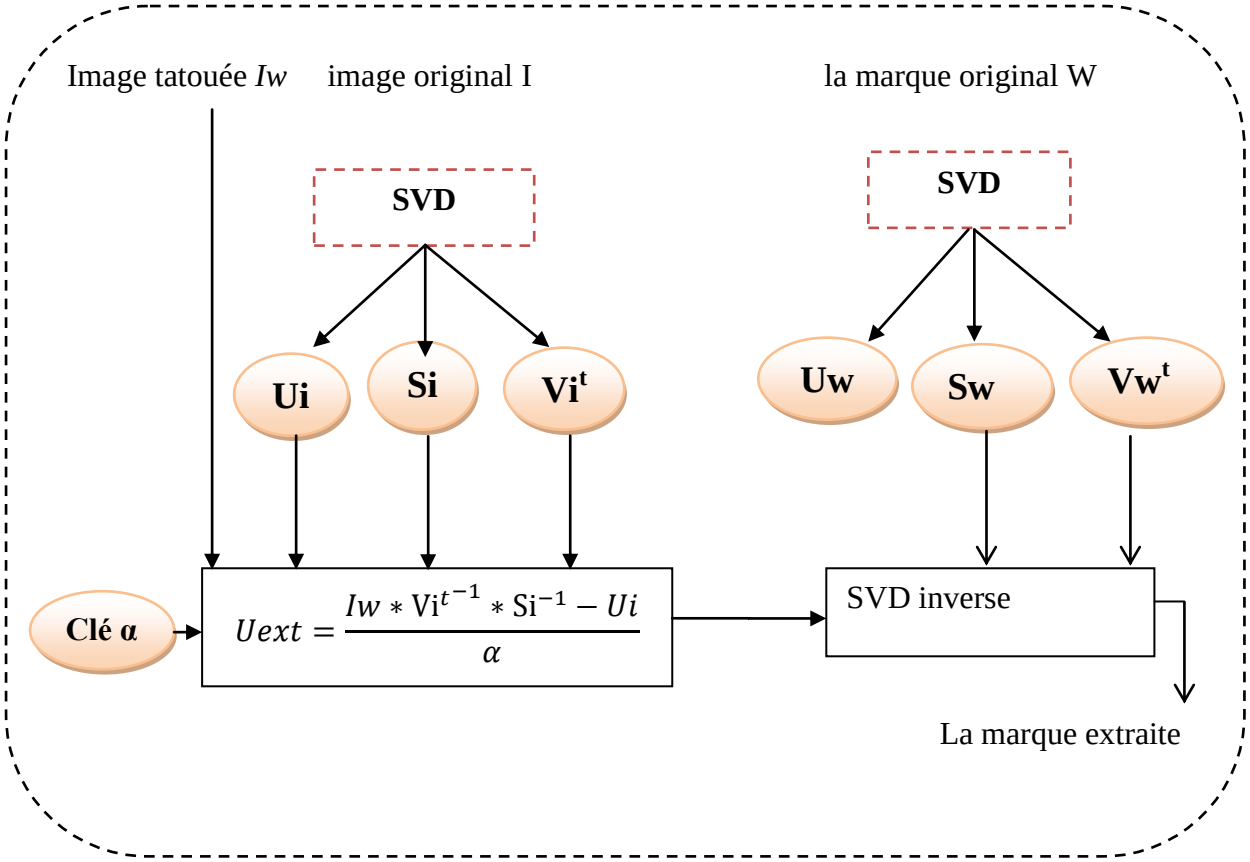


Figure3.3. Algorithme d'extraction du watermark

Exemple d'application



Watermark original image tatouée watermark extrait

Figure 3.4. Extraction du watermark avec une force du tatouage de 0.03

α	0.03
PSNR	63.6811
NC	1.0000



a)image original b) image tatouée c) watermark extrait

Figure 3.5.(a)Image cameraman, (b) image cameraman tatouée avec l'algorithme utilisant la matrice U, (c) le watermark extrait



a) image original b) image tatouée c) watermark extrait

Figure 3.6. (a)Image Lena, (b) image Lena tatouée avec l'algorithme utilisant la matrice U, (c) le watermark extrait

A partir de ces deux Figures, on peut voir qu'il est difficile de différencier entre les images originales et les images tatouées : alors la méthode est imperceptible.

Après l'extraction du watermark, le coefficient de corrélation est calculé. Ce coefficient Permet de juger de l'existence et l'exactitude de du watermark extrait. Les valeurs du PSNR et du NC entre W (original) et W∗(extrait) et entre l'image originale (I) et l'image tatouée (I∗) sont présentées dans le Tableau suivant :

L'image		PSNR	NC
cameraman	**Entre Wet W***	**267.4763**	**1.0000**
	Entre I et I*	**35.9716**	**0.9996**
Lena	**Entre W et W***	**262.3427**	**1.0000**
	Entre I et I*	**35.6565**	**0.9995**

Tableau 3.2. PSNR et NC entre les images hôte et marque après le tatouage

Propriété de robustesse

Une propriété très importante que doit garantir un algorithme de tatouage est la robustesse contre les attaques. Afin d'évaluer la robustesse de notre technique de tatouage, plusieurs types d'attaques ont été implanté comme la compression, l'ajout de bruit, le filtrage….etc.

- **Compression**

Nous nous sommes intéressées à la compression JPEG, car c'est le schéma de codage d'image le plus populaire et qui est généralement considéré comme une attaque dure contre les algorithmes de tatouage, la figure suivante présente les résultats obtenus pour différentes valeurs de Q (qualité de compression).

