

**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE**

**SCIENTIFIQUE**

**UNIVERSITE FERHAT ABBAS-SETIF**

**UFAS (ALGERIE)**

**MEMOIRE**

**Présenté à la Faculté de Technologie**

**Département d'Electronique**

**Pour l'Obtention du Diplôme de**

**MAGISTER**

**Option : Communication**

**Par**

***M<sup>elle</sup> : HETATACHE KARIMA***

**Thème :**

---

**Développement d'algorithmes de tatouage d'images basés sur  
la SVD et les transformées discrètes**

---

Soutenu le ...29/12/2014.....devant la commission d'examen :

M. FERHAT HAMIDA A/HAK	Professeur à l'université de Sétif1	<b>Président</b>
M. BOUGUEZEL Saad	Professeur à l'université de Sétif 1	<b>Examineur</b>
M. BOUROUBA Nacerdine	MCCA à l'université de Sétif 1	<b>Examineur</b>
M. AMARDJIA Nourredine	MCCA à l'université de Sétif 1	<b>Encadreur</b>

# *Remerciements*

*Dieu, Merci de m'avoir guidé sur le meilleur des chemins.*

*En cette occasion de soutenance de mémoire de magister ;*

*J'ai le plaisir de formuler mes plus humbles remerciements à :*

*En premier lieu, au Dr Nourredine Amardjia, mon encadreur dans ce travail et mon maître. Je le remercie pour ses conseils, sa compréhension, sa disponibilité, son aide ainsi que sa patience.*

*En second lieu, tous les enseignants, sans exception, qui m'ont honoré lors de mon cursus en me prodiguant le savoir avec dévouement.*

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

*Enfin, Messieurs les membres du jury, qui ont accepté de m'honorer en acceptant d'examiner, de juger et d'évaluer mon mémoire de fin d'études pour l'obtention du Magister.*

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

*A toute personne qui a contribué de près ou de loin à l'élaboration de ce travail, je dis, MERCI.*

**HETATACHE karima**

## *Table des abréviations*

<b>2D</b>	bidimensionnel
<b>3D</b>	tridimensionnel
<b>PAO</b>	Publication Assistée par Ordinateur
<b>pixel</b>	Picture element
<b>RVB</b>	Rouge Vert Bleu
<b>CMJN</b>	Cyan Magenta Jaune Noir
<b>BMP</b>	Bitmap
<b>TIFF</b>	Tagged Image Format
<b>GIF</b>	Graphic Information Format
<b>JPEG</b>	Joint Photograph Experts Group
<b>PNG</b>	Portable Network Graphics
<b>LSB</b>	Least Significant Bits - bits les moins significatifs
<b>DFT</b>	Discrete Fourier Transform - transformée de Fourier discrète
<b>DCT</b>	Discrete Cosine Transform - transformée en cosinus discrète
<b>DWT</b>	Discrete Wavelet Transform - transformée en ondelettes discrète
<b>SVD</b>	singular value decomposition- décomposition en valeurs singulières
<b>PSNR</b>	peak signal to noise ratio - rapport signal sur bruit de crête
<b>EQM</b>	Erreur Quadratique Moyenne
<b>NC</b>	normalized correlation - corrélation normalisée
<b>LL</b>	low-low - basse-basse
<b>HL</b>	high-low - haute-basse
<b>LH</b>	low-high - basse-haute
<b>HH</b>	high-high - haute-haute

## *INTRODUCTION GENERALE*

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 doit 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.

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

Le présent mémoire est organisé en quatre chapitres :

- **Le chapitre 1** présente une introduction aux images numériques. Plus précisément, nous présentons quelques terminologies et quelques notions pertinentes dans le domaine des images numériques telles que la numérisation, le codage et le stockage. Nous présentons

## *INTRODUCTION GENERAL*

---

aussi quelques aspects du traitement d'images, tels que le filtrage, la compression et le tatouage.

- **Le chapitre 2** décrit le principe général du tatouage ainsi que les domaines d'insertion, les applications et classifications des attaques.
- **le chapitre 3** consiste à l'étude du principe de la transformée SVD. Puis nous étudions et implémentons plusieurs méthodes de tatouage basées sur cette transformée.
- Dans **le chapitre 4** nous étudions et implémentons des algorithmes de tatouage basés sur la SVD combinée avec une autre transformée. Les algorithmes seront basés sur la DFT – SVD, la DWT – SVD et la DCT – SVD.

Nous terminons notre travail par une conclusion générale

# ***CHAPITRE 1 :***

Introduction aux images numériques

# Chapitre 1 : Introduction aux images numériques

---

## 1.1. Introduction :

L'image est partout. Elle est maintenant un des outils d'investigation les plus prisés de la recherche scientifique et technique. Son apport didactique, complémentaire au dialogue textuel et son caractère pluridisciplinaire ne sont en effet plus à démontrer.

Le traitement et l'analyse d'images trouvent leurs applications dans des domaines extrêmement variés de l'industrie et de la recherche. Ces méthodes sont utilisées dans de nombreuses disciplines scientifiques, citons en particulier les sciences des matériaux (céramurgie, matériaux pour l'électronique, etc.), les sciences de la terre, la géographie ( la cartographie et la géomorphologie), la robotique (pour le tri et la vérification de pièces électroniques) ou bien encore dans des domaines aussi variés tels que ceux qui ont trait à l'astronomie, l'identification, la pharmacologie.

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 continu bidimensionnel comme par exemple un appareil photo ou une caméra... Sur un ordinateur, on ne peut 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 (pixels).

Autrement dit, une image est une matrice  $M \times N$  de valeurs entières prises sur un intervalle borné  $[0, N_g]$  où  $N_g$  est la valeur maximale du niveau de gris[2].

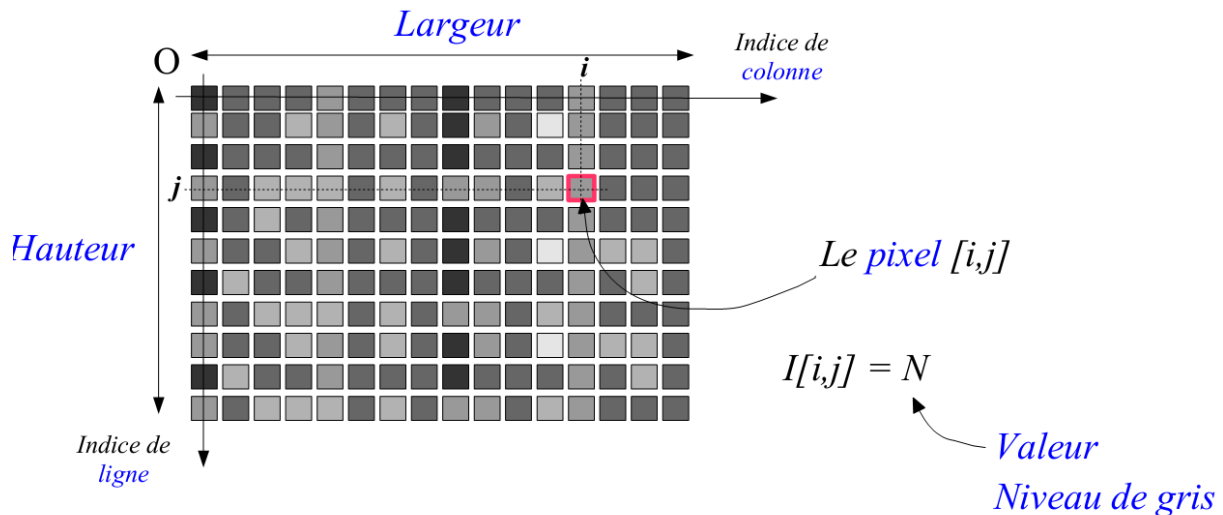


Figure 1.1 : image numérique I.

### 1.3.1. Image en niveaux de gris :

Une image en niveaux de gris autorise un dégradé de gris entre le noir et le blanc. En général, on code le niveau de gris sur un octet (8 bits) soit 256 nuances de dégradé. L'expression de la valeur du niveau de gris avec  $N_g = 256$  devient:  $p(i,j) \in [0, 255]$ .

### 1.3.2. Image couleur :

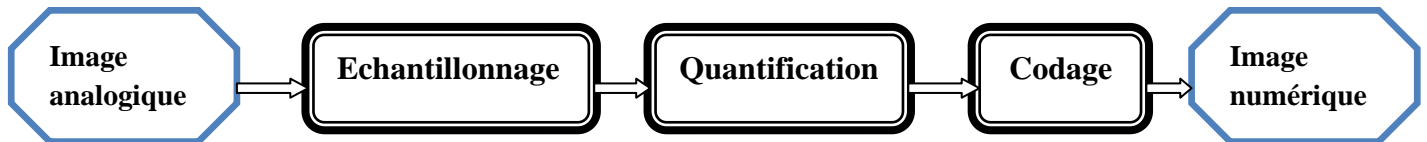
Une image couleur est la composition de trois (ou plus) images en niveaux de gris sur trois (ou plus) composantes. On définit donc trois plans de niveaux de gris, un rouge, un vert et un bleu. La couleur finale est obtenue par synthèse additive des ces trois (ou plus) composantes. [3].

### 1.4. Processus de numérisation :

La représentation informatique d'une image est nécessairement discrète, alors que l'image est de nature continue : le monde est continu, la transformation d'un signal analogique 2D nécessite à la fois une discrétisation de l'espace : c'est l'échantillonnage, et une discrétisation des couleurs : c'est la quantification. [4]

Le processus de numérisation est représenté dans la figure suivante :

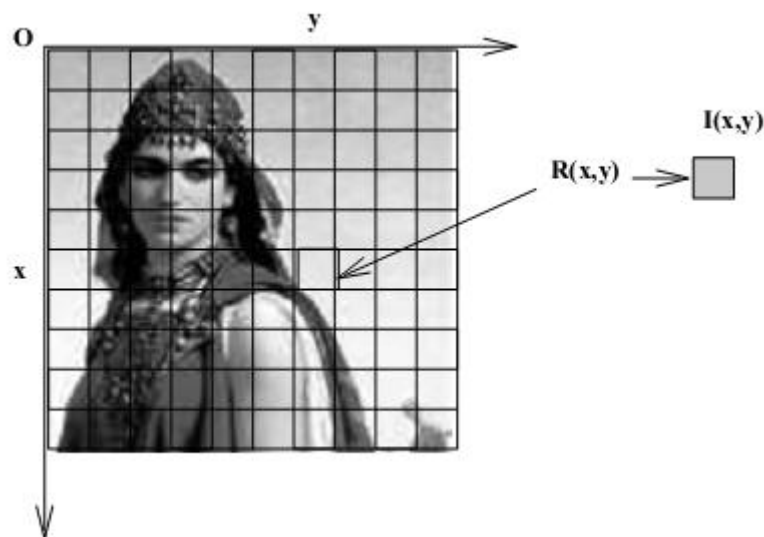




*Figure 1.2:* Processus de numérisation d'une image.

Le processus de numérisation d'une image suit les étapes suivantes :

**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 apparaître 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.

# Chapitre 1 : Introduction aux images numériques

---

## 1.4.3.2. Codage en niveaux de gris :

Si on code chaque pixel sur 2 bits on aura 4 possibilités (noir, gris foncé, gris clair, blanc).

L'image codée sera très peu nuancée.

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

## 1.4.3.3. Codage d'une image couleur :

On peut attribuer 3 valeurs à chaque pixel : Rouge (de 0 à 255), Vert (de 0 à 255) et Bleu (de 0 à 255). Chaque couleur est codée sur 1 octet = 8 bits. Chaque pixel sur 3 octets 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  $256 \times 256 \times 256 = 16777216$  (plus de 16 millions de couleurs différentes)

## 1.5. Les types d'images numériques :

Il existe 2 sortes d'images numériques : les images **matricielles** et les images **vectérielles**

### 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) proposent également de tels outils. 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 données sont stockées dans une matrice de points appelés « pixels ». **Les images matricielles** sont créées par les imprimantes, scanners, appareils photographiques et certains logiciels d'infographie 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 images 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 notamment par :

- ❖ sa définition
- ❖ sa résolution
- ❖ son codage ou profondeur de couleur exprimé en bit par pixel (bpp).
- ❖ son mode colorimétrique (RGB ou CMJN), composition des multiples couches.

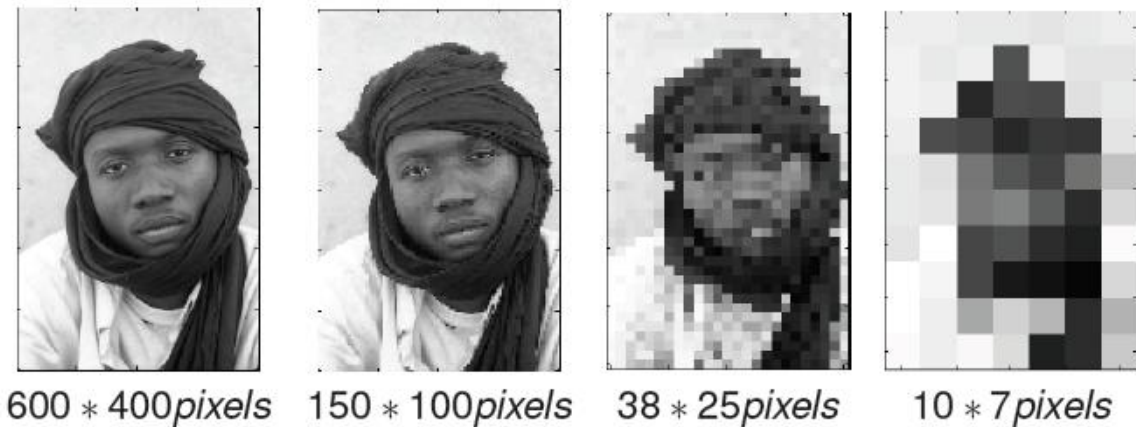
### 1.6.1. Définition d'une image :

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 :

C'est le nombre de points contenu dans une **surface précise** (en pouce). Elle est exprimée en points par pouce (PPP, en anglais: DPI pour Dots Per Inch). Un pouce mesure 2.54 cm [7].

- **La Résolution spatiale** : due à l'échantillonnage



*Figure 1.4: Résolution spatiale*

➤ **Résolution tonale** (de tons de gris) : due à la quantification



*Figure 1.5: Résolution tonale*

### 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 ce que l'on nomme le codage de couleurs 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).

$$\text{Poids (octet)} = \text{nombre de pixels total} * \text{codage couleur (octet)}$$

### 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 quelques formats :

# Chapitre 1 : Introduction aux images numériques

---

## 1.7.1. Principaux formats de fichiers non compressés :

Ces formats de fichiers utilisent en général beaucoup de mémoire. De part 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 Filea) été mis au point en 1987.

Le format TIFF est un ancien format graphique, permettant de stocker des images bitmap (raster) de taille importante (plus de 4 Go compressées), sans perte de qualité et indépendamment des plates formes ou des périphériques utilisés (Device-Independent Bitmap, noté DIB). 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.

### ✓ 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 et 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 codée en RGB (synthèse additive), le format lui-même supportant la palette 256 couleurs que le «true color». [8]

## 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, mais ne doivent pas être utilisés lors d'un travail de création sous Photoshop car chaque nouvel enregistrement détériore un peu plus le fichier. On les utilisera donc pour exporter des images destinées à la visualisation sur internet ou l'archivage.

# Chapitre 1 : Introduction aux images numériques

---

## ✓ 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.

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

## ✓ 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, 16, 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 Graphic (ISO 15948) a été développé par le W3C pour remplacer le GIF. Il surpasse ce dernier en ce qu'il n'est notamment pas limité à 256 couleurs. De même, le format est ouvert et permet une bonne compression sans perte. Son utilisation est recommandée à l'instar du GIF pour les petits logos. Côté photo, s'il permet une compression sans perte, le poids de la photo n'est pas compétitif avec les formats JPEG. Précisons que le PNG ne gère pas l'animation mais un format dérivé, le MNG, y est destiné.

[9]

## **1.8. Aspects du traitement d'images :**

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

### **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 apparaît 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) :**

Les filtres passe-haut atténuent les composantes de basse fréquence de l'image et permettent notamment d'accentuer les détails et le contraste, c'est la raison pour laquelle le terme de "filtre d'accentuation" est parfois utilisé. Ce filtre n'affecte pas les composantes de haute fréquence d'un signal, mais doit atténuer les composantes de basse fréquence.

Un filtre passe haut favorise les hautes fréquences spatiales, comme les détails, et de ce fait, il améliore le contraste.

#### **1.8.1.3. Filtre passe-bande (différentiation) :**

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

# Chapitre 1 : Introduction aux images numériques

---

## **1.8.2. La compression :**

La compression de données consiste à obtenir des fichiers plus légers, afin d'améliorer la vitesse de transfert sur internet 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 :**

Concernant essentiellement les fichiers de média (image, son, vidéo), elle consiste en une « réduction » de l'information basée sur notre propre limite humaine à percevoir ces médias. Puisque l'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 certains cas visible) appelée aussi signature, ou tatouage, dans une image ou d'autres documents numériques, pour divers buts tels 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]

Le principe de ce traitement est bien détaillé dans le chapitre suivant.



## **1.9. 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, le stockage. Nous avons également présenté quelques aspects du traitement d'image, tels que le filtrage, la compression et le tatouage, et c'est ce dernier qui est présenté le long de ce mémoire.

