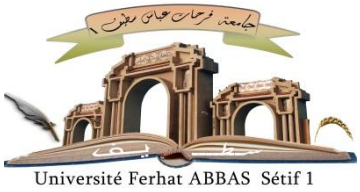
الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique




**UNIVERSITÉ FERHAT ABBAS - SETIF1**

**FACULTÉ DE TECHNOLOGIE**

# THÈSE

**Présentée au Département d'Electronique**

**Pour l'obtention du diplôme de**

# DOCTORAT

**Domaine : Sciences et Technologie**

**Filière: Electronique** **Option: Traitement du signal**

**Par**

**BELILITA Sarra**

# THÈME

# Développement et Implémentation d'algorithmes de tatouage robustes des images fixes et vidéo

**Soutenue le ……./……./2019 devant le Jury:**

| | | | |
|---|---|---|---|
| **NOM Prénom** | **Professeur** | **Univ. Ferhat Abbas Sétif 1** | **Président** |
| **AMARDJIA Nourredine** | **Professeur** | **Univ. Ferhat Abbas Sétif 1** | **Directeur de thèse** |
| **NOM Prénom** | **Professeur** | **Univ. Ferhat Abbas Sétif 1** | **Examinateur** |
| **NOM Prénom** | **Professeur** | **Univ.** | **Examinateur** |

# Remerciements

***Tout d'abord je remercie Dieu le tout puissant qui m'a donné la force, la volonté et le courage pour achever ce modeste travail.***

*Je tiens à exprimer toute ma reconnaissance :*

A mes parents Abdenacer et Safia qui ont toujours été là pour moi. Leur présence, leur écoute, leur confiance en moi et leur soutien constant m'assurent des bases solides et me permettent de persévérer et de me surpasser.

A mon directeur de recherche, Pr Amardjia Nourredine. Le mérite d'une thèse appartient certes à l'auteur, mais également à son directeur qui l'encadre. Dans mon cas, mon directeur a été d'un soutien et d'une attention exceptionnels. La confiance qu'il m'a accordée ainsi que son soutien moral m'ont permis d'accumuler des expériences marquantes qui font de moi une personne grandie.

A Messieurs les membres de jury d'avoir accepté de juger mon travail et de m'honorer par leur présence.

A Mr Bekkouche Tewfik pour ses directives ainsi que ses conseils précieux.

J'adresse mes sincères remerciements à tous mes professeurs durant mon cursus éducatif et universitaire.

Enfin, Je remercie ma sœur Ahlem et mon frère Anis qui m'ont toujours encouragée à mener à bien cette recherche. Trouvez ici l'expression de ma profonde gratitude.

# *Dédicaces*

Je dédie ce modeste travail à….

## L'âme de la légende de ma vie qui ne se répétera jamais ; à l'âme de mon très cher papa `Abdenacer´

Aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours eu pour vous.

Je vous dédie aujourd'hui ma réussite, rien que pour vous, homme de ma vie, mon exemple éternel et source de ma joie et de mon bonheur, celui qui s'est toujours sacrifié pour me voir réussir. Ce travail est le fruit de vos sacrifices que vous avez consentis pour mon éducation et ma formation.

J'espère que, du monde qui est sien maintenant, il apprécie cet humble geste comme preuve de reconnaissance de la part de sa fille qui a toujours prié pour le salut de son âme.

Que **Dieu** le miséricordieux, vous accueille dans son éternel paradis.

**A toi mon très cher papa.**

## Aussi….

A mes deux anges Abdenacer Idriss le gentil et la douce Rahma Malak, mes deux bijoux tous précieux. J'espère que ce travail vous rendra fiers de votre maman qui est prête à tout faire pour votre bonheur.

***Je vous adore mes chers trésors.***

# Table des matières

## Chapitre 2: Tatouage numérique d'images dans le domaine transformé

## Chapitre 3 Nouvelle technique de tatouage numérique basée sur la diffusion anisotrope



## Chapitre 4: Tatouage vidéo

# Liste des tableaux

# Liste des figures

## Chapitre 01 : Etat de l'art sur le tatouage numérique



## Chapitre2 : Tatouage numérique d'images dans le domaine transformé

# Chapitre3 : Nouvelle technique de tatouage numérique basé sur la diffusion anisotrope

# Chapitre 4 : Tatouage vidéo

# Liste des abréviations

| | |
|---|---|
| **bbp** | bits by pixel |
| **BCR** | Bit Correction Rate |
| **BER** | Bit Error Rate |
| **CC** | Continuous Components |
| **CIF** | Common Intermediate Format |
| **CR** | Cropping |
| **DCT** | Discrete Cosine Transform |
| **DFT** | Discrete Fourier Transform |
| **DWT** | Discrete Wavelet transform |
| **FA** | Frame Averaging |
| **FD** | Frame dropping |
| **FT** | Fourier Transform |
| **FR** | Frame Rate |
| **FS** | Frame Swapping |
| **GN** | Gaussien Noise |
| **HVS** | Human Visual System |
| **JPEG** | Joint Photographic Experts Group |
| **MF** | Median Filter |
| **MPEG** | Moving Picture Experts Group |
| **MR-SVD** | Multiresolution Singular Value Decomposition |
| **MSE** | Mean Square Error |
| **NC** | Normalized Coefficient |
| **NTSC** | National Television System Committee |
| **PAL** | Phase Alternation Line |
| **PDE** | Partial Differential Equation |
| **PDFT** | Parametric Discrete Fourier Transform |
| **PSNR** | Peak Signal to Noise Ratio |
| **QCIF** | Quarter Common Intermediate Format |
| **SH** | Sharpening |
| **SVD** | Singular Value Decomposition |

# *Introduction générale*

## Contexte général

Le domaine de la transmission numérique, à travers des réseaux de communication, qui sont largement utilisés pour l'échange des informations et des documents de différentes natures (sons, vidéos, images, textes…), représente un axe de recherche très fertile qui ne cesse d'évoluer. Cette évolution s'est accentuée du moment où la technologie s'est orientée vers la numérisation. Néanmoins, le progrès de ce domaine est accompagné par la naissance de divers problèmes. Les plus importants étant ceux liés à la sécurité des informations échangées qui est devenue une nécessité primordiale, afin d'assurer la distribution légale sur le réseau, la confidentialité, l'empêchement de toute modification ou exploitation non autorisée des données et la protection des droits d'auteurs. Ces derniers sont devenus une propriété essentielle dans beaucoup d'applications des organismes civils ou militaires, par exemple l'internet, la téléphonie mobile, les distributeurs de billets, les abonnements aux chaines de télévision payantes, le commerce électronique et les cartes à puce.

Pour contourner ces problèmes, une nouvelle technique appelée le tatouage numérique, en anglais « digital watermarking », a été développée. Elle s'inspire principalement de la cryptographie et de la stéganographie. Cette discipline consiste à introduire dans le document à protéger une marque visible ou invisible contenant les informations de droit d'auteur limitées au seul propriétaire de la couverture. Le tatouage numérique a rapidement suscité un fort engouement de la part de la communauté des chercheurs, du fait des problématiques qu'elle soulève mais aussi des enjeux qu'elle représente dans des communications numériques. La transmission des images et de la vidéo soulève donc un nombre important de problèmes qui ne sont pas encore tous résolus.

Il existe dans la littérature plusieurs techniques de tatouage numérique qui peuvent être classifiées dans deux catégories : le tatouage dans le domaine spatiale et le tatouage dans le domaine fréquentiel. Les algorithmes traditionnels de tatouage comme ceux qui modifient les bits de poids faibles (LSB : Least Significant Bit) des pixels de l'image hôte dans le domaine spatial [1], ne sont pas très robustes aux attaques comme la compression et l'ajout de bruit. Pour fournir une meilleure solution au problème de la robustesse des images tatouées, des techniques de tatouage d'images ont été proposées dans [2 - 7], où le tatouage se fait dans le domaine fréquentiel. La marque est insérée dans les coefficients obtenus par l'utilisation d'un processus de transformation sur l'image. Une catégorie de ces techniques est celle qui exploite les transformées discrètes telles que la transformée de Fourier discrète DFT (Discrete

Fourier Transform), la transformée en ondelettes discrète DWT (Discrete Wavelet Transform), la transformée en cosinus discrète DCT (Discrete Cosine Transform), etc.

Selon l'apparence ou non de la marque insérée, on distingue deux types de systèmes de tatouage: le tatouage visible et le tatouage invisible. Les systèmes de tatouage invisibles sont largement utilisés, puisque il est difficile de faire la distinction entre l'information originale (image, audio ou vidéo) et l'information tatouée d'une part, et d'autre part, une tentative de suppression de la marque insérée provoque une dégradation de manière significative de la qualité de la donnée tatouée.

## Objectif

Dans la présente thèse de doctorat, qui traite le sujet du tatouage numérique des images fixes et la vidéo, nous nous sommes concentrés sur les deux principaux défis qui contribuent dans un système de tatouage. Le premier défi est la proposition de systèmes de tatouage robuste contre la plupart des attaques que peut subir une image tatouée. Le second défi est d'avoir des systèmes de tatouage avec un choix optimal des blocs à tatouer qui garantit un bon compromis entre la robustesse et l'imperceptibilité, d'où la préservation de la qualité visuelle de l'image tatouée. L'idée est de définir, localiser et exploiter des régions qui favorisent le tatouage dans le but d'augmenter la robustesse et ce, sans nuire à l'aspect visibilité du contenu. Ces régions sont localisées en tenant compte de la faiblesse et des limites du Système Visuel Humain.

## Proposition

Comme il est mentionné précédemment, la solution proposée est d'élaborer des algorithmes de tatouage numérique invisible et robuste. Par exemple, un des algorithmes que nous avons développés dans cette thèse est basé sur ces deux propriétés. En ce qui concerne la robustesse, nous avons choisi la combinaison des caractéristiques de la Transformée en Cosinus Discrète bidimensionnelle (2D-DCT) et la Transformée en Valeurs Singulières (SVD). En ce qui concerne l'imperceptibilité, nous avons exploité la technique de diffusion anisotrope bien connue de Perona-Malik dans le tatouage numérique des images. Cette technique qui trouve son utilisation principale dans le domaine du débruitage d'image, est utilisée dans le choix des blocs qui peuvent accueillir le tatouage. Les régions choisies

présentent une concentration de bords relativement élevée car le système visuel humain est moins sensible dans les régions fortement texturées, les bords et à changement rapide.

## Organisation de la thèse

Pour la mise en œuvre de l'approche proposée, ce manuscrit est organisé comme suit :

- Le premier chapitre est une présentation de l'état de l'art sur le tatouage numérique. A ce propos, nous avons donné l'historique du tatouage numérique puis nous avons défini le tatouage et son lien avec la cryptographie et la stéganographie. Ensuite nous avons parlé du principe de tatouage suivi par les principaux défis lors de la conception d'un système de tatouage numérique. Une classification des techniques de tatouage numérique est aussi élaborée. Par la suite, les applications du tatouage numérique, les attaques, les outils d'évaluation sont présentés.

- Le deuxième chapitre fait l'étude du tatouage numérique des images dans le domaine des transformées. Tous d'abord, nous avons exposé les transformées discrètes fréquemment utilisées dans le tatouage des images fixes, nous avons également présenté une technique de tatouage aveugle basée sur la transformée de Fourier Discrète paramétrique (PDFT). Par la suite, une autre méthode de tatouage non aveugle d'images, basée sur la combinaison entre la SVD et sa forme Multi-Résolution (MR-SVD) est exposée.

- Le troisième chapitre est dédié à la présentation de notre contribution qui s'articule autour d'un schéma de tatouage, s'appuyant sur l'utilisation d'une combinaison entre deux transformées : la DCT et la SVD. La première partie du chapitre est consacrée à la présentation de la diffusion anisotrope de Perona-Malik, par ailleurs la deuxième partie se concentre sur les résultats de simulations sur les images de Lena, Baboon et Barbara après l'application de plusieurs types d'attaques.

- Le quatrième chapitre, présente le tatouage numérique de la vidéo. En effet, nous avons présenté les notions de base sur la vidéo ainsi que les propriétés du tatouage numérique de la vidéo. Nous avons évoqué les contraintes de tatouage de la vidéo, puis nous avons discuté les limites des schémas de tatouage des images dans le contexte vidéo suivi d'une classification des méthodes de tatouage de la vidéo. En dernier, nous avons détaillé une technique de tatouage vidéo robuste basée sur la combinaison entre la MR-SVD et la SVD ainsi que les résultats expérimentaux.

Ce manuscrit est clôturé par une conclusion générale résumant notre approche, rappelant les résultats trouvés et donnant des perspectives pour ce travail.

# Chapitre 1

# *Etat de l'art sur le tatouage numérique*

## 1.1. Introduction

L'explosion récente des systèmes de communication et de l'Internet, en tant que supports de collaboration, a ouvert la porte aux entreprises ou aux personnes souhaitant partager ou vendre leurs produits multimédias. Néanmoins, les avantages de ces supports ouverts peuvent entraîner de très graves problèmes pour les propriétaires de médias numériques qui ne souhaitent pas que leurs produits soient distribués sans leur consentement. Cela est dû à la facilité de reproduction, de manipulation et de distribution illégales de supports numériques échangés via des réseaux de communication ou sur des appareils multimédias. Le tatouage numérique est une solution efficace à ces problèmes et à d'autres problèmes de sécurité de l'information [8.9.10.11 32–35]. Il fournit des moyens pour incorporer un message ou une signature (le tatouage) prouvant la propriété d'un signal image, vidéo ou audio sans détruire sa valeur perceptuelle [12.13.14 36–38]. En dépit du fait que le tatouage numérique a de nombreuses applications, nous nous concentrons sur la protection des droits d'auteur en raison de sa domination. Le tatouage numérique a été spécialement conçu pour faire face aux problèmes de protection des droits d'auteur. Néanmoins, il peut facilement être appliqué à de nombreuses autres applications.

Vu l'intérêt grandissant de ce domaine, nous présentons dans ce chapitre un état de l'art sur le tatouage numérique. Après avoir relaté les phases les plus marquantes de l'histoire du tatouage numérique, nous présentons sa distinction par rapport à la cryptographie et la stéganographie. Nous détaillons après le principe d'un système de tatouage, ses principaux défis, sa classification, ses applications ainsi que les attaques qui menacent un tatouage numérique. La dernière partie de ce chapitre est consacrée aux outils d'évaluation de performances de ce dernier.

## 1.2. Historique

Bien que l'art de la fabrication du papier ait été initié en Chine il y a plus de mille ans, les tatouages en papier ne sont apparus en Italie qu'aux environ de 1282[15]. Les marques ont été créées en ajoutant des motifs métalliques minces aux moules en papier. Le papier serait légèrement plus fin là où se trouvait le fil et donc plus transparent. La signification et le but des premiers tatouages sont incertains. Ils peuvent avoir été utilisés à des fins pratiques telles que l'identification des moules sur lesquels des feuilles de papier ont été fabriquées ou en tant que marques de commerce pour identifier le fabricant de papier. En revanche, ils peuvent

avoir représenté des signes mystiques ou simplement servi de décoration. Au XVIIIe siècle, les tatouages sur papier fabriqués en Europe et en Amérique étaient devenus plus utilitaires. Ils étaient utilisés comme marques de commerce pour enregistrer la date de fabrication du papier et pour indiquer le format des feuilles originales. C'est également à cette époque que les tatouages ont commencé à être utilisés comme mesures anti-contrefaçon pour l'argent et d'autres documents.

Le terme tatouage semble avoir été créé vers la fin du XVIIIe siècle et pourrait provenir du terme allemand wassermarke [15-16] (bien que le terme allemand puisse également provenir de l'anglais [17]). Le terme est en fait un abus de langage, dans la mesure où l'eau n'est pas particulièrement importante dans la création de la marque. C'est probablement parce que les marques ressemblent aux effets de l'eau sur le papier. À peu près au moment où le terme tatouage a été inventé, les faussaires ont commencé à mettre au point des méthodes de falsification de tatouages qui servent à protéger le papier-monnaie. En 1779, le Gentleman's Magazine [18] rapportait qu'un homme du nom de John Mathison avait découvert une méthode de contrefaçon de la marque de l'eau du papier de banque, qui était auparavant considérée comme la principale garantie contre la fraude. Dans cette découverte, il proposa de révéler et d'enseigner au monde la méthode de détection de la fraude, à condition que le pardon soit obtenu, ce qui n'avait pourtant aucun poids pour la banque.

La contrefaçon a entraîné des avancées dans la technologie du tatouage. William Congreve, un Anglais, a inventé une technique pour créer des tatouages en couleurs en insérant un matériau teint au centre du papier lors de sa fabrication. Les marques résultantes ont dû être extrêmement difficiles à falsifier, car la Banque d'Angleterre elle-même a refusé de les utiliser au motif qu'elles étaient trop difficiles à créer. Un autre Anglais, William Henry Smith, a inventé une technologie plus pratique : remplacer les motifs fins métalliques antérieurs utilisés pour faire les marques par une sorte de sculpture en relief peu profonde, pressée dans le moule en papier. La variation résultante à la surface du moule a produit de magnifiques tatouages aux nuances de gris variables. C'est la technique de base utilisée aujourd'hui pour le visage du président Jackson sur le billet de 20 dollars. Des exemples de notion plus générale de tatouages - des messages imperceptibles sur les objets dans lesquels ils sont incorporés - remontent probablement aux civilisations les plus anciennes. David Kahn, dans son livre classique The « Codebreakers », fournit des notes historiques intéressantes [19]. Une histoire particulièrement pertinente décrit un message caché dans le livre Hypnerotomachia Poliphili, anonymement publié en 1499. Les premières lettres de

chaque chapitre précisent «Poliam Frater Franciscus Columna Peramavit », supposé signifier « le père Francesco Columna aime Polia. ».

## 1.3. Les techniques de protection

### 1.3.1. La cryptographie

Le mot cryptographie est d'origine grecque : "kruptos" pour dire caché et "graphein" pour dire écriture. Elle peut être définie alors comme étant une science mathématique qui vise la protection des données confidentielles. Autrement dit, la cryptographie est l'art de chiffrer et coder les messages. Elle est devenue aujourd'hui une science entière à part. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité [20]. Le mécanisme de la cryptographie est défini par un algorithme de cryptographie ou un chiffrement qui est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé (un mot, un nombre ou une phrase), afin de crypter une donnée. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé [21]. Cependant, le vendeur ne peut pas savoir comment le produit est traité après son décryptage par l'acheteur.

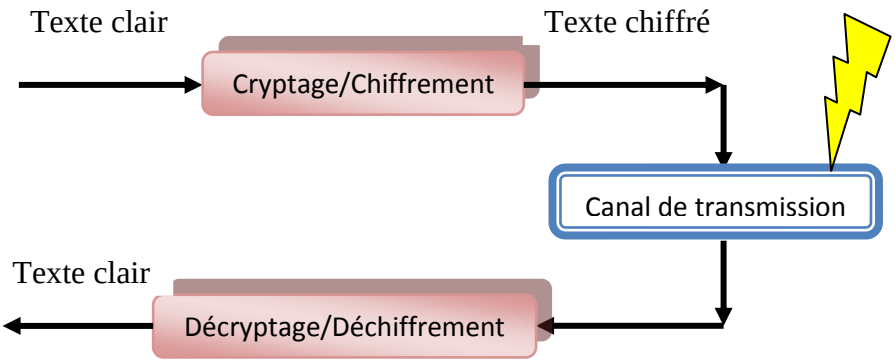



**Figure 1.1** Schéma général d'un système de cryptage.

Le cryptage protège le contenu pendant la transmission uniquement. Lorsqu'il est transmis au destinataire, les données doivent être déchiffrées pour être utiles. Une fois déchiffrées, les données ne sont plus protégées et deviennent vulnérables. L'acheteur peut s'avérer être un pirate qui distribue des copies illégales du contenu décrypté (non protégé).

### 1.3.2. La stéganographie

Le mot stéganographie est origine grecque et se compose de deux mots: "steganos" qui signifie couvert et "graphein" pour dire écriture. La stéganographie est l'art de la dissimulation, elle consiste à protéger un secret au sein d'un autre message anodin [22,23] de façon qu'on ignore même l'existence du message secret et seule personne connaissant l'astuce est apte à extraire le message caché. Pour mieux comprendre, on cite l'exemple de stéganographie connu sous le nom de "Principe de l'encre invisible". Cette technique était beaucoup utilisée dans le but d'envoyer des messages secrets. A cette époque, l'encre était réalisée à base de jus d'oignons et de chlorure d'ammoniac. Comme il est illustré dans la **figure1.2**, l'écriture était alors rendue claire en approchant le papier d'une flamme de bougie.

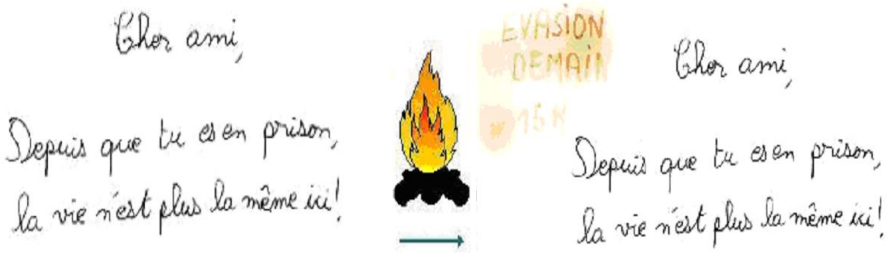



**Figure1.2** Exemple de stéganographie basé sur le "Principe de l'encre invisible".

### 1.3.3. Le tatouage

Le tatouage numérique, en anglais «watermarking », est une technologie qui suscite de plus en plus l'attention, car elle constitue une solution possible pour interdire la violation du droit d'auteur sur les données multimédia dans des environnements ouverts, extrêmement incontrôlés, où la cryptographie ne peut pas être appliquée correctement. Un tatouage numérique est une technique qui consiste à insérer une information distinctive (appelée la marque) aux données qu'il est destiné à protéger (appelées données de couverture ou données hôtes). Autrement dit, Le tatouage numérique incorpore directement un signal (généralement caché) dans un fichier hôte et il devient une partie intégrante de ce fichier et voyage avec ce dernier jusqu'à sa destination [24]. De cette façon, les données précieuses sont protégées tant que le tatouage y est présent et détectable. À tout moment, le signal caché peut être extrait pour obtenir les informations relatives au droit d'auteur. Ainsi, l'objectif d'un

tatouage est de rester toujours présent dans le fichier hôte. Toutefois, dans la pratique, un tatouage doit persister à toutes les manipulations possibles que les données hôtes peuvent subir.

### 1.3.4. Différence entre la cryptographie, la stéganographie et le tatouage

L'objectif principal de la cryptographie est de rendre le message incompréhensible à toute personne ne possédant pas l'information secrète adéquate. De plus, la cryptographie offre une sécurité plutôt à priori alors que la stéganographie offre une sécurité plutôt à posteriori, dans la mesure où le message secondaire est supposé rester accessible après recopies et manipulations du message primaire. Il existe aussi une différence importante entre le tatouage et la cryptographie qui réside dans le fait que des données cryptées doivent être illisibles pour une personne non autorisée [25-27]. Dans ce cas, les données en question sont le média numérique lui même (l'image, la séquence vidéo ou audio), alors que dans le cas du tatouage, les données tatouées doivent paraître originales mais l'information cachée dans ces données (le tatouage) doit être illisible pour toute personne non autorisée. On peut dire alors que le tatouage est semblable à la stéganographie puisque les deux sont basés sur le camouflage d'une information dans un medium mais les deux diffèrent au niveau de leurs objectifs. En effet, l'objectif de la stéganographie est de transmettre un message dissimulé au sein d'un medium qui n'a pas beaucoup d'importance par contre l'objectif du tatouage est de protéger le document qui contient l'information dissimulée. Une autre différence entre ces deux derniers réside dans le fait que dans la détection, il est indispensable d'extraire le message dans la stéganographie, par contre, dans le tatouage, soit on extrait le message soit on détecte simplement sa présence.

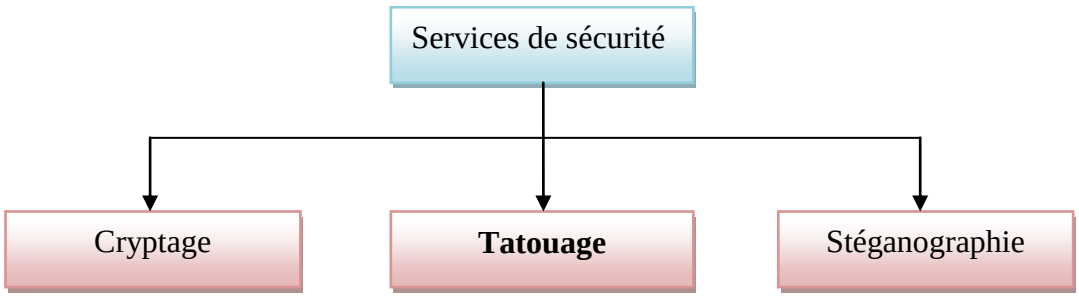



**Figure1.3** Services de sécurité.

## 1.4. Principe du système de tatouage

Considéré comme une tâche de communication, le processus de tatouage peut être divisé en trois étapes principales : l'incorporation du tatouage, la transmission par le canal du signal tatoué (soumis à des attaques éventuelles) et la récupération de tatouage (**figure 1.4**).