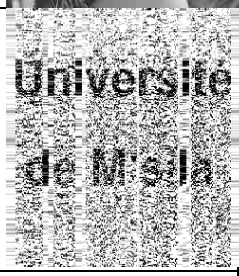
Q	Q=25	Q=50	Q=75	Q=100
Image tatouée				
Watermark extrait				
PSNR	3.6253	6.5409	9.7966	28.6655
NC	0.3709	0.5155	0.6653	0.9926

Figure 3.7. Images tatouées et watermark extrait avec le PSNR et NC pour différentes valeurs de Q

❖ **Ajout de bruit**

Nous avons ajouté à l'image tatouée (Lena) un bruit gaussien. L'extraction de la marque a donné les résultats suivants :

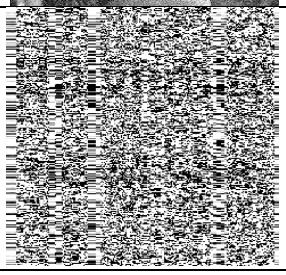
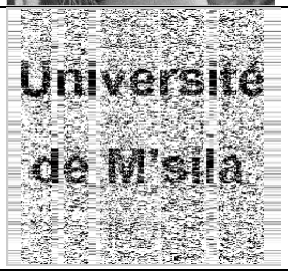
A	a=0.1	a=0.03	a=0.01
Image tatouée bruitée			
Watermark extrait			
PSNR	-5.8047	14.2720	34.3972
NC	0.1456	0.8368	0.9980

Figure 3.8. Images tatouées et watermark extrait avec le PSNR et NC pour différentes valeurs de a

❖ **Filtrage**

Nous avons appliqué un filtre passe-bas à l'image tatouée et l'extraction de la marque nous a donné le résultat montré dans la Figure suivante :

Image tatouée watermark extrait

Figure 3.9.Images tatouées et watermark extrait après le filtrage

PSNR = -4.3636 ; NC= 0.1713 **;**

Dans l'ensemble, nous avons remarqué selon les résultats obtenus, que le tatouage dans la matrice U résiste bien à la compression JPEG, moyennement au bruit et ne résiste pas au filtrage passe-bas.

Remarque : nous avons essayé le tatouage avec la matrice V et cela nous a donné des résultats similaires aux ceux obtenus avec la matrice U.

3.3.2. Algorithme utilisant la matrice S

Dans cet algorithme la marque est insérée dans la matrice diagonale S, selon les étapes suivante :

3.3.2.1. Algorithme d'insertion

L'algorithme d'insertion est expliqué par le schéma synoptique suivant la Figure 3.10.

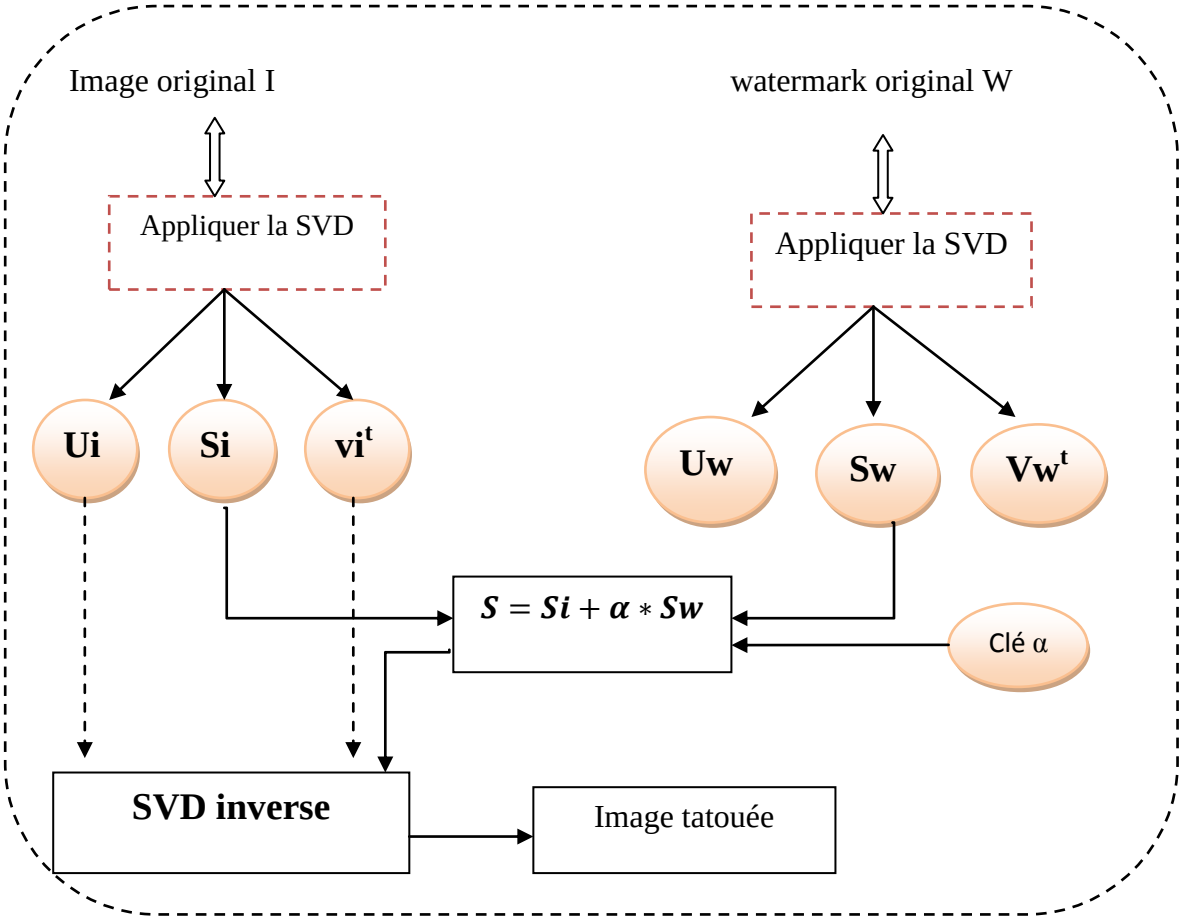


Figure 3.10. Algorithme d'insertion du watermark dans la matrice S

Exemple d'application de l'algorithme d'insertion

La Figure 3.11 montre un exemple de tatouage de l'image "Moon" sur l'image "cameraman" en utilisant la matrice S.

Image hôte

Watermark original

Figure 3.11. Images tatouées pour différentes valeurs de α

En variant la valeur de la force du tatouage **α,** on obtient plusieurs images tatouées. On remarque l'augmentation de α entraine la dégradation de l'image tatouée. Le Tableau suivant montre la variation du PSNR et du coefficient de corrélation normalisé en fonction de la variation de α.

α	**3**	**2**	**1**	**0.3**	**0.2**	**0.1**	**0.03**	**0.02**	**0.01**
PSNR	0.9651	2.5568	8.5774	19.0349	22.5568	28.5774	39.0349	42.5568	48.5574
NC	0.9877	0.9906	0.9951	0.9991	0.9995	0.9999	1.0000	1.0000	1.0000

Tableau3.3. Les valeurs de PSNR et NC pour déférents valeurs de la force du tatouage α

D'après les résultats du Tableau 3.3 nous avons choisi le tatouage avec α=0.03.