## ***CHAPITRE 2 :***

Etat de l'art sur le tatouage numérique des  
images

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

### 2.1. Introduction :

Le tatouage numérique est un domaine scientifique récent apparu au début des années 90 qui présente de multiples intérêts. Dans ce chapitre, on présentera le principe du tatouage numérique des images ainsi que quelques unes de ses applications. Après avoir donné un aperçu historique sur cette technique et sur les techniques de dissimulation de l'information, nous présenterons le tatouage numérique et ses différentes étapes qui conduisent à l'insertion de la marque. Ensuite nous décrirons quelques représentations de l'image dans le domaine spatial et fréquentiel. Nous présenterons les différentes applications possibles du tatouage numérique pour les images à la fin de ce chapitre nous présenterons brièvement l'évaluation en terme d'imperceptibilité et de robustesse des schémas de tatouage numérique des images. [11].

### 2.2. Historique et Terminologies

#### 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 a son origine dans la ville de Fabriano en Italie qui a joué un rôle important dans l'évolution de l'industrie papetière.

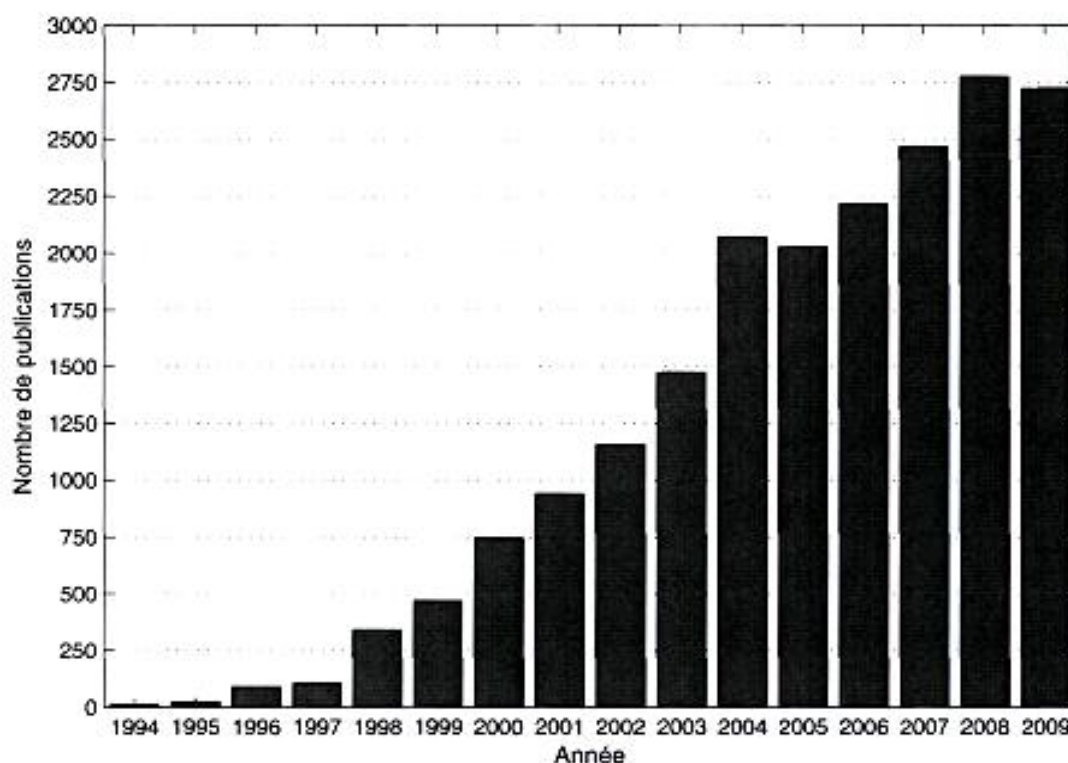
A la fin du troisième siècle, environ 40 fabricants du papier partageaient le marché du papier. La concurrence entre ces fabricants était très élevée et il était difficile que n'importe quelle partie maintienne une trace de la provenance du papier et ainsi que son format et sa qualité. L'introduction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

L'analogie entre le tatouage du papier et le tatouage numérique est évidente : les tatouages du papier des billets de banque et de timbres ont inspiré la première utilisation du terme «Marque d'eau» dans le contexte de données numériques. Les premières publications portant sur le tatouage d'images numériques ont été publiés par Tanaka et al. [2] en 1990 et par Tirkel et al. [3] en 1993.

## Chapitre 2 : État de l'art sur le tatouage numérique des images

En 1995, le temps est évidemment bien de prendre ce sujet, et il a commencé à stimuler l'augmentation des activités de recherche. Depuis 1995, le tatouage numérique a gagné beaucoup d'attention et a évolué très rapidement et alors qu'il y a beaucoup de sujets ouverts pour davantage de recherches, des méthodes de travail et des systèmes pratiques ont été développés. [12]

La *figure 2.1* montre le nombre de publications avec le mot clé "watermarking" sur la base de données bibliographiques INSPEC.



*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

## Chapitre 2 : État de l'art sur le tatouage numérique des images

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 afin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watermark est visible, alors elle peut être facilement attaquée. Néanmoins, nous trouvons des applications qui demandent que le watermark soit visible, c'est le cas du logo des sociétés dans les programmes télévisuels. Dans la catégorie du tatouage visible, [13]



*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 elles au contraire un watermark invisible, qui ne dégrade donc pas le contenu visuel, mais qui permet de détecter l'éventuelle source d'un vol. Le message caché par le tatouage peut être un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur [14].

Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs [15]. La majorité des techniques concernant la protection de propriété intellectuelle suit la branche du tatouage invisible.

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



a) : image originale



b) : image tatouée

*Figure 2.2* : 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.) ou à but d'information. Une des particularités du tatouage numérique par rapport à d'autres techniques, comme par exemple un stockage simple de l'information dans l'en-tête du fichier, est que le watermark est lié de manière intime et résistante aux données. De ce fait, le tatouage est théoriquement indépendant du format de fichier et il peut être détecté ou extrait même si le document a subi des modifications ou s'il est incomplet [16].

### 2.4. Modèle générique du tatouage :

Le schéma du tatouage numérique est résumé dans la *figure 1.3*.

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

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

La phase d'insertion génère en sortie un document tatoué  $I_w$ , Cette phase est modélisée par la fonction suivante :

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

$$I_w = E(I, W, K).$$

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

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

La phase de détection consiste à prouver la présence d'un watermark en utilisant une mesure de confidentialité  $\rho$ . Elle est modélisée par la fonction :

$$\rho = D(I_w^*, K, \dots).$$

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

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

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

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

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

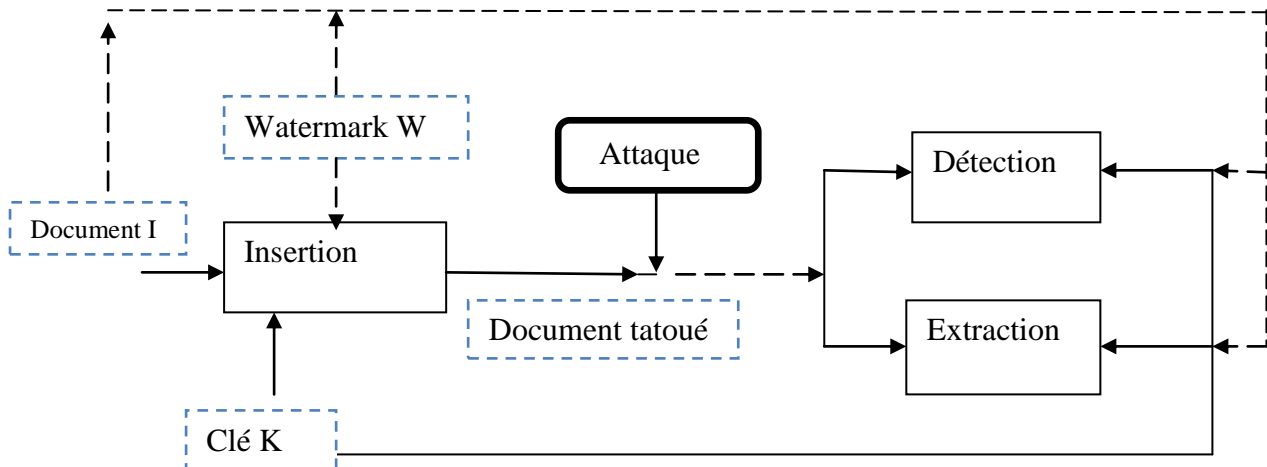


Figure 2.3 : Modèle générique d'un système du tatouage.

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

Les méthodes du tatouage requièrent différentes 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 :

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



## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

manipulations effectuées de bonne foi par un utilisateur. On retrouve dans cette catégorie : la compression JPEG, certaines transformations géométriques, 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 de 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 entend donc qu'elle n'a subi aucune modification malveillante. [17]

### ➤ Sécurité :

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

### 2.5. 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 ambiguïté 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 serve 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.

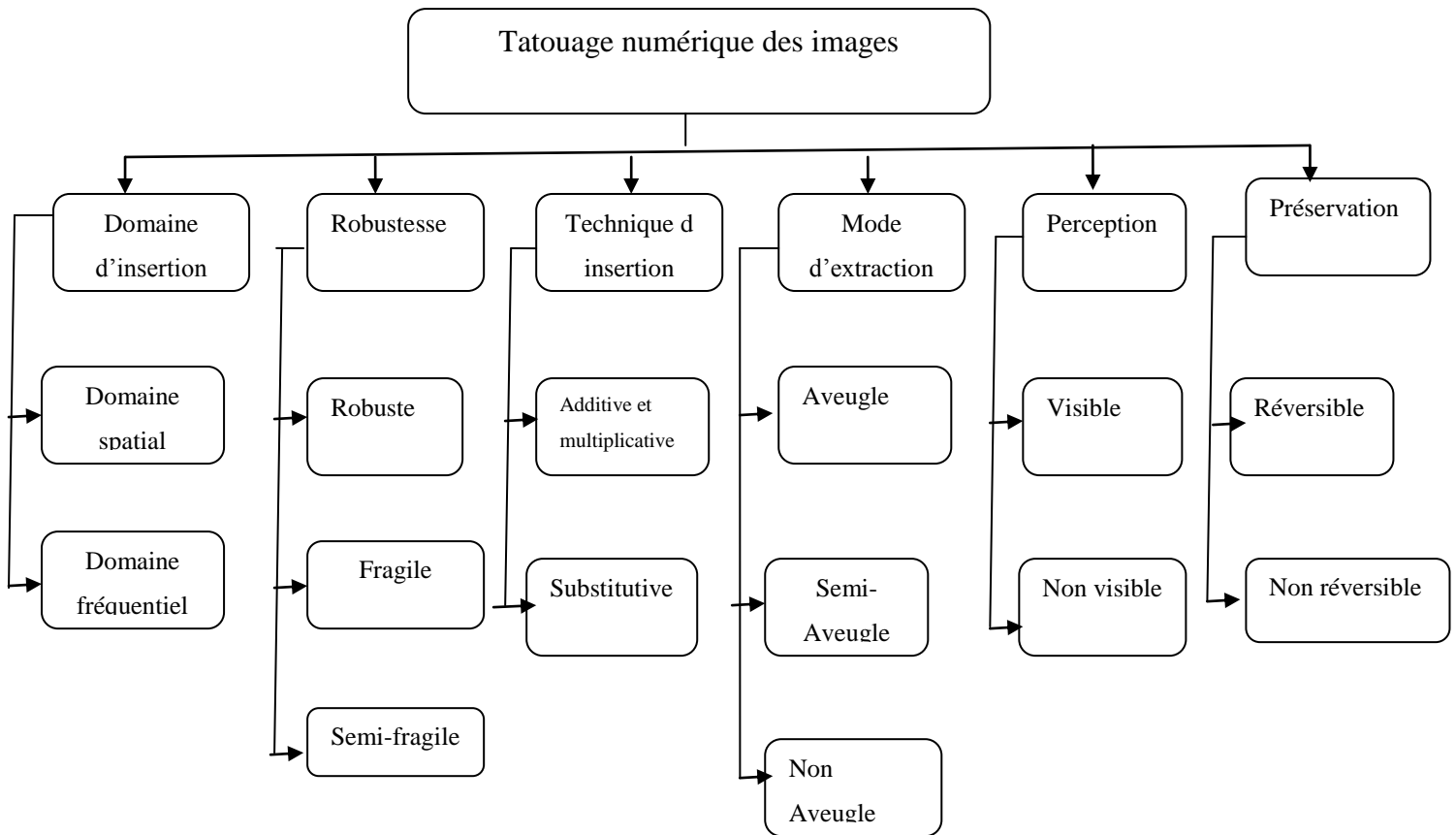
## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

- ✚ **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, si elle est malintentionnée, elle peut produire illégalement un nombre illimité de copies de ce document avec une qualité égale au document d'origine. Le tatouage numérique peut faire face à cette situation. Des informations relatives au nombre de copies autorisées sont encryptées dans la marque. Ce principe a été utilisé dans les vidéos où la marque indique si la vidéo peut être recopiée ou non.
- ✚ **Autres applications** : il existe d'autres applications telle 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. À 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 la préservation de l'image originale. La *figure 2.4* présente un organigramme de cette classification. [18]



**Figure 2.4 :** Organigramme de la 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 ancienne forme 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 :

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

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 de canal bruité ou de la technique d'insertion. La phase d'extraction peut requière le watermark ou l'image tatouée (l'image originale juste après l'incrustation du watermark, [19]).

la fonction d'extraction est modélisée comme suit :

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

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

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 :

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

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 pas toujours être garantie.

Les termes tatouage aveugle, semi aveugle et non aveugle peuvent être désignés respectivement par tatouage public, semi-privé et privé dans certains articles. [20].

### **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 reconnaître les perturbations malintentionnées et de 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. [21].

### **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.

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

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. [22]

### 2.7.5. Classification selon le domaine d'insertion :

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

#### 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 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. 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 contenues dans les bits LSB sont visuellement insignifiantes. Le watermark est généralement inséré en utilisant la connaissance de la séquence PN (et peut être la connaissance d'une clé secrète, comme la location du watermark). [23].

#### 2.7.5.2. Domaine Fréquentiel :

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

Des schémas du tatouage peuvent effectuer l'insertion du watermark dans des espaces transformés. Un espace transformé est obtenu après l'emploi d'une transformée telle que :

## Chapitre 2 : État de l'art sur le tatouage numérique des images

DCT, DFT, DWT, SVD, etc. Cette stratégie rend le watermark plus robuste à la compression, puisqu'elle utilise le même espace qui sert au codage de l'image. Contrairement au domaine spatial, le watermark insère dans le domaine fréquentiel est très sensible aux transformations géométriques parce que ce genre de transformations modifie considérablement les valeurs des coefficients transformés. [24]

### 2.7.5.2.1. 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 norme de compression connue JPEG est l'utilisée dans son implémentation et devient une norme de compression aimée actuellement.

La transformée en cosinus discrète (DCT) travaillant sur un signal discret. Elle prend un ensemble de points d'un domaine spatial et les transforme en une représentation équivalente dans le domaine fréquentiel. la DCT range une grande partie de l'énergie de signal dans les basses fréquences; celles-ci apparaissent dans le coin supérieur-gauche du DCT [25].

La transformation Cosinus discrète de l'image MxN est définie comme suite:

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

Et la transformation inversée de TCD – ITCD est définie comme suivante :

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

À cause de ces caractéristiques, la DCT est souvent utilisée dans les algorithmes de tatouage numérique des images, et La plupart des algorithmes basé sur cette transformée cache le message secret dans les moyennes fréquences. Les auteurs de ces méthodes espèrent ainsi en travaillant dans le domaine DCT, 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 comme suivante :

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

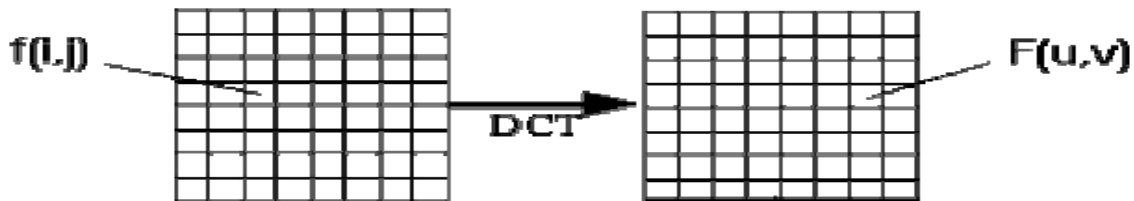
$$I(i, j) = \frac{1}{4} \sum_{i=0}^7 \sum_{j=0}^7 \Lambda(u) \cdot \Lambda(v) \cdot F(u, v) \cdot \cos\left[\frac{\pi u}{16} (2i + 1)\right] \cdot \cos\left[\frac{\pi v}{16} (2j + 1)\right]$$

$$\Lambda(i) = \begin{cases} \frac{1}{\sqrt{2}} & \text{si } i = 0 \\ \text{Oviceversa} & \end{cases}$$

$N, M$  : dimension de l'image

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

$F(u, v)$  : la coefficient TCD dans la ligne  $u$  et colonne  $v$ .



Les étapes principales de tout bloc basé L'algorithme de DCT sont : [26]

- deviser l'image dans les blocs non-recouverts de 8x8
- appliquer DCT sur chacun de ces blocs
- appliquer quelques critères de sélection de bloc (par exemple HVS)
- appliquer des critères de sélection de coefficient (par exemple le plus haut)
- insérer le watermarque en modifiant les coefficients choisis.
- appliquer DCT inverse sur chaque bloc

### Le choix de coefficient DCT :

Cette transformation ayant un caractère est la séparation entre des hautes fréquences, des bases fréquences et des fréquences moyennes. Les bases fréquences ayant les plus d'énergie car ses coefficients sont le plus grandes et la compression JPEG utilise cette caractère, donc, en utilisant DCT en tatouage, on peut diminuer ce type d'attaque. [27]

## Chapitre 2 : État de l'art sur le tatouage numérique des images

### 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 Beltrami et Jordan et pour les matrices complexes par Autonne en 1902. Récemment, la décomposition en valeurs singulières a été utilisée dans différentes applications du traitement d'image telle que la compression, la dissimulation de l'information et la réduction du bruit.