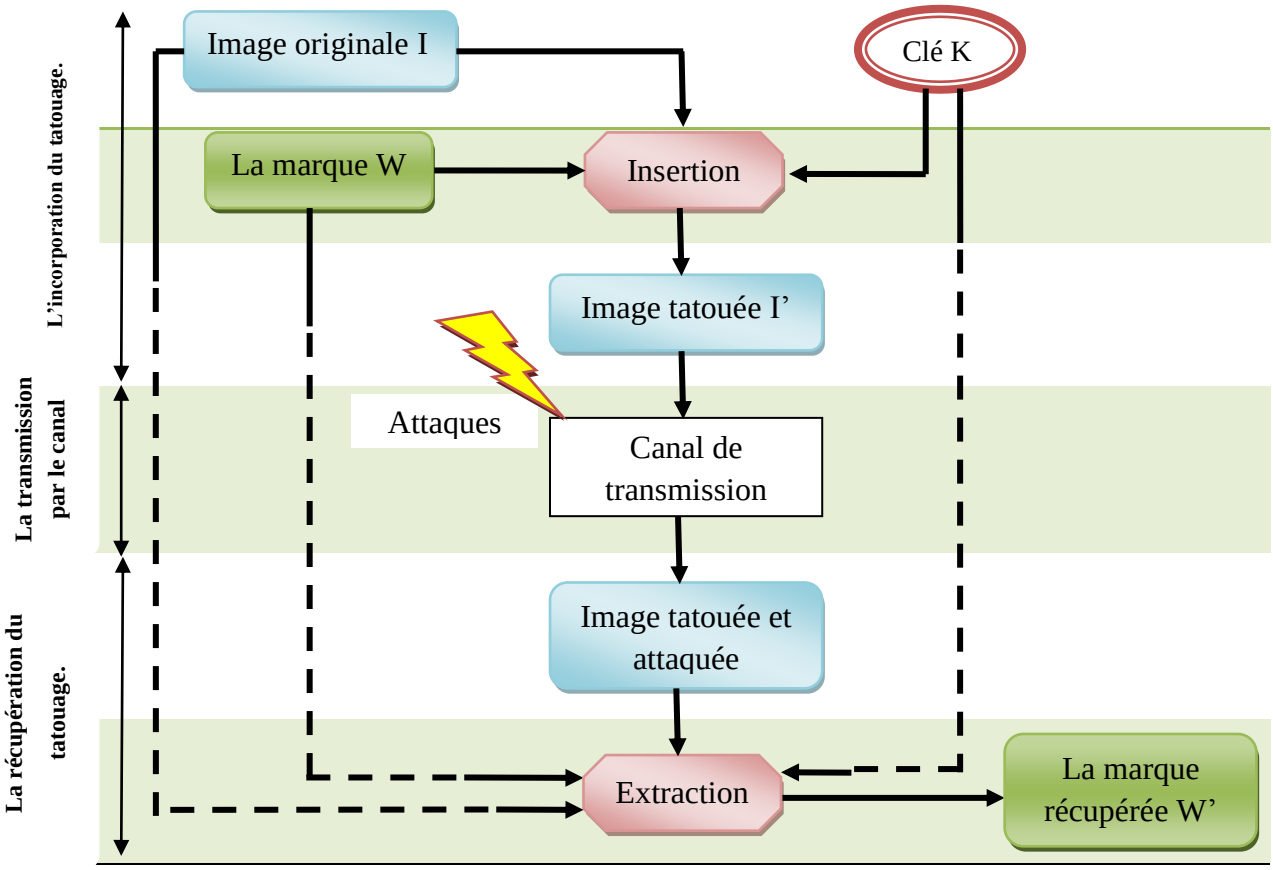



**Figure 1.4** Principe du système du tatouage.

### 1.4.1. L'incorporation du tatouage (Phase d'insertion)

La première étape dans la conception d'un système de tatouage est la définition de la procédure d'incorporation ou d'intégration de la marque. Cette tâche est cruciale, car les propriétés du tatouage dépendent fortement de la manière dont il est inséré dans les données.
La phase d'insertion nécessite comme entrées le document hôte (image dans notre cas) qu'on note I et la marque à insérer (généralement sous format binaire) qu'on note W(Watermark). Souvent, le schéma utilise en plus une clé d'insertion [28].

### 1.4.2. La diffusion dans le canal de transmission

L'image porteuse d'une marque, peut subir divers traitements : stockage dans une base de données, diffusion dans un réseau ou bien tout simplement des traitements visant des améliorations particulières. Au cours de ce processus, plusieurs attaques malveillantes ou

innocentes menacent la marque insérée. Les attaques malveillantes visent directement la marque par contre les attaques bienveillantes visent l'amélioration de l'exploitation de l'image tatouée.

### 1.4.3. La récupération du tatouage (Phase d'extraction)

L'objectif d'un système de tatouage consiste essentiellement à introduire des informations sur un support, puis à les extraire de manière aussi fiable que possible. Si nous considérons l'intégrateur de tatouage comme un émetteur dans une chaîne de communication, un extracteur de tatouage sera le récepteur. La détection peut avoir deux objectifs différents: décider si l'image testée contient un tatouage et extraire un message que le tatouage peut véhiculer. A la fin de cette phase, on aura soit une marque W' soit une décision indiquant si l'extraction a été faite avec succès ou non.

## 1.5. Principaux défis dans un système de tatouage

Depuis l'apparition du tatouage numérique, les chercheurs n'ont pas cessé de rénover les méthodes de marquage. Ces perfectionnements visent surtout à améliorer les principales propriétés du tatouage qui sont principalement : la robustesse ou fragilité, l'invisibilité, la capacité d'insertion et la sécurité de l'information secrète. Il doit y avoir un compromis entre les exigences et les propriétés du tatouage en fonction de ses applications. Dans ce qui suit, ces propriétés seront étudiées.

### 1.5.1. L'imperceptibilité

Elle représente une préoccupation majeure pour les types des tatouages invisibles. Elle signifie que la quantité de la dégradation provoquée par la marque est imperceptible. Certains algorithmes de tatouage utilisent la propriété de masquage du système visuel humain (HVS) pour insérer la marque dans les régions imperceptibles dans l'objet hôte. Ce critère repose sur l'idée que l'insertion de la marque n'influence pas sur la qualité visuelle de l'image pour deux raisons: pour ne pas perdre la qualité de l'image et aussi pour que la marque ne pourrait pas être détruite facilement par les pirates ou les attaques [29].

### 1.5.2. La robustesse

Ce critère représente la résistance ou non de la marque après des modifications subies par les attaques qui peuvent affecter le document hôte. En effet, plus le schéma est robuste, plus la probabilité d'extraire correctement la signature, après des altérations, est élevée. Cela nous

permet de définir la robustesse comme la capacité de détecter le tatouage après des opérations de modification. Par conséquent, plus la quantité d'information dans l'image augmente, plus la signature sera visible ou perceptible et donc la robustesse augmente.

### 1.5.3. La capacité

La capacité peut être définie par le taux d'intégration de la marque, c'est à dire la quantité des informations ou de la marque que l'on peut insérer dans l'image. En effet, l'insertion de la marque dépend du nombre de pixels aptes à être changés. En pratique, il est prouvé que plus la taille da la marque est grande plus la dégradation est grande (la marque est plus visible).

### 1.5.4. Sécurité de l'information secrète

L'objectif principal de tatouage numérique est la protection des données insérées. Ceci dépend du choix de la clé d'insertion. Ainsi, une technique de tatouage est vraiment sûre si la marque insérée ne sera jamais extraite par une personne non autorisée même si elle aura une idée sur les algorithmes d'insertion et d'extraction.

### 1.5.5. Compromis entre robustesse, imperceptibilité et capacité

La robustesse, l'invisibilité et le taux d'intégration sont des propriétés fortement liées les unes aux autres. L'évolution de l'une de ces trois attributs influe directement sur les deux restantes. Dans ce cadre, Chareyron [30] a confirmé que la croissance de taille de la marque à insérer, peut entrainer, soit une dégradation de l'aspect psycho-visuel de l'image soit une réduction au niveau de la sécurité des données à extraire. Alors, il est devenu très important de réfléchir lors de la phase d'insertion de faire un compromis de ces trois caractéristiques. La **figure 1.5** est une présentation du triangle de contraintes montrant la relation entre le taux d'intégration, l'invisibilité et la robustesse [22].

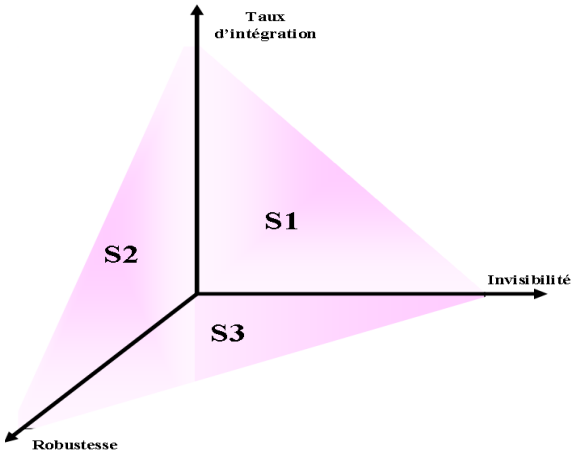



**Figure 1.5** Le triangle des contraintes.

## 1.6. Classification du tatouage numérique

Le tatouage numérique peut être classé en plusieurs catégories selon différentes caractéristiques comme résumé sur la **figure 1.6** [26-27,31-32].

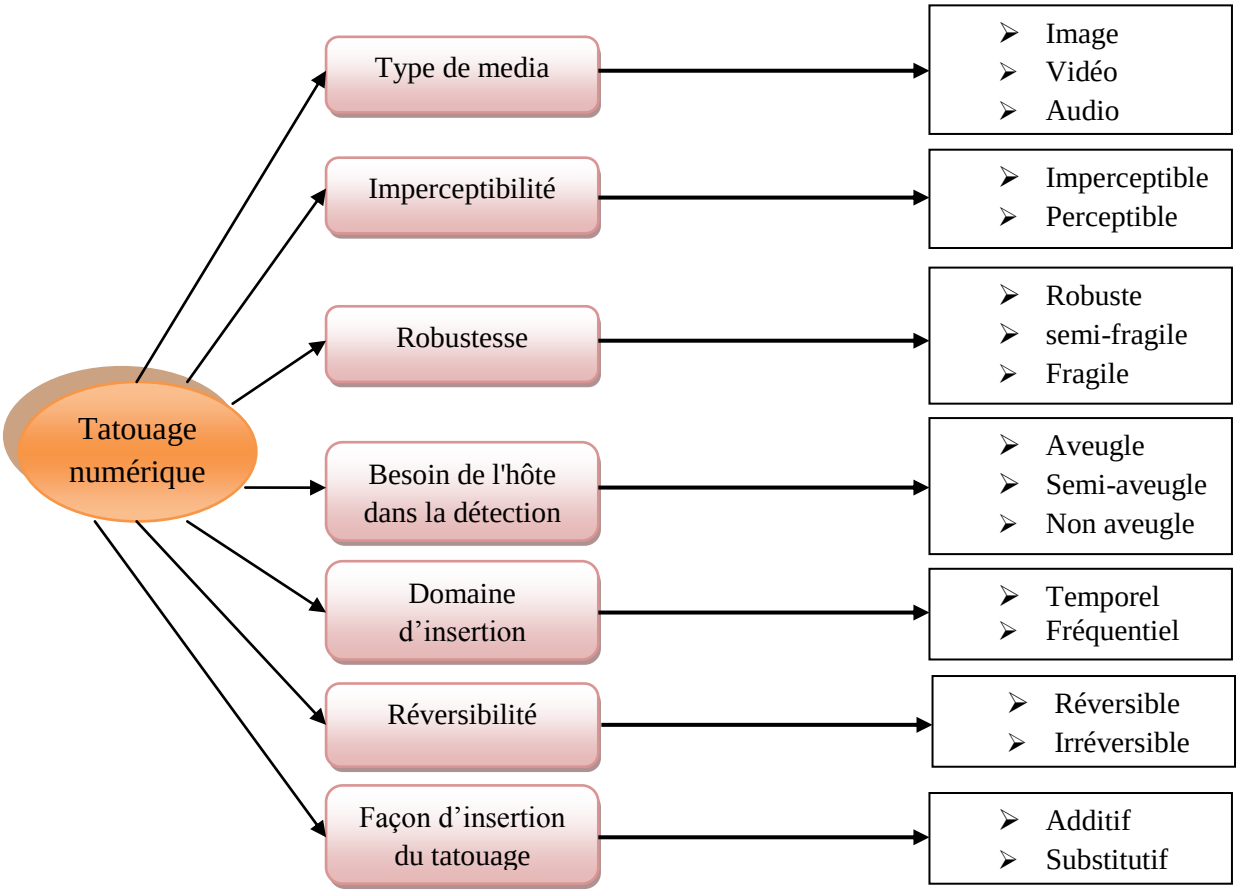



**Figure 1.6** Classification du tatouage numérique.

### 1.6.1. Les types de media (image, vidéo et audio)

Le tatouage vise trois signaux numériques : l'image, la vidéo et l'audio. Depuis le début de la recherche sur le tatouage, le domaine de l'image s'est bien développé et a attiré plus d'attention. La plupart des techniques de tatouage vidéo actuelles traitent les images vidéo comme une séquence d'images fixes et tatouent chacune d'elles en conséquence. Comparé au tatouage d'images et de vidéos, le tatouage audio est plus difficile en raison de la moindre redondance des signaux audio et de la sensibilité élevée du système auditif humain (HAS), qui est supérieure à celle du système visuel humain (HVS).

#### 1.6.1.1. Tatouage des images

Le tatouage d'images, comme indiqué précédemment, est un processus d'insertion d'un signal secondaire dans une image de telle sorte que le signal peut être détecté ou extrait ultérieurement.

#### 1.6.1.2. Tatouage des vidéos

Une vidéo est une succession d'images numériques (appelées trames) affichées à une certaine cadence. L'œil humain a comme caractéristique d'être capable de distinguer environ 20 images par seconde. Ainsi, en affichant plus de 20 images par seconde, il est possible de tromper l'œil et de lui faire croire à une image animée.

Le tatouage de vidéo numérique se résume souvent à des approches image par image [33-34] comme donné ci-dessous :

$$f'_t = f_t + \alpha w_t \quad (1.1)$$

où $f_t$ est la trame vidéo originale à l'instant $t$, $f'_t$ sa version tatouée, $\alpha$ est la force de tatouage et $w_t$ est le signal de tatouage. Par conséquent, chaque trame peut être considérée comme un document tatoué individuellement [35,36].

#### 1.6.1.3. Tatouage audio

Les signaux audio sont représentés par des échantillons dans l'intervalle de temps, et la quantité d'informations pouvant être intégrées de manière robuste et non audible est donc bien inférieure à celle des supports visuels [37]. Les exigences des techniques de tatouage audio sont les plus difficiles à satisfaire comparées à celles des autres applications du tatouage numérique. La tâche d'un encodeur de tatouage est de régler le signal à tatouer afin de garantir l'inaudibilité et d'intégrer simultanément le tatouage avec la puissance maximale en fonction du signal porteur pour fournir une robustesse maximale. Un encodeur de tatouage audio perceptuel comprend généralement plusieurs composants (voir **figure 1.7**). Le bloc de codage et de modulation code les informations $m$ au moyen d'une clé secrète $K$ et modifie des composantes de porteuse sélectionnées du signal audio, telles que l'amplitude, la phase et la fréquence. Le bloc modèle psycho-acoustique (PAM) analyse le signal original $c_o(t)$ afin de calculer des seuils de perception comme le seuil de masquage minimal. Il peut également représenter les paramètres de contrôle psycho-acoustique tels que la différence de phase maximale admissible ou les seuils de masquage temporel. Le modèle utilisé est déterminé par le type de modulation utilisé dans l'algorithme spécifique.

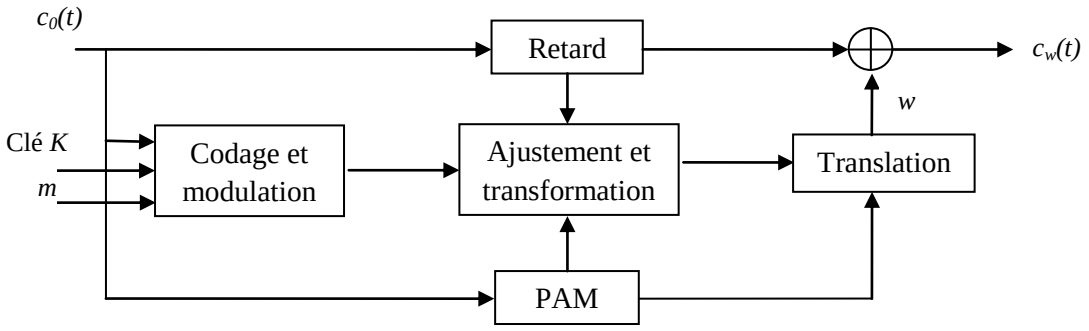



**Figure 1.7** Encodeur de tatouage audio et ses composants.

### 1.6.2. L'imperceptibilité / la perceptibilité

La perception humaine est également utilisée comme un critère pour classer les techniques de tatouage visible et invisible. Pour les images, les tatouages perceptibles sont des motifs visuels non obstructifs tels que des logos fusionnés dans un coin de l'image [29]. Bien que le tatouage perceptible soit pratiquement facile à détruire par les pirates, il n'est pas l'objet du tatouage numérique. Comme mentionné précédemment, le tatouage numérique a pour objectif d'insérer imperceptiblement le tatouage dans un support numérique. [37]

(a) (b)

**Figure 1.8** (a) Tatouage visible, (b) Tatouage invisible.

### 1.6.3. Tatouage robuste, semi-fragile et fragile

#### 1.6.3.1. Le tatouage robuste

Ce type de tatouage sert à garantir la protection des droits d'auteurs**.** Les algorithmes de tatouage robustes permettent de trouver la marque après d'éventuelles distorsions telles que la compression, le filtrage et le bruit.

#### 1.6.3.2. Tatouage semi-fragile

Ce type de tatouage est robuste à certains types de manipulations ou dégradations comme la compression avec perte, plusieurs méthodes et travaux reposent sur ce schéma ont été réalisés [29].

#### 1.6.3.3. Tatouage fragile

Pour le tatouage fragile, la marque insérée est sensible et fragile et elle ne doit pas résister aux modifications de l'image tatouée. Ce type de tatouage est utilisé pour détecter s'il y a eu une manipulation ou une modification sur le contenu numérique.

### 1.6.4. Tatouage non aveugle, semi-aveugle et aveugle

Selon le processus d'extraction de la marque, les techniques de tatouage sont classées en trois catégories: aveugle, non aveugle et semi-aveugle. Dans le tatouage aveugle, l'image originale et la marque ne sont pas requises dans le processus d'extraction, par contre le tatouage non aveugle nécessite l'utilisation de l'image originale et la clé. Dans la technique semi-aveugle, seules des informations partielles sur l'image originale (appelées informations secondaires) sont requises dans le processus d'extraction. Les informations secondaires sont d'une grande importance pour les tatouages semi-aveugles et doivent être transmises sur un canal haut fidélité [41]. Les techniques non aveugles sont moins intéressantes dans les applications pratiques, alors que les techniques semi-aveugles sont appropriées pour des applications telles que la protection contre la copie et les empreintes digitales [39-40], tandis que les techniques aveugles conviennent pour des applications telles que la communication secrète [37-38].

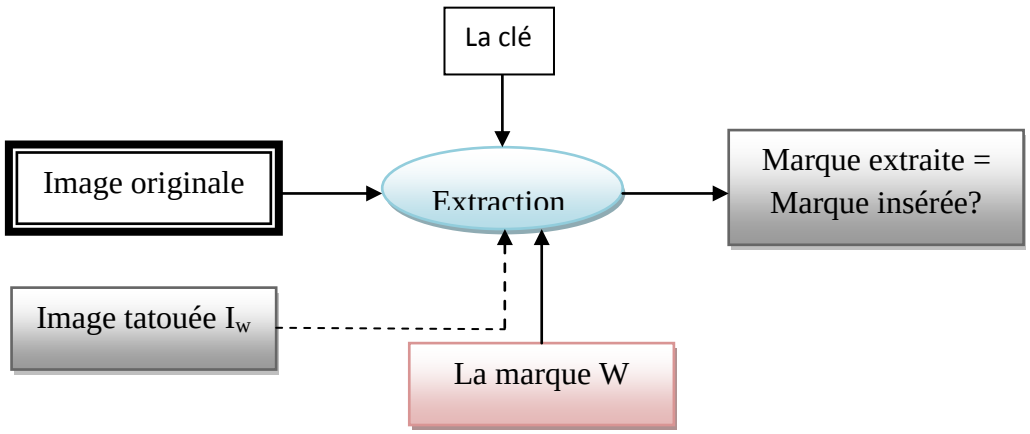



**Figure 1.9** Schéma d'extraction non aveugle d'une marque.

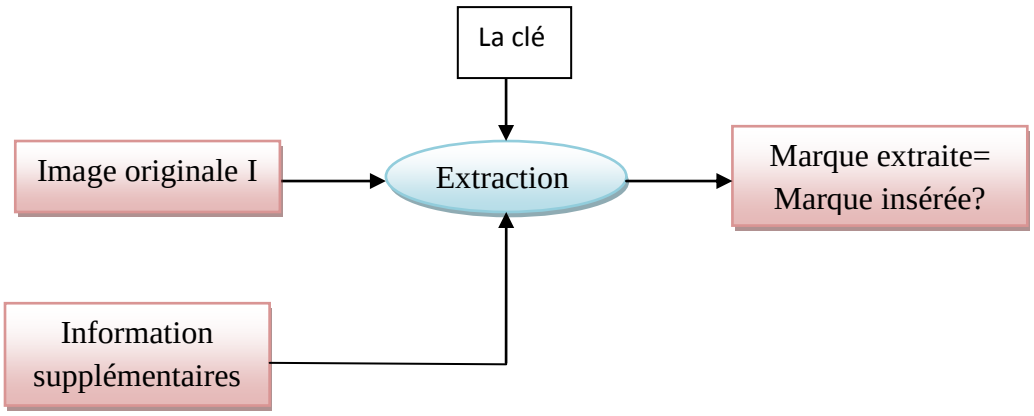



**Figure 1.10** Schéma d'extraction semi aveugle d'une marque.

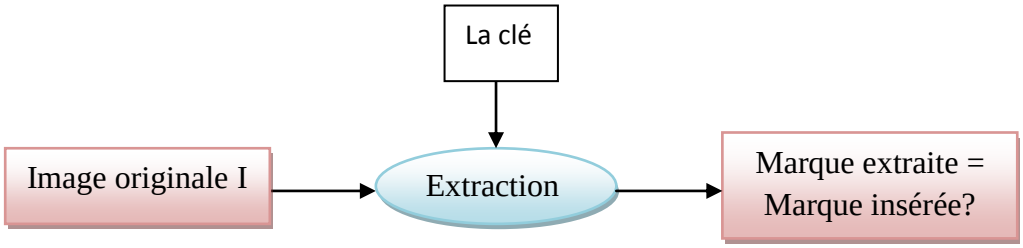



**Figure 1.11** Schéma d'extraction aveugle d'une marque.

### 1.6.5. Les tatouages temporel et fréquentiel

Selon le domaine d'insertion du tatouage, les techniques de tatouage numérique sont essentiellement classées en deux catégories : Les techniques dans le domaine temporel (spatial) et les techniques dans le domaine fréquentiel [6]. Les techniques dans le domaine spatial ont une faible robustesse et une complexité de calcul réduite, tandis que les techniques dans le domaine fréquentiel offrent une meilleure robustesse au prix d'une complexité de calcul plus élevée. De nombreuses transformées discrètes ont été utilisées avec succès par des techniques de tatouage numérique, telles que la transformée en cosinus discrète (DCT), la transformée de Fourier discrète (DFT) et la transformée en ondelettes discrète (DWT).

### 1.6.6. Les tatouages réversible et non réversible

En tatouage réversible, la marque peut être complètement supprimée de l'image tatouée, et donc la possibilité d'une reconstruction parfaite de l'image originale. Cependant, le prix d'une telle réversibilité implique une perte de robustesse, de sécurité et d'impercibilité. En

revanche, le tatouage non réversible introduit généralement une dégradation légère mais qui est une dégradation définitive de la qualité du signal d'origine [37, 42, 43].

### 1.6.7. Les tatouages additif et substitutif

#### 1.6.7.1. Le Tatouage additif

Le schéma additif consiste à ajouter la marque ou la signature *w* à l'image hôte *I* ou aux coefficients de transformation de celle-ci selon l'équation 1.2. La marque est générée à l'aide d'une clé *k* de façon pseudo aléatoire et est directement insérée dans l'image originale.

Pour le processus de détection dans ce type de tatouage pour les techniques aveugle, il est effectué à l'aide des méthodes statistiques. Dans ce cas, une mesure de corrélation peut être effectuée.

$$Iw = I + k.w \tag{1.2}$$

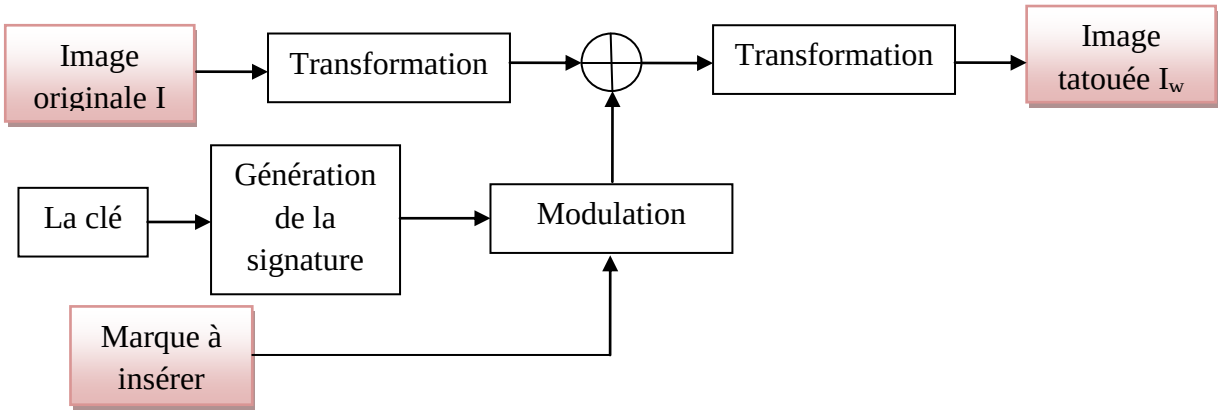



**Figure 1.12** Principe de l'insertion de la marque par addition.

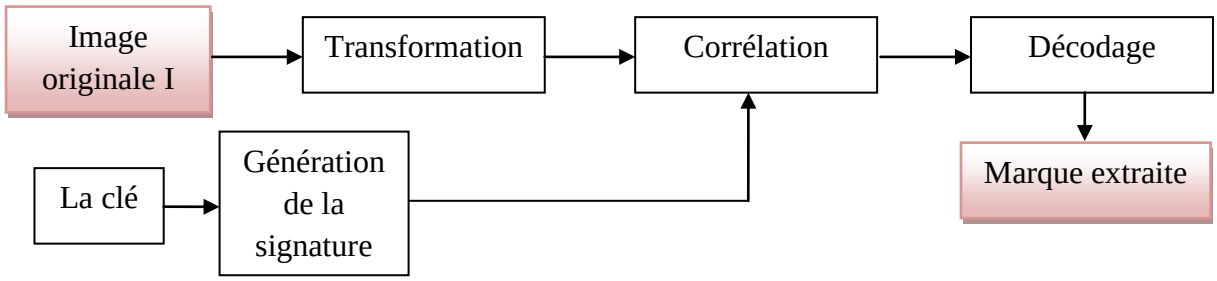



**Figure 1.13** Principe de l'extraction de la marque par addition.

#### 1.6.7.2. Tatouage substitutif

La marque n'est pas ajoutée mais substituée à des composants de l'image (pixel, coefficient de transformés,....) sélectionnés à l'aide d'une clé secrète. La signature est insérée selon des contraintes appliquées sur les composants de l'image. Dans la phase d'extraction, on calcule le degré de similitude entre la marque retrouvée à partir des composants de l'image tatouée et la marque originale. Le processus d'insertion et de l'extraction du schéma substitutif sont présentés sur les **figure 1.14** et **1.15** respectivement [29].