3.3.2.2. Algorithme extraction

Dans cette section nous présentons le schéma synoptique de l'algorithme d'extraction.

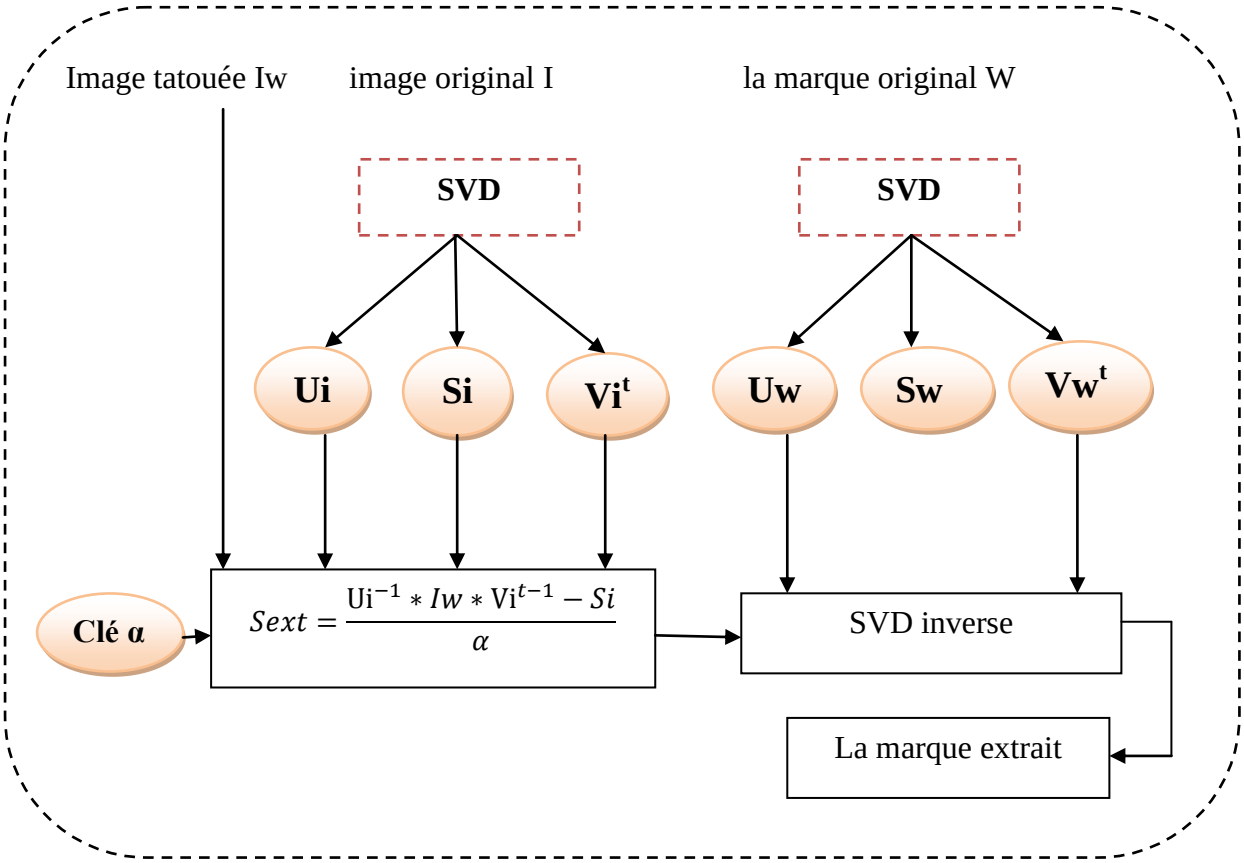


Figure 3.12. Algorithme d'extraction du watermark

Exemple d'application

a) Watermark original b) image tatouée c) watermark extrait

Figure 3.13. Extraction du watermark

α (force du tatouage)	0.03
PSNR (entre la marque originale et la marque extraite)	261.3947
NC (entre la marque originale et la marque extraite)	1.0000

Tableau3.4. La valeur de PSNR et NC pour α=0.03

Ce Tableau nous indique que la marque extraite est pratiquement similaire avec la marque originale.

Propriétés de robustesse

Avant l'attaque

La Figure 3.14 expose l'image hôte Lena, l'image de Lena tatouée et la marque originale de taille 256*256.

a) Image originale b) image tatouée c) watermark extrait

Figure 3.14.(a)Image Lena, (b) image Lena tatouée avec l'algorithme utilisant la matrice S, (c) le watermark extrait

Extraction de la marque après la modification de l'image tatouée

- **Compression**

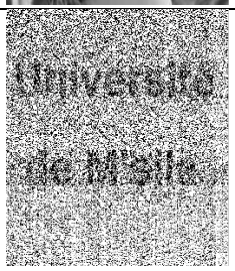
Q	Q=25	Q=50	Q=75	Q=100
Image tatouée				
Watermark extrait				
PSNR	-0.7178	1.3674	4.0090	25.1492
NC	0.1252	0.3124	0.4208	0.9833

Figure 3.15. Images tatouées et watermark extrait avec le PSNR et NC pour différentes valeurs de Q

- **Ajout de bruit**

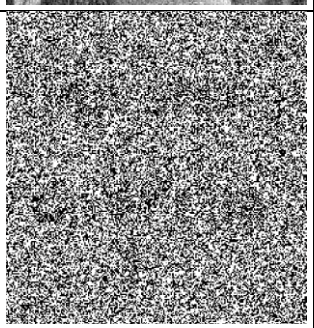
A	0.1	0.01	0.001
L'image tatouée			
Watermark extrait			
PSNR	-10.4259	9.5225	29.5665
NC	0.0501	0.6668	0.9938

Figure 3.16. Images tatouées et watermark extrait avec le PSNR et NC pour différentes valeurs de a

- **Filtrage passe-bas**

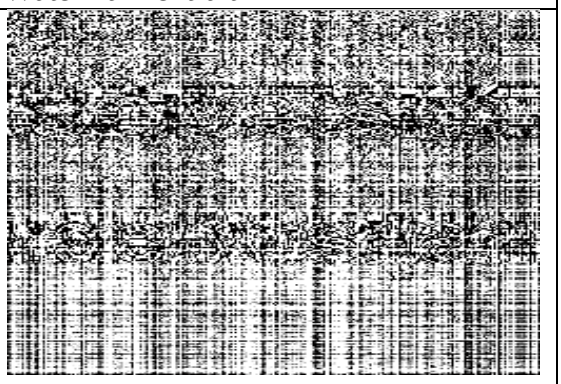
Image tatouée	Watermark extrait
	

Figure 3.17. Images tatouées et watermark extrait après le filtrage

PSNR1 = -4.3783 ; Nc1 = -0.0452

- **Recadrage**

Image tatouée	**Watermark extrait**
	

Figure 3.18.Images tatouées et watermark extrait après le recadrage

PSNR = -24.2480 ; NC = -0.6274

Remarques

- L'extraction de la marque après l'application de la compression JPEG à l'image tatouée donne des résultats plus ou moins bons (marque visible), cela dépend du facteur de compression Q figure 3.15.
- Pour l'ajout de bruit gaussien, la marque est perdue pour des valeurs de variances supérieures à 0.1figure 3.16.
- Concernant le filtrage passe-bas et le recadrage la marque est perdue après l'extraction.