#### Principe :

Soit  $\mathbf{A}$  une matrice quelconque de taille  $m \times n$  et de rang  $r$  (le rang de la matrice  $\mathbf{A}$  est le nombre de valeurs singulières non nulles). Alors il existe une matrice orthogonale  $\mathbf{U}$  d'ordre  $m \times m$ , une matrice orthogonale  $\mathbf{V}$  d'ordre  $n \times n$  et une matrice "pseudo-diagonale" (tous les éléments hors de la diagonale principale sont nuls, mais la matrice n'est pas carrée)  $\mathbf{S}$  de dimension  $m \times n$  (et donc de même dimension que  $\mathbf{A}$ ), telles que :

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

$$\left\{ \begin{array}{l} \mathbf{U} * \mathbf{U}^T = \mathbf{I}(m) \\ \mathbf{V} * \mathbf{V}^T = \mathbf{I}(n) \\ \mathbf{S}(m,n) = \begin{pmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_n \end{pmatrix} \end{array} \right. \quad \begin{array}{l} s_1, s_2, \dots, s_n \text{ sont les valeurs singulières de } \mathbf{A}. \\ \text{Ce sont des nombres réels et non négatifs et} \\ \text{qui respectent la condition : } s_1 > s_2 > s_3 > \dots > s_n \end{array}$$

#### L'intérêt de la SVD pour le traitement d'images :

Le principal intérêt de cette méthode vient du 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.



## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

- 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.

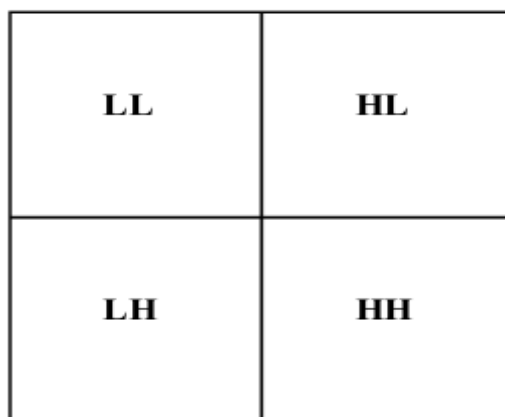
### 2.7.5.2.3. Transformée en Ondelette Discrète (DWT) :

La recherche sur la perception humaine indique que la rétine de l'œil coupe l'image en plusieurs canaux de fréquence. Les signaux dans ces canaux sont traités indépendamment. De même, dans une décomposition de multi-résolution, l'image est séparée dans des bandes de largeur de bande approximativement égale sur une échelle logarithmique. On s'attend à ce donc que l'utilisation de la transformée en ondelette discrète qui permettra le traitement indépendant des composants résultants sans interaction perceptible significative entre eux, et par conséquent rend le processus d'insertion imperceptible plus efficace.

La transformée en ondelettes utilise des filtres pour transformer l'image. Il y a beaucoup de filtres disponibles, les filtres les plus généralement utilisés pour le tatouage sont filtres ondelettes de Haar, filtres orthogonaux de Daubechies et filtres Bi-orthogonaux de Daubechies. Chacun de ces filtres décompose l'image en plusieurs fréquences.

La décomposition de niveau simple de l'image donne quatre représentations de fréquence. Ces quatre représentations s'appellent les sous-bandes LL, LH, HL, et HH comme montre la

*Figure 1.5*



*Figure 1.5* : Un niveau de décomposition en utilisant la DWT.

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

### Caractéristiques de DWT :

- 1) DWT décompose l'image en trois directions spatiales, c.-à-d. horizontale, verticale et diagonale.
- 2) DWT est efficace et peut être mise en application en employant la convolution simple de filtre.
- 3) l'importance de coefficients de DWT est plus grande dans les bandes (LL) à chaque niveau de décomposition et est plus petite pour d'autres bandes.

### Avantages de DWT- DCT :

- la DWT comprend le HVS plus étroitement que le DCT.
- 2) l'image codée par ondelette est une description de multi-résolution d'image. Par conséquent une image peut être montrée à différents niveaux de la résolution et peut être séquentiellement traité de la basse résolution à la haute résolution.
- 3) les objets façonnés de visuel présentés par des images codées par ondelette sont moins évident comparé à DCT parce que a DWT ne décompose pas l'image en blocs pour traitement. À la compression élevée les rapports bloquant des objets façonnés sont apparents dans DCT ; cependant, dans l'ondelette codée des images c'est beaucoup de clarifiant.
- 4) DFT et DCT en sont pleine armature transforment, et par conséquent le changement des coefficients de transformation affecte l'entier l'image exceptent si DCT est mis en application en utilisant un bloc basé approche. Cependant DWT a la localité spatiale de fréquence, ce qui signifie si le signal est inclus il affecte image

### Inconvénients de DWT DCT :

- la complexité de DWT davantage est comparée à DCT. Comme Feig (1990) a précisé il prend seulement 54 multiplications pour calculer DCT pour un bloc de 8x8, à la différence du DWT le calcul dépend de la longueur du filtre utilisé, qui est au moins 1 multiplication par coefficient. [28]

### 2.8. Classification des types d'attaques :

Un des critères fondamentaux à prendre en compte lors de la conception d'un algorithme de tatouage numérique est la robustesse de la marque. En effet, la marque doit résister aux différentes attaques, qu'elles soient bienveillantes ou malveillantes, sauf pour le tatouage numérique du type fragile.

• **Attaques bienveillantes** : regroupes les manipulations effectuées par un utilisateur qui n'ont pas initialement pour objectif d'empêcher la détection de la marque. Il peut s'agir des

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

dégradations dues à une compression (JPEG, JPEG2000), à un filtrage pour réduire le bruit, à une conversion de format, à un changement de résolution (zoom), etc. De plus, ces manipulations peuvent être combinées entre elles afin de créer des attaques plus complexes.

- **Attaques malveillantes** : regroupe les opérations qui ont pour objectifs de supprimer ou d'empêcher l'extraction correcte de la marque.

Il existe dans la littérature deux principales classifications détaillant de manière plus précise les différentes attaques que peut subir une image. La première classification est due à Hartung et al.: on classe les attaques qui ne détériorent pas de manière significative la fidélité perçue de l'image originale. Cette classification distingue les quatre catégories suivantes :

- 1. Attaques simples** : des attaques qui essaient de détériorer la marque insérée en manipulant l'ensemble des données de l'image tatouée, sans tenter d'identifier et d'isoler la marque. Cela peut inclure, le filtrage, la compression JPEG, l'ajout de bruit, quantification dans le domaine spatial et la correction gamma.

- 2. Attaques de détection infaisable** : ou attaques de synchronisation, ce sont des attaques qui tentent à rendre la récupération de la marque impossible ou de rendre infaisable le processus de détection, principalement par des déformations géométriques comme la mise à l'échelle (scaling), la rotation, le cisaillement, le recadrage, la permutation des pixels, ou toute autre transformation géométrique. Une caractéristique de ce type d'attaque est que la marque reste dans les images tatouées et attaquées : elle peut typiquement être récupérée en utilisant des méthodes sophistiquées de détection.

- 3. Attaques d'ambiguïté** : ou attaques de confusion, attaques d'inversion, attaques de la marque truquée. Ces attaques tentent de produire une tentative de confondre en produisant des images tatouées truquées. Un exemple de ce type d'attaque est l'attaque IBM qui essaie de discréditer l'autorité de la marque en insérant une ou plusieurs marques additionnelles afin qu'il soit difficile de déterminer la marque originale.

- 4. Attaques d'enlèvement** : il s'agit d'attaques qui tentent d'analyser les images tatouées, estiment la marque ou l'image originale, séparent l'image tatouée en donnant l'image originale et la marque qui sera jetée. Cette catégorie regroupe les attaques suivantes : l'attaque de collusion, le débruitage, certaines opérations de filtrage non linéaire et certaine méthode de compression. Cette catégorie inclut aussi les attaques conçues spécialement pour un schéma de tatouage numérique en exploitant les faiblesses cryptographiques le rendant vulnérable à une attaque spécifique. Pour une attaque de collusion, un attaquant peut utiliser plusieurs copies d'images tatouées : chacune d'elle est tatouée par une marque différente de l'autre. À

## Chapitre 2 : État de l'art sur le tatouage numérique des images

---

partir de ces copies, l'attaquant peut construire une copie de l'image originale qui ne contient aucune marque. [29]

### **2.9. Conclusion :**

Dans ce chapitre, nous avons présenté la technologie du tatouage numérique d'une manière générale. Nous nous sommes intéressés aux terminologies et notions liées aux techniques du tatouage invisible des images numériques. Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle.

Nous avons présenté aussi une taxonomie des techniques du tatouage selon différents critères : type de l'algorithme, champ d'application et le domaine d'insertion. Selon le dernier critère les techniques du tatouage peuvent être regroupées en deux catégories : ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel. Dans cette dernière catégorie plusieurs transformées peuvent être utilisées telles que la DFT, DCT, DWT, et la SVD.

## ***CHAPITRE 3 :***

Simulation des algorithmes de tatouage

### **3.1. Introduction :**

Les premiers algorithmes de tatouage numérique des images ont été conçus pour opérer dans le domaine spatial, mais ces dernières années l'utilisation des transformées des données a permis de concevoir des algorithmes permettant d'approcher les critères souhaités : Robustesse, transparence,... . Les transformées les plus populaires en traitement d'image sont la DFT, la DCT, la DWT, la SVD...etc.

L'objectif de ce chapitre est de jeter la lumière sur les différents résultats de simulation dans le contexte du tatouage numérique des images, en présentant quelques algorithmes très connus qui utilisent ces transformées pour insérer des watermarks numériques.

### **3.2. La décomposition en valeurs singulières SVD :**

Une matrice est un tableau de nombres dont il est parfois difficile d'extraire les caractéristiques intéressantes pour résoudre un problème donné. Une stratégie efficace pour mettre en évidence les propriétés d'une matrice est de la décomposer (ou factoriser) en un produit de matrices plus simples et dont les caractéristiques sont clairement identifiables et interprétables. La factorisation la plus générale, et peut-être la plus utile, est la Décomposition en Valeurs Singulières (que l'on désigne souvent par son acronyme anglo-saxon "SVD", pour "Singular Value Decomposition").

Le principe de la décomposition d'une matrice SVD est déjà expliqué au deuxième chapitre.

### **3.3. Algorithmes de tatouage d'image au niveau de gris utilisant la transformée SVD :**

Dans cette section je présente quelques algorithmes de tatouage d'images en niveau de gris basés sur la transformée SVD. La marque à insérer pourra se faire dans l'une des matrices U, S ou V, selon un choix approprié.

#### **3.3.1. Algorithme utilisant la matrice V :**

Dans cet algorithme la marque est insérée dans la matrice orthogonale V

### 3.3.1.1. Algorithme d'insertion :

L'algorithme d'insertion est expliqué par le schéma synoptique suivant (voir Figure). Le résultat dépend de la constante  $\mu$ . Elle est choisie expérimentalement et elle peut être vue comme une clé privée (elle ne sera connue que des personnes ayant droit d'extraire le watermark).

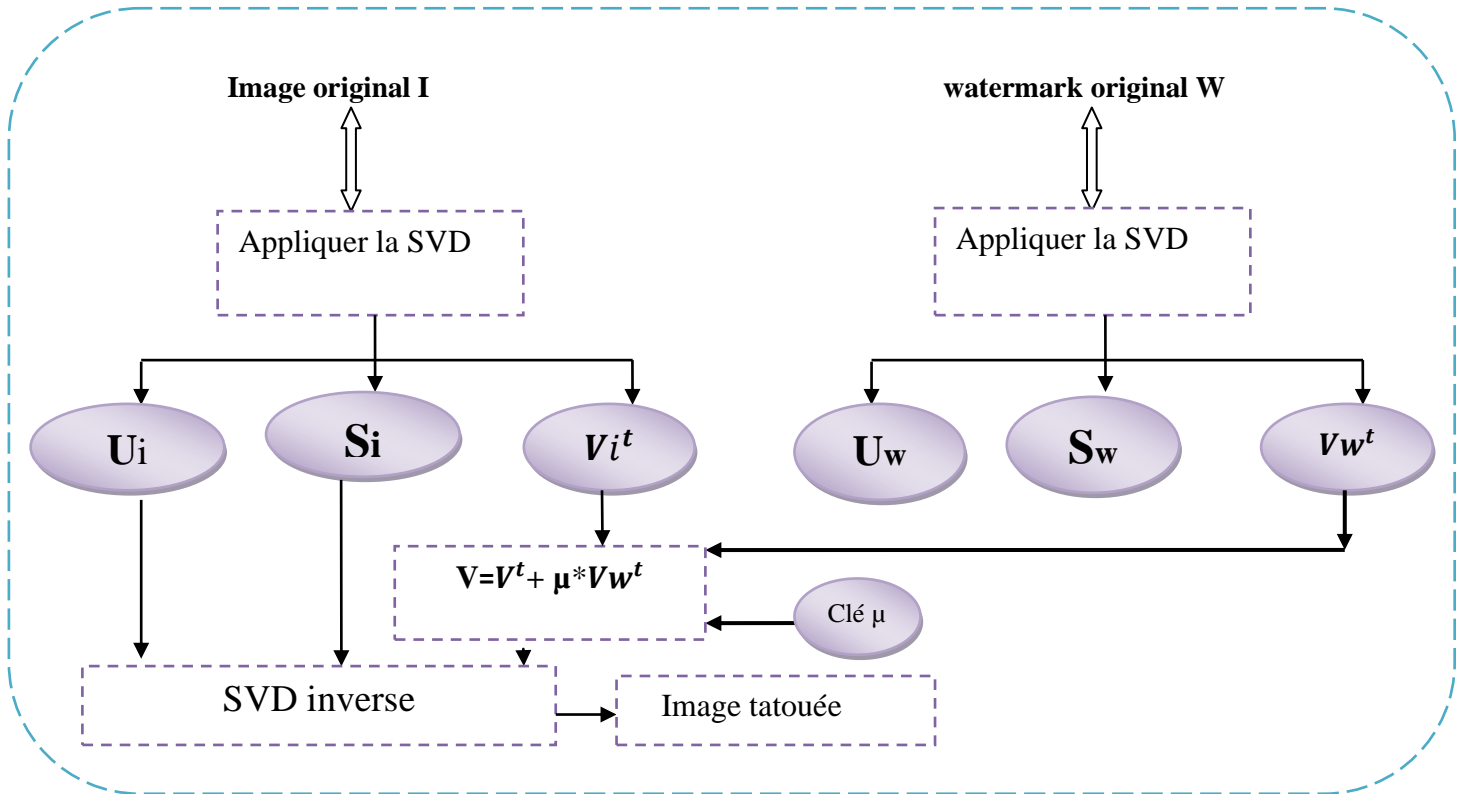


Figure 3.1 : Algorithme d'insertion du watermark dans la matrice V

- 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'images. L'image tatouée est représenté sur la Figure 3.2.



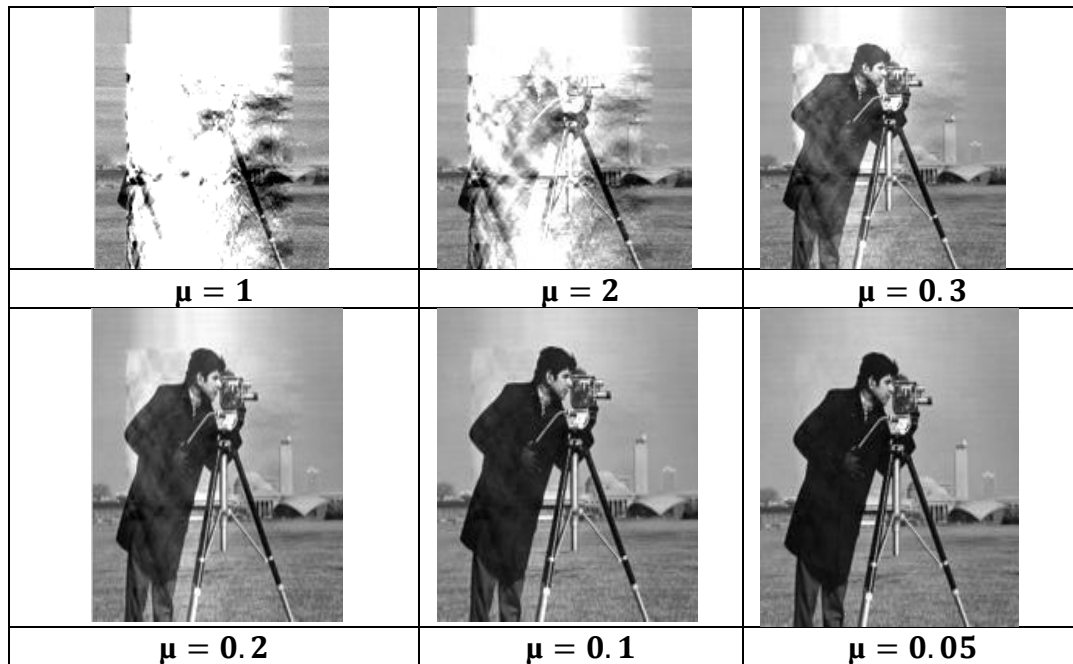
(a) :

Image hôte



(b) :

watermark original.