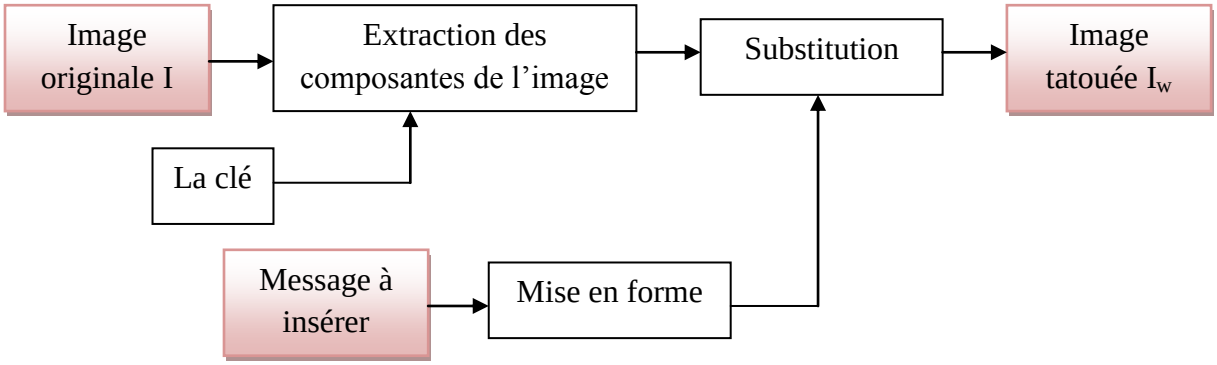



**Figure 1.14** Principe de l'insertion par substitution.

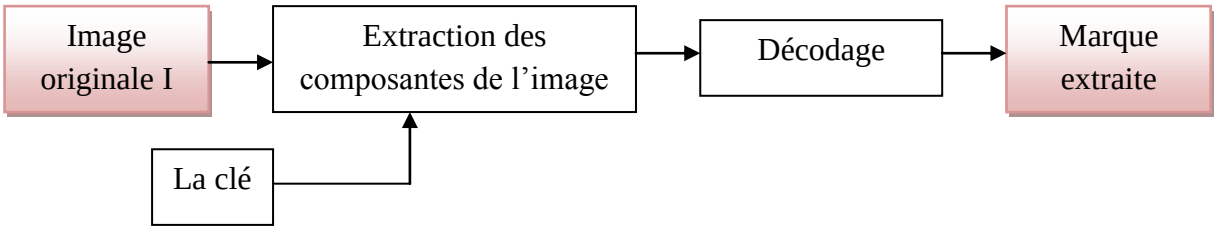



**Figure 1.15** Principe de l'extraction de marque par substitution.

## 1.7. Les applications du tatouage numérique

Dans cette section, nous présentons certaines applications du tatouage numérique et leurs exigences. Les principales applications du tatouage sont l'identification du propriétaire / la preuve de propriété [22], l'authentification (également appelée vérification du contenu, intégrité des données ou protection contre la falsification) [26-27], les tatouages transactionnels, le contrôle de copie, la communication secrète et la surveillance de diffusion [22, 31, 39-40].

### 1.7.1. L'identification du propriétaire et la prévue de propriété

Un avis de droit d'auteur traditionnel sous la forme «© date, propriétaire» ajouté sur une image ou une image vidéo n'est plus un moyen sûr de garantir les droits d'auteur [22]. Bien que ces annotations soient toujours recommandées, elles peuvent facilement être découpées ou traitées, ce qui permet de supprimer ou de modifier les informations de propriété. Par conséquent, la violation du droit d'auteur nuit aux intérêts des fournisseurs plutôt qu'à ceux des clients. Dans la mesure où un tatouage numérique, une fois intégré, devient une partie imperceptible et inséparable des données de l'hôte, il peut être utilisé pour fournir une fonctionnalité de marquage des droits d'auteur. Le propriétaire de la propriété intellectuelle ajoute ses informations de droits d'auteur sous la forme d'un tatouage haute fidélité, robuste et sécurisé. Même si le document subit des manipulations (intentionnelles ou non), il sera toujours possible d'extraire ou de détecter le tatouage aussi longtemps que les données de l'hôte seront sous une forme valable. En outre, l'image paraîtra plus attrayante pour les yeux, car elle n'a pas besoin d'avis textuels qui pourraient la perturber sur le plan esthétique.
Le niveau de sécurité requis pour prouver la propriété est supérieur à celui requis pour l'identification du propriétaire. Prouver la propriété signifie prouver qu'un document est la propriété de quelqu'un et qu'il n'appartient à personne. Cela vient du fait qu'un pirate peut saper le tatouage original sans le supprimer.

### 1.7.2. La gestion des transactions (Empreintes digitales)

Les tatouages transactionnels, également appelés empreintes digitales, permettent à un propriétaire de propriété intellectuelle ou à un distributeur de contenu d'identifier la source d'une copie illicite en marquant chaque copie légale du document d'un tatouage unique et distinct. Si un document marqué d'un tatouage de transaction est utilisé à mauvais escient (distribué illégalement), le propriétaire peut déterminer qui est le responsable. Il existe deux applications bien connues du monde des empreintes digitales. L'une est la distribution des quotidiens de films. Un film quotidien est le résultat de la photographie de chaque jour et il est distribué à un certain nombre de personnes impliquées. Bien que ces quotidiens soient hautement confidentiels, un quotidien est parfois divulgué à la presse. Le tatouage, différent dans chaque copie, sert de suivi pour trouver la source des fuites. L'autre application a été déployée par la société DivX, aujourd'hui disparue. En fait, ils ont conçu et commercialisé un nouveau lecteur qui a placé un tatouage unique sur chaque vidéo diffusée. Si quelqu'un fait

des copies de ce film après l'avoir vu, le tatouage apparaît sur toutes les copies identifiant le lecteur sur lequel il a été joué. Si ces copies sont vendues illicitement, le DivX pourrait obtenir l'une des copies et trouver le transgresseur [44].

### 1.7.3. L'authentification du contenu

Avec les progrès des outils informatiques disponibles pour le traitement du signal numérique, la modification d'un document numérique devient plus facile tout en sachant que le contenu modifié devient plus difficile à détecter. Le problème de l'authentification des messages a été bien étudié en cryptographie [44]. La solution offerte par la cryptographie est une signature numérique et une méthode largement acceptée. Seule la source autorisée connaît la clé valide pour le chiffrement, un adversaire qui tente de modifier le message ne peut pas créer une signature valide correspondante pour le message modifié. L'inconvénient des signatures numériques est qu'elles doivent être complétées sous forme de métadonnées dans les données d'origine sous forme d'informations séparées avant la transmission. Il est donc facile de perdre les signatures lors d'une utilisation quotidienne, même sans aucune opération malhonnête. La conversion de format est le meilleur exemple pour ces situations. Si la signature est enregistrée dans les champs d'en-tête de certains formats de données (JPEG, par exemple), elle sera ignorée lorsque nous passons à un autre format sans espace pour une signature dans l'en-tête. Lorsque la signature est perdue, le travail ne peut plus être authentifié. La supériorité du tatouage vient à ce point. Étant donné que les informations de tatouage sont acheminées directement sur les bits de l'œuvre originale, nous ne les perdons pas si le champ d'en-tête du fichier numérique est supprimé. Certaines marques d'authentification sont conçues pour ne plus être valides à la moindre modification sur des données protégées. Ces marques sont appelées tatouages fragiles. Dans les systèmes de signature incorporés, le calcul de la signature dépend du signal de l'hôte car une signature est un résumé des données à protéger. Cependant, lorsque nous intégrons la signature dans les données, le contenu des données est modifié. Même cette modification est petite; la signature pourrait ne plus représenter les données modifiées. Pour résoudre ce problème, il est suggéré de séparer les données en deux parties: une pour le calcul de la signature et une pour l'intégration de la signature [45-46]. En tant que partie intégrante des données de l'hôte, le tatouage est modifié de la même manière que les données originales en tatouage. Voici un autre avantage de la détection des altérations utilisant des tatouages: la possibilité d'en apprendre davantage sur la façon dont les données sont modifiées.

### 1.7.4. La surveillance de diffusion

Les publicités sont vitales pour la survie des chaînes de radio et de télévision. Les entreprises réservent une heure précise de l'air à une heure précise de la journée et présentent leurs produits à l'auditoire en payant pour le temps qu'elles réservent. Le prix qu'ils paient varie également de temps en temps dans une journée. Réserver le midi est beaucoup moins cher que de réserver le soir, qu'on appelle à des heures de grande écoute. Par conséquent, les entreprises planifient et préparent soigneusement leurs publicités et leur accordent une grande importance. C'est pourquoi les entreprises utilisent un système de surveillance de la radiodiffusion datant d'au moins 1975 [32]. Ce ne sont pas seulement les publicités qui doivent être surveillées. Certains articles peuvent avoir une valeur de plusieurs centaines de milliers de dollars par heure. Cela les rend très vulnérables aux violations des droits de propriété intellectuelle. Une autre utilisation des données d'identification de diffusion est utilisée dans les études de marché concurrentielles [38]. Une entreprise peut vouloir savoir combien l'entreprise concurrente investit sur sa nouvelle marque sur le marché et ajuster sa propre politique de marketing en fonction de ces données. Une troisième application possible est la détection de rediffusions illégales (non autorisées) de contenus protégés par le droit d'auteur par des stations pirates. Les propriétaires de propriété intellectuelle seront plus intéressés par ces types de systèmes [36].

### 1.7.5. Le contrôle de copie

Les applications que nous avons mentionnées jusqu'à présent ont pour philosophie de prouver qu'il y a eu violation du droit d'auteur au lieu d'essayer d'empêcher que l'infraction se produise. Les tatouages que nous avons mentionnés sont utilisés après que nous soupçonnions qu'un contenu est modifié ou distribué illégalement. Cependant, avec l'aide d'un matériel intelligent, nous pouvons contrôler les processus de duplication, de modification et de distribution, qui sont les principales sources d'action illégale. Les technologies de contrôle de copie peuvent avoir un effet dissuasif contre de telles actions. Le chiffrement est encore une fois une solution au problème. Le contenu est distribué aux utilisateurs légitimes dans un format crypté et seuls ces utilisateurs disposent d'une clé unique pour le décryptage. La clé est dans un format spécial qu'il est difficile de dupliquer et de distribuer. Par exemple, les sociétés de diffusion de télévision par satellite offrent à leurs clients une carte à puce (très semblable aux cartes SIM des téléphones cellulaires), qui est insérée dans le décodeur, servant de clé. Sans la clé, le décodeur ne peut pas décrypter les signaux entrants et tout ce que vous

pouvez voir est une vidéo brouillée. Un système basé sur le cryptage ne peut pas empêcher le piratage des données après qu'un client légal avec une clé légalement reçue les déchiffre. C'est le point le plus faible d'un mécanisme de protection cryptographique. Par conséquent, nous avons besoin d'une technologie permettant de visualiser les médias, mais d'empêcher leur enregistrement. Deux exemples sont le système de protection analogique (APS, développé par Macrovision [43]), qui modifie le signal vidéo de manière à confondre le contrôle de gain automatique sur les enregistreurs, et le système de gestion de la génération de copies sur DVD, composé d'une paire de bits dans l'en-tête du flux MPEG, qui codent les autorisations de copie. Il existe déjà des logiciels de contrôle de copie commerciaux sur le marché. En fait, MarkAny [45] propose bien plus que la simple prévention de la copie illégale. Leur produit s'appuie sur des tatouages pour contrôler les fonctions Ouvrir, Télécharger et Imprimer en fonction des droits de l'utilisateur, même après que le contenu a été ouvert par un utilisateur non authentifié.

### 1.7.6. Le contrôle de l'appareil

Le contrôle de périphérique est une vaste catégorie d'applications dans lesquelles des périphériques spécialement conçus réagissent aux tatouages détectés dans le contenu. Les premières applications de contrôle de périphérique avec tatouages remontent à 65 ans. En 1953, Tomberlein et al. [48] ont décrit un système permettant de distribuer de la musique dans des bureaux, des magasins et d'autres locaux. La diffusion est tatouée pour marquer le début et la fin des publicités, discussions et autres éléments autres que la musique, de sorte qu'ils soient ignorés et ne soient pas diffusés au bureau, dans un magasin, etc. RH Baer de Sanders Associates Inc. [49] a obtenu un brevet en 1976 pour un tatouage vidéo destiné aux applications de télévision interactive. Un autre brevet a été attribué à Broughton et Laumeister en 1989 pour une autre application de télévision interactive [50]. Leur technique permettait aux jouets d'action d'interagir avec les programmes de télévision. Un autre brevet dans le domaine du contrôle des appareils a été attribué à Ray Dolby de Dolby Labs [51] en 1981. Le Dolby-FM était une technique de réduction du bruit utilisée par les stations de radio. Certaines radios étaient équipées de décodeurs spéciaux pour exploiter pleinement Dolby-FM. Dolby a inventé un tatouage à insérer dans la diffusion Dolby-FM qui activera automatiquement le circuit de décodeur spécial des récepteurs radio compatibles. Une application plus récente est le système MediaBridge de Digimarc [52], qui utilise des tatouages qui permettent à un ordinateur de répondre aux documents en tatouage présentés à une caméra Web compatible. Il suffit de maintenir le document imprimé (contenant un tatouage) sur une caméra Web

compatible Digimarc et la technologie Digimarc MediaBridge permet d'accéder au site Web associé sans avoir à taper ou cliquer.

### 1.7.7. L'indexation

On peut envisager l'utilisation du tatouage afin de faciliter l'accès à des banques de données. La marque n'a pas besoin d'être robuste à de nombreux types d'attaques, puisqu'il ne s'agit plus de protection mais d'identification. Par exemple, un médecin peut inclure dans une radiographie, de façon discrète afin de ne pas la dénaturer, le nom du patient traité, son diagnostic et ses observations. Ce cas est le plus simple, puisqu'une attaque visant à détruire la marque ne présente aucun intérêt et n'est donc a priori pas à craindre. Selon [1, 47], ce type de documents est appelé documents auto-indexé, car la marque contient sa propre description, afin de permettre son stockage dans une base de données sans problème de changement de format.

## 1.8. Les attaques menaçant le tatouage

Dans la terminologie du tatouage, une attaque est un traitement qui peut entraver la détection du tatouage ou la communication des informations véhiculées dans le tatouage. Les données tatouées traitées sont ensuite appelées données attaquées. La robustesse est un aspect important de tout système de tatouage. Sa notion est claire: un tatouage est robuste s'il ne peut pas être altéré sans rendre également inutilisables les données de l'hôte. Par conséquent, une attaque est dite réussite si elle annule la technique du tatouage tout en conservant la qualité requise en fonction des contraintes spécifiées du scénario de l'application.

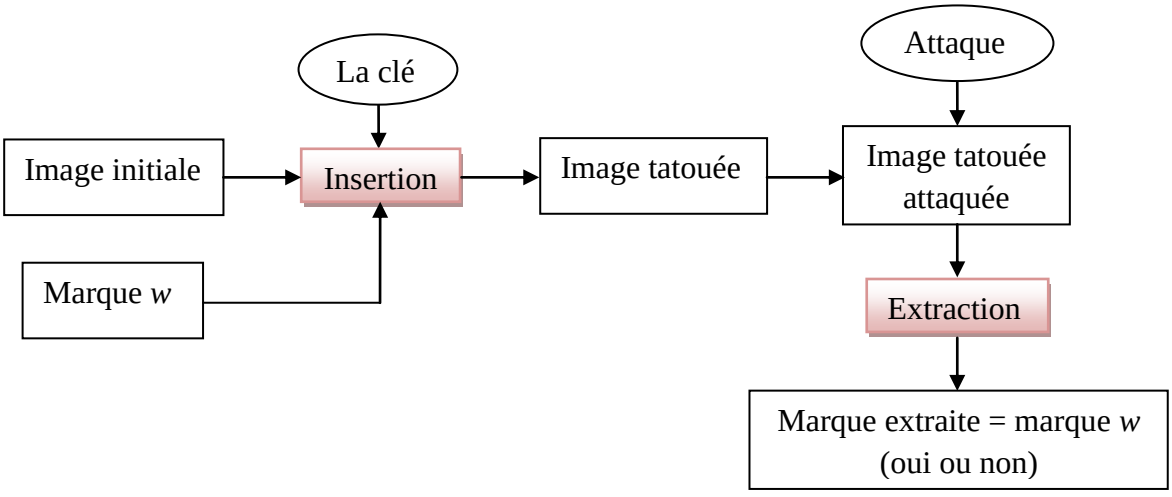



**Figure 1.16** Exemple d'un schéma général d'un système de tatouage qui subit des attaques.

Par la suite, nous allons classer ces attaques en quatre classes principales à savoir :

- Les attaques d'effacement ou de suppression,

- Les attaques géométriques,

- Les attaques cryptographiques

- Les attaques de protocole.

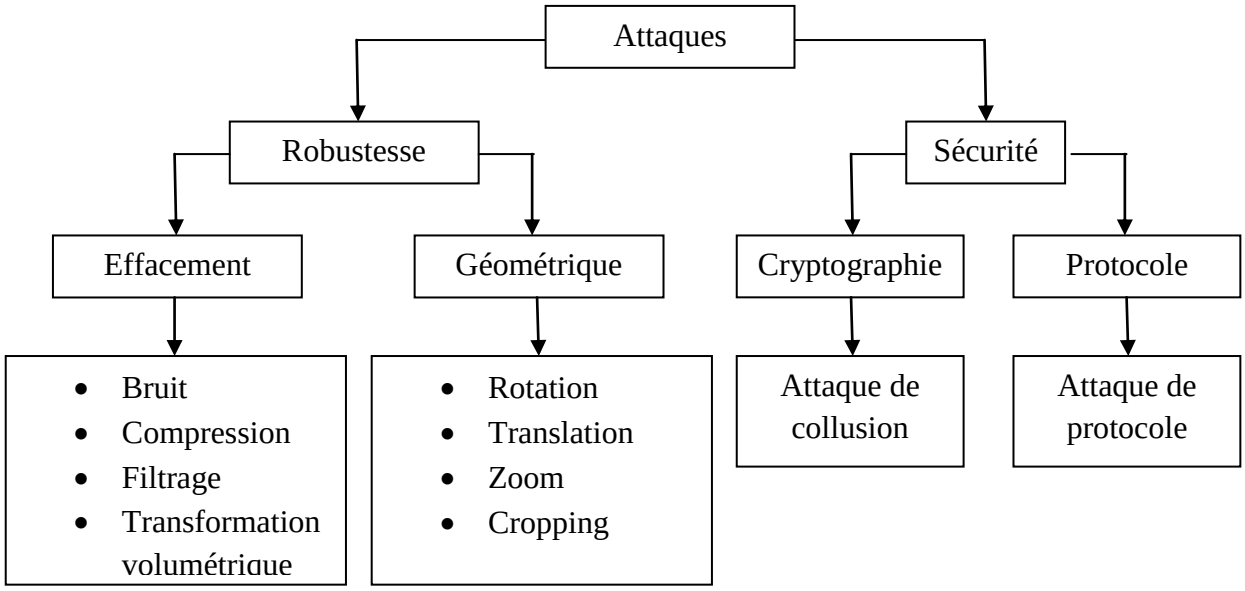



**Figure 1.17** Classification des attaques.

### 1.8.1. L'attaque d'effacement issue des attaques de traitement d'image

Permet de supprimer la marque et s'inspire du domaine de traitement d'image qui tente d'évaluer ou d'estimer l'image originale à partir de l'image tatouée en appliquant plusieurs traitements (compression, lissage, conversion analogique numérique, addition de bruit, filtrage,.....).

#### 1.8.1.1. Le bruitage

En général, on peut définir le bruit, comme étant tout signal non désirable pouvant être combiné avec l'image originale. Dans ce cas, une dégradation visuelle aura lieu ou bien tout simplement une modification du contenu de l'image hôte. Des exemples de bruit artificiel peuvent être :

- Le bruit gaussien qui consiste à un ajout successif de valeurs générées aléatoirement à chaque pixel de l'image.

– Le bruit Salt&Pepper (sel et poivre) qui transforme aléatoirement des pixels de l'image en pixels noir ou blanc.

#### 1.8.1.2. Le filtrage et le lissage

Le filtrage est utilisé dans le cas de l'addition d'un bruit à une image afin de la rendre plus nette, d'où l'amélioration de sa qualité visuelle. Parmi les filtres les plus importants à utiliser on cite le filtre passe-bas, le filtre médian et le filtre Gaussien... Malgré leurs importances, les filtres restent des attaques graves qui peuvent dégrader ou bien même détruire une marque insérée.

#### 1.8.1.3. La compression

Les nécessités d'archivage ou de transmission sur internet des images numériques exigent que nous fassions appel à des outils de compression dans le but de réduire les tailles des fichiers des images dont le format JPEG, une technique de compression avec pertes qui supprime les informations redondantes et les données les moins significatifs de l'image. Dans le domaine du tatouage numérique, les attaques par compression, sont trop dangereuses. En effet, les algorithmes de compression ne gardent de l'image hôte que les composantes essentielles à sa compréhension ce qui n'est pas le cas pour un tatouage invisible.

#### 1.8.1.4. Les transformations volumétriques

Ces attaques consistent à modifier la luminance de l'image par une fonction non-linéaire. Nous distinguons dans ce type d'attaques l'étalement d'histogramme, l'égalisation d'histogramme, la transformation Gamma, etc…

### 1.8.2. Les attaques géométriques

Les transformations géométriques agissent directement soit sur l'aspect visuel de l'image, soit sur la marque. Parmi les plus importants on cite la réduction de la taille de l'image, le cropping, la rotation, la translation, etc. Contrairement aux attaques de suppression, une attaque géométrique ne fait pas enlever la marque insérée, mais tente de déformer la synchronisation de l'extracteur de la marque. Une désynchronisation engendre par des problèmes lors de la phase de détection.

#### 1.8.2.1. La rotation

Des petits angles de rotation appliqués peuvent rendre la marque non détectable.

#### 1.8.2.2. Stirmark

Est une succession de distorsions géométriques aléatoires appliquées dans plusieurs points ou pixels de l'image d'une façon globale ou locale.

#### 1.8.2.3. Cropping

Il consiste à supprimer ou couper une partie de l'image.

#### 1.8.2.4. Scaling (modification des dimensions)

Ce type d'opération est appliqué quand une image numérique (image imprimée est scannée) de haute résolution est utilisée pour des applications électroniques.

### 1.8.3. Les attaques sur la sécurité

Parmi les attaques sur la sécurité nous citons:

#### 1.8.3.1. Les attaques cryptographiques

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

#### 1.8.3.2. Les attaques de protocole

Ces attaques visent à trouver une faille dans le protocole de tatouage, puis d'accéder aux informations confidentielles, ou de tatouer un document avec une fausse marque.
Craver et al.**[Vol01]** ont mentionné une attaque, comme l'attaque d'inversion de la marque ou l'attaque IBM, qui produit un faux schéma de tatouage qui peut être appliqué sur une image tatouée et qui permet à créer un doute sur ce qui a été inséré en premier. L'attaque de copier est un autre type d'attaque de protocole. Dans ce cas, la marque est prédite en utilisant un ensemble de données tatouées. Ce watermark prévu est inséré dans une autre donnée en adaptant les caractéristiques locales pour satisfaire son imperceptibilité.

## 1.9. Évaluation des performances des algorithmes de tatouage de l'image

### 1.9.1. Performance de l'imperceptibilité

L'imperceptible du tatouage est estimée en mesurant le PSNR (Peak Signal to Noise Ratio) [53]. Le PSNR es²t calculé comme suit :

$$PSNR = 10log_{10}(\frac{256^2}{MSE}) \quad (1.3)$$

où MSE est l'erreur quadratique moyenne entre l'image hôte *x* et l'image tatouée *y*. Elle est définie par :

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |x(i,j) - y(i,j)|^2 \quad (1.4)$$

### 1.9.2. Performance de robustesse

La robustesse de tout système de tatouage est une exigence très importante. Pour comparer les similitudes entre le tatouage original $W$ et le tatouage extrait $W'$, nous utilisons le Coefficient Normalisé (NC), le taux d'erreur sur les bits (BER) [53] et le taux de correction de bit (BCR) [54]. Ils consistent à comparer les valeurs des deux images pixel par pixel pour l'évaluation de la similarité entre les deux. Le NC, le BER et le BCR sont respectivement calculés comme suit:

$$NC(W, W') = \sum\sum \frac{W(i,j)W'(i,j)}{|W(i,j)|^2} \quad (1.5)$$

$$BER = \frac{1}{p} \sum_{j=1}^{p} |W'(j) - W(j)| \quad (1.6)$$

où $W$, $W'$ et p représentent le tatouage originale, le tatouage extrait et la taille du tatouage.

$$BCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \overline{W_{ij} \otimes W'_{ij}}}{M \times N} \quad (1.7)$$

où $\otimes$ est l'opérateur « OR » exclusif, $(M, N)$ est la taille du tatouage, $W$ la valeur binaire du tatouage incrusté et $W'$ la valeur binaire du tatouage extrait. La corrélation entre $W$ et $W'$ est très élevée lorsque NC ou bien le BCR est proche de 1.