3.4. Tatouage numérique basé sur la DCT et la SVD

3.4.1. Algorithme utilisant la matrice U

3.4.1.1. Algorithme d'insertion

Les deux Figures suivantes présentent l'algorithme de tatouage en combinant la SVD avec la DCT. Notons que l'insertion de la marque est effectuée dans la matrice U.

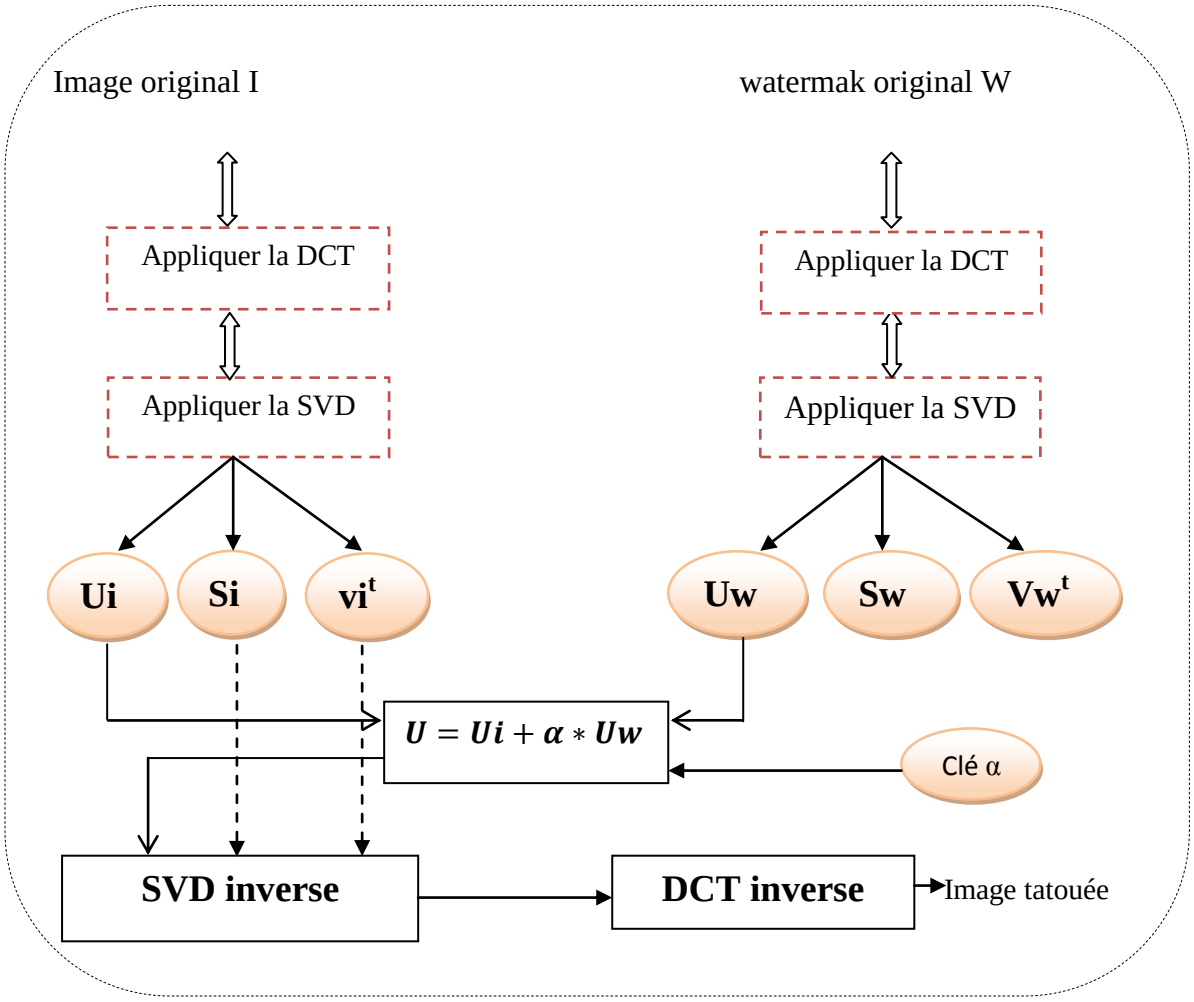


Figure 3.19. Algorithme d'insertion du watermark

3.4.1.2. Algorithme de l'extraction

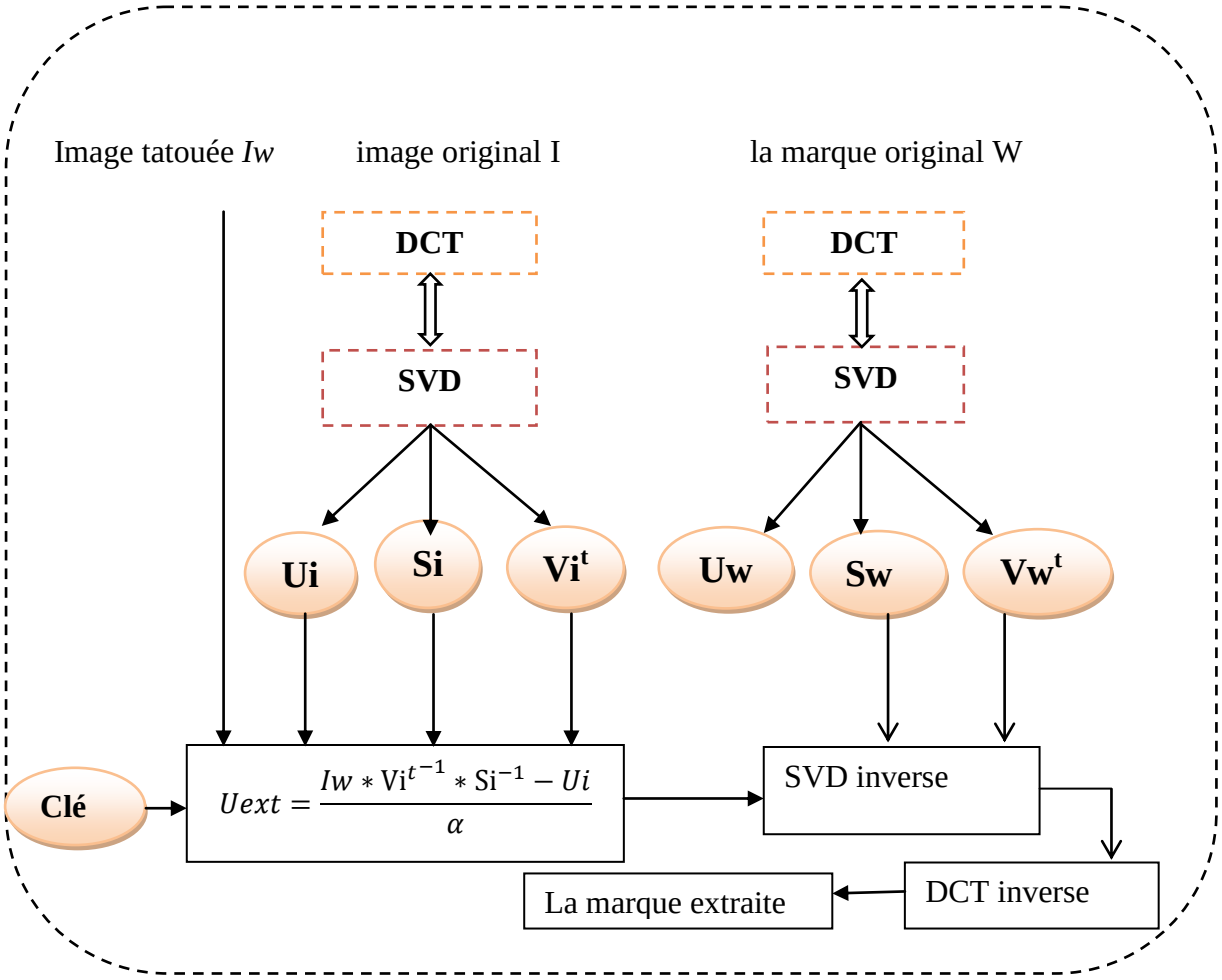


Figure3.20. Algorithme d'extraction du watermark

α		**3**	**2**	**1**	**0.3**	**0.2**	**0.1**	**0.03**	**0.02**	**0.01**
SVD	**PSNR**	-4.0284	-0.5066	5.5140	15.9716	19.4994	25.5140	35.9716	39.4934	35.9716
	NC	0.2781	0.3777	0.9991	0.9243	0.9636	0.9904	0.9991	0.9996	0.9991
SVD et DCT	**PSNR**	-4.0284	-0.5066	5.5140	15.9716	19.4934	25.5140	35.9716	39.4934	45.5140
	NC	0.1887	0.2966	0.5543	0.9186	0.9617	0.9901	0.9991	0.9996	0.9999

Tableau 3.5.Comparaison entre les valeurs de PSNR et NC pour les deux algorithmes de tatouage

Le Tableau 3.5présente une comparaison des valeurs du PSNR et NC entre l'image hôte et tatouée, et cela entre les deux algorithmes les premier utilisant la SVD seulement et le deuxième qui utilise la SVD_DCT. Nous avons trouvé une petite différence entre le tatouage numérique basé sur la SVD et le tatouage numérique base sur la SVD_ DCT de la matrice U. La meilleure valeur de α est 0.03.

3.4.2. Simulations et résultats expérimentaux

La Figure 3.13 expose l'image hôte Lena, l'image de Lena tatouée et la marque originale de taille 256*256.



a) Image hôte. b) Image tatouée c) Watermark original

Figure 3.21.(a)Image Lena, (b) image Lena tatouée avec l'algorithme utilisant la matrice u, (c) le watermark extrait