**Tableau 3.2:** images tatouées pour différents valeurs de poids  $\mu$ .

Le **Tableau 3.2** montre les effets des diverses valeurs de poids  $\mu$  sur l'image tatouée. On peut voir que le choix d'un poids élevé provoque une déformation significative sur l'image tatouée et la marque devient visible, par contre quand le poids est trop petit la marque devient irrécupérable. Alors il faut choisir un poids optimal et j'ai trouvé expérimentalement qu'un poids de 0.05 ( $\mu=0.05$ ) permet une imperceptibilité de la marque. Pour la suite, l'image tatouée sera traitée en utilisant  $\mu=0.05$ . Cette valeur représentant la clé pourra être changée à la guise de l'utilisateur et devra être gardée secrète.

### 3.3.1.2. Algorithme Extraction :

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



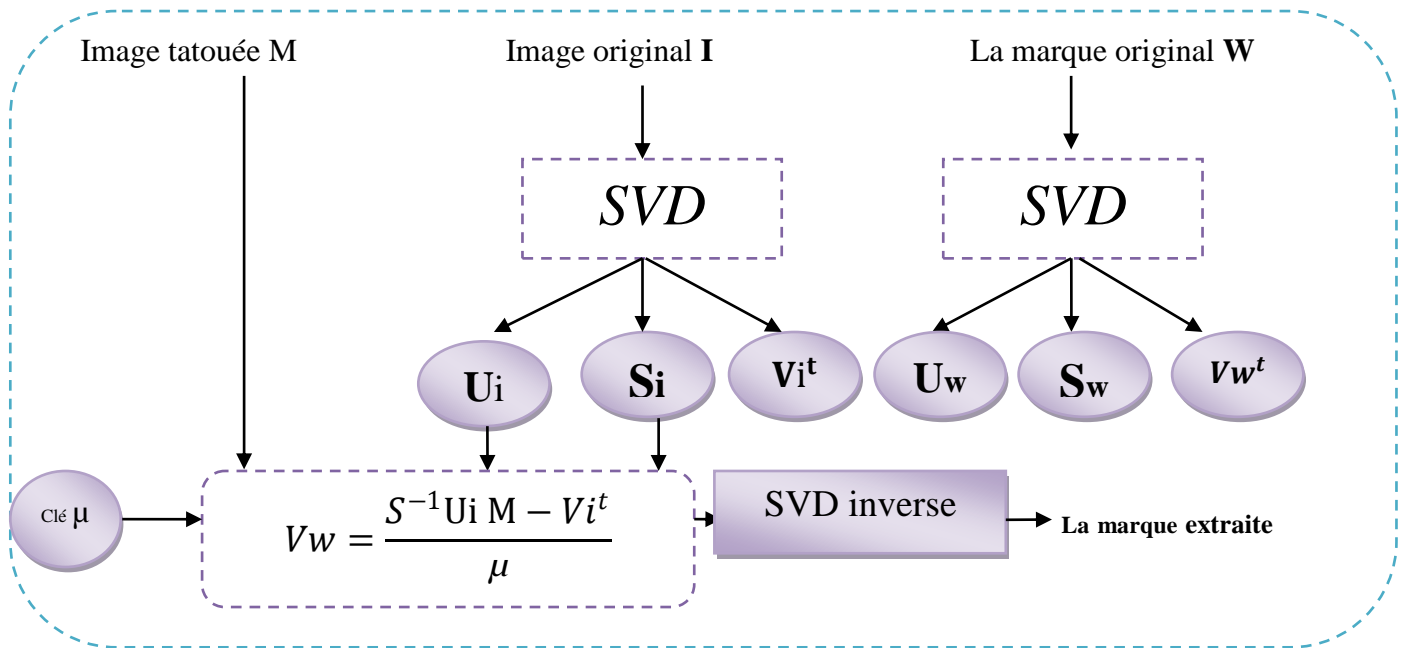


Figure 3.3: Algorithme d'extraction du watermark.

• Exemple d'application :



a) watermark original



b) image tatouée



c) watermark extrait

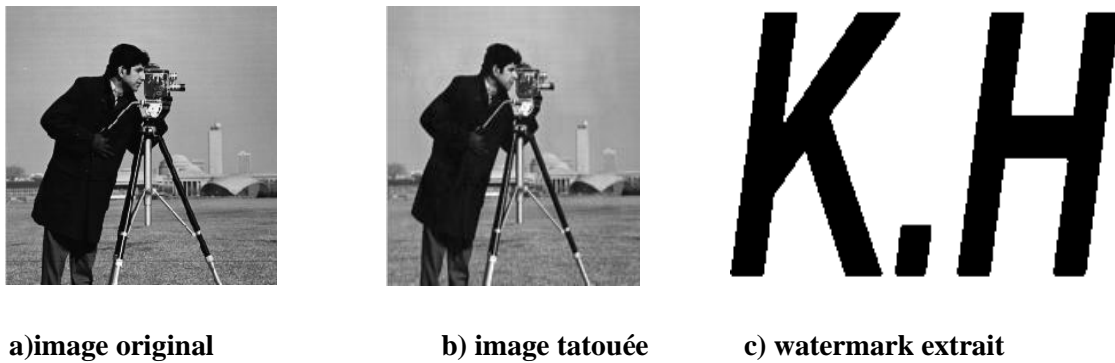
Figure 3.4 : extraction du watermark avec un poids de 0.05

3.3.2.3. Performance de l'algorithme

Dans cette partie, nous évaluons les performances de notre méthode en termes d'imperceptibilité et de robustesse. Les résultats expérimentaux sont séparés en deux parties : dont la première est consacrée au teste de la propriété d'imperceptibilité alors que la deuxième est consacrée à l'analyse de la robustesse contre quelques types d'attaques standards.

❖ Propriété d'imperceptible

Pour vérifier la propriété d'imperceptibilité de cet algorithme, on va appliquer celui-ci sur les deux images standards : cameramen et Lena de taille 512\*512 et la marque suivante :



**Figure 3.5 :** (a)Image cameraman, (b) image cameraman tatouée avec l’algorithme utilisant la matrice  $V$  , (c) le watermark extrait



**Figure 3.6 :** (a)Image Lena, (b) image Lena tatouée avec l’algorithme utilisant la matrice  $V$  , (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 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 :

## Chapitre 3 : simulation des algorithmes de tatouages.

L'image		NC	PSNR
cameraman	Entre W et W*	0.9990	27.2821
	Entre I et I*	0.9996	30.4479
Lena	Entre W et W*	0.9984	25.3350
	Entre I et I*	0.9997	30.4546




**Tableau3.3** : la PSNR et le coefficient de corrélation concernant l'algorithme utilisant la matrice V .

### ❖ 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 implantés comme la compression, le débruitage... etc.



### ❖ Compression

On s'intéresse d'abord à la compression JPEG, car c'est le schéma de codage d'images le plus populaire et qui est généralement considéré comme une attaque dure contre les algorithmes de tatouage d'images. En effet, plusieurs méthodes ne sont pas robustes à ce type d'attaque

	JPEG facteur 10	JPEG facteur 20	JPEG facteur 40
Watermark extrait			
NC	0.9984	0.9966	0.9711

### ❖ Filtrage

Nous avons effectué comme attaques les deux types de filtre : le filtre médian et le filtre sharpen.




Filtre médian	Filtre sharpen
	
NC = 0.9620	NC = 0.9759

Le tableau suivant montre les watermarks extraits après les divers types de filtre utilisés. Les watermarks sont identifiables et les coefficients de corrélation sont proches de 1. On peut alors conclure que la méthode est robuste contre certains types de filtres.



### ❖ Débruitage

En utilisant l'application Jasc Software's Paint Shop Pro version 7, pour faire des perturbations avec des pourcentages variables de bruit uniformément distribué.

Le tableau suivant montre que la méthode est robuste au débruitage mais l'augmentation de pourcentage de bruit va diminuer le coefficient de corrélation mais on peut identifier le watermark facilement.

Pourcentage de bruit	1%	4%	12%
Watermark extrait			
NC	0.9902	0.59722	0.38056

Dans le tableau suivant, on présente d'autres types d'attaques (le bruit gaussien et le bruit salt and pepper) :

Bruit gaussien (M=0.001, V=0.001)	Le bruit Salt and pepper (d=0.02)
	
NC=0.82624	NC=0.4512

Les résultats précédents montrent que le débruitage de l'image ne détruira pas complètement le watermark.

### 3.3.2. Algorithme utilisant la matrice S :

Dans cet algorithme on insère la marque dans les basses ou moyennes fréquences selon un compromis robustesse / imperceptibilité. C'est pourquoi nous avons choisi le coefficient  $\lambda_3$  pour insérer la marque. (Ou  $\lambda_3$  est le troisième SV) [28].

#### 3.3.2.1. Insertion de la marque :

L'algorithme d'insertion de la marque est décrit comme suit :

- Partitionnement de l'image I en blocs carrés de  $8 \times 8$
  - Choix d'un nombre b de blocs en fonction d'une clé qui exprime la position de chaque bloc
  - Calcul de la SVD sur chacun des blocs choisis ;
  - Insertion des bits de la marque W dans la matrice S de l'image I selon les règles suivantes :
  - On calcule pour chaque bloc  $Moy = \frac{\lambda_2 + \lambda_4}{2}$ 
    - ↪ Pour marquer un « 1 », choisir  $\lambda_3$  telle que :  $Moy < \lambda_3$
    - ↪ Pour marquer un « 0 », choisir  $\lambda_3$  telle que  $\lambda_3 < Moy$ .
  - On note  $S_w$  la nouvelle matrice S tatouée.
  - Reconstruction de l'image tatouée en calculant :  $U * S_w * V^T$
- ❖ Exemple d'application de l'algorithme d'insertion :

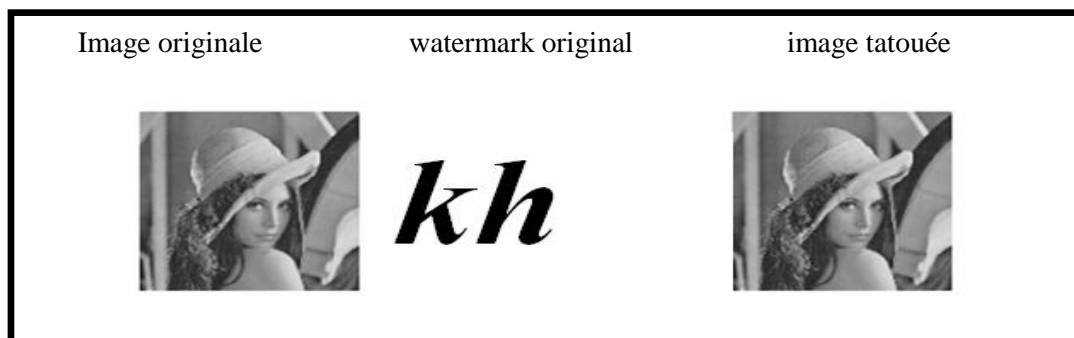


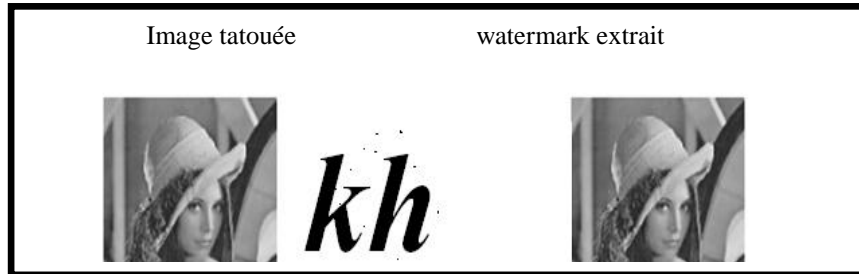
Figure 3.7 : Application de l'algorithme d'insertion utilisant la matrice S sur l'image Lena

#### 3.3.2.2. Extraction de la marque :

- Partitionnement de l'image tatouée en blocs carrés de  $8 \times 8$
- Calcul de la SVD sur chacun des blocs choisis ;
- On calcule pour chaque bloc :  $Moy = \frac{\lambda_2 + \lambda_4}{2}$

☐ Si  $(\lambda_3 > \text{moy})$  alors bit de la marque = 1    Sinon bit de la marque = 0

❖ Exemple d'application de l'algorithme d'extraction :

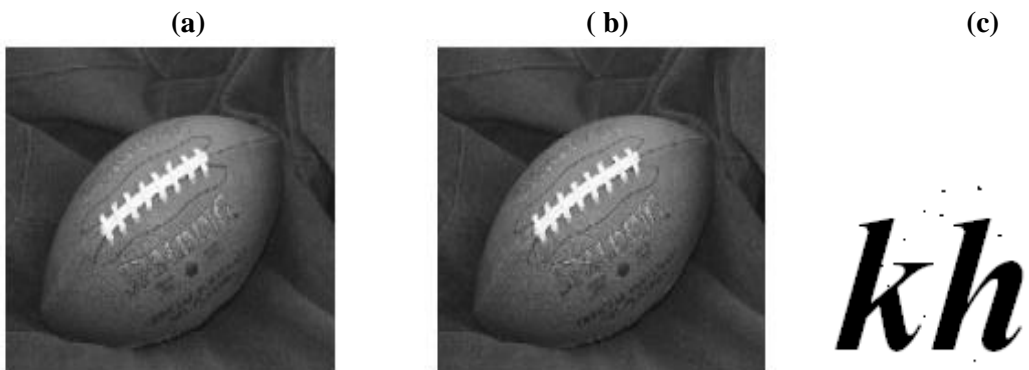


**Figure 3.8:** extraction du watermark a partir de l'image Lena tatouée avec l'algorithme qui utilise la matrice S

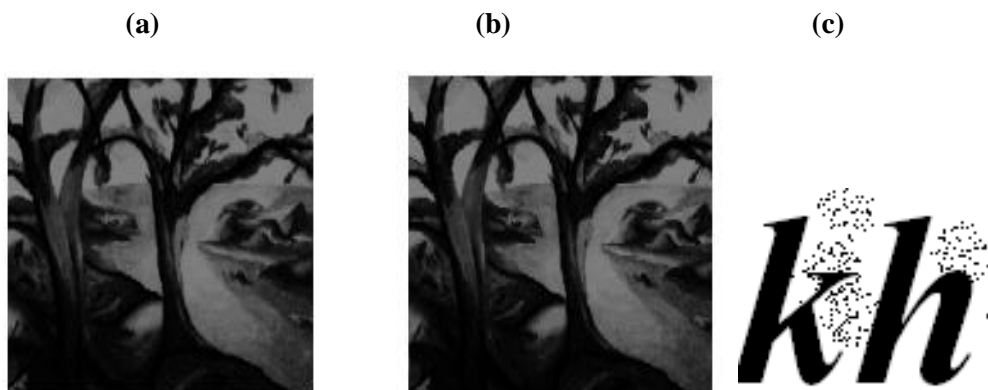
### 3.3.2.3. Performance d'algorithme :

❖ *Propriété d'imperceptibilité*

Pour voir cette propriété on va appliquer l'algorithme sur les deux images football de taille 256\*320 et trees de taille 258 \* 350



**Figure3.9:** (a) image football , (b) image football tatouée avec l'algorithme utilisant la matrice S, (c) le watermark extrait



**Figure3.10 :** (a) image trees , (b) image trees tatouée utilisant la matrice S , (c) le watermark extrait

## Chapitre 3 : simulation des algorithmes de tatouages.

A partir des figures 3.9 et 3.10, on peut voir qu'il est difficile de différencier entre les images originales et leurs images tatouées. Pour évaluer concrètement la qualité de notre méthode, on utilise le PSNR pour estimer la distorsion des images tatouées.




IMAGE	ENTRE	PSNR	NC
<b>Lena</b>	I et I*	43.9521	0.9974
	W et w*	72.7931	0.9974
<b>Football</b>	I et I*	43.9521	0.9983
	W et w*	73.4626	0.9983
<b>Trees</b>	I et I*	43.9521	0.9664
	W et w*	73.4626	0.9664

**Tableau3.2** : la PSNR et le coefficient de corrélation concernant l'algorithme utilisant la matrice

### ❖ *Propriété de robustesse* :

Nous avons testé cette technique aux attaques de traitement d'images : Compression JPEG, filtrage avec un filtre shapen et l'ajout de Bruit salt end pepper

Le tableau suivant présente les watermarks extraits et les coefficients de corrélation pour chaque type d'attaque :

Compression JPEG (facteur 5)	Salt end peper (d =0.005)	Sharpen filtre
		
NC=0.092538	NC= 0.48367	NC=0.30922

On remarque que cet algorithme est peu robuste aux attaques et surtout à la compression, ou un facteur de compression de 5 va diminuer le coefficient de corrélation jusqu'à 0.09 mais la marque est encore identifiable.

### 3.4. Algorithme Bloc-SVD de Chandra :

Dans cet algorithme l'image hôte est décomposée en blocs  $B_i$  de taille  $8 \times 8$ , et la SVD est appliquée sur chaque bloc  $B_i$ . Le principe de cet algorithme est présenté ci-dessous. [29]

#### 3.4.1. Algorithme d'insertion :

La décomposition de l'image hôte  $I$  en blocs  $B_i$  de taille  $8 \times 8$

Pour chaque bloc  $B_i$  faire :

↪ Décomposition de  $B_i$  en valeurs singulières :  $B_i = U_i * S_i * V_i^T$

↪ Insertion d'un bit du watermark ( $W_i$ ) dans la plus grande SV ( $\lambda_1$ ) du bloc  $B_i$  comme suit :

$$\lambda_w = \lambda_i^1 + \alpha * W_i$$

↪ Insertion d'un bit du watermark ( $W_i$ ) dans la plus grande SV ( $\lambda_1$ ) du bloc  $B_i$  comme suit :

$$\lambda_w = \lambda_i^1 + \alpha * W_i$$

$\alpha$  : est un scalaire choisi pour maintenir la qualité de l'image tatouée,

$\lambda_w$  ; est la plus Grande SV du bloc tatoué  $B_{wi}$ .