## 1.10. Conclusion

Dans ce chapitre, nous avons présenté l'état de l'art du tatouage numérique. Nous avons commencé par présenter les périodes historiques les plus marquantes qu'a connues cette science. Puis nous avons discuté de son identification par rapport aux autres techniques : la cryptographie et la stéganographie. Dans le paragraphe 4 nous avons élaboré les principes d'un système de tatouage numérique des images. Les principaux défis dans un système de tatouage, sa classification, ses applications et les différentes attaques menaçant le tatouage numérique ont été présentés, successivement, dans les paragraphes 5, 6, 7 et 8. Le dernier paragraphe de ce chapitre a été destiné aux notions d'évaluation des performances des algorithmes de tatouage de l'image.

# Chapitre 2

# *Tatouage numérique d'images dans le domaine transformé*

## 2.1 Introduction

Le défi et la nécessité de sécuriser parfaitement les informations dans les réseaux de communication modernes ont poussé les chercheurs à accroître les efforts et à développer des techniques de tatouage efficaces. En effet, plusieurs techniques de tatouage ont été proposées dans la littérature et elles sont classées en deux catégories : les techniques temporelles/spatiales et les techniques fréquentielles. Les techniques fréquentielles de tatouage d'images exploitent les algorithmes rapides des transformées discrètes telles que la transformée de Fourier discrète, la transformée en cosinus discrète, la transformée en ondelette, la décomposition en valeurs singulières,…etc. De plus, les transformées paramétriques discrètes qui sont de nouvelles philosophies, et qui peuvent avoir une implémentation relativement commode en hardware, ont été considérées dans la conception des techniques de tatouage d'images. Elles offrent un espace de clés secrètes supplémentaires grâce à leurs paramètres arbitraires [26] - [31].

Dans ce qui suit, nous présentons une technique de tatouage d'image basée sur la transformée de Fourier paramétrique bidimensionnelle (2D-PDFT). Selon la représentation binaire du tatouage, deux séquences pseudo-aléatoires, basées sur une clé secrète, sont incorporées dans l'image de couverture. La technique est aveugle car ni l'image originale ni le tatouage ne sont requis pour la détection. La corrélation est utilisée pour la récupération du tatouage. Nous présenterons aussi une autre technique de tatouage numérique d'images non aveugle basées sur une combinaison entre la décomposition en valeurs singulières (MR-SVD) Multi-résolution et la décomposition en valeurs singulières (SVD). La méthode est performante et offre une très bonne résistance à diverses attaques.

Le chapitre est organisé de la manière suivante : Dans la section 2, nous présentons les transformées du domaine fréquentiel les plus fréquemment utilisées en tatouage numérique d'images ainsi que le contexte théorique de la DFT paramétrique. Nous proposons dans la section 3, une technique de tatouage d'images fragile et aveugle en utilisant la transformée de Fourier discrète paramétrique. Puis, dans la section 4, nous décrivons une technique de tatouage des images basée sur la décomposition en valeurs singulières et sa forme multi-résolution et nous terminons par une conclusion.

## 2.2 Transformées discrètes fréquemment utilisées en tatouage numérique des images.

Les techniques fréquentielles de tatouage d'images qui exploitent les algorithmes rapides des transformées discrètes sont particulièrement robustes comparées aux techniques spatiales. Le domaine de transformation incorpore le tatouage ou marque en modifiant légèrement les coefficients de transformation de l'image originale. Un certain nombre de transformées peuvent être appliquées dans le tatouage des images numériques, mais il en existe notamment quatre qui sont les plus couramment utilisées. Ce sont la transformée de Fourier discrète (DFT), la transformée en cosinus discrète (DCT), la transformée en ondelette (DWT) et la décomposition en valeurs singulières (SVD). Cependant, de nouvelles transformées ont été considérées dans la conception des techniques de tatouage d'images qui seront plus robustes et plus adaptées aux applications récentes des services de communication. Les transformées paramétriques discrètes qui ont une complexité de calculs réduite et qui sont aptes à être implémentées en hardware, peuvent présenter une solution pour une exécution plus rapide ou en temps réel. En plus, les paramètres arbitraires de ces transformées peuvent être exploités comme une clé secrète supplémentaire. Dans ce qui suit nous présentons les transformées que nous avons utilisées dans les techniques de tatouage développées et présentées dans cette thèse.

### 2.2.1. La transformée en cosinus discrète bidimensionnelle (2D-DCT)

La 2D-DCT est la transformée par excellence dans le contexte du traitement des images numériques et du traitement du signal [27]. Elle transforme une image, de sa représentation spatiale à sa représentation fréquentielle. De nombreuses techniques de compression sont développées dans le domaine DCT (JPEG, MPEG, MPEG1 et MPEG2) en raison de son avantage de concentration de l'énergie du signal transformé dans la plage des basses fréquences et de son implémentation facile. Gardant cela à l'esprit, de nombreuses méthodes de tatouage d'images utilisant la 2D-DCT incorporent le tatouage dans la bande des fréquences médianes de l'image originale pour gagner en robustesse face à la compression JPEG. La 2D-DCT est généralement réalisée non pas sur l'image entière mais sur des blocs de taille $8 \times 8$ pixels. En effet la 2D-DCT offre de nombreux atouts :

– Elle présente une bonne localisation fréquentielle et une compaction de l'énergie qui surpasse celle obtenue avec la transformée de Fourrier discrète bidimensionnelle (2D-DFT).

– Elle est facile à implémenter et a, notamment, l'avantage de générer un signal transformé réel.

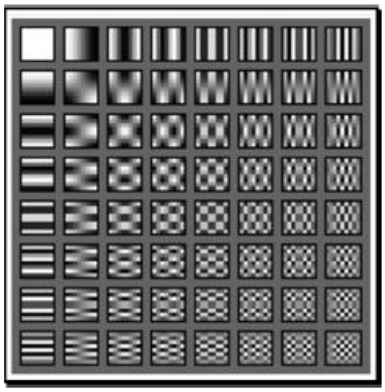


**Figure2.1.** La transformée en cosinus discrète bidimensionnelle d'un bloc $8 \times 8$ de l'image de cameraman.

La **figure 2.2** représente l'image de cameraman et sa 2D-DCT. On remarque que les valeurs les plus élevées se concentrent dans le coin supérieur gauche (basses fréquences) et les valeurs les plus faibles dans le coin inférieur droit (hautes fréquences) [57].

**Figure2.2.** Image Cameraman et sa transformée 2D-DCT.

Pour une image de taille $N \times N$, la 2D-DCT et son inverse 2D-IDCT sont données respectivement par les formules (2.1) et (2.2) [56].

$$F(u,v) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(u)C(v)f(i,j)cos\left[\frac{\pi(2i+1)u}{2N}\right] \times cos\left[\frac{\pi(2j+1)v}{2N}\right] \qquad (2.1)$$

$$f(i,j) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)F(u,v)cos\left[\frac{\pi(2i+1)u}{2N}\right] \times cos\left[\frac{\pi(2j+1)v}{2N}\right] \quad (2.2)$$

avec

$$C(u) = \begin{cases} \sqrt{\frac{1}{N}} & u = 0 \\ \sqrt{\frac{2}{N}} & u = 1,2,\dots N-1 \end{cases} \qquad C(v) = \begin{cases} \sqrt{\frac{1}{N}} & v = 0 \\ \sqrt{\frac{2}{N}} & v = 1,2,\dots N-1 \end{cases} \quad (2.3)$$

### 2.2.2. La transformée en ondelettes discrète bidimensionnelle (2D-DWT)

La transformée en ondelettes bidimensionnelle permet la transformation de l'image du domaine spatiale vers le domaine fréquentiel. Cette transformation est basée sur deux étapes : l'échantillonnage et le filtrage. Le filtrage permet de décomposer l'image en sous bandes passe-haut et passe-bas et l'échantillonnage permet de diminuer la résolution de chaque sous bande **[**29]. La 2D-DWT sépare une image en quatre petites images représentant : (1) une approximation de l'image originale de résolution inférieure (LL) et (2) ses détails horizontaux (HL), verticaux (LH) et diagonaux (HH) (**figures 2.3** et **2.4**).

La sous-bande LL est le résultat d'un filtrage passe-bas sur à la fois les lignes et les colonnes et contient une description approximative de l'image. La sous bande HH est issue d'un filtre passe-haut et contient les composantes hautes fréquences. Les images HL et LH sont des résultats de filtrage passe-bas et passe-haut respectivement. Après le traitement de l'image par la transformée en ondelettes, la plupart des informations de l'image originale sont contenues dans la partie LL. La sous bande LH contient les informations des détails verticaux qui correspondent aux bords horizontaux. La sous bande HL représente les informations des détails horizontaux et relatifs aux bords verticaux. Le processus peut être répété pour calculer plusieurs niveaux de décomposition en ondelettes comme il est illustré dans les **figures 2.3** et 2.4. Pour reconstruire l'image, on calcul l'inverse de la 2D-DWT à partir des quatre sous bandes d'ondelette [29].

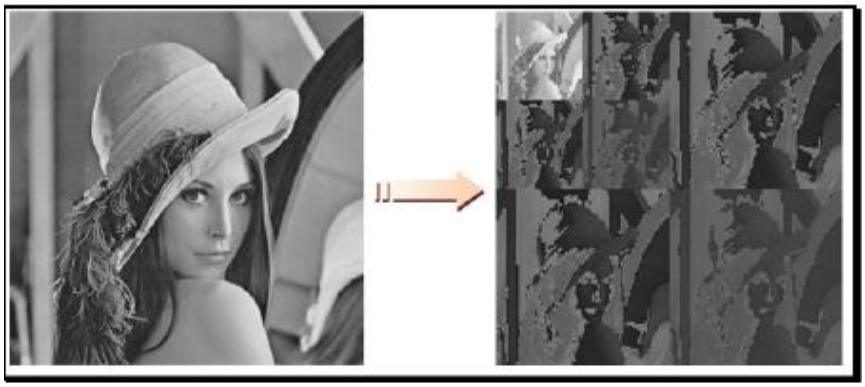


**Figure 2.3** Décomposition en ondelette au 2ème niveau de l'image de Lena.

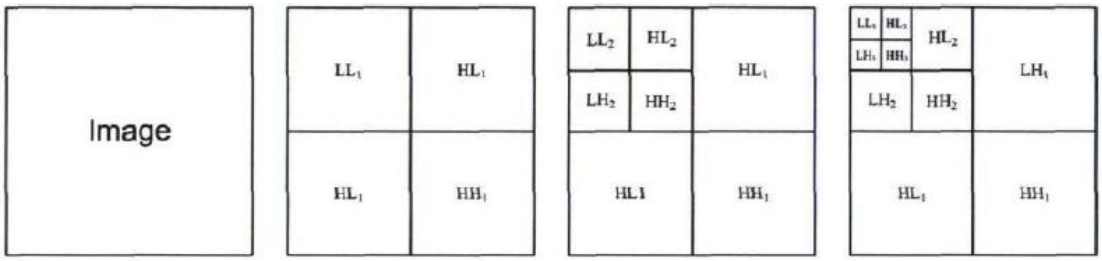



**Figure 2.4** La représentation à échelles séparés d'une décomposition successive par la transformée en ondelettes discrète.

### 2.2.3. La Transformée de Fourier discrète (DFT)

La transformée de Fourier (FT) est l'une des transformées les plus utilisées dans le traitement de signal. Cela est dû essentiellement à sa large utilisation dans un grand nombre d'applications dans plusieurs domaines de la science et de l'ingénierie. C'est une transformée unitaire à valeurs complexes possédant plusieurs propriétés très intéressantes en traitement de signal. [58]. La transformée de Fourier discrète DFT $X(n)$ d'une séquence réelle $x(k)$ de longueur $N$ est définie comme suit :

$$X(n) = \sum_{k=0}^{N-1} x(k) W_N^{nk}, \qquad 0 \leq n \leq N-1 \tag{2.4}$$

et sa transformée inverse est :

$$x(k) = \frac{1}{N} \sum_{n=0}^{N-1} X(n) W_N^{-nk}, \qquad 0 \leq k \leq N-1 \tag{2.5}$$

avec $W_N = e^{-j\frac{2\pi}{N}}$ et $j = \sqrt{-1}$

Pour une image carrée de taille $N \times N$, la transformée de Fourier discrète à deux dimensions (2D-DFT) est donnée par [57] :

$$F(u,v) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j) \cdot e^{-2i\pi(\frac{ui}{N}+\frac{vj}{N})} \quad (2.6)$$

où $f$ est l'image dans le domaine spatial et le terme exponentiel est la fonction de base correspondant à chaque point $F(u,v)$ dans l'espace de Fourier. L'équation peut être interprétée comme étant la valeur de chaque point $F(u,v)$ qui est obtenue en multipliant l'image spatiale par la fonction de base correspondante et en additionnant le résultat. Les fonctions de base sont des ondes sinus et cosinus avec des fréquences croissantes : $F(0,0)$ représente la composante continue de l'image qui correspond à la luminosité moyenne et $F(N-1, N-1)$ représente la fréquence la plus élevée. De même, l'image de Fourier peut être retransformée en domaine spatial. La transformée de Fourier inverse est donnée par:

$$f(a,b) = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} F(k,l) \cdot e^{2i\pi(\frac{ka}{N}+\frac{lb}{N})} \quad (2.7)$$

La DFT d'une image peut être écrite ainsi sous forme matricielle comme suit:

$$X = F_N . x \quad (2.8)$$

Les entrées de $F_N$ sont les facteurs de transformation racines de l'unité (en anglais : twiddle factors) $f_N(n,k)$ obtenus en divisant le cercle unitaire en $N$ points équidistants.

$$f_N(n,k) = W_N^{nk} \quad (0 \leq n,k \leq N-1) \quad (2.9)$$

En organisant ces facteurs dans un vecteur en commençant de $W_N^0 = 1$ et en allant dans le même sens des aiguilles d'une montre, nous obtenons le vecteur du noyau $V_F$ de la DFT.

$$V_F = [1 \quad W_N^1 \quad W_N^2 \ \ldots\ldots\ W_N^{N-1}] \quad (2.10)$$

Les entrées de $F_N$ peuvent être alors exprimées par les éléments de $V_F$ comme suit :

$$f_N(n,k) = v_F(nk \bmod N) \quad (0 \leq n,k \leq N-1) \quad (2.11)$$

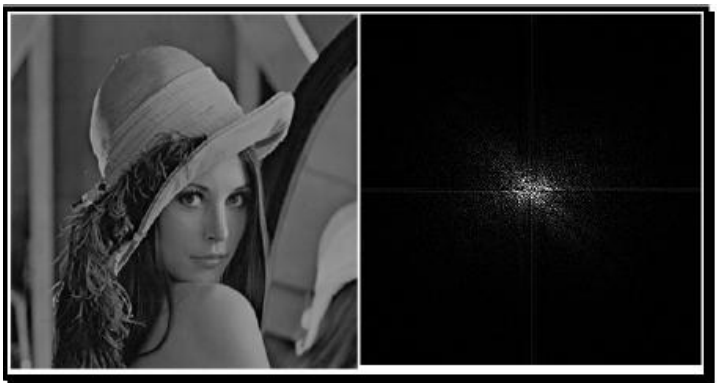


**Figure 2.5** Image de Lena et sa Transformée de Fourier.

### 2.2.4. Transformée de Fourier paramétrique (PDFT)

Ces dernières années, il y a eu un énorme intérêt à développer des versions paramétriques des transformées fixes existantes [59, 60]. Il a été montré dans ces articles que la paramétrisation des transformées peut avoir une plus large gamme d'applications comparées à leurs versions originales et peuvent fournir plus de flexibilité dans la représentation, dans l'interprétation et dans le traitement des signaux [59]. L'importance des paramètres indépendants dans les transformées discrètes peut clairement être vu dans les travaux présentés dans [61-63]. Dans [59], Bouguezel et al. ont introduit des paramètres indépendants dans la DFT en vue de réaliser une meilleure performance dans leurs applications. Dans ce qui suit, nous allons rappeler la construction et le développement mathématiques de cette transformée.

#### 2.2.4.1. Développement mathématique

En se basant sur la transformée de Fourier discrète DFT, Bouguezel et al. ont proposé dans [59] la DFT paramétrique à trois paramètres obtenus en remplaçant convenablement quelques éléments spécifiques dans le vecteur du noyau de la DFT classique par des paramètres indépendants. La DFT paramétrique à trois paramètres est de taille $N$, où $N$ est une puissance de deux, c'est-à-dire $N=2^r$, avec $r$ étant un entier positif $r > 3$ [64]. Elle est définie comme suit:

$$X^{a,b,c}(n) = \sum_{k=0}^{N-1} x(k)\, v_{F^{a,b,c}}(nk \bmod N), \quad 0 \le n \le N-1 \tag{2.12}$$

Sa transformée inverse est donnée par :

$$x(k) = \frac{1}{N}\sum_{n=0}^{N-1} X^{a,b,c}(n)\frac{1}{v_{F^{a,b,c}}(nk \ mod \ N)}, \ \ 0 \le n \le N-1 \tag{2.13}$$

où $v_{F^{a,b,c}}(i)$, $0 \le i \le N-1$, sont les entrées du vecteur noyau (kernel vector) données par :

$$V_{F^{a,b,c}} = [1 \quad V \quad c \quad -jV \quad -1 \quad -V \quad -c \quad jV] \tag{2.14}$$

avec :

$$V = [\, W_N^1 \ \ldots \ W_N^{\left(\frac{N}{16}\right)-1} \ \ a \ \ W_N^{\left(\frac{N}{16}\right)+1} \ \ldots \ W_N^{\left(\frac{N}{8}\right)-1} \ \ b \ \ W_N^{\left(\frac{N}{8}\right)+1} \ldots \ W_N^{\left(\frac{3N}{16}\right)-1} \ \ -ja^* \ \ W_N^{\left(\frac{3N}{16}\right)+1} \ \ldots W_N^{\left(\frac{N}{4}\right)-1} \,] \tag{2.15}$$

$a, b, c$ sont trois paramètres différents de zéro qui peuvent être choisis arbitrairement dans le plan complexe.

$$a = e^{j\alpha} \ , \ b = e^{j\beta} \ et \ c = e^{j\gamma} \tag{2.16}$$

Les équations (2.12) et (2.13) peuvent être écrites sous forme matricielle comme suit :

$$X^{a,b,c} = F_N^{a,b,c}.x \tag{2.17}$$

$$x = (F_N^{a,b,c})^{-1} \cdot X^{a,b,c} \tag{2.18}$$

où $(F_N^{a,b,c})^{-1}$ est la matrice inverse de $F_N^{a,b,c}$

Les éléments de $F_N^{a,b,c}$ sont donnés par:

$$f_N^{a,b,c}(n,k) = v_{F^{a,b,c}}(nk \ mod \ N) \tag{2.19}$$

où $0 \le n,k \le N-1$ et $v_{F^{a,b,c}}(nk)$ sont les éléments du vecteur $V_{F^{a,b,c}}$.

Pour $\alpha = \frac{\pi}{6}$ on tombe sur un cas particulier qui réduit considérablement le nombre de multiplications de la PDFT. L'utilisation de la $F_{16}^{\frac{\pi}{6}}$ dans la 2D-PDFT pour transformer une image de taille $512 \times 512$, divisée en sous-blocs de taille $16 \times 16$, nécessite 4718592 opérations d'addition réels, 524288 multiplications réelles et 262144 opérations de décalage de bits [59, 60]. En revanche, l'utilisation de la matrice DFT nécessite le même nombre

d'additions réelles mais 786432 multiplications. Et puisque la multiplication prend, dans une large mesure, plus de temps qu'une opération de décalage de bits, l'utilisation de $F_{16}^{\frac{\pi}{6}}$ dans notre technique (section 2.3) a été très efficace en ce qui concerne la complexité de calcul.

#### 2.2.4.2. Propriétés de la DFT paramétrique

- La matrice $F_N^{a,b,c}$de la DFT paramétrique est une matrice réciproque-orthogonale qui vérifie l'équation suivante :

$$F_N^{a,b,c} \cdot (F_N^{a,b,c})^{-1} = F_N^{a,b,c} \cdot (F_N^{a,b,c})^{RT} = N \cdot I_N \qquad (2.20)$$

où $(.)^{RT}$ est la matrice réciproque transposée, et $I_N$ est la matrice identité d'ordre $N$.

- L'un des cas particuliers les plus intéressants de la DFT à trois paramètres peut être obtenu lorsque $a = e^{j\alpha}$, avec $\alpha$ étant un paramètre qui peut être choisi arbitrairement dans l'intervalle$[-2\pi, 0]$, $b = W_N^{N/8}$ et $c = W_N^{N/4}$. Ce cas conduit à une DFT à un paramètre notée DFT$^{\alpha}$ qui sera désignée sous forme matricielle par $F_N^{a}$.

- Dans le cas particulier où $a = W_N^{N/16}$, $b = W_N^{N/8}$ et $c = W_N^{N/4}$, la DFT paramétrique devient la transformée de Fourier discrète classique c'est-à-dire: $\alpha = \frac{-\pi}{8}$, $\beta = \frac{-\pi}{4}$ et $\gamma = \frac{-\pi}{2}$.

Soient $x_1(k)$, $x_2(k)$ et $x(k)$ trois séquences complexes ayant comme transformées :

$$x_1(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} X_1^{a,b,c}(n)$$

$$x_2(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} X_2^{a,b,c}(n)$$

$$x(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} X^{a,b,c}(n)$$

$$x(k) \overset{DFT^{\alpha}}{\longleftrightarrow} X^{\alpha}(n)$$

- **Linéarité** : Soient $i$ et $j$ deux constantes arbitraires, nous avons :

$$ix_1(k) + j\,x_2(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} iX_1^{a,b,c}(n) + j\,X_2^{a,b,c}(n)$$

- **Dualité :**

$$x^{\alpha}(k) \overset{DFT^{\alpha}}{\longleftrightarrow} Nx(N-n)$$

- **Symétrie :**

$$x^{*}(k) \overset{DFT^{\alpha}}{\longleftrightarrow} (X^{\alpha}(N-n))^{*}$$

$$x^{*}(N-k) \overset{DFT^{\alpha}}{\longleftrightarrow} (X^{\alpha}(n))^{*}$$

$$Re(x(k)) \overset{DFT^{\alpha}}{\longleftrightarrow} \frac{1}{2}(X^{\alpha}(n) + \left(X^{\alpha}(N-n)\right)^{*})$$

$$j \times Im(x(k)) \overset{DFT^{\alpha}}{\longleftrightarrow} \frac{1}{2}(X^{\alpha}(n) - \left(X^{\alpha}(N-n)\right)^{*})$$

$$\frac{1}{2}\left(x(n) + \left(x(N-k)\right)^{*}\right) \overset{DFT^{\alpha}}{\longleftrightarrow} Re(X^{\alpha}(n))$$

$$\frac{1}{2}\left(x(k) + \left(x(N-k)\right)^{*}\right) \overset{DFT^{\alpha}}{\longleftrightarrow} j \times Im(X^{\alpha}(n))$$

avec $Re(.)$: partie réelle et $Im(.)$: partie imaginaire.

- **Propriétés de symétrie pour les séquences réelles:**

$$s(k) \overset{DFT^{\alpha}}{\longleftrightarrow} F^{\alpha}(n) = (F^{\alpha}(N-n))^{*}$$

$$\frac{1}{2}\left(s(k) + s(N-k)\right) \overset{DFT^{\alpha}}{\longleftrightarrow} Re(F^{\alpha}(n))$$

$$\frac{1}{2}\left(s(k) + \left(s(N-k)\right)\right) \overset{DFT^{\alpha}}{\longleftrightarrow} j \times Im(F^{\alpha}(n))$$

### 2.2.5. La décomposition en valeurs singulières (SVD)

La décomposition en valeurs singulières SVD est un sujet important dans le domaine de l'algèbre linéaire pour de nombreux mathématiciens. Elle trouve son utilité dans plusieurs applications telles que la compression d'images et le tatouage [64-66]. La particularité de la SVD est qu'elle peut être effectuée sur des matrices réelles, par exemple une image $M$ de taille $N \times N$ qui est décomposée en un produit de trois matrices spécifiées par l'équation (2.21).

$$M = U \cdot S \cdot V^T \tag{2.21}$$

où $S$ est une matrice diagonale, c'est-à-dire $S = diag(\lambda_1, \lambda_2, \dots, \lambda_N)$ avec $\lambda_i$ des valeurs réelles positives appelées valeurs singulières de $M$ et satisfaisant $\lambda_1 > \lambda_2 > \cdots > \lambda_N$. $U$ et $V$ sont des matrices orthogonales, c'est-à-dire $U^T \cdot U = V^T \cdot V = I_N$. Les colonnes de $U$ et celles de $V$ sont appelées respectivement les vecteurs singulier gauche et singulier droit de $M$. $M$ peut être également écrite comme suit :

$$M = \lambda_1 \cdot U_1 \cdot V_1^T + \lambda_2 \cdot U_2 \cdot V_2^T + \dots \lambda_r \cdot U_r \cdot V_r^T \tag{2.22}$$

où *r* est le rang de la matrice *M*.

Lorsque la SVD est appliquée sur une image composée de plusieurs calques ou couches, il est important de noter que chaque valeur singulière spécifie la luminance d'un calque de l'image, tandis que la paire de vecteurs singuliers correspondante spécifie la géométrie de celui-ci.