Le Tableau suivant présente les valeurs du PSNR et du NC entre la marque W (originale) et W∗ (extraite) et entre l'image originale (I) et l'image tatouée (I∗). La marque extraite est très similaire à l'originale et l'image tatouée à une bonne qualité visuelle.

L'image		**PSNR**	**NC**
Cameraman	**Entre W et W***	**271.7860**	**1.0000**
	Entre I et I*	**35.9716**	**0.9996**
Lena	**Entre W et W***	**265.7235**	**1.0000**
	Entre I et I*	**35.6565**	**0.9995**

Tableau 3.6.le PSNR et le coefficient de corrélation

La compression				
Q	Q=25	Q=50	Q=75	Q=100
PSNR (svd)	3.6253	6.5409	9.7966	28.6655
NC (svd)	0.3709	0.5155	0.6653	0.9926
PSNR (svd-dct)	3.6480	6.5445	9.8364	29.4656
NC (svd-dct)	0.3868	0.5129	0.6730	0.9938

L'ajout de bruit			
A	a=0.1	a=0.03	a=0.01
PSNR (svd)	-5.7280	4.6652	14.2675
NC (svd)	0.1390	0.4501	0.8371
PSNR (svd-dct)	1.1399	4.7388	14.9339
NC (svd-dct)	0.1538	0.4478	0.8417

Tableau 3.7. les valeurs de PSNR et NC dans la méthode SVD, SVD_DCT

Le Tableau 3.7 présente une comparaison entre les valeurs du PSNR et NC entre la marque originale et la marque extraite de l'image Lena et cela après avoir effectué la compression et l'ajout du bruit sur l'image Lena.

Nous avons remarqué que la combinaison SVD_DCT apporte une très légère amélioration de la qualité de la marque extraite par rapport celle obtenue par la SVD seule, pour la compression et pour l'ajout de bruit. Toute fois pour le filtrage passe-bas la marque extraite est perdue même avec l'algorithme SVD_DCT.

3.4.3. Algorithme SVD_DCT utilisant la matrice S

3.4.3.1. Algorithmes d'insertion

Les deux Figures suivantes présentent l'algorithme de tatouage en combinant la SVD avec la DCT. Notons que l'insertion de la marque est effectuée dans la matrice S.