↪  $S_w$  est la matrice diagonale  $S_i$  où le premier élément est remplacé par  $\lambda_w$ . Cette matrice

est utilisée pour construire le bloc tatoué  $B_{wi}$  comme suit:  $B_{wi} = U_i * S_w * V_i^T$

Construction de l'image tatouée à partir des blocs tatoués.

#### 3.4.2. Algorithme d'extraction :

La décomposition de  $I_w$  en blocs  $B_i$  de taille  $8 \times 8$

Pour chaque bloc  $B_i$  faire :

↪ La décomposition de  $B_i$  en valeurs singulières :  $B_i = U_i * S_i * V_i^T$

↪ Le bit  $W_i$  du watermark est obtenu à partir du la plus grande du bloc tatoué  $I_w$  et celle du

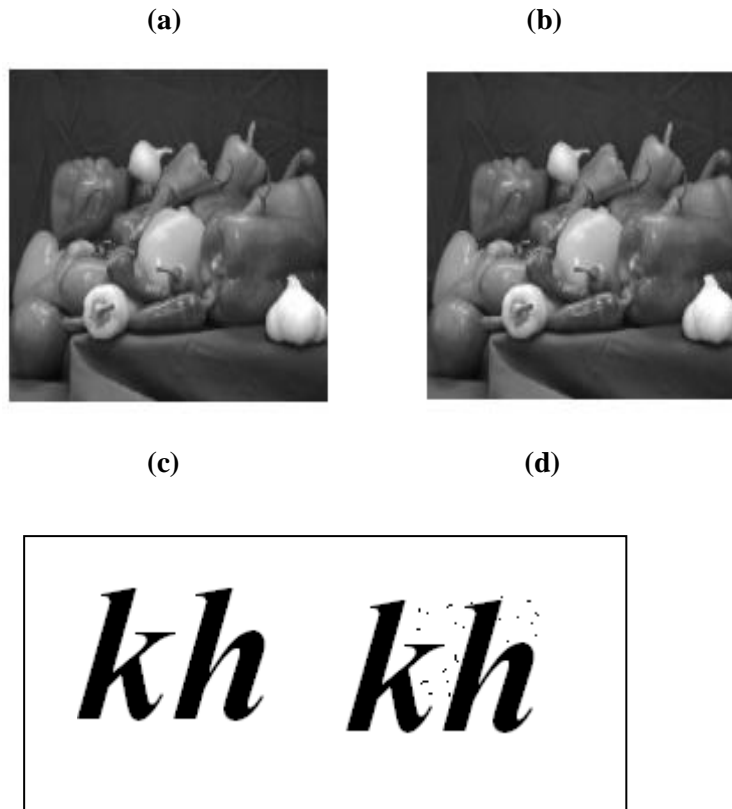
bloc original  $I$  comme suit :  $W_i = \frac{I_w - I}{\alpha}$

Construire le watermark  $W^*$  à partir des bits  $W_i$ .



### 3.3.3.3. Résultats de simulation :

Dans toutes ces expériences, la clé  $\alpha$  est égale à 0.05. Les résultats de simulation de l'algorithme de tatouage sur l'image Peppers de taille 384\*512 sont représentés dans la figure 3.11.



**Figure 3.11** : (a) image Peppers, (b) image peppers tatouée avec l'algorithme bloc- svd de Chandra , (c)watermark original , (d) watermark extrait

### 3.3.3.4. Performance de l'algorithme :

#### ❖ *Propriété d'impercibilité*

Pour voir cette propriété on va appliquer l'algorithme sur les deux images Cameraman de taille 256\*256 et Lena de taille 512 \* 512



**Figure 3.12 :** (a) image Cameraman , (b) image Cameraman tatouée avec l’algorithme de Chandra, (c) watermark extrait








**Figure 3.13 :** (a) image Lena ,(b) image Lena tatouée avec l’algorithme de chandra, (c) watermark extrait

A partir de ces deux figures, on peut voir qu’il est difficile de différencier entre les images originales et leurs images tatouées. Donc, la méthode est imperceptible. Pour voir la qualité des images tatouées on calcule les valeurs du PSNR et du NC entre  $W$  (original) et  $W^*$  (extrait) et entre l’image originale ( $I$ ) et l’image tatouée ( $I^*$ ). Ces valeurs sont présentées dans le tableau suivant :

**Table 3.3 :** Le PSNR et le coefficient de corrélation des images tatouées et des watermarks extraits par l’algorithme Bloc-SVD de Chandra

Image		NC	PSNR
Peppers	Entre $W$ et $W^*$	0.98273	25.6290
	Entre $I$ et $I^*$	0.99991	42.525
Cameraman	Entre $W$ et $W^*$	0.96940	23.9083
	Entre $I$ et $I^*$	0.99995	43.4323
Lena	Entre $W$ et $W^*$	0.98742	26.0855
	Entre $I$ et $I^*$	0.99992	42.2586

### ❖ *Propriété de robustesse*

JPEG 60	bruling	Bruit salt & pepper	Filtre Sharpen	Filtre médian
				
NC=0.29633	NC=0.14325	NC=0.17324	NC=0.43839	NC=0.43316

Le tableau précédent montre que les watermarks extraits après les divers types d'attaque peuvent être identifiables malgré que les coefficients de corrélation sont petits. On remarque aussi que la méthode est robuste jusqu'à une compression correspondant à un facteur de qualité de 60%. Donc On peut conclure que cette méthode est robuste contre certains types de d'attaques

### 3.3.4. Algorithme utilisant la transformée d' Arnold :

#### 3.3.4.1. La transformation d'Arnold :

Pour augmenter la sécurité du tatouage, le watermark peut être prétraité avant de l'insérer dans l'image originale. Cela peut se faire par la transformée d'Arnold grâce à son processus de Périodicité qui consiste à changer les places des pixels d'une image carrée de taille  $N \times N$

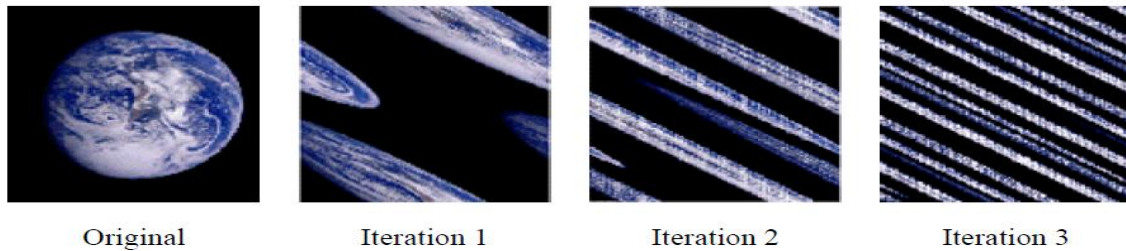
selon le système suivant :  $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}$

$(x, y) \in \{0, 1, \dots, N-1\}$ , et  $(x', y')$  sont les coordonnées des pixels après la transformation d'Arnold.

Le tableau suivant donne la période  $T_N$  nécessaire pour chaque nombre de pixels  $N$

N	10	25	50	60	125	128	256	480	512
$T_N$	30	50	150	60	250	96	192	120	384

En appliquant la transformée d'Arnold sur l'image Earth on voit qu'après la première itération l'image est complètement changée.[30]



**Figure 3.14 :** Application de la transformée d'Arnold sur l'image Earth

### 3.4.1.2. L'algorithme de tatouage :

Le schéma général du tatouage qui utilise la transformation d'Arnold est représenté sur la figure 3.15.[31]



**Figure 3.15 :** Le schéma général du tatouage qui utilise la transformée d'Arnold

#### ❖ *Algorithme d'insertion*

- La décomposition de l'image hôte  $I$  en valeurs singulières :  $I = U * S * V^T$
- Application de la transformation d'Arnold sur le watermark  $W : W(x, y) \rightarrow W(x', y')$
- La décomposition du watermark par la transformation d'Arnold  $w(x', y')$  en valeurs singulières :  $W(x', y') := U_w * S_w * V_w^T$
- Construction d'une nouvelle matrice diagonale  $S_y$  dont les valeurs diagonales sont  $\lambda_{yi}$  selon la formule suivante :  $\lambda_y = \lambda + \alpha * \lambda_w$ 
  - $\alpha$  : est un scalaire choisi pour maintenir la qualité de l'image tatouée.
  - $\lambda$  : les éléments diagonaux de  $S$
  - $\lambda_w$  : les éléments diagonaux de  $S_w$
  - $\lambda_y$  : les éléments diagonaux de  $S_y$
- Reconstruction de l'image tatouée  $I_w$  en utilisant  $S_y$  et les matrices orthogonales ( $U, V$ ) de l'image originale comme suit :  $I^* = U * S_y * V^T$

### ❖ *Algorithme d'extraction*

❑ La décomposition de l'image  $I_w$  en valeurs singulières :  $I^* = U_y * S_y * V_y^T$

❑ Le calcul de la matrice diagonale  $S_w$  du watermark :  $S_i = \frac{(s_y - s)}{\alpha}$

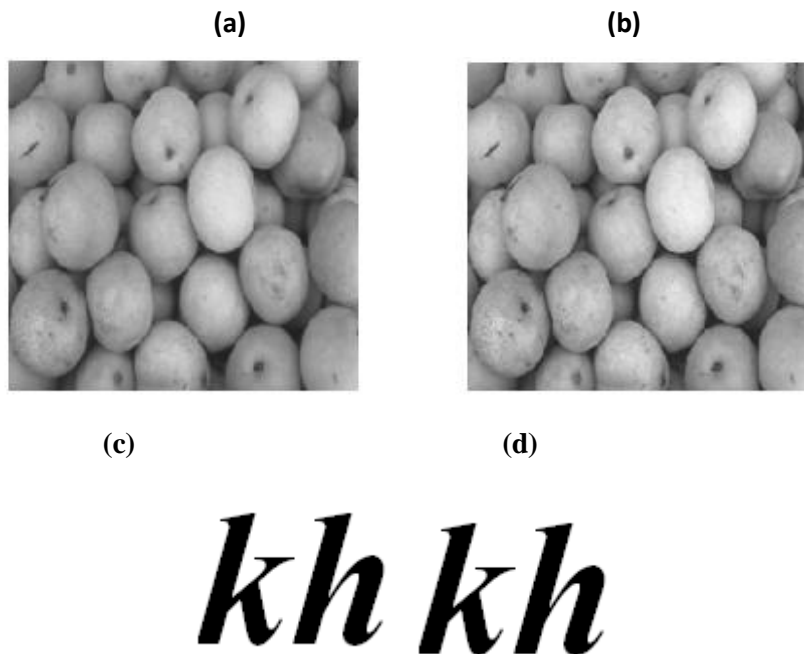
❑ Reconstruction du watermark  $W^*$  en utilisant  $S_i$ ,  $U_w$  et  $V_w$  comme suit :

$$W^* = U_w * S_i * V_w^T$$

❑ Application la transformation d'Arnold pour récupérer le watermark

### 3.3.4.3. Les résultats expérimentaux :

Dans toutes ces expériences, la clé  $\alpha$  est égale à 0.05. Les résultats de simulation de l'algorithme de tatouage sur l'image Pears de taille 486\*732 sont représentés dans la Figure 3.16

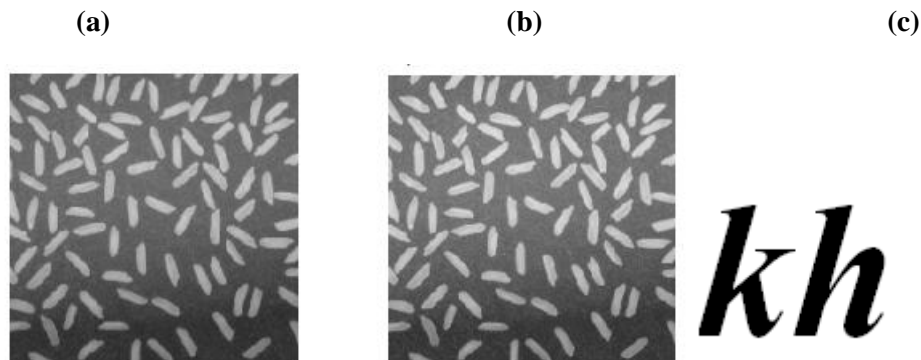


**Figure 3.16:** (a) Image Pears, (b) image Pears tatouée par l'algorithme utilisant la transformée d'Arnold, (c) Watermark Original, (d) Watermark extrait

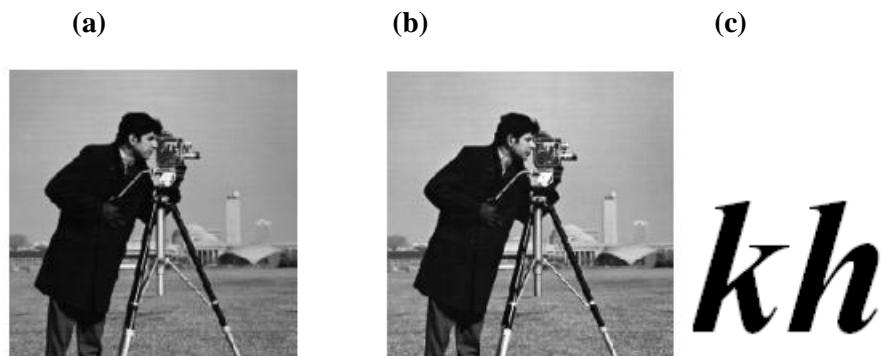
### 3.3.4.4. Performance de l'algorithme :

#### ❖ *Propriété d'impercibilité*

Afin de tester la propriété d'impercibilité de notre méthode de tatouage, on va les appliquer sur les deux images Rice et Cameraman de taille 256× 256 et le watermark de taille 256\*256



**Figure3.17 :** (a) image Rice originale, (b) image Rice tatouée avec l’algorithme utilisant la transformée d’Arnold ,(c) le watermark extrait



**Figure3.18 :** (a) image Cameraman originale, (b) image Cameraman tatouée utilisant par l’algorithme utilisant la transformée d’Arnold, (c) le watermark extrait





les figures précédentes montrent que l’image originale et l’image tatouée sont presque identiques et on ne peut pas visualiser la différence entre les deux. Donc on peut dire que cette méthode est imperceptible. Pour voir la qualité des images on calcule les valeurs du PSNR et du NC entre  $W$  (original) et  $W^*$  (extrait) et entre l’image originale ( $I$ ) et l’image tatouée ( $I^*$ ) qui sont présentées dans le tableau suivant:

Image		NC	PSNR
pears	Entre W et W*	1	61.5842
	Entre I et I*	0.99837	26.3973
rice	Entre W et W*	0.99999	59.3566
	Entre I et I*	0.99948	26.3974
Cameraman	Entre W et W*	0.999079	40.7152
	Entre I et I*	0.99932	26.4215

**Tableau3.4** : le PSNR et le coefficient de corrélation d'images tatouées et du watermark extraits de l'algorithme qui utilise la transformée d'Arnold

❖ *Propriété de robustesse*

Nous avons testé la robustesse de cet algorithme à quelques attaques de traitement d'images.

Bruit gaussienne	Bruit salt 1& peppers	Rotation de 1°	Compression jpeg
			
NC=0.97919	NC=0.75162	NC=0.70181	NC=0.90001

Le tableau ci-dessus montre que la méthode est robuste contre plusieurs attaques (Bruits, compression et même au attaques géométriques).