Dans la SVD, la matrice $U$ montre deux caractéristiques importantes liées aux éléments de la première colonne: tous ces éléments ont le même signe et leurs valeurs sont très proches. Ceci est montré dans l'exemple suivant avec une matrice $M$ de taille $4 \times 4$ issue d'une image [10] :

$$M = \begin{bmatrix} 76 & 77 & 79 & 87 \\ 82 & 86 & 86 & 95 \\ 74 & 75 & 76 & 84 \\ 77 & 79 & 82 & 83 \end{bmatrix}$$

Après application de la SVD à la matrice, on obtient la matrice $U$ suivante:

$$U = \begin{bmatrix} -0.4912 & -0.2831 & -0.4798 & -0.6696 \\ -0.5374 & -0.3098 & 0.7835 & -0.0362 \\ -0.4757 & -0.2601 & -0.3948 & 0.7418 \\ -0.4936 & 0.8696 & 0.0048 & -0.0091 \end{bmatrix}$$

### 2.2.6. Décomposition en valeurs singulières multi-résolution

La MR-SVD représente un signal sous la forme d'une série d'approximations et de détails comme la 2D-DWT. Cette section explique le fonctionnement de la MR-SVD, introduit dans [67].

#### 2.2.6.1. Décomposition en valeurs singulières multi-résolution unidimensionnelle (1D)

Soit $X = [x\,(1) \ldots x\,(N)]$ qui représente un signal 1D d'étendue finie. Supposons que $N$ est divisible par $2L$ avec $L \geq 1$. Supposons que la matrice de données du premier niveau, notée $X_1$, soit construite de manière à ce que sa rangée supérieure contienne les échantillons à nombres impairs et que la rangée inférieure contienne les échantillons à nombres pairs comme suit:

$$X_1 = \begin{pmatrix} x(1) & x(3) \cdots & x(N-1) \\ x(2) & x(4) & x(N) \end{pmatrix}$$

Soit $U_1$ la matrice de vecteurs propres amenant la matrice de dispersion $T_1 = X_1$ sous forme diagonale:

$$U_1^T \cdot T_1 \cdot U_1 = S_1^2 \tag{2.23}$$

où $S_1^2 = diag\,\{s_1^2\,(1)\,, s_1^2\,(2)\}$ contient les carrés des deux valeurs singulières, avec $s_1(1) \geq s_1(2)$.

On pose :

$$X'_1 = U_1^T \cdot X \tag{2.24}$$

La rangée supérieure de $X'_1$, notée $X'_1(1,:)$, contient le composant d'approximation qui correspond à la plus grande valeur propre. La rangée inférieure de $X'_1$, notée $X'_1(2,:)$, contient le composant de détail qui correspond à la plus petite valeur propre.

Soit $\Phi_1 = X'_1$ (1, :) et $\Psi_1 = X'_1$ (2, :) les composantes d'approximation et de détail respectivement. Les niveaux de décomposition successifs répètent la procédure décrite ci-dessus en plaçant la composante d'approximation $\Phi_1$ à la place de $X$. La MR-SVD peut donc s'écrire comme suit:

$$X \rightarrow \{\Phi_L, \{\Psi_1\}_{l=1}^{L}, \{U_1\}_{l=1}^{L}\} \tag{2.25}$$

où $L$ est le niveau souhaité de la décomposition

#### 2.2.6.2. Décomposition en valeurs singulières multi-résolution bidimensionnelle (2D)

Nous décrivons brièvement ici la 2D-MR-SVD. La décomposition du premier niveau de l'image se déroule comme suit : Diviser l'image $X$ de taille $M \times N$ en blocs de taille $2 \times 2$ non chevauchants puis arranger chaque bloc dans un vecteur $4 \times 1$ en empilant les colonnes pour former la matrice de données $X_1$. Comme exemple, la décomposition propre de la matrice de diffusion $4 \times 4$ est:

$$T_1 = X_1 \cdot X_1^T = U_1 \cdot S_1^2 \cdot U_1^T \tag{2.26}$$

$$X'_1 = U_1^T \cdot X_1 \tag{2.27}$$

La rangée supérieure de la matrice résultante, $X'_1(1, :)$, est réorganisée pour former une matrice $\frac{M}{2} \times \frac{N}{2}$ qui est considérée comme la composante lisse (approximation) de l'image. Les lignes restantes de, $X'_1(2, :)$, $X'_1(3, :)$, $X'_1(4, :)$ contiennent les composants de détails, qui sont indiqués respectivement. La transformation complète peut être représentée comme suit:

$$X \rightarrow \{\Phi_L, \{\Psi_1^1, \Psi_1^2, \Psi_1^3\}_{l=1}^{L}, \{U_1\}_{l=1}^{L}\} \tag{2.28}$$

L'image originale $X$ peut être reconstruite à partir des composantes de la dernière étape, car les calculs sont réversibles.

À titre d'exemple, la décomposition à un seul niveau de l'image de Cameraman par MR-SVD à l'aide d'un programme écrit en Matlab est illustrée sur la **figure 2.3**.

$(a)$ $(b)$

**Figure 2.6** (a) Image de Cameraman originale, (b) sa forme 2D-MR-SVD à un seul niveau.

## 2.3 Technique de tatouage aveugle d'images basée sur la transformée de Fourier discrète paramétrique

Dans cette section, une technique de tatouage numérique d'images utilisant la transformée de Fourier discrète paramétrique est décrite. Cette transformée surpasse la transformée de Fourier discrète classique en termes de complexité de calcul. Selon la représentation binaire du tatouage, deux séquences pseudo-aléatoires, basées sur une clé secrète, sont incorporées dans l'image de couverture. La technique est aveugle car ni l'image originale ni la marque ne sont requises dans la phase d'extraction. La corrélation est utilisée pour la détection de la marque. La méthode proposée est robuste contre diverses attaques telles que la compression JPEG, l'addition de bruit et le filtrage comme le montreront les résultats de simulation. Les deux sous-sections ci-dessous fournissent des informations détaillées sur les étapes des processus d'insertion et d'extraction du tatouage. Dans notre schéma de tatouage, l'image originale est d'abord décomposée en sous-blocs de taille $16 \times 16$ et $F_N^\alpha$ se réduit à $F_{16}^\alpha$ .

### 2.3.1 Algorithme d'insertion du tatouage

Le schéma de l'algorithme d'incorporation de la marque est présenté sur la **figure 2.7**.

1. Deux séquences pseudo-aléatoires non corrélées ($X$ et $Y$) basées sur une clé secrète choisie sont générées. Ces séquences seront intégrées à l'image originale dans certaines conditions (décrites ci-dessous) liées à l'image de la marque. Le choix de deux séquences au lieu d'une seule vise à augmenter efficacement le taux de détection lors du processus d'extraction.

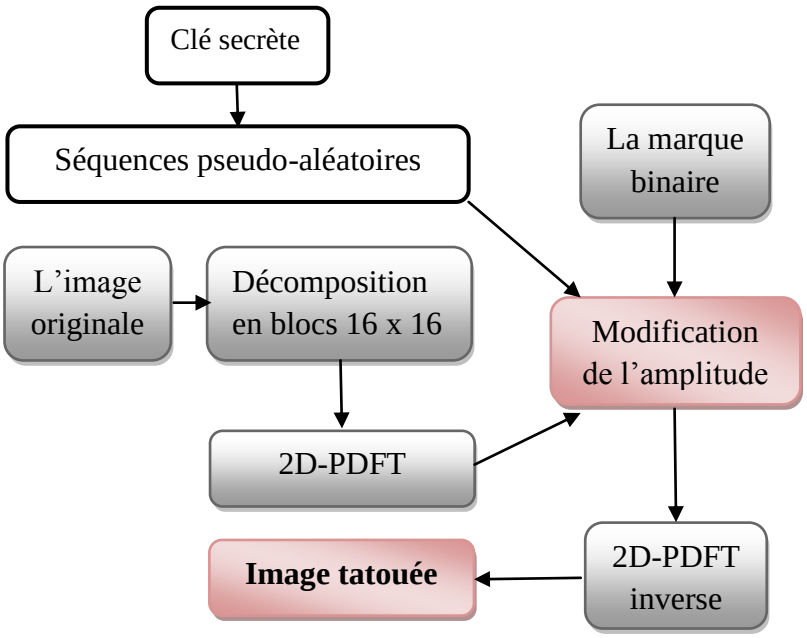



**Figure 2.7** Processus d'insertion de la marque.

2. La matrice de la marque, est réorganisée sous forme vectorielle.
3. L'image originale est divisée en blocs de taille $16 \times 16$ pixels et la transformation 2D-PDFT est exécutée sur chacun d'eux. Un décalage «FFT-shift» est ensuite effectué, en positionnant les composantes continues (CC) au centre du spectre. Les éléments CC ne doivent pas être touchés dans le processus de tatouage pour des raisons de visibilité (dans le programme de simulation, un masque de filtre $16 \times 16$ adéquat sera utilisé). La longueur du vecteur tatouage doit être égale au nombre de blocs. En effet, le tatouage de chaque bloc est directement lié à la valeur d'un bit du tatouage.
4. En fonction de la valeur 0 ou 1 d'une entrée du vecteur de tatouage, l'une des séquences pseudo-aléatoire, $X$ ou $Y$, sera intégrée dans les éléments correspondants du spectre d'amplitude de l'image originale. L'incorporation est basée sur l'équation donnée par (2.29). Le facteur $\beta$ représente la force d'intégration et a une influence directe sur la robustesse et la visibilité du tatouage. Un facteur élevé de $\beta$ améliore la robustesse mais la marque devient visible. Un faible facteur $\beta$ a un résultat opposé.

$$Abs\left[PDFT2\left(bloc(i,j)\right)\right] = Abs\left[PDFT2\left(block(i,j)\right)\right] * \left(1 + \beta * sequence\ (k)\right) \quad (2.29)$$

5. Un décalage «FFT-shift» de la 2D-PDFT inverse est effectué pour obtenir le bloc d'image tatouée.
6. L'image tatouée est construite en utilisant tous les blocs tatoués.

### 2.3.2 Algorithme d'extraction du tatouage

Dans le processus d'extraction (**figure 2.8**), seules l'image tatouée et la clé secrète sont nécessaires.

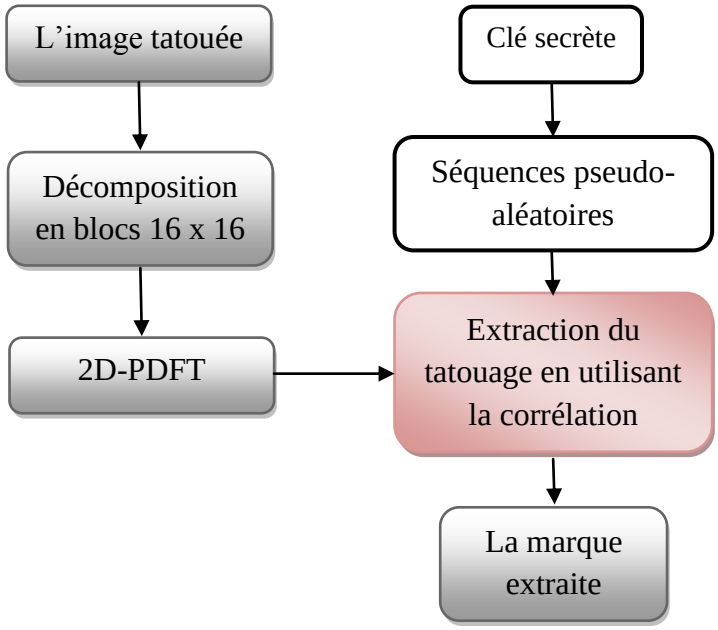



**Figure 2.8** Processus d'extraction de la marque.

1. Les deux mêmes séquences pseudo-aléatoires non corrélées utilisées dans le processus d'insertion sont régénérées à l'aide de la clé secrète utilisée dans la phase d'insertion.
2. L'image tatouée est divisée en blocs de taille $16 \times 16$ et la transformation 2D-PDFT est exécutée sur chacun d'eux suivie d'un décalage «FFT-shift».
3. Grace à l'utilisation du masque de filtrage de taille $16 \times 16$ pour chaque bloc, une séquence est récupérée selon le principe de l'opération d'intégration (étape 4 du processus d'insertion). En utilisant la corrélation entre cette séquence et les séquences pseudo-aléatoires générées par la clé secrète, le vecteur de la marque est reconstruit, c'est-à-dire que si la séquence du tatouage incorporé est plus corrélé avec $X$ qu'avec $Y$, le bloc a été incorporé avec la séquence $X$ (0 dans le vecteur de tatouage) et s'il est plus corrélé avec $Y$, le bloc a été incorporé avec la séquence $Y$ (1 dans le vecteur de tatouage). Puisque nous utilisons MATLAB pour coder notre algorithme, la fonction « $corr2$ » est utilisée pour calculer cette corrélation. Le vecteur de tatouage est ensuite extrait et, à l'aide de la taille du tatouage originale, le vecteur est converti

en une matrice qui représente la marque extraite et qui a la même taille que la marque insérée.

### 2.3.3 Résultats expérimentaux

Dans la simulation du programme, nous avons utilisé une image en niveaux de gris Lena de taille $512 \times 512$ pixels et une image binaire de taille $32 \times 32$ pixels pour la marque incorporée. La performance de la technique proposée est évaluée en termes d'imperceptibilité en utilisant le PSNR (voir équation 1.5) et de robustesse en utilisant le NC (voir équation 1.3). Pour un facteur d'intégration $\beta = 0.7$, le PSNR entre l'image originale et l'image tatouée était de 56,9696 dB, comme indiqué sur la **figure 2.9**. Cette valeur de PSNR relativement élevée prouve l'imperceptibilité du schéma.

$(a)$ $(b)$

$$PSNR = 56.9696$$

$(c)$ $(d)$

$$NC = 1$$

**Figure 2.9** (a) Image originale de Lena, (b) image tatouée (β = 0,7).

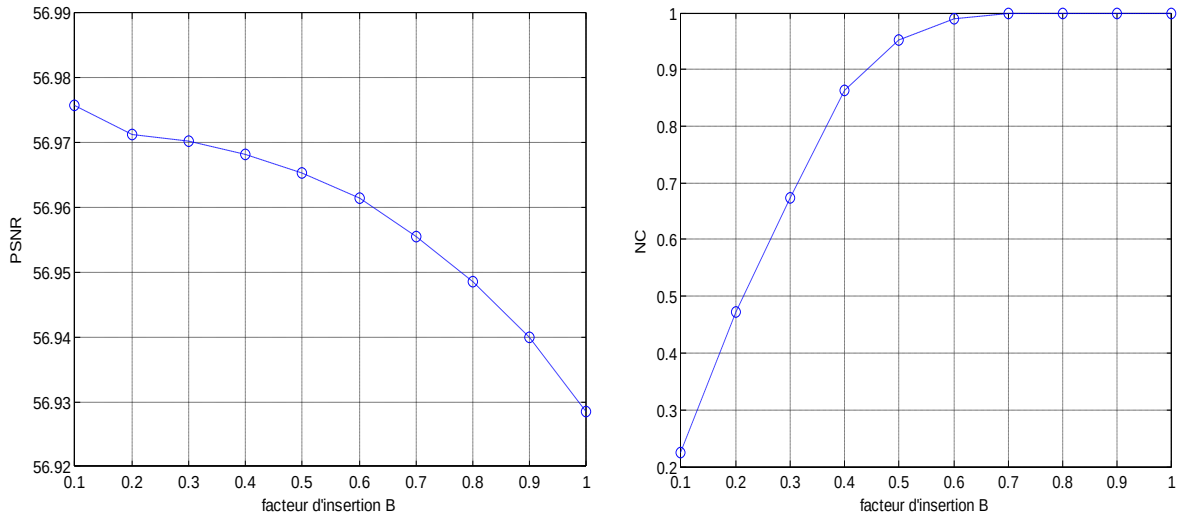
(c) Marque insérée, (d) marque extraite.

En se référant à la **figure 2.9** nous constatons visuellement qu'il n'y a aucune différence entre l'image originale et l'image tatouée ni entre la marque insérée et extraite. Cette constatation reste subjective et nécessite une argumentation scientifique à travers les mesures objectives du PSNR et du NC. Le tableau ci-dessous présente les valeurs du PSNR ainsi que les valeurs du NC correspondantes. Il est clair que l'ordre de grandeur pour les mesures du

PSNR pour différentes valeurs de $\beta$ est d'une moyenne de 56.95852 qui est une valeur très satisfaisante en tatouage d'image et qui prouve la confirmation du critère d'imperceptibilité de notre algorithme proposé et son efficacité à insérer la marque désirée sans altérer la qualité visuelle de l'image originale. Cela d'une part, d'autre part les valeurs du NC sont très proches de 1 pour les valeurs allant de 0.5 à 1. Ce qui confirme la grande ressemblance entre la marque insérée et la marque récupérée pour ces valeurs de $\beta$.

| $\beta$ | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| **PSNR** | 56.9758 | 56.9713 | 56.9703 | 56.9683 | 56.9653 | 56.9615 | 56.9556 | 56.9486 | 56.9400 | 56.9285 |
| **NC** | 0.2255 | 0.4721 | .6738 | 0.8636 | 0.9520 | 0.9888 | 1 | 1 | 1 | 1 |

**Tableau 2.1** Mesures des PSNR et NC pour différentes valeurs de $\beta$.



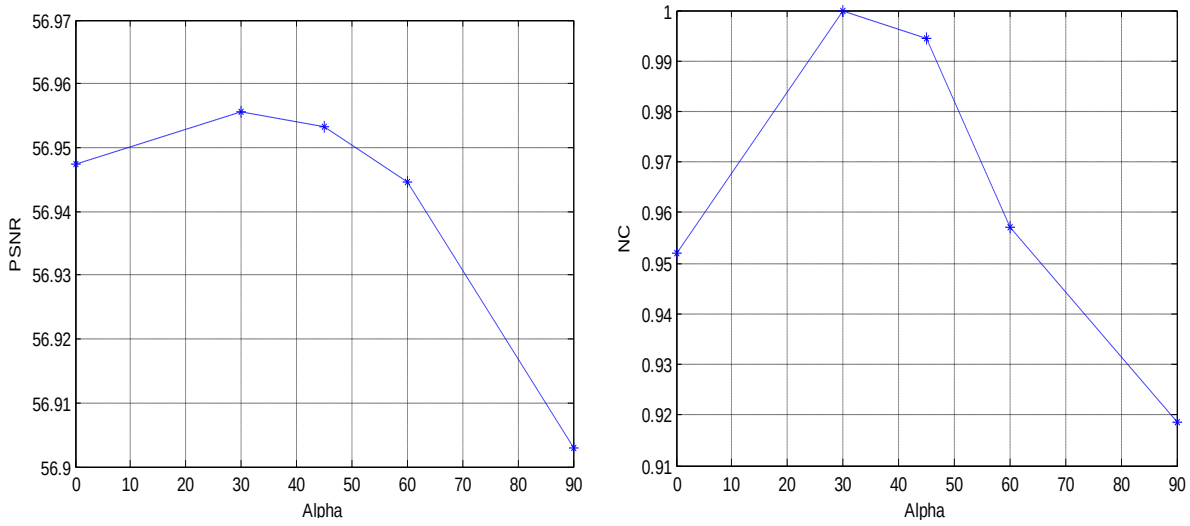

$(a)$ $(b)$

**Figure 2.10** $(a)$ Mesure du PSNR en fonction de $\beta$, $(b)$ mesure de NC en fonction de $\beta$.

Le **tableau 2.2** illustre les mesures expérimentales du PSNR et du NC pour différentes valeurs de l'angle $\alpha$. Il est bien clair que les valeurs du PSNR varient entre 56.7408 et 56.9556. Ces grandeurs sont fortement souhaitables dans le domaine du tatouage d'images, ce qui nous permet de qualifier l'algorithme proposé d'imperceptible et ayant un meilleur résultat pour $\alpha = -\frac{\pi}{6}$. Quant aux mesures du NC, elles sont tout proche de 1. Ce qui est traduit par la forte ressemblance entre la marque originale et celle extraite et il garde sa meilleure performance pour $\alpha = -\frac{\pi}{6}$.

| **Alpha ($\alpha$) en radian** | $-\frac{\pi}{6}$ | $-\frac{\pi}{4}$ | $-\frac{\pi}{3}$ | $-\frac{\pi}{2}$ | $-\pi$ |
|---|---|---|---|---|---|
| **PSNR (dB)** | 56.9556 | 56.9533 | 56.9447 | 56.9029 | 56.7408 |
| **NC** | 1 | 0.9943 | 0.9570 | 0.9185 | 0.9520 |

**Tableau 2.2** Valeurs du PSNR et de NC pour différentes valeurs de $\alpha$.




$(a)$ $(b)$

**Figure 2.11** (a) Valeurs du PSNR en fonction de $\alpha$, (b) valeurs du NC en fonction de $\alpha$.

| **Attaques** | **Tatouage récupéré** | **NC** |
|---|---|---|
| **Compression JPEG à 25%** |  | 0.8149 |
| **Bruit gaussien à 1%** |  | 0.8519 |
| **Bruit uniforme** |  | 0.8938 |
| **Bruit random à 5%** |  | 0.8634 |
| **Le fitre sharpen** |  | 0.9281 |
| **Le filtre median** |  | 0.8533 |

**Tableau 2.3** Mesures de NC ainsi que les images de la marque extraite après différentes attaques.

Pour tester la robustesse de la technique proposée, nous avons appliqué plusieurs attaques sur l'image tatouée telles que la compression JPEG, l'ajout de bruit et le filtrage. Nous avons mesuré le coefficient de corrélation entre la marque originale et la marque extraite suite à chaque attaque. Le **tableau 2.3** récapitule les mesures des coefficients de corrélation ainsi que la présentation de l'image de la marque extraite. La méthode proposée est robuste contre toutes ces attaques.

## 2.4 Une technique de tatouage des images basée sur la décomposition en valeurs singulières et sa forme multi-résolution

Dans cette section, nous présentons une technique de tatouage numérique d'images qui utilise une combinaison entre la SVD et la MR-SVD. L'utilisation de la MR-SVD assurera une meilleure résistance à la compression JPEG en prenant en compte l'aspect HVS (Human Visual System). La technique est appliquée aux images en niveaux de gris. Dans ce qui suit, des informations détaillées sur les étapes des processus d'insertion et d'extraction sont présentées.

### 2.4.1 Principe de l'algorithme d'incorporation de la marque

Soit $W$ l'image de la marque. La phase d'insertion est illustrée sur la **figure 2.12**.

1) La décomposition MR-SVD à un seul niveau est appliquée à l'image pour obtenir des composantes d'approximation $\Phi$ et de détails: $\{\Psi_1, \Psi_2, \Psi_3\}$.
2) La SVD est appliquée sur la composante $\Phi$ du MR-SVD de l'image originale.

$$\Phi = U_\Phi \cdot S_\Phi \cdot V_\Phi^T \tag{2.30}$$

3) La marque $W$ est ajoutée à la matrice $S_\Phi$ à l'aide d'un facteur secret $\beta$ appelé force de tatouage.

$$E = S_\Phi + \beta \cdot W \tag{2.31}$$

4) La SVD est appliquée sur la matrice E

$$E = U \cdot S_w \cdot V^T \tag{2.32}$$

5) La SVD inverse est appliquée aux valeurs singulières modifiées $S_w$ et aux valeurs $(U_\Phi, V_\Phi)$, obtenues à partir de (2.30), pour construire la partie d'approximation modifiée $\Phi_w$.

$$\Phi_w = U_\Phi \cdot S_w \cdot V_\Phi^T \tag{2.33}$$

6) La MR-SVD inverse est appliquée sur la partie d'approximation modifiée pour obtenir l'image tatouée.