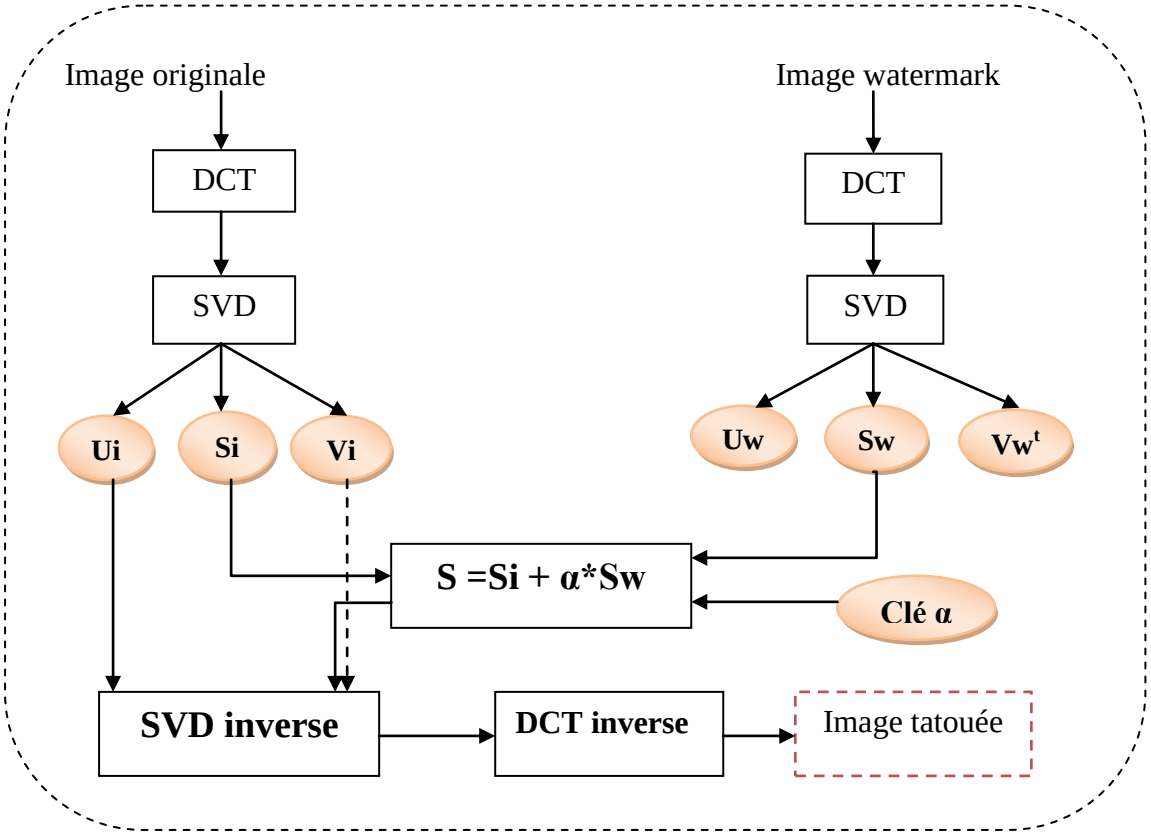


Figure 3.22. Algorithme d'insertion du watermark

α		3	2	1	0.3	0.2	0.1	0.03	0.02	0.03
SVD	**PSNR**	0.9651	2.5568	8.5774	19.0349	22.568	28.5774	39.0349	42.5568	48.5574
	NC	0.9877	0.9906	0.9951	0.9991	0.9995	0.9999	1.0000	1.0000	1.000
SVD et DCT	**PSNR**	-9.1598	-5.6380	0.3826	10.8402	14.3620	20.3826	30.8402	34.3620	40.3826
	NC	0.9831	0.9858	0.9909	0.9976	0.9987	0.9996	1.0000	1.0000	1.0000

Tableau3.8. Comparaison entre les valeurs de PSNR et NC pour les deux algorithmes de tatouage

Le Tableau 3.8présente une comparaison des valeurs du PSNR et NC entre l'image hôte et tatouée, et cela entre les deux algorithmes les premier utilisant la SVD seulement et le deuxième qui utilise la SVD_DCT. Nous avons trouvé une petite différence entre le tatouage numérique basé sur la SVD et le tatouage numérique base sur la SVD_ DCT de la matrice S. La meilleure valeur de α est 0.03.