### 3.4.Algorithme de tatouage d'images en couleurs utilisant la transformée SVD :

Malgré l'intérêt capital des images en couleurs, la plupart des méthodes de tatouage d'images sont pointées vers les images à niveaux de gris. Pour cette raison, nous avons étudié une nouvelle méthode de tatouage numérique d'images en couleurs. Nous avons présenté un algorithme du tatouage qui vise à insérer un watermark en couleurs RGB dans une image en couleurs RGB. [32]

### 3.4.1. Algorithme d'insertion :

Dans cette section, nous présentons l'algorithme d'insertion par le schéma synoptique suivant :

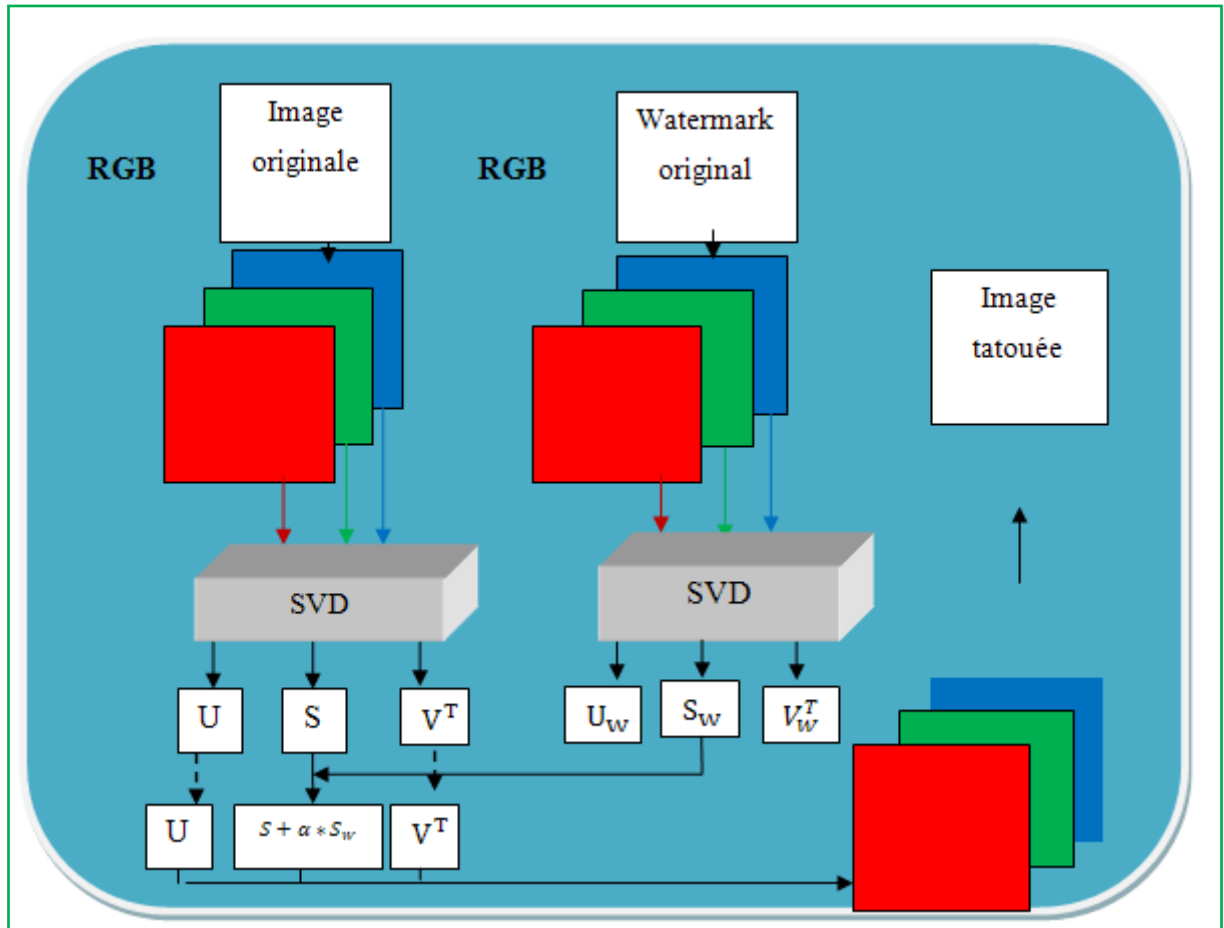


Figure 3.19 : Algorithme d'insertion de la marque dans une image en couleurs

### 3.6.2. Algorithme d'extraction :

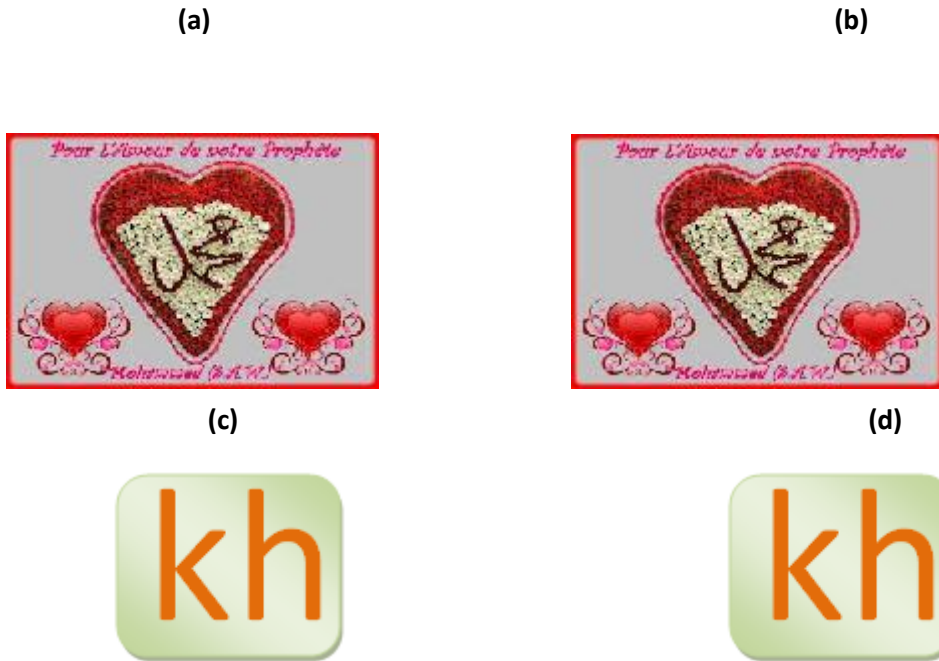
- Séparez les espaces des couleurs R, G, B de l'image tatouée
- pour chaque espace de couleur faire :
  - ↪ la décomposition singulière des valeurs (SVD),
  - ↪ extraire la matrice orthogonale  $S_w$  du watermark à partir de l'espace de couleur de l'image tatouée et de l'image originale  $S_w = (S^* - S)/\alpha$  où  $S_w$  est la matrice diagonale de l'image tatouée et  $\alpha$  est un scalaire choisi pour maintenir la qualité de l'image tatouée,
  - ↪ appliquer la SVD inverse pour obtenir le coefficient de chaque espace de couleur du watermark
- Combiner les espaces des couleurs R, G, B pour obtenir la marque extraite



## Chapitre 3 : simulation des algorithmes de tatouages.

### ✓ Résultats de simulation :

Les résultats de simulation de l'algorithme de tatouage sur l'image « Ahmed » de taille 400\*400 sont représentés sur la Figure 3.20 avec une clé  $\alpha$  égale à 0.05



**Figure 3.20 :** (a ) Image en couleurs originale, (b) image en couleurs tatouée, (c) watermark en couleurs original, (d)watermark en couleurs extait

	PSNR	NC
<b>Image tatouée</b>	29.0592	0.9995
<b>La marque extraite</b>	47.3541	0.9999

**Table3.5 :** le PSNR et le coefficient de corrélation de l'image en couleurs tatouée et du watermark en couleurs extrait

### Robustesse de l'algorithme :

Nous avons testé cette technique aux attaques suivantes : la Compression JPEG ,le filtrage et Ajout de Bruit



**Bruit gaussian**



**bruit salt end pepper**



**bruit poisson**



**Compression jpeg**



**filtre sharpen**

Type d'attaque	Bruit gaussian	bruit salt and pepper	bruit poisson	Compression JPEG facteur 60	filtre sharpen
<b>PSNR</b>	13.1835	11.8603	11.8761	26.8555	19.4796
<b>NC</b>	0.6470	0.5827	0.5765	0.9740	0.8989

**Table3.6** : le PSNR et le coefficient de corrélation du watermark extrait après les différents types d'attaques

La figure 3.21 et le tableau 3.6 montrent que la marque peut être récupérée pour différents types de attaques telles que la compression, le filtrage...etc. La qualité du watermark reste acceptable. Donc on peut dire que cette méthode de tatouage d'image en couleurs est robuste

### 3.5. Conclusion :

Dans ce chapitre nous avons étudié plusieurs algorithmes de tatouage par la SVD, et les résultats de simulation montrent que :

- ❑ le premier algorithme qui insère la marque dans la matrice orthogonale  $V$  est performant en termes d'imperceptibilité et de robustesse contre les attaques d'effacement (la compression, filtrage...etc.), mais elle possède des inconvénients comme la difficulté d'extraire la marque et la fragilité contre les attaques géométriques.
- ❑ Le deuxième algorithme qui intègre la marque dans les moyennes fréquences de la matrice diagonale  $S$  et exactement dans le troisième  $SV$  ( $\lambda_3$ ) est imperceptible et efficace car elle peut extraire facilement le watermark en utilisant seulement l'image tatouée. d'autre part la méthode n'est pas performante car elle est peu robuste aux attaques et elle nécessite un temps de calcul très important.

## Chapitre 3 : simulation des algorithmes de tatouages.

---

- L'algorithme Bloc-SVD de Chandra consiste à ajouter le watermark dans le grand SV c'est à dire ( $\lambda_1$ ) qui représente la plus grande concentration d'énergie de l'image. Cet algorithme est imperceptible et robuste surtout à la compression JPEG de grand facteur de compression.
- L'algorithme qui utilise la transformée d'Arnold est robuste quand il est confronté aux attaques de traitement d'image est surtout aux attaques d'effacement mais l'avantage principal de cette méthode c'est la haute sécurité.

Nous pouvons conclure que le tatouage dans le domaine des valeurs singulières possède beaucoup d'avantages comme la simplicité des calculs, l'imperceptibilité, la robustesse contre les attaques d'effacements, la sécurité ...etc., d'autre part, nous avons remarqué que la robustesse aux attaques géométriques des algorithmes présentés est réduite.

## ***CHAPITRE 4 :***

Tatouage d'images basé sur la DFT-SVD, la DWT-SVD  
et la DCT-SVD

#### 4.1. Introduction :

Dans le chapitre précédent, nous avons remarqué que la tatouage dans le SVD possède des inconvénients comme la fragilité au quelque type d'attaque ; pour pallier à ces inconvénients on le combine avec une autre transformée telle que la DFT, la DWT ou la DCT ce qui nous donne des algorithmes de tatouage basés sur la DFT-SVD, la DWT-SVD ou la DCT-SVD.

#### 4.2. Tatouage numérique basé sur la DFT et la SVD

Dans cette section, on présente l'algorithme de tatouage numérique basé sur la transformée de Fourier discrète (DFT) et la décomposition en valeurs singulières (SVD) qui a été proposé par Dodi Sudiana et Darmawan Apriyadi.

##### 4.2.1. Algorithme d'insertion de la marque :

La procédure d'insertion de la marque est représentée dans la figure 4.1

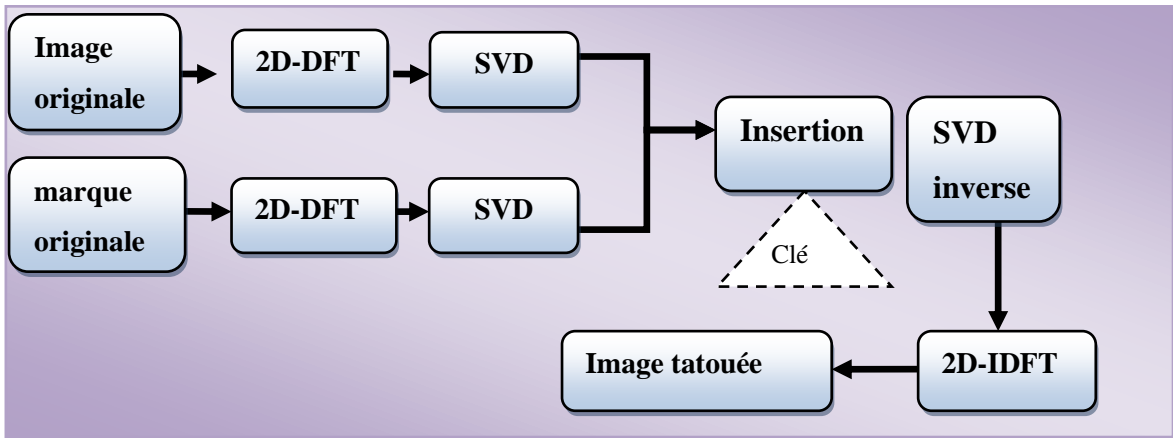


Figure 4.1 : Procédure d'insertion de l'algorithme de tatouage numérique basé sur la DFT - SVD

##### 4.2.2. Extraction de la marque :

La procédure d'extraction de la marque est la suivante :

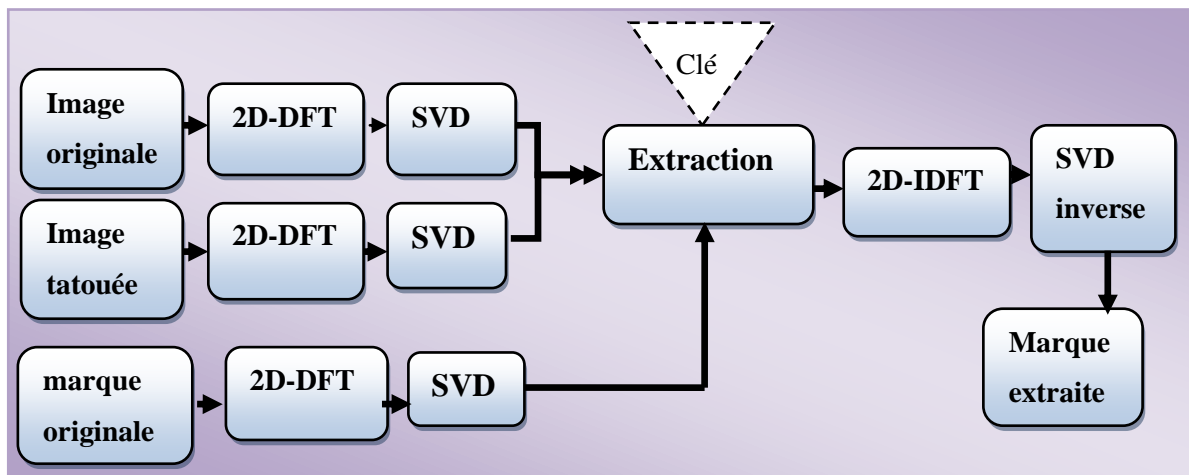


Figure 4.2 : Procédure d'extraction de l'algorithme de tatouage numérique basé sur la DFT - SVD

### 4.2.3. Simulations et résultats expérimentaux

Nous appliquons les algorithmes décrits ci-dessus à trois images hôtes qui sont très utilisées en traitement d'images : Lena de taille 512\*512, cameraman de taille 256\*256 et liftingbody de taille 512\*512. Dans toutes ces expériences, la clé  $\alpha$  est égale à 0.05



Figure 4.3 Images hôtes utilisées



Figure 4.4: Watermark original



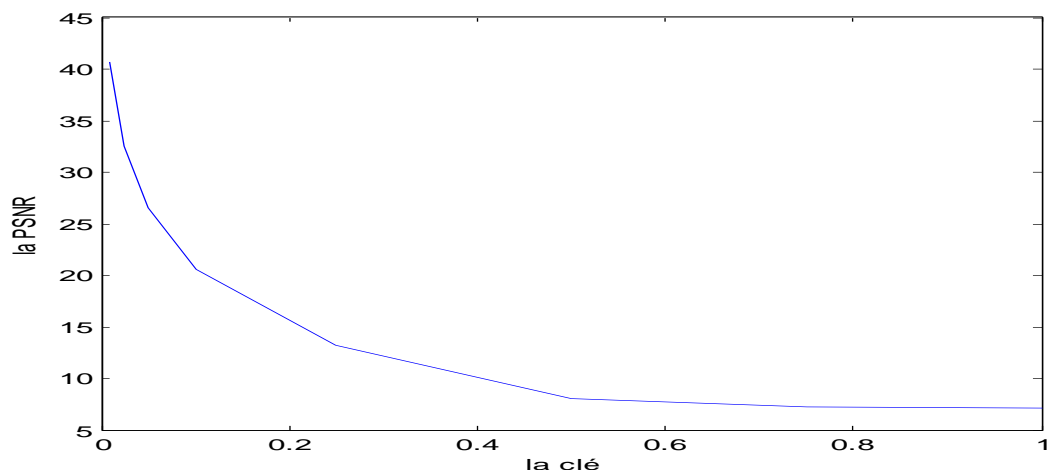
Figure 4.5 : Images tatouées utilisant l'algorithme basé sur la DFT - SVD



**Figure 4.6 :** watermarks extraits utilisant l'algorithme basé sur la DFT et la SVD

A partir de ces figures, on peut voir qu'il est difficile de différencier entre les images originales et leurs images tatouées.

Pour évaluer concrètement la qualité de notre méthode, on utilise le PSNR pour estimer la Distorsion des images tatouées. La figure 4.7 montre que l'image tatouée a une bonne qualité (PSNR > 30 dB) pour un facteur de graduation (la clé  $\alpha$ ) inférieur à 0,025



**Figure 4.7 :** la qualité d'image tatouée en fonction de la clé  $\alpha$

Après l'extraction du watermark, le coefficient de corrélation est calculé en utilisant le watermark original et celui extrait. Ce coefficient permet de juger l'existence et l'exactitude du watermark extrait.. Les valeurs du PSNR et du NC entre W et W\* sont présentées dans le Tableau 4.1




**Tableau 4.1 :** Qualité des images tatouées et corrélation entre W et W\*

Images	PSNR	NC
Lena	31.4895	1
cameraman	32.3325	0.9999
liftingbody	31.1524	0.9962

#### 4.2.4. robustesse de la méthode :




Afin d'évaluer la robustesse de cette technique de tatouage, plusieurs types d'attaques ont été implémentés. Dans cette partie, les expériences sont conduites sur l'image hôte lena de taille  $512 \times 512$ . Les attaques contre la robustesse étudiées dans cette partie d'expériences sont classifiées comme présenté dans la Section 2.6. La première classe consiste en les attaques géométriques visant à déformer suffisamment le document tatoué. Tandis que, la deuxième classe consiste en les attaques d'effacement visant à supprimer le watermark.

✓ **Attaque géométrique :**

Rotation de $2^\circ$	flipping	
	Vertical	horizontal
		
NC= 0.6536	NC=1	

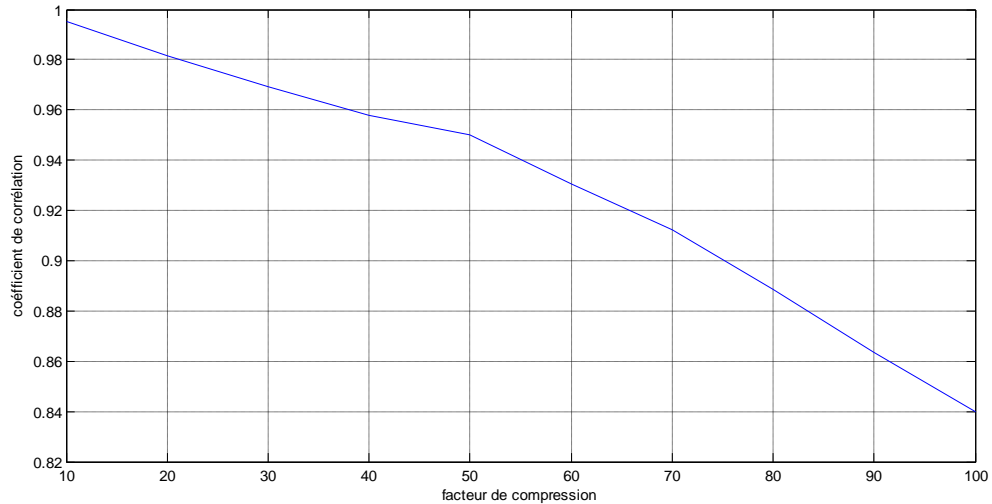
La valeur de NC dans le tableau ci-dessus montre que cette méthode de tatouage résiste contre des petits angles de rotation. Mais elle est très robuste au flipping horizontal et vertical.