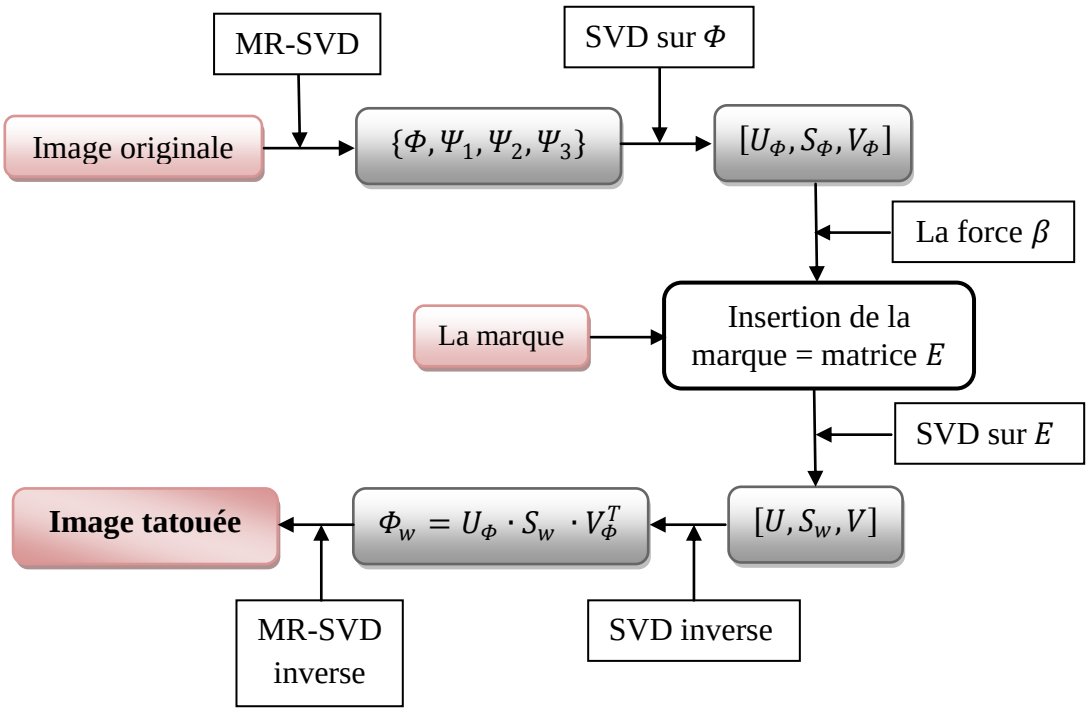



**Figure 2.12** Schéma bloc de la phase d'insertion.

### 2.4.2 Principe de l'algorithme d'extraction de la marque

La phase d'insertion de l'algorithme de notre technique de tatouage est illustrée sur la **figure 2.13.**

1) La décomposition MR-SVD à un seul niveau est appliquée à l'image tatouée pour obtenir des composantes d'approximation $\Phi_w$ et de détails: $\{\Psi_{w1}, \Psi_{w2}, \Psi_{w3}\}$.
2) La décomposition MR-SVD à un seul niveau est appliquée à l'image originale pour obtenir des composantes d'approximation $\Phi$ et de détails: $\{\Psi_1, \Psi_2, \Psi_3\}$.
3) La SVD est appliquée à la composante $\Phi_w$ de l'image tatouée :

$$\Phi_w = U_w \cdot S_w \cdot V_w^T \tag{2.34}$$

4) La SVD est appliquée à la composante $\Phi$ de l'image originale :

$$\Phi = U \cdot S \cdot V^T \tag{2.35}$$

5) Calculer la matrice D telle que :

$$D = S + \beta \cdot W \tag{2.36}$$

6) La SVD est appliquée à la matrice $D$ :

$$D = U_D \cdot S_D \cdot V_D^T \tag{2.37}$$

7) Création de la matrice $D'$ telle que :

$$D' = U_D \cdot S_w \cdot V_D^T \tag{2.38}$$

8) La marque est extraite de l'image tatouée comme suit :

$$W' = \frac{D' - S_\Phi}{\beta} \tag{2.39}$$

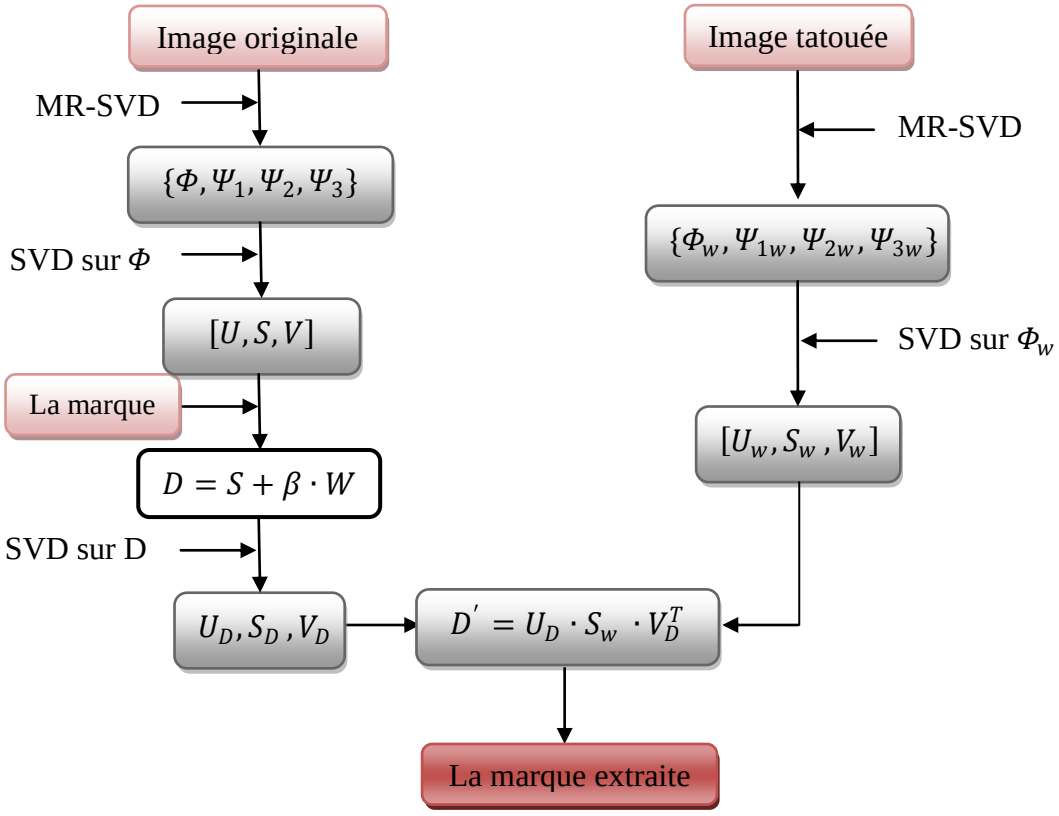
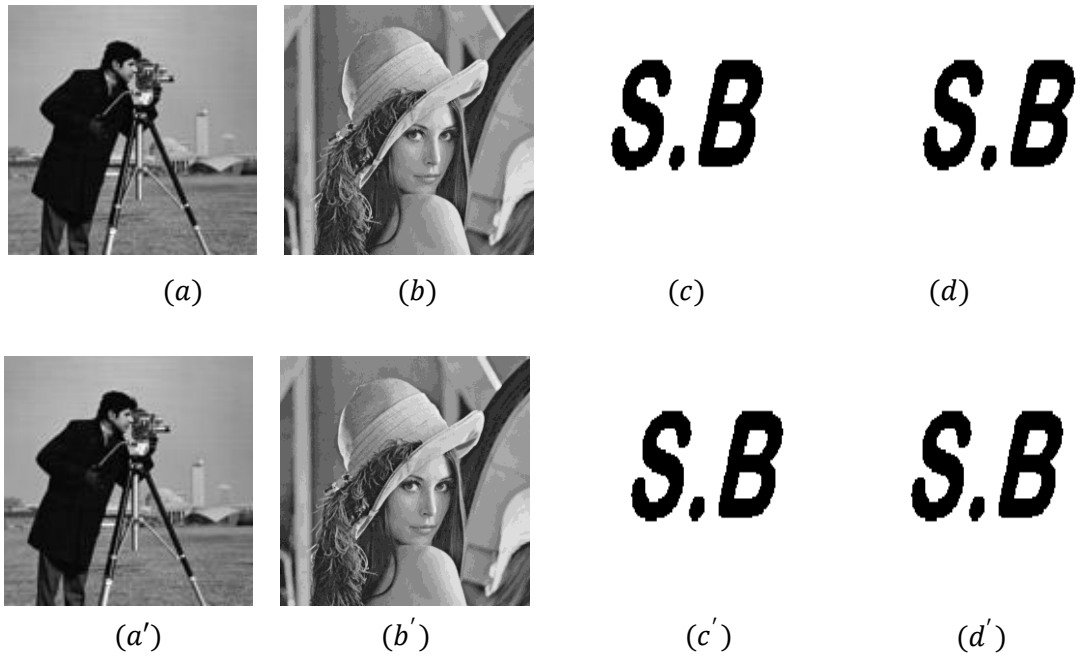



**Figure 2.13** Schéma bloc de la phase d'extraction.

### 2.4.3 Résultats expérimentaux

Les simulations sont faites en utilisant des images de test standard de Lena de taille $512 \times 512$ et de Cameraman de taille $256 \times 256$ pixels comme images originales et des images de taille $256 \times 256$ et $128 \times 128$ valeurs binaires comme des marques pour tatouer les

images précédentes respectivement sous environnement Matlab. La performance de cette technique est évaluée en termes d'imperceptibilité et de robustesse pour une force de tatouage $\beta = 9$. Les PSNR entre l'image originale et l'image tatouée qui est de l'ordre de 52.26649 pour l'image Cameraman et 51.0068 pour l'image Lena, comme indiqué sur la **figure 2.14**, sont relativement élevés et prouve l'imperceptibilité de cette technique.




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

$(a')$ $(b')$ $(c')$ $(d')$

**Figure 2.14** Images originales de : $(a)$ Cameraman $(b)$ lena, $(c)$ et $(d)$ marques originales. Images tatouées de : $(a')$ Cameraman tatouée, $(b')$ Lena tatouée, $(c')$ et $(d')$ tatouages récupérés.

Les **tableaux 2.4** et **2.5** confirment la relation entre la force et les performances du tatouage. En effet nous constatons qu'il y a une proportionnalité remarquable entre le NC et $\beta$ qui se traduit par une augmentation de robustesse à chaque fois que la force du tatouage augmente. Toutefois nous remarquons une proportionnalité inverse entre le PSNR et $\beta$ qui s'interpréte par diminution de l'imperceptibilité à chaque fois que cette force de tatouage augmente.

| $\beta$ | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|
| **PSNR** | 58.6320 | 56.5447 | 54.9562 | 53.5438 | 52.26649 | 51.0148 |
| **NC** | 0.9978 | 0.9993 | 0.9996 | 0.9996 | 0.9996 | 1 |

**Tableau 2.4** Mesures des PSNR et NC pour différentes valeurs de $\beta$ pour l'image de Cameraman.

| $\beta$ | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|
| **PSNR** | 58.9776 | 56.2701 | 54.2160 | 52.4971 | 51.0068 | 49.7997 |
| **NC** | 0.9966 | 0.9986 | 0.9993 | 0.9999 | 1 | 1 |

**Tableau 2.5** Mesures de PSNR et NC pour différentes valeurs de $\beta$ pour l'image de Lena.

Toute image tatouée peut être corrompue pendant la transmission par plusieurs attaques telles que le bruit, le filtrage et la compression. Pour vérifier la robustesse de cette technique de tatouage d'image, on applique à l'image tatouée de Lena la compression JPEG, le filtrage (filtre median et sharpen) et on lui ajoute le bruit gaussien, salt and pepper et Speckle. Les valeurs du NC ainsi que les images de la marque extraite pour chaque cas sont représentées dans le **tableau 2.6.** En examinant les résultats de ce tableau et des **tableaux 2.4** et **2.5**, nous constatons que cette technique est performante en termes de robustesse et d'imperceptibilité.

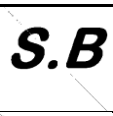
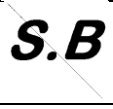
| L'attaque appliquée | La marque extraite | NC |
|---|---|---|
| **Compression JPEG à 90%** |  | 0.9931 |
| **Salt and pepper à 10%** |  | 0.9101 |
| **Le bruit gaussian à 1%** |  | 0.9864 |
| **Le bruit Speckle à 20%** |  | 0.8713 |
| **Le filtre Sharpen** |  | 0.9990 |
| **Le filtre median** |  | 0.9870 |

**Tableau 2.6** Mesures de NC ainsi que les images de la marque extraite après différentes attaques.

## 2.5 Conclusion

Dans ce chapitre, nous avons commencé par la présentation des transformées les plus utilisées dans le domaine du tatouage numérique des images, puis nous avons exposé deux méthodes de tatouage numérique. La première est une technique de tatouage aveugle (car elle nécessite uniquement l'image tatouée lors de phase d'extraction) qui introduit l'utilisation de

la transformée de Fourier discrète paramétrique bidimensionnelle. Nous avons incorporé une marque binaire dans l'image originale à l'aide de deux séquences pseudo-aléatoires non corrélées $X$ et $Y$ . Si la valeur du vecteur de la marque insérée est égale à 0 on utilise la séquence $X$ pour incorporer la marque dans l'image originale, sinon on utilise la séquence $Y$. La deuxième technique non aveugle (car elle nécessite l'image originale, l'image tatouée ainsi que la marque inséré) est basée sur une combinaison entre la SVD et la MR-SVD. L'utilisation de ces deux transformées offre une très bonne robustesse contre les attaques, spécialement la compression JPEG, l'ajout de bruit et le filtrage.

Dans le chapitre suivant, nous allons proposer une nouvelle approche entièrement différente de celles proposées dans ce chapitre, car elle est basée sur la sélection des blocs adéquats pour l'incorporation de la marque.

# Chapitre 3

# *Nouvelle technique de tatouage numérique basée sur la diffusion anisotrope*

## 3.1. Introduction

Le tatouage numérique des images est une discipline qui a connu ces dernières années un essor remarquable. De nombreuses techniques de tatouage ont été développées spécialement au niveau de l'image fixe. Bien que plusieurs méthodes ont été déjà étudiées et validées, malheureusement jusqu'à maintenant aucune d'entre elles n'est totalement robuste à toutes les attaques connues (bienveillantes et malveillantes). Dans ce cadre, et à la lumière des travaux existants, nous proposons une nouvelle approche hybride utilisant la SVD et la 2D-DCT comme espace d'insertion pour dissimuler une marque dans l'image originale. La nouveauté introduite dans notre méthode est d'exploiter de manière avantageuse la technique de diffusion anisotrope de Perona-Malik dans le tatouage d'images. Cette technique, qui trouve son utilisation principale dans le domaine du débruitage d'images, a été utilisée dans notre méthode lors de la sélection des blocs à tatouer de l'image originale afin de conserver la qualité psycho-visuelle de l'image à tatouer. L'incrustation du tatouage est effectuée dans un nombre limité de régions de l'image à tatouer. Les régions choisies pour accueillir la marque présentent une concentration de bords relativement élevée car le Système Visuel Humain (HVS) est moins sensible dans les régions texturées, les bords et les régions à changement rapide [68].

Dans ce chapitre, nous présentons la diffusion de Perona – Malik ainsi que son développement mathématique. Nous exposons ensuite l'algorithme de tatouage proposé, avec ses phases d'insertion et d'extraction, puis nous discutons les résultats expérimentaux des images aux niveaux de gris ainsi que les images couleurs. Des conclusions sont présentées dans la dernière section.

## 3.2. La diffusion de Pérona-Malik

L'homogénéité de l'image est évaluée en fonction de la quantité de variations brusques des valeurs spatiales de l'image et qui s'exprime donc par la proportion de la contribution des hautes fréquences dans l'énergie de l'image. Pour étudier cette perturbation, nous devons trouver un moyen de mesure efficace et nous devons également définir une échelle de mesure, ce qui nous permet de distinguer et de comparer les différents niveaux d'homogénéité. Dans ce chapitre, nous utilisons les modèles basés sur la diffusion proposée par Perona-Malik dans la construction d'un opérateur de diffusion qui, en fonction des propriétés locales de l'image,

permet de créer un filtre qui continue à voir les contours et à dissimuler les zones à faible gradient.

Dans le traitement d'image, la technique de diffusion anisotrope de Perona-Malik a été utilisée à l'origine pour réduire le bruit dans une image sans supprimer les parties importantes de son contenu, telles que les bords, les lignes ou d'autres détails importants pour l'interprétation de l'image [69-71].

En utilisant le même raisonnement que dans le débruitage de l'image, notre idée consiste à incorporer la marque dans des emplacements convaincants permettant de prendre en considération du compromis robustesse et imperceptibilité, tout en préservant les propriétés d'image telles que les bords, les lignes et d'autres détails importants.

### 3.2.1. Formules mathématiques

L'équation de diffusion présentée par Pietro Perona et Jitendra Malik dans [72] utilise une Equation Différentielle Partielle (PDE) qui est une équation qui inclut les dérivées partielles d'une fonction inconnue de plus d'une variable indépendante [73-74].

Considérons l'équation de diffusion anisotrope dans le domaine continu:

$$\begin{cases} \frac{\partial u(x,y,t)}{\partial t} = div(g|\nabla u(x,y,t)|) \cdot \nabla u(x,y,t) \\ u(x,y,0) = u_0(x,y) \end{cases} \quad (3.1)$$

où $div$ : l'opérateur de divergence.

$\nabla$ : l'opérateur de gradient.

$|.|$: le module de $\nabla u$.

$u_0$ : l'image d'origine.

$g(|\nabla u|)$ est le coefficient de diffusion positif et strictement décroissant, qui satisfait aux conditions aux limites suivantes :

$$\begin{cases} g(0) = 1 \\ \lim_{x\to\infty} g(\nabla u) = 0 \end{cases} \quad (3.2)$$

Perona et Malik ont proposé une fonction qui répond aux deux conditions précédentes. C'est la fonction lorentzienne définie par la relation:

$$g(|\nabla u|) = \frac{1}{1+\left(\frac{|\nabla u|}{k}\right)^2} \quad (3.3)$$

où $k$ est le seuil de gradient à partir duquel nous décidons si l'amplitude du gradient est forte (pixels de bord) ou faible (pixels de région) [72].

Si $|\nabla u| \leq k$ alors le PDE améliore les contours. Les points de la norme de gradient qui sont inférieurs à ce seuil sont considérés comme du bruit alors que les autres sont considérés comme des contours. En d'autres termes, il sert à définir la limite entre les gradients forts et les gradients faibles.

### 3.2.2. Discrétisation de l'équation de Pérona- Malik

Le développement de l'équation (3.1) devient :

$$\frac{\partial u\,(x,y,t)}{\partial t} = \nabla g(x,y,t) \cdot \nabla u(x,y,t) + g(x,y,t) \cdot \nabla^2 u(x,y,t) \tag{3.4}$$

On note $\nabla^2 = \Delta$. $\Delta$ est le Laplacien.

**a) Discrétisation du terme $\frac{\partial u(x,y,t)}{\partial t}$**

$$\frac{\partial u\,(x,y,t)}{\partial t} = \frac{u_{i,j}^{n+1} - u_{i,j}^{n}}{\partial t} \tag{3.5}$$

**b) Discrétisation du terme $\nabla g(x,y,t) \cdot \nabla u(x,y,t)$**

$$\nabla g(x,y,t) \cdot \nabla u(x,y,t) \rightarrow \nabla g_{i,j}^{n} \cdot \nabla u_{i,j}^{n}$$

$$\nabla g_{i,j}^{n} \cdot \nabla u_{i,j}^{n} = \left(g_{i+1,j}^{n} - g_{i,j}^{n}\right)\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) + \left(g_{i,j+1}^{n} - g_{i,j}^{n}\right) \cdot \left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) \tag{3.6}$$

$$\nabla g_{i,j}^{n} \cdot \nabla u_{i,j}^{n} = g_{i+1,j}^{n}\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) - g_{i,j}^{n}\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) + g_{i,j+1}^{n}\left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) - g_{i,j}^{n}\left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) \tag{3.7}$$

**c) Discrétisation du terme $g(x,y,t) \cdot \nabla^2 u(x,y,t)$**

$$g(x,y,t) \cdot \nabla^2 u(x,y,t) \rightarrow g_{i,j}^{n} \cdot \nabla^2 u_{i,j}^{n}$$

$$\nabla^2 u_{i,j}^{n} = \Delta u_{i,j}^{n} = u_{i+1,j}^{n} + u_{i-1,j}^{n} + u_{i,j+1}^{n} + u_{i,j-1}^{n} - 4 \cdot u_{i,j}^{n} \tag{3.8}$$

$$g_{i,j}^{n} \cdot \Delta u_{i,j}^{n} = g_{i,j}^{n}\left(u_{i+1,j}^{n} + u_{i-1,j}^{n} + u_{i,j+1}^{n} + u_{i,j-1}^{n} - 4 \cdot u_{i,j}^{n}\right) \tag{3.9}$$

Donc :

$$\frac{u_{i,j}^{n+1} - u_{i,j}^{n}}{\partial t} = g_{i+1,j}^{n}\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) - g_{i,j}^{n}\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) + g_{i,j+1}^{n}\left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) - g_{i,j}^{n}\left(u_{i,j+1}^{n} - ui,jn+gi,jn(ui+1,jn+ui-1,jn+ui,j+1n+ui,j-1n-4\cdot ui,jn)\right. \tag{3.10}$$

Après développement et simplification on trouve

$$\frac{u_{i,j}^{n+1}-u_{i,j}^{n}}{\partial t} = g_{i+1,j}^{n}\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) + g_{i,j+1}^{n}\left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) + g_{i,j}^{n}\left(u_{i,j-1}^{n} - u_{i-1,j}^{n} - 2\cdot u_{i,j}^{n}\right) \quad (3.11)$$

$$= g_{i,j+1}^{n}\left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) + g_{i+1,j}^{n}\left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) + g_{i,j}^{n}\left(u_{i,j-1}^{n} - u_{i,j}^{n}\right) + g_{i,j}^{n}\left(u_{i,j-1}^{n} - u_{i,j}^{n}\right) \quad (3.12)$$

$$u_{i,j}^{n+1} = u_{i,j}^{n} + \partial t \left( \begin{matrix} g_{i,j+1}^{n} & \left(u_{i,j+1}^{n} - u_{i,j}^{n}\right) + & g_{i+1,j}^{n} & \left(u_{i+1,j}^{n} - u_{i,j}^{n}\right) & +g_{i,j}^{n} & \left(u_{i,j-1}^{n} - u_{i,j}^{n}\right) & +g_{i,j}^{n} & \left(u_{i-1,j}^{n} - u_{i,j}^{n}\right) \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ G_N & U_N & G_E & U_E & G_W & U_W & G_S & U_S \end{matrix} \right) \quad (3.13)$$

$$u_{i,j}^{n+1} = u_{i,j}^{n} + \partial t \left(G_N \cdot U_N + G_E \cdot U_E + G_W \cdot U_W + G_S \cdot U_S\right) \quad (3.14)$$

avec $G_w = G_s = g_{i,j}^{n}$

On note :

$$G_N = g_{i,j+1}^{n} \; ; U_N = u_{i,j+1}^{n} - u_{i,j}^{n}$$

$$G_E = g_{i+1,j}^{n} \; ; U_E = u_{i+1,j}^{n} - u_{i,j}^{n}$$

$$G_W = g_{i,j}^{n} \; ; U_W = u_{i,j-1}^{n} - u_{i,j}^{n}$$

$$G_S = g_{i,j}^{n} \; ; U_S = u_{i-1,j}^{n} - u_{i,j}^{n}$$

### 3.2.3. Algorithme de la diffusion anisotrope de Pérona- Malik

**a) Initiation des paramètres**

- Donner la valeur du pas temporel ($0 \leq \partial t \leq 0.25$)
- Fixer le nombre d'itération à N.

**b) Calcul du gradient dans les différentes directions**

$U_N = u_{i,j+1}^{n} - u_{i,j}^{n}$, $U_E = u_{i+1,j}^{n} - u_{i,j}^{n}$, $U_W = u_{i,j-1}^{n} - u_{i,j}^{n}$, $U_S = u_{i-1,j}^{n} - u_{i,j}^{n}$

**c) Calcul des coefficients de diffusion dans les différentes directions du gradient**

$$G_N = \frac{1}{1+\left(\frac{U_N}{k}\right)^2} \; , G_E = \frac{1}{1+\left(\frac{U_E}{k}\right)^2} \; , \; G_W = \frac{1}{1+\left(\frac{U_W}{k}\right)^2} \; , G_s = \frac{1}{1+\left(\frac{U_s}{k}\right)^2}$$

## 3.3. L'algorithme de tatouage proposé

Dans cette section, nous présentons les processus d'insertion et d'extraction proposés et qui sont illustrés dans les **figures 3.2** et **3.3** respectivement. La technique de diffusion de

Perona-Malik est présentée sur la **figure 3.1**. Elle est utilisée dans la sélection des bords où nous allons incruster la marque, ce qui augmente la robustesse du tatouage contre la plupart des attaques sans affecter la qualité visuelle de l'image.