3.4.3.2. Algorithme de l'extraction

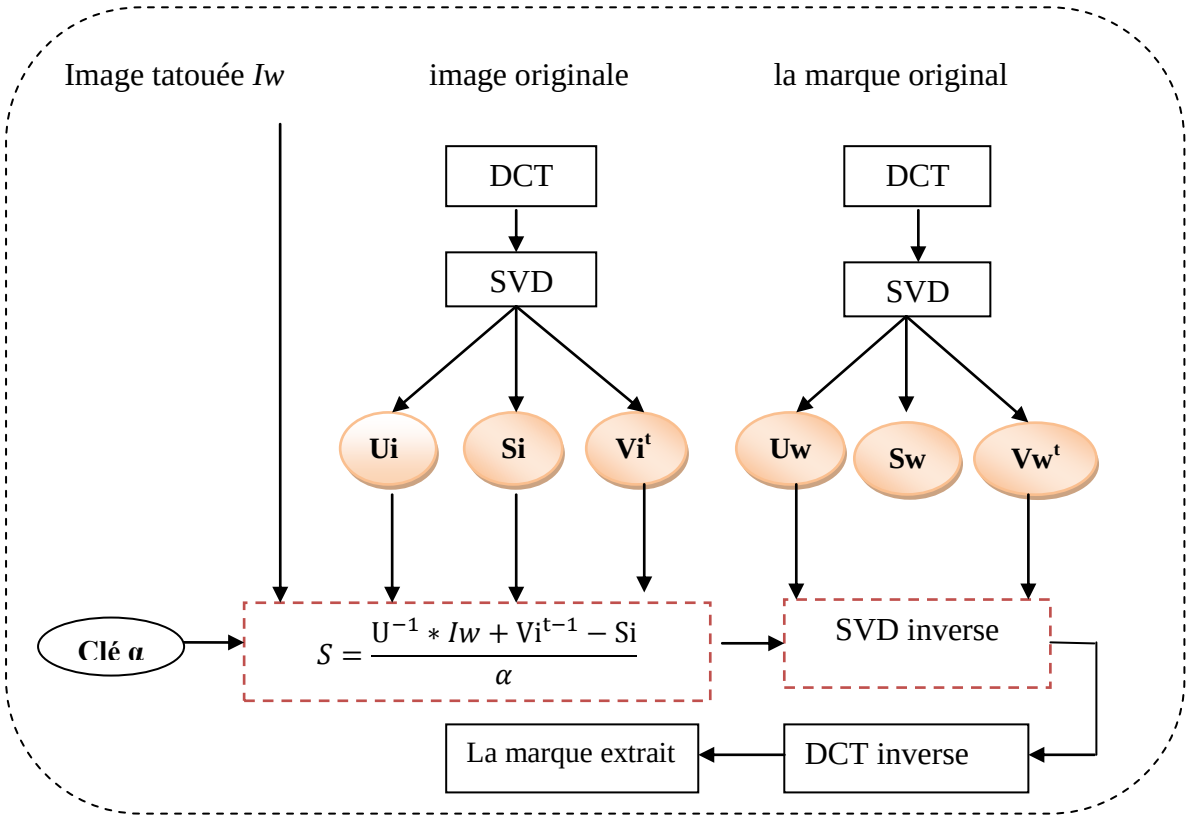


Figure 3.23. Algorithme d'extraction du watermark

Propriétés de robustesse

Avant l'attaque

La Figure 3.24 expose l'image hôte Lena, l'image de Lena tatouée et la marque originale de taille 256*256.

a)Image originale b) Image tatouée c) watermark originale

Figure 3.24.(a)Image Lena, (b) image Lena tatouée avec l'algorithme utilisant la matrice U, (c) le watermark extrait

❖ **Compression**

Q	Q=25	Q=50	Q=75	Q=100
Image tatouée				
Watermark extrait				
PSNR(svd-dct)	10.3559	15.6358	23.1234	45.5019
NC (svd-dct)	0.6945	0.8762	0.9743	0.9998

Figure 3.25. Images tatouées et watermark extrait avec le PSNR et NC pour différentes valeurs de Q.

Les résultats que présente la Figure 3.25 montrent que l'extraction de la marque est réussite après l'application de la compression JPEG, même pour un facteur de qualité de 25%. En comparant ces résultats avec celle de Figure 3.15, nous remarquons l'amélioration de la qualité visuelle ainsi que le PSNR et le NC de la marque extraite, cela est dû à l'introduction de la DCT à l'algorithme de tatouage.

❖ **Ajout de bruit**

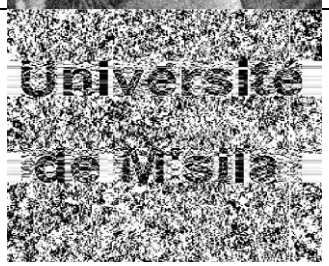
A	0.1	0.01	0.001
L'image tatouée			
Watermark extrait			
PSNR	-5.7696	26.2579	53.8795
NC	0.2858	0.9872	1.0000

Figure 3.26. Images tatouées et watermark extrait avec le PSNR et NC pour différentes valeurs de a

- **Filtrage passe-bas**

Figure 3.27. Images tatouées et watermark extrait après le filtrage

PSNR = 8.8663 ; NC = 0.5443.

❖ **Recadrage**

Image tatouée	Watermark extrait
	

Figure 3.28. Images tatouées et watermark extrait après le recadrage

PSNR =-19.9719 ; NC =-0.9627.

Les Figures (3.26), (3.27) et (3.28) présente respectivement la marque extraite, après l'ajout du bruit gaussien, le filtrage passe-bas et le recadrage. La comparaison entre ces résultats et ceux obtenus par l'algorithme de tatouage basé sur la SVD seulement montre l'amélioration visuelle, le PSNR et le NC de la marque extraite qu'a apporté l'introduction de la DCT à notre algorithme originale.

3.5. Conclusion

Dans ce chapitre, nous avons présenté deux méthodes de tatouages : la première est basée sur la SVD et la deuxième sur la combinaison de la DCT et la SVD. Nous avons inséré la marque dans la matrice orthogonale U et dans la matrice diagonale S issues de la décomposition en en valeurs singulières (SVD) de l'image hôte.

Les résultats de simulations ont montré que :

- Le tatouage en utilisant la matrice S est plus robuste vis à vis des attaques comme la compression, le filtrage et l'ajout de bruit, que celui avec la matrice U.
- La combinaison DCT_SVD a amené une très légère amélioration à la robustesse du tatouage dans la matrice U. Tandis qu'elle a nettement amélioré la robustesse du tatouage dans la matrice S.

Conclusion générale

A cause des utilisations illicites des documents numériques, le tatouage numérique a été introduit comme une technique efficace pour la protection des droits d'auteurs, la protection de copie ou anti-copie et l'authenticité.

Nous avons présenté dans ce mémoire deux méthodes de tatouage numérique basées sur la SVD et la combinaison entre la DCT et la SVD. Les deux algorithmes utilisent respectivement la matrice U et la matrice S dans le tatouage et ils sont appliqués sur des images en niveau de gris.

La performance des deux techniques de tatouage proposées est validée à l'aide des attaques de compression, filtrage, bruitage et recadrage..etc. Les résultats obtenus ont montré que le tatouage sur la matrice S est robuste que celui utilisant la matrice orthogonale U, pour les deux méthodes. Alors que le tatouage basé sur la combinaison DCT-SVD donne de meilleurs résultats que celui basé sur la SVD, en terme de robustesse de la marque extraite contre les différentes attaques effectués. En ce qui concerne la visibilité, nous avons constaté l'apparition la dégradation de l'image hôte à partir de la valeur de la force de tatouage (α>0.03). On a utilisé couramment le PSNR (power peak signal to noise ration) et le coefficient de corrélation normalisé NC quantifier ces dégradations. D'après nos résultats toutes les images tatouées sont visuellement de bonne qualité.

Nos perspectives sont d'essayer d'élaborer de nouveaux algorithmes qui pourraient s'appliquer aux images en couleurs et qui peuvent apporter plus de robustesse et par conséquent plus de sécurité par rapport aux droits d'auteur .

On a vu que l'algorithme présentés des avantages comme la simplicité du calcule (PSNR, NC) , l'imperceptibilité, et la robustesse contre les attaques que au traitement d'image (compression, filtrage, ajout de bruit recadrage).

En plus, nous avons utilisé des méthodes qui combinent la SVD avec une autre, telle que la DCT. Cela nous donne des algorithmes de tatouage basé sur la DCT-SVD.