✓ **Attaque d'effacement**

compression	Filtre médian	Bruit gaussien
		
Nc=0.9462	Nc= 0.9466	Nc= 0.7055



La figure suivante montre que la méthode est robuste jusqu'à une compression correspondant à un facteur de qualité de 100%. Mais l'augmentation de facteur de compression va diminuer la qualité d'image (coefficient de corrélation diminué)



**Figure 4.8 :** Test de robustesse face à la compression JPEG

### 4.3. Algorithme de tatouage numérique basé sur la DWT et la SVD

Dans cette section, on présente l'algorithme de tatouage numérique basé sur la transformée en ondelettes discrète et la SVD [33]

#### 4.3.1. Algorithme d'insertion :

La procédure d'insertion de la marque est représentée à la figure 4.9, et se résume par les étapes suivantes :

- ↪ Utiliser la transformée DWT pour décomposer l'image hôte  $I$  en quatre sous-bandes: LL, HL, LH, and HH.
- ↪ Appliquer la SVD pour chaque sous-bande :  $I_k = U_k * S_k * V_k^T$ . Avec  $k$  : LL, HL, LH, and HH
- ↪ La décomposition du watermark en valeurs singulières :  $W = U_w * S_w * V_w^T$
- ↪ Les sous bande de l'image  $I$  sont modifiées selon l'équation suivante :  

$$\lambda^{*k} = \lambda^k + \alpha * \lambda_w$$
- ↪ Appliquer la SVD inverse pour les quatre sous -bande modifiées.
- ↪ Calculer la transformée inverse de la DWT afin de produire l'image tatouée  $I^*$

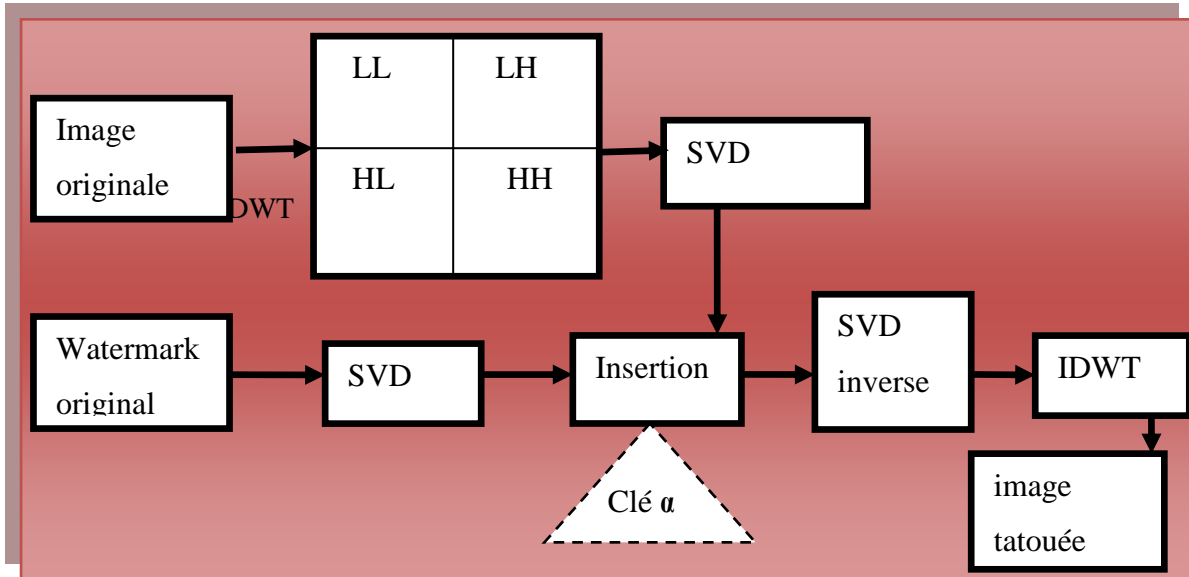


Figure 4.9 : Procédure d'insertion de l'algorithme de tatouage numérique basé sur la DWT - SVD

#### 4.3.2. Algorithme d'extraction :

La procédure d'extraction de la marque (voir la figure 4.10), se résume aux étapes suivantes :

- ↻ Utiliser la transformée DWT pour décomposer l'image tatouée  $I^*$  en quatre sous-bandes
- ↻ Appliquer la SVD pour chaque sous-bande :  $I_k^* = U_k^* * S_k^* * V_k^T$
- ↻ Extraire les valeurs singulières de chaque sous-bande :  $\lambda_w = (\lambda_k^* - \lambda_k) / \alpha$
- ↻ Construire les quatre watermark à partir des valeurs singulières extraites des quatre sous-bandes :  $W^* = U_w * S_w^* * V_w^T$

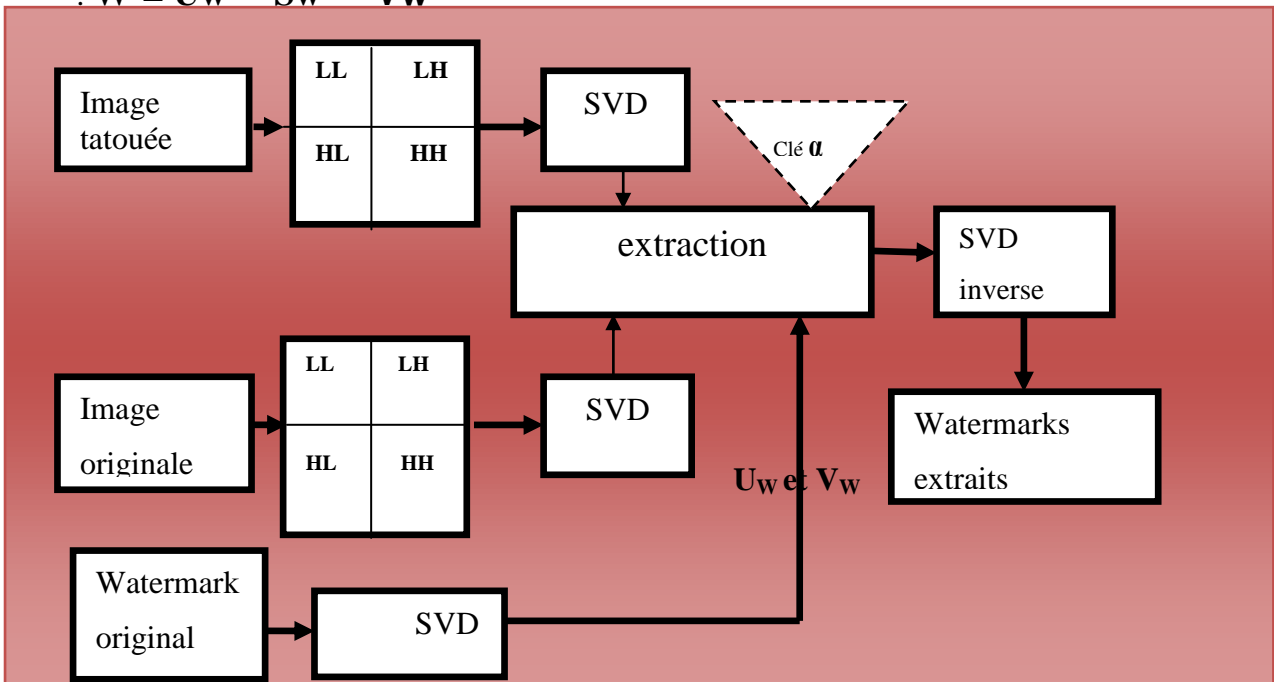


Figure 4.10 : Procédure d'extraction de l'algorithme de tatouage numérique basé sur la DWT - SVD

### 4.3.3. Simulations et résultats expérimentaux

La figure 4.11 expose l'image hôte woman de taille 512x512, la marque originale de taille 128\*128, l'image woman tatouée, et les marques extraits. Image woman tatouée donne un PSNR de 32.31 dB pour une clé  $\alpha$  égale à 0,05 pour la sous-bande LL et 0,005 pour les trois autres sous-bandes



(a)



(b)



(c)




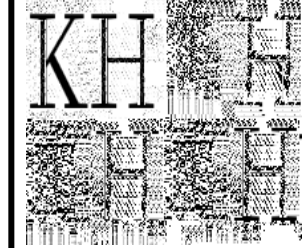






(d)

**Figure 4 .11:** (a) image woman originale,(b) watermark original,(c) image woman tatouée avec l'algorithme basé sur la DWT et la SVD ,(d) watermarks extraits

### 4.3.4. Robustesse de la méthode

Pour tester la robustesse de cet algorithme de tatouage, il faut simuler des attaques aux images reçues après la phase d'insertion. Dans cette partie, nous introduisons quelques types d'attaques qui peuvent se passer à une image

<i>Rotation 20°</i>	<i>Flipping horizontal</i>	<i>Zoome 256-512</i>	<i>Bruit gaussien</i>
			
0.0660    0.2502	1.00 00    1.0000	0.4258    0.5993	0.9581    0.3658
-0.5896    0.2620	0.9999    0.9999	0.6850    0.2004	0.2415    0.3741
<i>filtre médian</i>	<i>Filtre sharpen</i>	<i>Correction gamma 0.6</i>	<i>Compression</i>
			
0.8745    0.4885	0.9962    0.7550	-0.9850    0.9552	0.9992    0.0325
- 0.3256    -0.5622	0.8471    0.7852	0.7244    0.9553	0.3230    0.0240

Selon le tableau si dessus, les watermarks extraits pour les quatre sous-bandes sont différents pour chaque attaque :

- ✚ La marque extraite dans la sous-bande de LL est résistant aux attaques suivantes: flipping, bruit gaussien, filtre médian, filtre sharpen et la compression
- ✚ La marque extraite dans la sous-bande de HH est résistant aux attaques comprenant à la correction gamma et Flipping horizontal
- ✚ La marque enfonçant dans la sous-bande HL est résistant à la rotation malgré que ce coefficient de corrélation est négative (comme un film négatif, des parties plus claires de l'image deviennent plus foncées et des parties plus foncées deviennent plus claires)
- ✚ La marque enfonçant dans la sous-bande LH est résistant aux attaques comprenant au filtre sharpen et Flipping horizontal et correction gamma .

#### 4.4. Tatouage numérique basé sur la DCT et la SVD :

Nous avons employé la même idée de tatouage basé sur la DWT-SVD dans le domaine de la DCT-SVD, le principe de cette méthode c'est de tracer les coefficients de fréquence le plus bas au plus haut dans un ordre de zigzag à 4 quatre blocs comme elle indique la figure 4. Et on insère la marque dans chacun. [34]

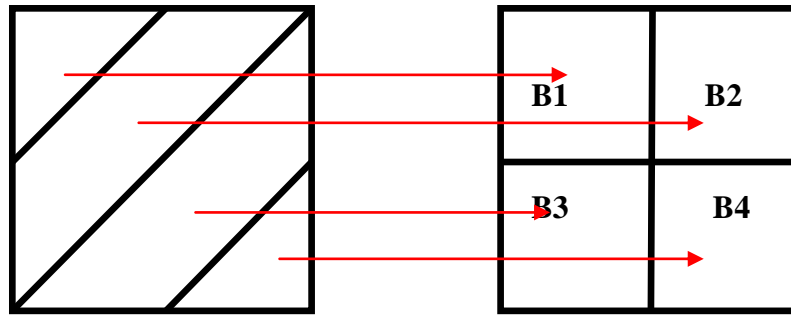


Figure 4.12 : Tracé des coefficients de la DCT dans 4 blocs

#### 4.4.1. Algorithme d'insertion

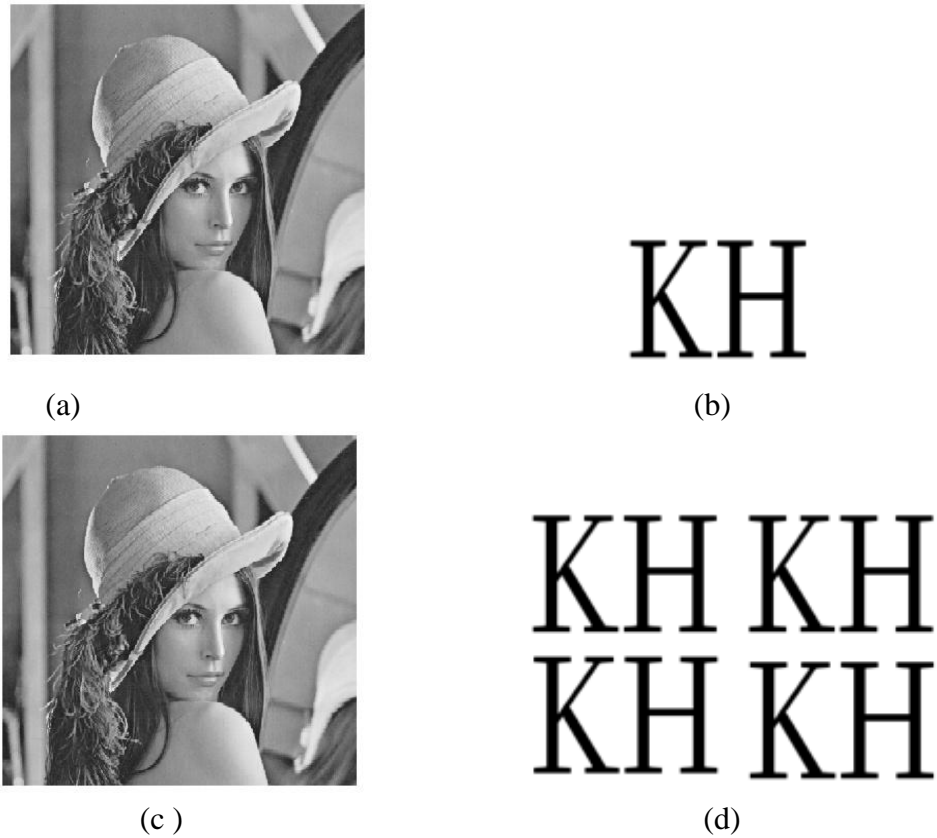
- appliquer la DCT à l'image hôte I.
- En utilisant l'ordre de zigzag pour tracer les coefficients de DCT dans 4 blocs : B1, B2, B3, et B4. (voir figure 4.12).
- Appliquer la SVD à chaque blocs :  $I_k = U_k * S_k * V_k^T$   $k=1, 2, 3, 4$ .
- Appliquer la DCT au watermark original W.
- Appliquer la SVD au coefficient de la DCT du watermark :  $W_{DCT} = U_W * S_W * V_W^T$ .
- Modifier les valeurs singulières dans chaque blocs :  $\lambda^{*k} = \lambda^k + \alpha * \lambda_w$ .
- Appliquer la SVD inverse pour les quatre blocs modifiés.
- Tracez les coefficients modifiés de la DCT à leurs positions originales.
- Calculer la transformée inverse de la DCT afin de produire l'image tatouée  $I^*$ .

#### 4.4.2. Algorithme d'extraction

- appliquer la DCT à l'image tatouée I.
- En utilisant l'ordre de zigzag pour tracer les coefficients de DCT dans 4 blocs : B1, B2, B3, et B4.
- SVD la à chaque blocs :  $I_k^* = U_k * S_k^* * V_k^T$   $k=1, 2, 3, 4$ .
- Extraire les valeurs singulières de chaque blocs :  $\lambda_w = (\lambda_k^* - \lambda_k) / \alpha$ 
  - Construire les coefficients de DCT de quatre watermarks, employer les vecteurs singuliers  $U_w$  et  $V_w$  du watermark original :  $W^* = U_w * S_w^* * V_w^T$
  - Appliquer la DCT inverse à chaque bloc pour construire les quatre watermarks.

#### 4.4.3. Simulations et résultats expérimentaux

La figure 4.11 expose l'image hôte lena, la marque originale de taille 256\*256, l'image lena tatouée, et les marques extraits.