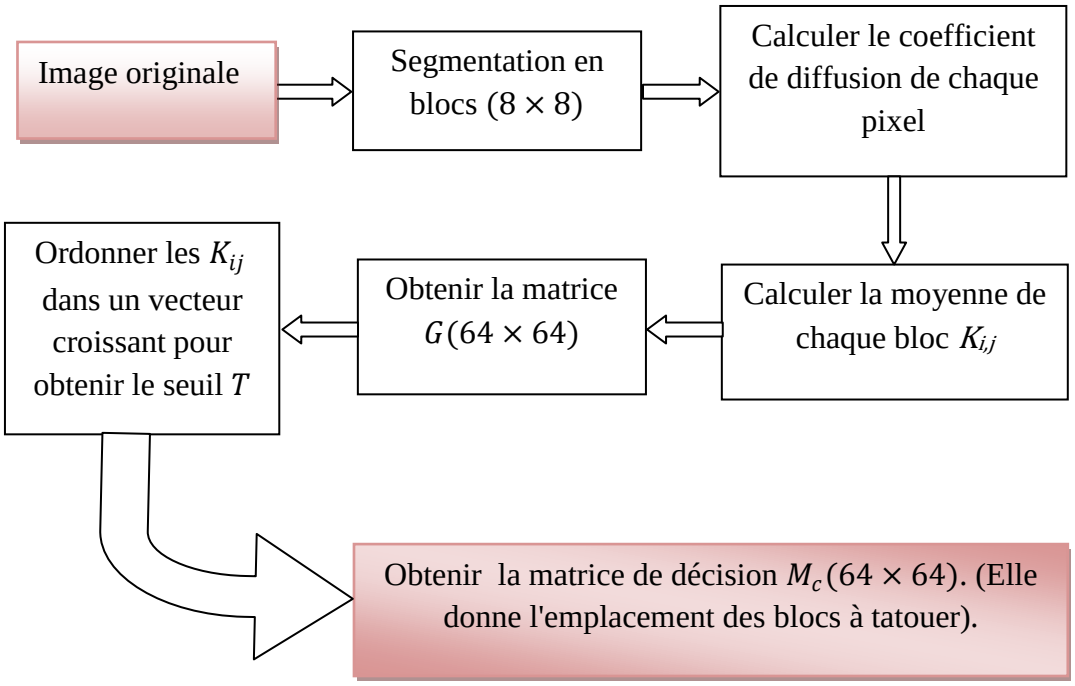



**Figure 3.1.** Schéma fonctionnel de la sélection des blocs à tatouer à base de la technique Perona-Malik.

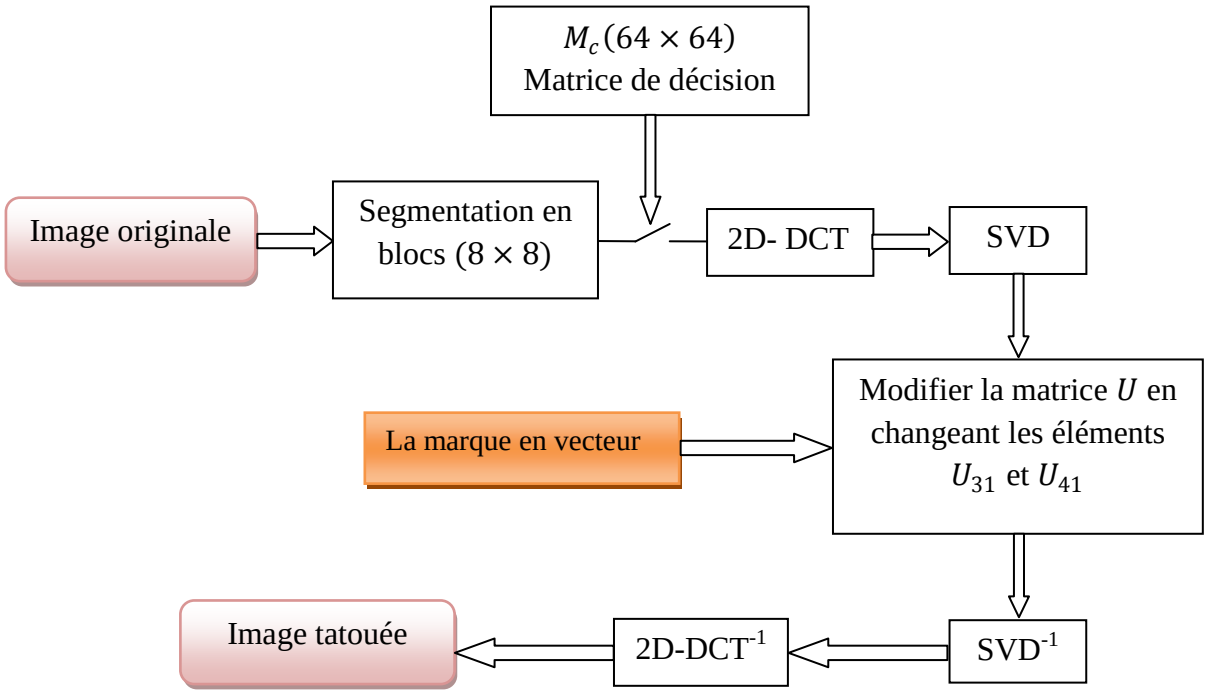



**Figure 3.2**. Schéma fonctionnel du processus d'intégration du tatouage.

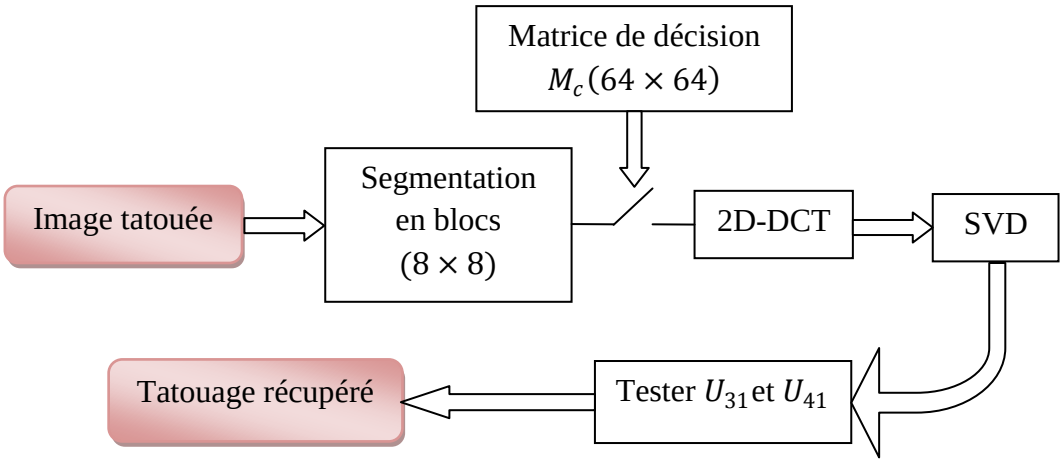



**Figure 3.3.** Schéma fonctionnel du processus d'extraction du tatouage.

### 3.3.1. La phase d'insertion

L'image originale est de taille $m \times n$ et la marque est de taille $m_1 \times n_1$. La procédure de l'incrustation de la marque est la suivante :

**Etape 01**: L'image originale $I$ est d'abord partitionnée en blocs $8 \times 8$ pixels, puis le coefficient de diffusion est calculé pour chaque pixel de ces blocs.

**Etape** 02: Un coefficient de diffusion moyen $K_{i,j}$ est calculé pour chaque bloc $(i,j)$ et une matrice $G$ de taille $(\frac{m}{8} \times \frac{n}{8})$ est construite et complétée avec tous ces coefficients de diffusion tels que : $1 \leq i \leq \frac{m}{8}$ et $1 \leq j \leq \frac{n}{8}$.

**Etape 03:** Les coefficients de diffusion $K_{i,j}$ sont ordonnés dans un vecteur par ordre croissant dont le but est de choisir un seuil $t$ qui permettra de sélectionner les blocs appropriés pour l'insertion de la marque.

**Etape 04:** Une matrice binaire $M_c$ de taille $(\frac{m}{8} \times \frac{n}{8})$, qui est une matrice clé et à la base de laquelle la décision d'insertion de la marque est prise ou non. Elle est créée de la manière suivante:

$$\begin{cases} M_c(i,j) = 0 & Si\ G(i,j) \leq t\ \ décision\ de\ non\ incrustation \\ M_c(i,j) = 1 & Ailleurs \qquad décision\ d'incrustation \end{cases} \tag{3.15}$$

avec $1 \leq i \leq \frac{m}{8}$ et $1 \leq j \leq \frac{n}{8}$.

**Etape 05** : La marque binaire $W$ est transformée en un vecteur de longueur $1 \times m_1 \times n_1$

**Etape 06**: Si $M_c(i,j) = 1$ (avec $1 \leq i \leq \frac{m}{8}$ et $1 \leq j \leq \frac{n}{8}$) , décision d'incrustation, alors :

Appliquant la 2D-DCT puis la SVD aux blocs sélectionnés $(i,j)$ en vu de l'obtention de la matrice $U(i,j)$ résultat de ces deux transformées consécutivement.

Calculer $x$ tel que:

$$x = \frac{(|U_{31}|+|U_{41}|)}{T} \tag{3.16}$$

avec $T$ est un seuil et $U_{31}$ et $U_{41}$ sont les troisième et quatrième éléments de la matrice $U(i,j)$ respectivement.

**Etape 07:** Modifier la matrice $U(i,j)$ de chaque bloc sélectionné comme suit:

$$\begin{cases} U_{31} = x + \frac{T}{2}, & U_{41} = x - \frac{T}{2} \quad si\ w(l) = 1 \\ U_{31} = x - \frac{T}{2}, & U_{41} = x + \frac{T}{2} \quad si\ w(l) = 0 \end{cases} \tag{3.17}$$

avec $1 \leq l \leq m_1 \times n_1$

**Etape 08:** Appliquant la SVD inverse puis la 2D-DCT inverse sur chaque bloc sélectionné pour obtenir l'image tatouée $I_w$.

### 3.3.2. La phase d'extraction

**Etape 01:** Utiliser la matrice clé $M_c$ pour obtenir les blocs tatoués.

**Etape 02:** Appliquer la 2D-DCT, puis la SVD aux blocs tatoués pour obtenir la matrice $U'(i,j)$ résultat de ces deux transformées consécutivement.

**Etape 03:** La marque est extraite sous forme d'un vecteur $w'$ à l'aide de l'équation suivante :

$$\begin{cases} w' = 0 & si \quad U'_{31} \geq U'_{41} \\ w' = 1 & si \quad U'_{31} \leq U'_{41} \end{cases} \tag{3.18}$$

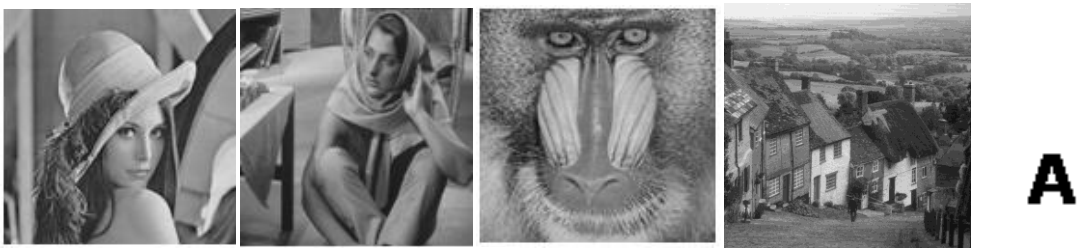
où $U'_{31}$ et $U'_{41}$ sont respectivement le troisième et le quatrième élément de la première colonne de la matrice $U'$.

**Etape 04:** La marque extraite $W'$ est obtenue en convertissant le vecteur $w'$ en une matrice.

### 3.3.3. Résultats expérimentaux

Dans cette section, nous avons effectué quelques expériences afin d'évaluer les performances du schéma de tatouage proposé à l'aide de l'outil de programmation MATLAB.

Quatre images standards de taille $512 \times 512$ pixels en niveaux de gris, à savoir Lena, Baboon, Barbara et Goldhill, ont été utilisées comme images de test. La marque est une image binaire de taille $32 \times 32$. Les images de test ainsi que la marque insérée sont illustrées sur la **figure 3.4**. Quant aux images tatouées et les marques extraites correspondantes, elles sont à leur tour présentées sur la **figure 3.5**.



$(a)$ $(b)$

**Figure 3. 4** Images de test et la marque à insérer : (a) : Lena ; Barbara ; Baboon et Goldhill (b) Marque à insérer.

**Figure 3.5**. Images tatouées de: Lena ; Barbara ; Baboon et Goldhill et leurs marques extraites correspondantes.

Le **tableau 3.1** résume les résultats du PSNR et du BCR obtenus pour différentes images de test. À l'exception de l'image de Baboon, les valeurs du PSNR montrent une grande imperceptibilité de la technique proposée. Les valeurs de BCR sont égales à 1 pour les images de Lena, Barbara et Gold Hill, il est très proche de 1 pour l'image de Baboon. Étant donné que l'image de Baboon est fortement texturée et présente des composantes haute fréquence, de légères erreurs d'arrondi peuvent être générées lors de l'extraction du tatouage. Cela affecte le calcul du BCR. Néanmoins, cette erreur est minimale (de l'ordre de 0,0001) et n'a pas d'influence sur les performances de tatouage. Ces résultats prouvent que la marque extraite est très similaire à celle incrustée.

Le **tableau 3.2** présente les résultats du $PSNR$ et du $BCR$ en utilisant quatre valeurs différentes de seuil $T$: 0,002, 0,012, 0,02 et 0,04. Ces résultats montrent que plus le seuil $T$ est élevé, plus le PSNR est bas et plus le BCR est élevé. Cela signifie qu'un seuil élevé T fournit une faible imperceptibilité mais une robustesse élevée et inversement.

| | **PSNR** | **BCR** |
|---|---|---|
| **Lena** | 46.1090 | 1.00000 |
| **Baboon** | 34.7189 | 0.99990 |
| **Barbara** | 42.9475 | 1.00000 |
| **Gold hill** | 38.6053 | 1.00000 |

**Tableau 3.1** Les valeurs des PSNR et BCR pour les images de: Lena, Baboon, Barbara et Goldhill pour un seuil $T = 0{,}02$.

| **Seuil** | **0.002** | **0.012** | **0.02** | **0.04** |
|---|---|---|---|---|
| **PSNR** | 54.9890 | 49.6954 | 46.1090 | 40.4730 |
| **BCR** | 0.9639 | 1.00000 | 1.00000 | 1.00000 |

**Tableau 3.2.** Valeurs des PSNR et BCR pour l'image de Lena avec différentes valeurs de seuils.

Dans le **tableau 3.3**, une comparaison des valeurs du PSNR liées à l'image de Lena est effectuée entre notre méthode et les méthodes présentées dans [4], [5], [6] et [7] pour différentes valeurs de seuil sans attaques. En tenant compte des valeurs du **tableau 3.3**, nos résultats sont supérieurs à ceux de [4], [5] et [6], à l'exception de [7] dans le cas de $T = 0.002$. Cependant, lorsque nous examinons les résultats fournis avec des seuils supérieurs à 0,002, les nôtres surpassent ceux de [7].

Afin d'évaluer la robustesse de la méthode proposée, plusieurs attaques sont appliquées à l'image tatouée (**tableau 3.4**): compression JPEG, ajout de bruit (bruit gaussien, salt and pepper et speckle), filtrage (filtre médian et Sharpening) et cropping. Ces attaques sont

également étendues aux images tatouées de Baboon et de Barbara, comme indiqué dans le **tableau 3.7**. Les résultats obtenus sont satisfaisants, notamment pour les tests de compression et de filtrage.

| Seuil | Chang et al [4] | Chung et al [5] | Fan et al [6] | Lai [7] | Ours |
|---|---|---|---|---|---|
| **0.002** | 48.80 | 50.17 | 48.91 | 61.69 | 54.98 |
| **0.012** | 48.02 | 47.83 | 48.12 | 49.37 | 49.65 |
| **0.02** | 46.90 | 45.94 | 46.98 | 44.75 | 46.10 |
| **0.04** | 43.74 | 42.04 | 43.81 | 38.51 | 40.47 |

**Tableau 3.3.** Performances des valeurs du PSNR pour l'image de Lena sous différentes valeurs de seuil.

| Attaques | BCR |
|---|---|
| **La compression JPEG 70%** | 0.9600 |
| **Le bruit Gaussian 1%** | 0.7627 |
| **Le bruit Salt and pepper1%** | 0.9131 |
| **Le bruit Speckle 4%** | 0.7275 |
| **Le filtre Median 3 × 3** | 1.0000 |
| **Sharpening** | 1.0000 |
| **Supérieur droite Cropping** | 0.8506 |

**Tableau 3.4** valeurs du BCR pour l'image de Lena sous différentes attaques avec un seuil $T = 0{,}02$.

Une comparaison, en termes de valeurs du $BCR$, entre notre méthode et les techniques présentées dans [4], [5], [6] et [7] sous diverses attaques de l'image de Lena est donnée dans les **tableaux 3.5** et 3.**6** (CR: cropping, GN: Bruit gaussien, MF: filtre médian, compression

JPEG, SH: sharpening). Les résultats présentés dans les **tableaux 3.5** et 3.**6** montrent que la méthode proposée surpasse les méthodes citées en termes de robustesse et d'imperceptibilité alors que [7] est un peu meilleure que notre méthode en termes de $BCR$. Cela confirme l'efficacité de la méthode proposée.

| **Attacks** | **Chang et al [4]** | **Chung et al [5]** | **Fan et al [6]** | **Lai [7]** | **Ours** |
|---|---|---|---|---|---|
| **Supérieur gauche CR** | 0.8115 | 0.8115 | 0.8115 | 0.8476 | 0.8506 |
| **GN 1%** | 0.6230 | 0.7080 | 0.6250 | 0.5928 | 0.6680 |
| **MF 3×3** | 0.5283 | 0.4980 | 0.5292 | 0.9688 | 0.9980 |
| **JPEG70%** | 0.6806 | 0.6855 | 0.6806 | 0.9941 | 0.9463 |
| **SH** | 0.7056 | 0.7323 | 0.7066 | 0.8805 | 1.0000 |

**Tableau 3.5**. Performance de la valeur du BCR sous différentes attaques avec un seuil $T = 0.012$.

| **Attacks** | **Chang et al [4]** | **Chung et al [5]** | **Fan et al [6]** | **Lai [7]** | **Ours** |
|---|---|---|---|---|---|
| **Supérieur gauche CR** | 0.8125 | 0.8125 | 0.8125 | 0.8477 | 0.8506 |
| **GN 1%** | 0.8750 | 0.9179 | 0.8740 | 0.9521 | 0.9199 |
| **MF 3×3** | 0.5507 | 0.5107 | 0.5468 | 1.0000 | 1.0000 |
| **JPEG70%** | 0.9687 | 0.9794 | 0.9658 | 1.0000 | 1.0000 |
| **SH** | 0.8847 | 0.9892 | 0.9873 | 1.0000 | 1.0000 |

**Tableau 3.6**. Performance de la valeur du BCR sous différentes attaques avec un seuil $T = 0.04$.

| Attaques | Lena | Baboon | Barbara |
|---|---|---|---|
| **Sans attaques** |  BCR = 1.0000 |  BCR =0.9990 |  BCR =1.0000 |
| **Compression 75%** |  BCR = 0.7119 |  BCR = 0.9287 |  BCR = 0.6918 |
| **Cropping supérieur gauche** |  BCR = 0.8506 |  BCR = 0.8652 |  BCR = 0.6777 |
| **Cropping inférieur gauche** |  BCR = 0.9209 |  BCR = 0.7129 |  BCR = 0.8115 |
| **Cropping supéieur droit** |  BCR = 0.7568 |  BCR = 0.8535 |  BCR = 0.9082 |
| **Cropping inférieur droit** |  BCR = 0.6748 |  BCR = 0.7686 |  BCR = 0.8057 |
| **Salt & pepper 0.01** |  BCR = 0.9160 |  BCR = 0.9189 |  BCR = 0.8750 |
| **Bruit gaussian** |  BCR = 0.7588 |  BCR = 0.7334 |  BCR = 0.6953 |
| **Bruit speckle** |  BCR = 0.7080 |  BCR = 0.7432 |  BCR = 0.7266 |
| **Filtre Median** |  BCR = 1 |  BCR = 0.9814 |  BCR = 0.9932 |
| **Sharpening** |  BCR =1 |  BCR = 0.9805 |  BCR = 0.9971 |

**Tableau 3.7.** Qualité visuelle des marques extraites et performance de la valeur du BCR après différentes attaques pour les images de Lena, Baboon et Barbara.

## 3.4. Application aux images en couleur

Afin de confirmer l'efficacité de notre technique proposée, nous avons jugé utile de l'appliquer sur des images en couleurs de Lena, Baboon, Airplaine et Peppers ayant une taille de $512 \times 512$. La marque binaire insérée est de taille $32 \times 32$ (**figure 3.6**). Nous indiquons que l'image couleur à tatouer est convertie du domaine $RGB$ (Red- Green and Blue) vers le domaine $YC_bC_r$ ($Y$: luminance, $C_b$ : chrominance bleue, $C_r$ : chrominance rouge) et l'insertion est faite au niveau de la composante de luminance $Y$ de l'image couleur en question. La **figure 3.7** illustre les images tatouées et leurs marques extraites correspondantes.

$(a)$ $(b)$

**Figure 3.6** Images originales et la marque à insérer : (a) : Lena ; Baboon ; Aireplaine et peppers (b) Marque à insérer respectivement.

**Figure 3.7** Images tatouées de : Lena ; Baboon ; Aireplaine et peppers et leurs marques extraites correspondantes.

Les résultats du tableau ci-dessous donnent les valeurs de test du PSNR et du BCR du tatouage de l'image de Lena couleur pour différentes valeurs de seuils. Il est à remarquer que les valeurs du PSNR sont comprises entre 39.7566 et 49.6916 qui sont fortement acceptables pour évaluer la robustesse de l'algorithme proposé. Par ailleurs, les valeurs du BCR sont quasiment égales à 1 sauf pour le cas où le seuil est égal à 0.02. Cela confirme l'imperceptibilité de la marque insérée et par conséquent prouve l'efficacité de la méthode

proposée pour les images couleurs.

| Seuil | 0.002 | 0.012 | 0.02 | 0.04 |
|---|---|---|---|---|
| **PSNR** | 49.6916 | 47.1887 | 44.6689 | 39.7566 |
| **BCR** | 0.9375 | 1.00000 | 1.00000 | 1.00000 |

**Tableau 3.8** Valeurs des PSNR et BCR de l'image de Lena couleur pour différentes valeurs de seuils.

Le **tableau 3.9** est une généralisation de l'application de la méthode proposée sur un ensemble d'images couleurs : Lena, Baboon, Airplaine et Peppers. Les résultats de test du PSNR sont acceptables et varient de 35.6127 à 44.6689 par contre ceux du BCR sont quasiment égale à 1 pour l'ensemble ces images. Ces deux mesures confirment respectivement la robustesse et l'imperceptibilité de la méthode proposée appliquée aux images couleurs.

| | PSNR | BCR |
|---|---|---|
| **Lena** | 44.6689 | 1.0000 |
| **Baboon** | 35.6127 | 1.0000 |
| **Airplaine** | 37.3483 | 1.0000 |
| **Peppers** | 41.5117 | 0.9941 |

**Tableau 3.9** Les valeurs des PSNR et BCR des images hôtes de : Lena, Baboon, Barbara et Goldhill avec un seuil $T = 0{,}02$.

L'évaluation de la méthode de tatouage proposée étendue aux images en couleur est aussi testée vis-à-vis des différentes attaques telles que la compression, le filtrage et l'ajout de bruit. Le tableau ci-dessous récapitule les résultats du BCR obtenus suite à l'application de ces attaques sur les images tatouées de Lena, Baboon et Peppers. Nous constatons que la marque extraite semble, à l'œil nu, identifiable et ressemble à la marque insérée. Cela est confirmé objectivement par les mesures du BCR qui varient généralement de 0.8262 à 1 et qui nous permet de qualifier l'algorithme proposé de robuste vis-à-vis des attaques citées.

| Attaques | Lena | Baboon | Peppers |
|---|---|---|---|
| **Compression 75%** |  BCR =0.9111 |  BCR = 0.9629 |  BCR =0.7822 |
| **Salt & pepper 0.01** |  BCR = 0.9717 |  BCR = 0.9648 |  BCR =0.9199 |
| **Bruit Gaussian 1%** |  BCR =0.8779 |  BCR = 0.8438 |  BCR = 0.8262 |
| **Bruit speckle** |  BCR = 0.8906 |  BCR = 0.9170 |  BCR = 0.8828 |
| **Filtre Median** |  BCR = 1 |  BCR = 1 |  BCR = 0.9941 |
| **Sharpening** |  BCR =1 |  BCR = 0.9854 |  BCR = 0.9824 |

**Tableau 3.10.** Qualité visuelle des marque extraites et performance de la valeur du BCR après différentes attaques pour les images de Lena, Baboon et Barbara.

## 3.5. CONCLUSION

Dans ce chapitre, une technique de tatouage d'image hybride basée sur la DCT-SVD et les caractéristiques visuelles humaines est présentée. La technique exploite pleinement les caractéristiques pertinentes de la SVD, qui caractérise efficacement les propriétés algébriques fondamentales d'une image. L'utilisation des caractéristiques HVS, fournie par l'approche de diffusion de Perona-Malik, permet de sélectionner des blocs d'incorporation de tatouage pour

un bon compromis entre la robustesse et l'imperceptibilité du tatouage. Les résultats expérimentaux de la technique proposée ont montré son efficacité par rapport aux travaux existants en termes d'imperceptibilité et de robustesse contre différentes attaques notamment la compression JPEG, l'ajout de bruit, le filtrage et le cropping. Une perspective pour les travaux futurs consiste à mettre en œuvre notre méthode dans le contexte du tatouage numérique de la vidéo, car une vidéo peut être décomposée en un ensemble d'images numériques consécutives.

# Chapitre 4

# *Tatouage vidéo*

## 4.1 Introduction

L'arrivée de la vidéo numérique, distribuée à travers les DVD, HDTV et DBS ou encore d'autres media, permet de proposer aux utilisateurs des vidéos de haute qualité. De plus, la démocratisation de l'internet a démontré le potentiel commercial du marché du multimédia numérique. Cependant, cette venue engendre de nouvelles craintes des propriétaires de contenus, provenant de la disponibilité de l'enregistrement des DVDs, D-VHS et des ordinateurs personnels multimédia. En utilisant ces nouveaux produits, les utilisateurs peuvent réaliser aisément des copies illégales. Le tatouage apparait donc comme étant une alternative à la protection de la propriété intellectuelle des supports multimédia. Le domaine d'application de cette technologie encore jeune, s'étend du monde $1D$ (l'audio), jusqu'au monde $3D$ (et $3D + t$), en passant par le $2D$ et le $2D + t$ (vidéo). Actuellement, il apparait que le tatouage seul ne peut pas répondre `a une protection suffisamment fiable et complète dans un milieu grand public, où les degrés de liberté (en terme de manipulation des contenus) sont trop élevés. Il semble de plus en plus évident que l'on ne pourra jamais empêcher le piratage grand public, `a moins de créer des systèmes complètement propriétaires, mais dans ce cas, il n'est encore pas assuré que la protection soit totale.

Dans ce chapitre, nous commençons par donner quelques notions de la vidéo avec un aperçu sur les différents formats, compressées et non compressées de la vidéo numérique. Puis, nous présentons les propriétés du tatouage numérique de la vidéo. Ensuite, nous exposons ses contraintes ainsi que ses défis majeurs. Dans la section suivante nous discutons les limites des schémas de tatouage dans le contexte de la vidéo suivi d'une classification des techniques de tatouage vidéo. A la fin, nous présentons une technique de tatouage vidéo basée sur la décomposition en valeurs singulières multi-résolution et nous terminons par une conclusion.

## 4.2 Notions de vidéo

Avant d'aborder les détails des techniques et des défis du tatouage vidéo, nous présentons ci-dessous une vue fondamentale de la vidéo.

### 4.2.1 Définition de la vidéo

Le terme vidéo fait référence aux informations visuelles capturées par une caméra et s'applique généralement à une séquence d'images variant dans le temps. Une vidéo est un flux

composée d'une part d'une suite d'images (25 f/s en Europe, 30 f/s aux USA), donnant l'illusion du mouvement et d'autre part d'une composante sonore. Chaque image est décomposée en lignes horizontales. Chaque ligne est considérée comme une succession de points. La lecture et la restitution d'une image s'effectue donc séquentiellement ligne par ligne comme un texte écrit : de gauche à droite puis de haut en bas. Une vidéo peut être décomposée en trois unités: images, séquences et scènes. Une séquence est un enchaînement d'images enregistrées lors d'une seule opération de caméra et une scène est un ensemble de prises de vue consécutives présentant une similitude sémantique quant aux objets, aux personnes, à l'espace et au temps [75].