Bibliographie

[1] J. Seitz. « Digital Watermarking for Digital Media ». Information Science Publishing 2004.

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

[3] A. Tirkel, G.Rankin, R. Schyndel, W. Ho, N. Mee, and C. Osborne. « Electronic watermark ». In DICTA 1993, pages 666-672, 1993.

[4] S. Mohanty, N. Ranganathan, and K. Namballa. « VLSI Implementation of Visible Watermarking for Secure Digital Still Camera design ». In 17th International conference on VLSI Design, pages 1063-1068, 2004.

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

[6] S. Katzenbeisser and F. Petitcolas. « Information Hiding Techniques for steganography and Digital Watermarking ». Artech House, 2000.

[7] C. Rey and J. Dugely. « Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images ». Traitement du signal, vol.18, no. 4, pages 283-295 2001.

[8] D. Zheng, Y. Liu, J. Zhao, and A. Saddik. « A survey of RST Invariant image Watermarking Algorithms. » ACM Computing Surveys, Volume 39, Issue 2, 2007.

[9] Vidyasagar M. Potdar, Song Han, Elizabeth chang. « A Survey of Digital Image Watermarking Techniques ». School of Information Systems, Cutrin University of Technology, Perth, western Australie. 2009.

[10] I. Gharzouli. « Filtrage linéaire à 2D et applications sur le signal image » Mémoire de fin d'études, université Sétif, 2006.

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

[12] K. Loukhaoukha, « Tatouage numérique des images dans le domaine des ondelettes basé sur ladécomposition en valeurs singuliers et l'optimisation multi-objective », mémoire de doctorat, université LAVAL QUEBEC, 2010.

[13] R. Isdant, « Traitement numérique de l'image », 2009.

[14] http://www.cardinalmercier.be/multimudia/cours/Mu003/Mu003-01.html.

[15] G. Burel, « introduction au traitement d'image », paris, Hermés Science Publicationoctobtre 2001.

[16] A. Marion, « Bases du Traitement d'image », cours de master Imagerie 1, 12 février 2007.

[17] A. Bouderbala, « Implémentation d'un algorithme de tatouage vidéo robuste dans le domaine compressé », mémoire de magister en électronique, université MENTOURI CONSTANTINE, 2008.

[18] P. Patrick, B. Chassery & J. Marc, « Tatouage couleur adaptatif fondé sur l'utilisation d'espaces perceptifs uniformes ». Traitement du signal, 2004.

[19] A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu & A. Vernone, « A Novel Block-based Watermarking scheme using the SVD Transform », Departement of Computer science, Université DEGLI STUDIDI TORINO, Italy.

[20] A. Parisis, P. Carre, A. Tremeau, « Introduction au tatouage d'images couleur » Laboratoire SIC –FRE-CNRS 2731, Université de Poitiers Boulevard Marie et Pierre curie, 2005.

[21] S. Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, & J. Su, « Attacks on Digital Watermarks ». Classification, Estimation-basedAttaksans Benchmarks. IEEE CommunMag, 118-126, 2001.

[22] F. Petitcolas, R. Anderson, M. Kuhn «Attacks on copyright Marking Systems », Lecture Notes in computer Sciences(LNCS), vol. 1525 : pp. 219-239, 1998.

[23] S.Voloshynovskiy, F. Deguillaume, T. Pun « Multibit digital watermarking robust against local nonlinear geometrical distorsion », proceedings of the IEEE International Conference on Image Processing(ICIP), IEEE Computer Society Press, Los Alamitos CA, pp.999-1002, 2001.

[24] C. Serdean, M. Ambroze, M. Tomlinson, G. Wade « Dwt based video watermarking for copyright protection invariant to geometrical attacks», International Symposium on

Communication Systems, networks and Digital Signal Processing »,(Staffordshire University, UK), july 15-17,2002.

[25] A. Keskinarkaus, A. Pramila, T. Seppanen « Image watermarking with a directed peridicpattem to embed multibit messages resilient to print-scan and compound attacks »journal of systems and software, vol. 83(10) : pp. 1715-1725, 2010.

[26] J.P. Linnartz, M.V. Dijk « Analysis of sensitivity attack against electronic watermark sin image, proceedings of 2nd workshop on information Hiding, Portland, verlag-LNCS avril1998.

[27] P. Nguyen et S. Baudry « le tatouage des données audiovisuelles, les cahiers du numérique, vol. 4 :pp. 135-165, 2003.

[28] J.P.Boyer, P.Duhamel, J.Blanc- Talon « Taouage semi-fragile et théorie des jeux » Etude d'un système basé sur le SCS, compression et représentation des signaux audiovisuels CORESA, Renne, 2005.

Résumé

Le développement des technologies de l'information et de la communication a conduit à la nécessité d'utiliser les techniques de protection de droit d'auteur et de contrôle les copies illégales de ces médias. La plus importante de ces techniques est le tatouage numérique.

Nous proposons dans ce travail, des schémas de tatouage basés sur l'insertion d'une marque dans une image hôte par l'utilisation de la décomposition en valeur singulière SVD et par la transformée en cosinus discrète DCT. Le procédé de l'extraction de la marque est réalisé par l'algorithme inverse à l'insertion . Des tests réalisés sur des images numériques célèbres ont permis d'évaluer le performance de ces techniques et vérifier leur robustesse face aux diverses attaques.

الملخص

أدى تطور تكنولوجيا المعلومات و الاتصالات إلى الحاجة لتقنيات حماية حق المؤلف ومراقبة النسخ الغير قانونية من هذه الوسائط. وأهم هذه التقنيات الوشم الرقمي.

ونقترح في هذا العمل، أنماط الوشم على أساس إدخال علامة في صورة المضيف عن طريق استخدام قيمة فريدة SVD و جيب التمام منفصلة تحويل DCT، يتم تنفيذ عملية استخراج علامة من قبل خوارزمية معكوس الإدراج. الاختبارات المطبقة على الصور الرقمية الشهيرة استخدمت لتقييم أداء هذه التقنيات و اختبار قوة ضد الهجمات المختلفة.

Abstract

The development of information and communication technologies has led to the need to use copyright protection and control techniques to illegally copy these media. The most important of these techniques is the digital tattoo.

We propose in this work watermarking schemes based on the insertion of a mark in a host image by the use of the singular value decomposition SVD and by the discrete cosine transform DCT. The method of extracting the mark is performed by the inverse algorithm at insertion. Tests carried out on famous digital images made it possible to evaluate the performance of these techniques and to check their robustness in the face of various attacks.