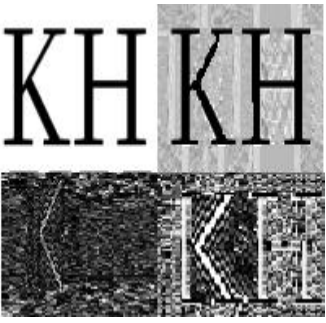
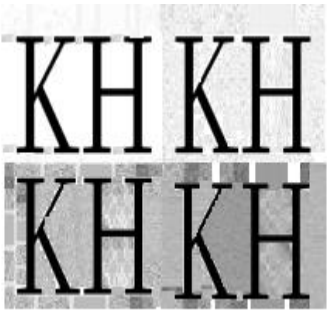
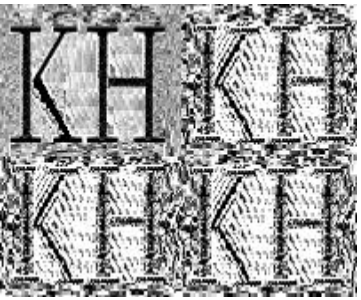



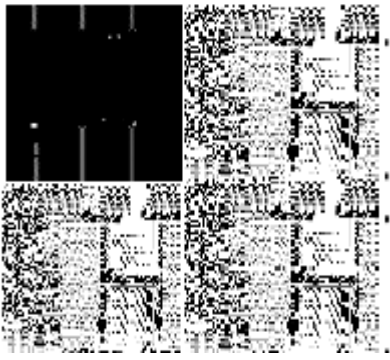

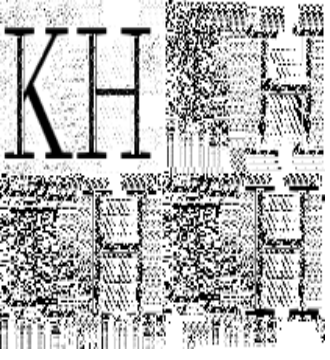


**Figure 4.13 :** (a) image lena originale, (b) watermark original, (c) image mandrill tatouée avec l'algorithme basé sur la DCT et la SVD, (d) watermarks extraits

#### 4.4.4. Robustesse de l'algorithme

Nous avons testé cette méthode aux attaques de traitement d'images



<p><i>Rotation 20°</i></p> 	<p><i>Flipping vertical</i></p> 	<p><i>Zomme 12-1024</i></p> 
<p>0.9950      0.3265 0.28547      0.2415</p>	<p>0.9865      0.9741 0.9154      0.9025</p>	<p>0.5482      0.3021 0.3025      0.3152</p>
<p><i>Compression facteur 60</i></p> 	<p><i>Filtre médian</i></p> 	<p><i>Correction Gamma 0.6</i></p> 
<p>0.9932      0.9199 0.0254      0.3562</p>	<p>0.8145      -0.3754 - 0.4125      -0.4550</p>	<p>0.3156      0.7445 0.7485      0.7540</p>
<p><i>Filtre Laplacian</i></p> 	<p><i>Bruit gaussien</i></p> 	<p><i>Bruit poisson</i></p> 
<p>-0.1542      0.3988 0.4522      0.4752</p>	<p>0.9965      0.3599 0.3566      0.3411</p>	<p>0.9965      0.6020 0.4522      0.4520</p>

Selon le tableau ci-dessus, les watermarks extraits pour les quatre blocs sont différents pour chaque attaque :

Les watermarks extraits dans le bloc B1 sont robustes aux attaques suivantes : rotation, compression, filtre médian, bruit gaussien, bruit poisson, Flipping vertical, et le zomme

Les watermarks extraits dans le bloc B2 sont robustes aux Flipping vertical et aux compression JPEG ,aux bruit poisson

Les watermarks extraits dans le bloc B3 sont robustes aux Correction gamma et filtre lapalcian

Les watermarks extraits dans le bloc B4 sont robustes aux attaques suivant : Correction Gamma et Filtre Laplacian .

#### 4.5. Conclusion

Dans ce chapitre, nous présentons trois méthodes de tatouage basés sur : DFT-SVD, DWT-SVD et DCT-SVD, les résultats de simulations montrent que :

- Le premier algorithme basé sur la DFT et la SVD est impeccable et l'image tatouée a une bonne qualité d'image pour un  $\alpha$  inférieur à 0.025 . La méthode est robuste aux attaques suivantes : fliping vertical et horizontal, filtre médian, bruit gaussien et compression JPEG de grand facteur (jusqu'à un facteur 100%), mais elle résiste juste aux petits angles de rotation.
- L'algorithme basé sur DWT-SVD et DCT-SVD utilisent le même principe. Ils sont imperceptibles et l'image tatouée a une bonne qualité d'image .les watermarks insérés dans les plus basses fréquences (le bloc B1 pour la DCT et la sous bande LL Pour DWT) sont résistants à un groupe d'attaques, et les watermarks incorporés dans les fréquences les plus élevées ( le bloc B4 pour la DCT et sous-bande de HH pour la DWT) sont résistants à un autre groupe d'attaques. Donc le watermark est enfoncé dans 4 blocs serait extrêmement difficile d'enlever
- On peut conclure que le tatouage basé sur DWT-SVD et DCT-SVD est plus performant que le tatouage basé sur la SVD seul où la DFT-SVD



## *CONCLUSION GENERALE*

---

### **Conclusion générale :**

Au cours de ce mémoire nous avons étudié et implémenté plusieurs méthodes de tatouage numérique basées sur la décomposition en valeurs singulières (SVD). Les quatre premiers algorithmes (algorithme utilisant la matrice  $V$ , algorithme utilisant la matrice  $S$ , algorithme Bloc-SVD de Chandra, et algorithme utilisant la transformée d'Arnold) sont appliqués sur des images en niveau de gris (Cameraman, Lena ...etc.). Alors que le dernier algorithme est appliqué sur une image RGB.

On a vu que les algorithmes présentés possèdent beaucoup d'avantages comme la simplicité des calculs, l'imperceptibilité, et la robustesse contre les attaques dues au traitement d'image (compression, filtrage, transformations géométriques).

En plus, nous avons utilisé des méthodes qui combinent la SVD avec une autre transformée, telle que la DFT, la DWT ou la DCT. Cela nous donne des algorithmes de tatouage basés sur la DFT-SVD, la DWT-SVD ou la DCT-SVD. Ces méthodes introduisent une sécurité supplémentaire, et on a remarqué que l'algorithme basé sur la DCT-SVD résiste bien aux attaques géométriques telles que la rotation, le flipping ...etc.

Ce travail m'a permis de me familiariser avec les techniques relatives au traitement d'images et plus particulièrement aux techniques du tatouage numérique des images fixes. Les perspectives sont d'appliquer ces techniques, avec quelques changements, aux fichiers vidéo.

---

# 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 1990 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 a 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] **M. Yeung and F. Mintzer.** « On Resolving Rightful Ownership's of Digital Images by Invisible Watermarks ». 1997.
- [8] **C. REY and J. DUGELAY.** « Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images ». Traitement du Signal, 18(4) :283–295, 2001
- [9] **D. Zheng, Y. Liu, J. Zhou, and A. Saddik.** « A survey of RST Invariant Image Watermarking Algorithms. » ACM Computing Surveys, 39(2), 2007.
- [10] **Vidyasagar M. Potdar, Song Han, Elizabeth Chang.** « A Survey of Digital Image Watermarking Techniques ». School of Information Systems, Curtin University of Technology, Perth, Western Australia. 2009.

- [11] **14] Melle : GharzouliIbtissem.** « Filtrage linéaire à 2D et ses applications sur le signal image » Mémoire de fin d'études, Sétif, 2006.
- [12] **Jean Luc Le Luron.** « Les images numériques, généralités ». 2003.
- [13] <http://www.crdp.ac-grenoble.fr/image/general/general.htm>.
- [14] **R.ISDANT,** « Traitement numérique de l'image », 2009.
- [15] <http://www.cardinalmercier.be/multimedia/cours/Mu003/Mu003-01.html> .
- [16] **G. BUREL,** « introduction au traitement d'images », paris, Hermès Science Publication, octobre 2001.
- [17] **A. MARION,** « TP Bases du Traitement d'image », in cours master Imagerie 1, 12 février 2007.
- [18] **D. ZHENG, Y. LIU, J. ZHOA, & A. SADDIK,** « a survey of RST Invariant Image Watermarking Algorithms », ACM Computing Surveys, 2007.
- [19] **Mr : BOUDERBALA AHMED.** « Implémentation d'un algorithme de tatouage Vidéo robuste dans Le domaine compressé », mémoire de magister en électronique, université MENTOURI CONSTANTINE
- [20] **P. PATRICK, B. CHASSERY & J. MARC,** « Tatouage couleur adaptatif fonde sur l'utilisation d'espaces perceptifs uniformes ». Traitement du signal, 2004.
- [21] **Mr : KHALED 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, université LAVAL QUÉBEC, 2010
- [22] **A. BASSO, F. BERGADANO, D. CAVAGNINO, V. POMPONIU & A. VERNONE,** « A Novel Block-based Watermarking Scheme Using the SVD Transform », Department of Computer Science, Université DEGLI STUDI TORINO, Italy
- [23] **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
- [24] **S. VOLOSHYNOVSKIY, S. PEREIRA, T. PUN, J. EGGERS, & J. SU,** « Attacks on Digital Watermarks ». Classification, Estimation-based Attacks and Benchmarks. IEEE CommunMag, 118–126, 2001.
- [25] **H. B. RAZAFINDRADINA & P. A. RANDRIAMITANTSOA,** « Robust end Blind watermarking in the singular values domain », Journal Marocain de l'Automatique, de l'Informatique et du Traitement de Signal, Jan 2010

[26]Mr : **Mohamed KOUBAA**, « Tatouage robuste de vidéo basé sur la notion de régions d'intérêt », mémoire de doctorat, université BORDEAUX, 2010

[27][http://www.aiaccess.net/f\\_gm.htm](http://www.aiaccess.net/f_gm.htm)

[28] **J-L DUGELAY & S ROCHE**, « INTRODUCTION TO IMAGE WATERMARKING », institute EURECOM, dept. of Multimedia Communications.

[29] **E.ARNAUD & E.BOYER**, « Analyse d'images », Université Joseph Fourier

[30] **S.P. MATTHEW**, « Digital Watermarking with the Singular Value Decomposition », université Math 843, November 29, 2006.

[31] **D-V.CHANDRA**, « Digital Image Watermarking using Singular Value Decomposition », In 45<sup>th</sup> IEEE Midwest Symposium on Circuit and Systems, Tulsa, volume 3, pages 264–267, 2002.

[32] **D. SAXENA**, « Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform », International Journal of Electronics and Computer Science Engineering, Volume 1, 2011

[33] **Y. JIE**, « Algorithm of Image Information Hiding Based on New Anti-Arnold transform and Blending in DCT Domain », Université NANJING, China.

[34] **V.KUMARI & B. CHITRA**, « Comparison of SVD based image watermarking techniques implemented for gray scale and color images », International Journal of Machine Intelligence IGMI, Volume 3, Issue 4, pp-359-363, 2011.

# Sommaire

## Remerciements

## Table d'abréviations

## Introduction générale .....

## Chapitre 1 : Introduction aux images numériques

1.1.	Introduction .....	1
1.2.	Définition d'une image réelle .....	1
1.3.	Définition d'une 'image numérique .....	1
1.3.1	Image en niveaux de gris .....	2
1.3.2	Image couleur .....	2
1.4.	Processus de numérisation .....	2
1.4.1.	L'échantillonnage .....	3
1.4.2.	La quantification .....	3
1.4.3.	Le codage.....	3
1.4.3.1.	Codage en noir et blanc .....	3
1.4.3.2.	Codage d'une image en niveaux de gris.....	4
1.4.3.3.	Codage d'une image couleur .....	4
1.5.	Les types d'images numériques.....	4
1.5.1.	L'image vectorielle .....	4
1.5.2.	L'image matricielle.....	5
1.6.	Les caractéristiques de l'image numérique .....	5
1.6.1.	La définition.....	5
1.6.2.	La résolution .....	5
1.6.3.	Profondeur de couleur.....	6
1.7.	Format des images sur disque.....	6
1.7.1.	Principaux formats de fichiers non compressés.....	7
1.7.2.	Principaux formats de fichier compressés .....	7
1.8.	Quelques aspects du traitement d'image .....	9

1.8.1. Le filtrage.....	9
1.8.2. La compression.....	10
1.8.3. Le tatouage.....	10
1.9. Conclusion.....	11

## **Chapitre 2 : État de l'art sur le tatouage numérique des images**

2.1. Introduction .....	12
2.2. Historique et terminologie.....	12
2.2.1 Historique .....	12
2.2.2 Terminologie .....	13
a) Tatouage visible .....	13
b) Tatouage non visible .....	14
2.3. Définition du tatouage numérique.....	15
2.4. Modèle de tatouage numérique d'image .....	15
2.5. Conditions requises pour les techniques du tatouage d'images numériques .....	17
. Imperceptibilité.....	17
. Robustesse .....	17
. Sécurité .....	18
2.6. Les applications du tatouage d'image : .....	18
2.7. Classification des algorithmes de tatouage .....	19
2.7.1. L'algorithme de détection : Aveugle, Semi-aveugle et Non aveugle .....	20
2.7.2. La robustesse de l'algorithme : Fragile, Semi-fragile et Robuste .....	21
2.7.3. La préservation de l'image originale : Inversible et Non-inversible.....	21
2.7.4 La technique d insertion .....	21
2.7.5 Classification selon la technique d insertion .....	22
2.7.5.1. Le domaine spatial.....	22
2.7.5.2. Le domaine fréquentiel .....	22
2.7.5.2.1. Transformée en Cosinus Discrète (DCT).....	23

2.7.5.2.2. La Décomposition en Valeurs Singulières (SVD) .....	25
2.7.5.2.3. Transformée en Ondelette Discrète (DWT) .....	26
2.8. Classification des attaques géométriques : .....	27
• Attaques bienveillantes: .....	27
• Attaques malveillantes .....	28
2.9. Conclusion : .....	29

### **Chapitre 3 : simulation des algorithmes de tatouage**

3.1. Introduction .....	30
3.2. La décomposition en valeurs singulières SVD .....	30
3.3. Algorithmes de tatouage d'image au niveau de gris utilisant la transformée SVD .....	30
3.3.1. Algorithme utilisant la matrice V .....	30
3.3.1.1. Algorithme d'insertion .....	31
3.3.1.2. Algorithme d'extraction .....	32
3.3.2.3 Performance de l'algorithme .....	33
3.3.2. Algorithme utilisant la matrice S .....	37
3.3.2.1. Insertion de la marque .....	37
3.3.2.2. Extraction de la marque .....	37
3.3.2.3. Performance de l'algorithme .....	38
3.3.3. Algorithme Bloc-SVD de Chandra .....	40
3.3.3.1. Algorithme d'insertion .....	40
3.3.3.2. Algorithme d'extraction .....	40
3.3.3.3. Résultats de simulation .....	41
3.3.3.4. Performance de l'algorithme .....	41
3.3.4. Algorithme utilisant la transformée d' Arnold .....	43
3.3.4.1. La transformation d'Arnold .....	43
3.3.4.2. L'algorithme de tatouage .....	44
3.3.4.3. Les résultats expérimentaux .....	45
3.3.4.4. Performance de l'algorithme .....	45

3.4.	Algorithme de tatouage d'images couleur utilisant la transformée SVD.....	47
3.4.1.	Algorithme d'insertion.....	48
3.4.2.	Algorithme d'extraction.....	48
3.4.3.	Résultats de simulation.....	48
3.5.	Conclusion.....	50

#### **Chapitre 4 : : Tatouage d'image basé sur la DFT-SVD, la DWT-SVD et la DCT-SVD**

4.1.	Introduction : .....	52
4.2.	Tatouage numérique basé sur la DFT et la SVD.....	52
4.2.1.	Algorithme d'insertion de la marque .....	52
4.2.2.	Algorithme d'extraction de la marque : .....	52
4.2.3.	Simulations et résultats expérimentaux .....	53
4.2.4.	robustesse de la méthode : .....	55
4.3.	Algorithme de tatouage numérique basé sur la DWT et la SVD .....	56
4.3.1.	Algorithme d'insertion : .....	56
4.3.2.	Algorithme d'extraction : .....	57
4.3.3.	Simulations et résultats expérimentaux .....	58
4.3.4.	Robustesse de de la méthode .....	58
4.4.	Tatouage numérique basé sur la DCT et la SVD : .....	59
4.4.1.	Algorithme d'insertion.....	60
4.4.2.	Algorithme d'extraction.....	60
4.4.3.	Simulations et résultats expérimentaux .....	60
4.4.4.	Robustesse de l'algorithme .....	61
4.5.	Conclusion .....	63

**Conclusion générale**.....

**Bibliographie** .....



الاسم: كريمة

اللقب: حططاش

المؤطر : ن.عمارجية

**المذكّرة:** تطوير خوارزميات الوشم على الصور الرقمية على أساس SVD و التحويلات القطعية في هذه المذكرة قمنا بإعطاء حوصلة حول الوشم على الصور الرقمية. ثم قدمنا بعض الخوارزميات على أساس SVD هذه الخوارزميات برمجت على MATLAB و تم اختبارها ضد بعض الهجمات المعروفة في معالجة الصور. و في الأخير قمنا بتطوير بعض الخوارزميات تعتمد على SVD-DCT ;SVD-DFT ;SVD-DWT .  
**الكلمات المفتاحية:** الصورة الرقمية.الوشم. SVD, DCT.DFT. DWT.

**Title:** Development of algorithms of watermarking of images based on SVD and the discrete transforms

**Name :** HETATACHE

**First Name:** Karima

**Directed by:** N. AMARDJIA

**Abstract :**

In this memory, we first enumerate the state of the art of the watermarking of the digital images. Then, we presented some algorithms based on the SVD (singular value decomposition). These algorithms were implemented on MATLAB and were tested against possible attacks met in the image processing field. At last, we developed algorithms based on the SVD and another transform (the DFT-SVD, the DWT-SVD and the DCT-SVD).

**Key words:** Digital image, Watermarking, SVD, DCT, DFT, DWT .

**Titre :** Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformées discrètes

**Nom :** HETATACHE

**Prénom :** KARIMA

**Encadreur :** Dr Noureddine Amardjia

**Résumé:**

Dans ce mémoire, nous avons donné l'état de l'art sur le tatouage des images numériques. Ensuite, nous avons présenté quelques algorithmes basés sur la SVD (singular value decomposition - décomposition en valeurs singulières). Ces algorithmes ont été implémentés sur MATLAB et testés contre des attaques possibles rencontrées dans le traitement d'images. Enfin, nous avons développé des algorithmes basés sur la SVD et une autre transformée (la DFT-SVD, la DWT-SVD et la DCT-SVD).

**Mots clés :** Image numérique, Tatouage, SVD, DCT, DFT, DWT.