### 4.2.2 Propriétés de la vidéo

La vidéo numérique peut être caractérisée par quatre propriétés différentes: fréquence des trames, résolution des trames, profondeur de pixels et débit binaire.

a. **Fréquence (taux de trame):** Elle correspond au nombre de trames capturées par seconde. Tous les profils analytiques fournissant l'illusion de mouvement nécessitent un minimum de 12 trames par seconde. Si la fréquence des trames est inférieure à l'exigence minimale, les objets ne sont pas détectés et suivis efficacement. Dans un système NTSC, la cadence est de 29,97 trames par seconde. Pour le système PAL, la cadence est de 25 trame par seconde [53, 76].

b. **Résolution de trame**: est le nombre de pixels contenus dans chaque trame. Plus il y a de pixels, plus la trame est nette. Il existe différents formats de vidéo, tels que CIF (352x288), QCIF (176x144), UIT-R709 (1920x1080) etc. [77].

c. **Profondeur de pixels**: le nombre de bits utilisé pour représenter la couleur d'un pixel unique dans une trame vidéo est également appelé « Profondeur de couleur », dont l'unité est le nombre de bits par pixel (bpp) [78].

d. **Débit binaire**: est le nombre de bits transmis ou traités par unité de temps. Plus le débit binaire est élevé, meilleure est la qualité de la vidéo. Par exemple, une vidéo YouTube avec une résolution de $854 \times 480$ a une plage de débits comprise entre 500 et 2000 Kbps [79, 80].

### 4.2.3 Différents formats vidéo

Un signal vidéo peut être sous une forme brute (non compressée) ou bien sous une forme compressée.

#### 4.2.3.1 Formats non compressés

- **Le standard S-Vidéo** : Le standard S-Vidéo, parfois appelé **Y/C** ou **vidéo à composantes séparées**, est un mode de transmission vidéo qui utilise des câbles différents pour faire transiter les informations de luminance (luminosité) et de chrominance (couleur). Plus précisément, le signal vidéo luminance non modulé est séparé du signal de chrominance composite modulé, ce qui permet d'éviter la dégradation de l'image due à l'interférence entre ces deux signaux. Cette séparation se retrouve concrètement dans le câble qui transmet le signal puisque les deux composantes (luminance et chrominance) sont véhiculées sur deux fils différents.

- **Le standard YUV :** (appelé aussi CCIR 601), auparavant baptisée $YC_bC_r$, est un modèle de représentation de la couleur dédié à la vidéo analogique. Il se base sur un mode de transmission vidéo à composantes séparées utilisant trois câbles différents pour faire transiter les informations de luminance (luminosité) et les deux composantes de chrominance (couleur). Il s'agit du format utilisé dans les standards PAL (Phase Alternation Line) et SECAM (Séquentiel Couleur avec Mémoire). Le paramètre *Y* représente la luminance (c'est-à-dire l'information en noir et blanc), tandis que *U* et *V* permettent de représenter la chrominance, c'est-à-dire l'information sur la couleur. Ce modèle a été mis au point afin de permettre de transmettre des informations colorées aux téléviseurs couleurs, tout en s'assurant que les téléviseurs noir et blanc existant continuent d'afficher une image en tons de gris. Voici les relations liant *Y* à *R, G et B*, puis *U* à *B* et à la luminance *Y*, et enfin *V* à *R* et à la luminance :

  - $Y = 0.299R + 0.587\,G + 0.114\,B$
  - $U = -0.147R - 0.289\,G + 0.436B = 0.492(B - Y)$ (4.1)
  - $V = 0.615R - 0.515G - 0.100B = 0.877(R - Y)$

  Ainsi U est parfois noté *Cr* et V noté *Cb*, d'où la notation *YCrCb*.

- **Le modèle YIQ :** Ce modèle est très proche du modèle $YUV$. Il est notamment utilisé dans le standard vidéo NTSC (utilisé entre autres aux États-Unis et au Japon). Le paramètre *Y* représente la luminance. *I* et *Q* représentent respectivement l'*Interpolation* et la *Quadrature*. Les relations entre ces paramètres et le modèle RGB sont les suivantes :

- $Y = 0.299R + 0.587G + 0.114B$
- $I = 0.596R - 0.275G - 0.321\,B$ (4.2)
- $Q = 0.212R - 0.523G + 0.311B$

#### 4.2.3.2 Formats compressés

Le ci-dessous récapitule les formats vidéo, leurs propriétés et leurs supports usuels.

| Format | codec | Stockage | Résolution |
|---|---|---|---|
| DVD Vidéo | MPEG-2 | DVD-R | PAL / 720×576 pixels |
| **Qualité :** films de qualité irréprochable, supporte plusieurs pistes audio pour le son home cinéma.<br>**Stockage :** On peut stocker de 120 minutes (DVD-R de 4,7Go) à 240 minutes (pour les DVD double couche).<br>**Notes :** supporte les sous-titres et menus | | | |
| S-VCD / Super vidéo-CD | MPEG-2 | CD-R | PAL / 480×576 pixels |
| **Qualité :** elle se rapproche de celle du DVD, mais ne supporte que 2 canaux audio (stéréo).<br>**Stockage :** 35 à 60 minutes sur des CD-R de 650 Mo.<br>**Notes :** supporte les sous-titres et menus | | | |
| VCD / Vidéo-CD | MPEG-1 | CD-R | PAL / 352×288 pixels |
| **Qualité :** qualité d'un bon enregistrement sur cassette VHS (à condition d'être bien encodé), son stéréo. La qualité dépend beaucoup du temps de la vidéo à stocker. Si la vidéo est courte<br>**Stockage :** environ 70 minutes sur des CD-R de 650 Mo.<br>**Notes :** ne supporte pas les sous-titres et menus, contrairement aux SVCD et DVD. | | | |
| Divx / XviD / WMV | MPEG4 | CD-R | PAL / 640×480 pixels |
| **Qualité :** qualité d'un bon enregistrement sur cassette VHS (à condition d'être bien encodé), son stéréo. La qualité dépend beaucoup du temps de la vidéo à stocker. Si la vidéo est courte<br>**Stockage :** environ 120 minutes sur des CD-R de 650 Mo.<br><br>**Notes :** ne supporte pas les sous-titres et menus, contrairement aux SVCD et DVD. | | | |

**Tableau 4.1** Les formats vidéo, leurs propriétés et leurs supports usuels.

- **asf** : très compressé, ce format propriétaire privilégie la taille à la qualité. Même incomplète, une vidéo .asf peut être lue par la plupart des lecteurs ; mais pour pouvoir accéder rapidement aux différentes parties, il faut l'avoir téléchargé en entier.
- **mpeg ou mpg** : est le deuxième format le plus populaire. La qualité est moins bonne que celle du DiVx à taille égale. C'est aussi le seul format compatible avec les lecteurs DVD de salon classique, à condition d'être encodé à un bitrate et une résolution bien définie correspondant aux normes VCD ( mpeg1) ou SVCD (mpeg 2).
- **avi** : c'est le format du DiVx par excellence, la meilleur qualité actuellement, mais la multiplication des codecs rend leur lecture parfois difficile. Des informations essentielles figurent à la fin de ces fichiers, ce qui explique pourquoi il est normalement impossible de lire une vidéo .avi incomplète.
- **ogm** :[ogg media] ce format est supporté par les lecteurs habituels et nécessite simplement le code « oggvorbis » pour que la bande son soit lue.
- **rmvb** (real media variable bitrat) : encore connu sous le nom RV9, d'apparition récente, son rapport « qualité/ capacité de compression » est meilleure à bas débit que DiVx ou le Xvid. Malheureusement il s'agit d'un format du propriétaire Real Video, et de nombreux lecteurs sont incapables de lire ce format.

## 4.3 Propriétés du tatouage numérique de la vidéo

Dans un flux vidéo, il est possible de tatouer les images de type intra et inter [81-82]. De nombreux schémas développés peuvent être appliqués aux séquences vidéo. Ces dernières présentent cependant d'autres propriétés, qui peuvent être exploitées pour l'insertion de la marque :

- la taille brute d'une séquence vidéo est beaucoup plus importante que la taille d'une image fixe. L'espace d'insertion de la signature en est considérablement augmenté.
- la dimension temporelle du signal traité peut être utilisée pour l'insertion de la signature. Celle-ci peut, par exemple, être insérée dans le mouvement des différents objets de la séquence.
- la complexité du schéma de tatouage doit être faible. L'insertion et la détection de la signature doivent pouvoir s'effectuer en même temps, dans la plupart des applications. La contrainte de temps réel s'applique essentiellement à la phase de détection.
- le mouvement des objets augmente souvent la visibilité de la signature : ainsi, une signature "fixe" ajoutée sur un objet en mouvement, sera d'avantage perceptible que si l'objet est statique.

- le flux vidéo est souvent compressé de manière à réduire la taille originale des séquences. L'insertion de la signature peut alors directement s'effectuer lors de la compression. L'insertion sur le format décompressé ne doit pas entraîner, après compression, une augmentation significative de la taille des données.
- la présence de la signature dans la séquence vidéo peut permettre d'autres attaques que celles liées aux images fixes. Si la signature est redondante dans la séquence, elle peut être estimée en calculant la moyenne des différentes images de la séquence. La signature doit pouvoir être détectée après une perte de synchronisation, produite par la sélection d'une séquence précise ou la perte d'images de la séquence.

## 4.4 Contraintes et défis majeurs du tatouage vidéo

Les algorithmes de tatouage vidéo sont plus difficiles à développer que ceux qui fonctionnent sur les images. Ceci est essentiellement dû à la dimension temporelle, qui nécessite des exigences spécifiques. Cette section présente les trois défis majeurs pour le tatouage vidéo numérique [83, 84].

### 4.4.1 La robustesse

Comme nous avons vu précédemment, un des points forts d'un tatouage efficace réside dans sa robustesse. Elle représente la capacité que possède un algorithme de tatouage à résister aux attaques extérieures. Pour la vidéo, les attaques peuvent être des traitements visant soit à brouiller soit à enlever la marque de protection.

#### 4.4.1.1 Attaques de traitement d'image

Puisque une vidéo est une succession d'images fixes, on peut alors appliquer la plupart des attaques de l'image fixe à la vidéo. Cependant, certaines attaques couramment utilisées sur les images fixes ne sont pas applicables à la vidéo. C'est le cas par exemple de l'attaque stirmark [85], qui n'a pas d'intérêt en vidéo, si elle est appliquée sans être adaptée. Les attaques courantes de traitement d'images sont des attaques de destruction de la marque telle que : le bruit additif et multiplicatif ( bruit gaussien, uniforme, speckle, mosquito), le filtrage, la compression avec perte (JPEG) et le transcodage (H.263 → MPEG-2, GIF → JPEG) et des attaques de synchronisation telles que les distorsions dues aux modifications géométriques des données comme la translation, la rotation, la mise à échelle (scaling) et le découpage (shearing) et la réduction des données: « cropping, clipping ».

#### 4.4.1.2 Attaques de synchronisations temporelles

La synchronisation temporelle est le processus de modification des structures temporelles dans les images de la vidéo tatouée. Ces transformations comprennent la moyenne de trame (FA : Frame Averaging), la permutation de trame (FS : Frame Swapping) et la suppression de trame (FD : Frame Dropping). En FA, la valeur de chaque pixel de la vidéo attaquée est obtenue en faisant la moyenne des valeurs de pixel des images vidéo corrélées. Cependant, en mode FD, certaines images d'une séquence vidéo tatouée sont supprimées de manière aléatoire et remplacées par celles correspondantes dans la vidéo originale. D'autre part, la FS modifie l'ordre de certaines images dans une vidéo tatouée. Ceci peut être imperceptible par l'œil humain [86].

#### 4.4.1.3 Attaques de compression vidéo

Afin de réduire les besoins en stockage, les propriétaires de contenu codent souvent les fichiers vidéo avec une compression avec perte telle que : MPEG-1, MPEG-2, MPEG-4, H.264 / AVC et H.265 / HEVC. Cette compression peut dégrader la qualité perceptuelle de la vidéo car elle supprime la redondance spatiale et temporelle d'une vidéo et, par conséquent, supprime la marque insérée. Dans le cas où la marque est insérée directement dans une vidéo compressée, les utilisateurs peuvent convertir la vidéo (conversion de format, par exemple, MPEG1 → H.264), ce qui peut également supprimer la marque [86].

### 4.4.2 L'imperceptibilité

L’imperceptibilité dans les tatouages vidéo est plus difficile à obtenir que dans les tatouages des images fixes. Cela est dû au mouvement des objets dans les séquences vidéo, ce qui rend la visibilité de la marque plus intense. Ainsi, une marque fixe ajoutée à un objet en mouvement sera plus perceptible que si l'objet est statique [87]. Par conséquent, la dimension temporelle de la vidéo doit être prise en compte afin d'éviter toute distorsion entre les images.

### 4.4.3 La complexité

En tatouage d'image, l'insertion et l'extraction de la marque ne prennent que quelques secondes. Cependant, un tel retard est irréaliste dans le contexte de la vidéo en raison du nombre important d'images à traiter dans un signal vidéo (25 images / s). Pour cette raison, la

complexité de l'algorithme de tatouage doit évidemment être aussi faible que possible pour pouvoir implémenter en temps réel et à faible coût [53].

## 4.5 Limites des schémas de tatouage d'images dans le contexte de la vidéo

Théoriquement, tout schéma de tatouage d'image peut s'appliquer dans le contexte de la vidéo. Il suffit d'appliquer ce schéma sur toutes les images de la vidéo de manière indépendante. Or, la vidéo est une suite d'images qui sont fortement corrélées et il n'est pas évident de traiter chaque image à part sans considérer ses voisins. La vidéo représente un champ très vaste d'informations. Il offre, par rapport à une image, beaucoup plus de possibilités d'attaques ayant pour objectif de détruire ou même de récupérer la marque. Exploitant la redondance d'informations qui existe entre les images, un utilisateur malhonnête peut remplacer une image par la moyenne de ses voisins, supprimer certaines images en faisant un échantillonnage régulier afin de garantir la cohérence du signal et sans nuire à l'aspect visibilité. Une compression avec perte peut être aussi envisageable pour détruire la marque. Toutes ces attaques qui considèrent l'aspect temporel dans la vidéo, représentent un handicap aux schémas de tatouage d'images fixes. Toutefois, certains de ces schémas peuvent être adaptés au contexte vidéo et ce, en tenant compte de la composante temps dans les phases d'insertion et de détection [82].

## 4.6 Classification des schémas du tatouage vidéo

Les algorithmes de tatouage vidéo proposés dans la littérature peuvent être classés en trois catégories principales: (1) tatouage d'image fixe (trame par trame); (2) intégration de la dimension temporelle; (3) exploitation du format de compression vidéo.

### 4.6.1 Schémas dérivés du tatouage d'images fixes : tatouage image par image

Etant donné qu'une séquence vidéo numérique est considérée comme un ensemble d'images fixes [14], alors la plus part des techniques de tatouage d'images qui existe dans la littérature ont été étendues à la vidéo. Les techniques de tatouage image par image utilisent deux stratégies principales pour l'insertion de la marque: (1) l'incorporation de la même marque dans chaque image, ou (2) l'incorporation de marques différentes (non corrélées) dans

chaque trame de la vidéo. L'avantage de ces méthodes est la simplicité de l'implantation de l'algorithme de tatouage. Mais en revanche, de tels schémas souffrent souvent des performances de robustesse médiocres face à diverses attaques de traitement vidéo en raison de grandes quantités de données et de la redondance inhérente entre les trames (c'est-à-dire que de nombreuses trames sont visuellement similaires les unes aux autres) [88]. Par exemple, lorsque la marque incorporée n'est pas la même pour toutes les images d'une séquence vidéo, les données cachées peuvent être désynchronisées avec une opération simple, telle qu'une suppression d'image. De plus, ces techniques nécessitent beaucoup de calcul du fait de la redondance du même processus sur toutes les images de la vidéo. Les **figures 4.1** et **4.2** présentent les deux stratégies d'intégration image par image en utilisant la méthode d'intégration additive.

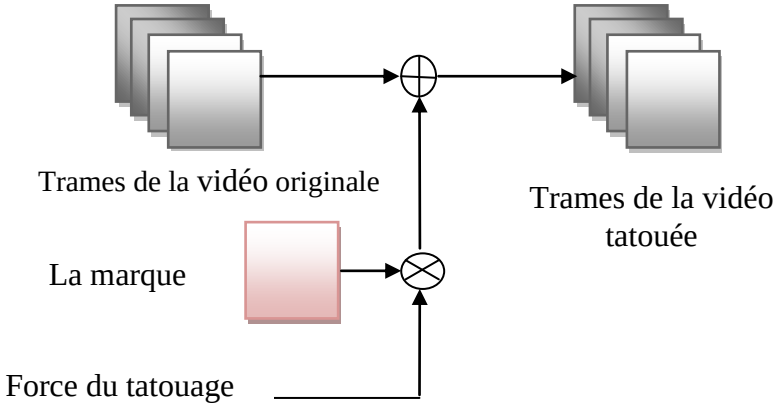



**Figure 4.1** Insertion de la même marque par la méthode d'image par image dans toutes les trames de la vidéo.

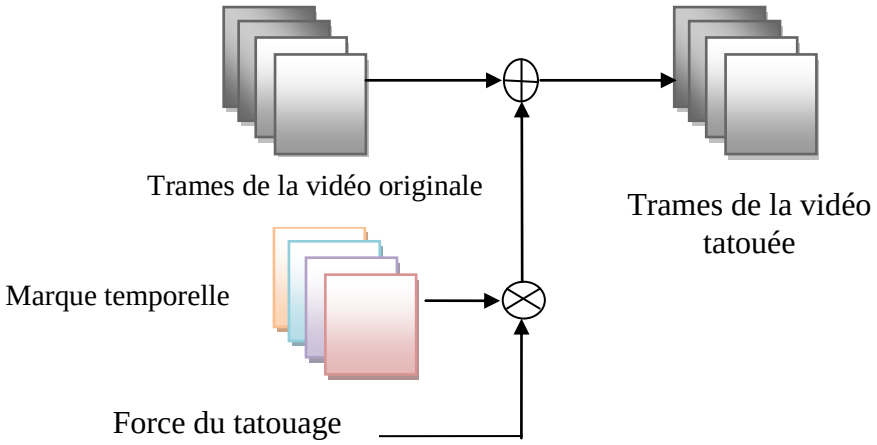



**Figure 4.2** Insertion de différentes marques par la méthode image par image dans chaque trame de la vidéo.

### 4.6.2 Exploiter le format de compression vidéo

Dans le tatouage vidéo, une marque peut être insérée dans un signal vidéo avant la compression, pendant le processus de compression ou après le processus de compression [89].

#### 4.6.2.1 Incorporation de la marque avant la compression

La marque est insérée directement sur le flux vidéo non compressée avec l'intention de conserver la marque après la compression des vidéos tatouées à l'aide d'une compression quelconque. Les techniques d'insertion « image par image » mentionnées précédemment sont des exemples d'insertion non compressée. Le principal avantage de cette technique est que les données vidéo peuvent être compressées avec différents standards et débits de données, comme indiqué sur la **figure 4.3**, à condition que la marque insérée soit robuste à la compression. Cependant, son coût de calcul est élevé [90].

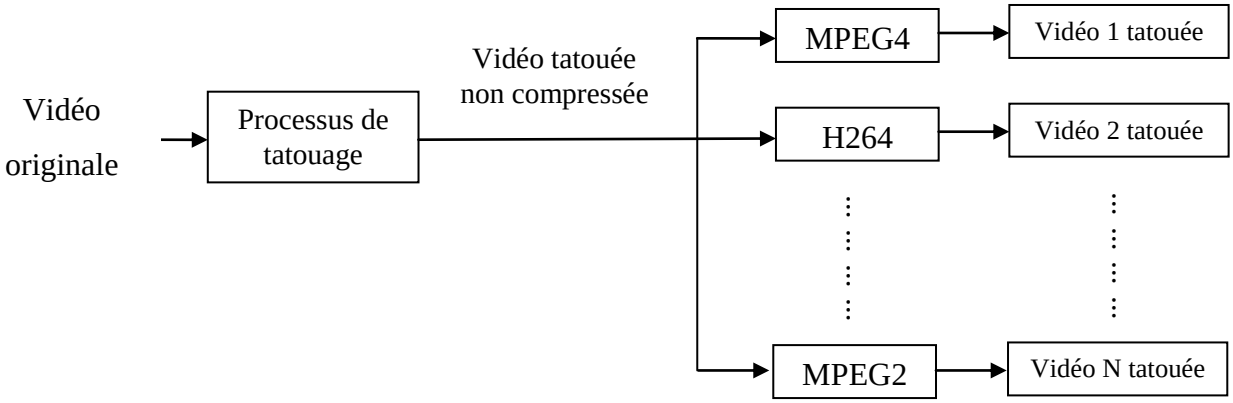



**Figure 4.3** Tatouage vidéo dans le domaine non compressé.

#### 4.6.2.2 Incorporation de la marque pendant la compression

Dans cette technique, la compression et l'incorporation de la marque sont combinées. La marque est insérée lors d'un flux de bits codé et généré à l'aide des codeurs conformes aux normes MPEG2, MPEG4, H.264… etc. Cette technique a été largement utilisée puisqu'elle offre la possibilité d'obtenir une grande robustesse et aussi l'impact visuel sur la vidéo tatouée est très faible ainsi que l'insertion et la détection de la signature peuvent être effectuées en temps réel. Il convient de noter que la plupart de ces techniques sont utilisées dans le domaine de la transformée en cosinus discrète (DCT), comme présenté sur la **figure 4.4**. Dans ces algorithmes, l'insertion de la marque est généralement effectuée soit : (1) sur un vecteur de mouvement, (2) sur des mots de code VLC, soit (3) en modifiant les coefficients DCT (voir

**figure 4.4**) [86-90]. Ces techniques offrent un haut niveau de flexibilité et procurent donc des schémas de tatouage robustes et imperceptibles. Cependant, ils ne sont pas extensibles à un grand nombre d'utilisateurs car chaque utilisateur nécessite un codage individuel [83, 90].

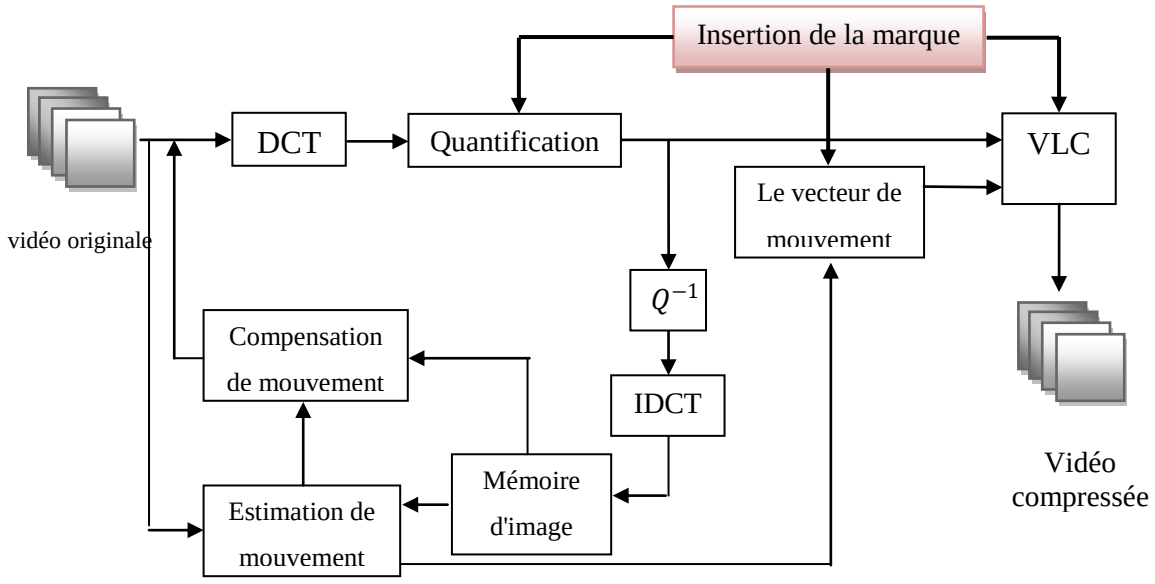



**Figure 4.4** Insertion de la marque pendant la compression.

### 4.6.2.3 Incorporation de la marque après la compression

Afin de réduire les besoins en stockage, les propriétaires de contenus ré-encodent souvent les fichiers vidéo avec un taux de compression différent ou selon un format de compression différent. L'insertion de la marque directement dans le flux vidéo compressé permet souvent un traitement en temps réel de la vidéo. Cependant, l'introduction d'un seul changement dans le domaine compressé peut jouer sur la préservation de la qualité. C'est un problème dans de telles méthodes. De plus, ces techniques sont intrinsèquement liées à un standard de compression vidéo et peuvent ne pas être robustes en conversion de format vidéo [84].

## 4.6.3 Intégration de la dimension temporelle

Les principaux problèmes des techniques de tatouage vidéo image par image sont dus au fait que la nouvelle dimension temporelle n'est pas prise en compte. Des solutions à ce problème sont proposées dans la littérature en tenant compte que le contenu vidéo est considéré comme un signal tridimensionnel et tenant compte aussi des propriétés du système visuel humain (HVS).

#### 4.6.3.1 Contenu vidéo considéré comme un signal tridimensionnel

En considérant la vidéo comme un signal tridimensionnel, de nombreuses transformations 3D telles que la transformée de Fourier discrète 3D (DFT) [57], la transformée en ondelettes 3D (3D-DWT) [58] et la transformée 3D en cosinus discret (3D-DCT) [3D-DCT) [91] peuvent être exploitées pour le tatouage vidéo en incorporant le marque dans la zone de moyenne fréquence pour fournir une bonne robustesse et une grande imperceptibilité. L'avantage de cette technique est la grande robustesse à la modification temporelle. Cependant, les coûts de calcul requis sont importants.

#### 4.6.3.2 Considération des propriétés du système visuel humain (HVS)

De nombreux chercheurs ont étudié comment réduire l'impact visuel de l'intégration d'une marque dans les images fixes en prenant en compte les propriétés du système visuel humain (HVS), telles que le masquage de fréquence, le masquage de luminance et le masquage de contraste. Ces études sont facilement exportées vers la vidéo en utilisant les techniques « image par image ». Cependant, ces techniques ne prennent pas en compte les propriétés temporelles d'une vidéo. Le mouvement est la caractéristique la plus importante de la vidéo, nous devons donc créer de nouvelles mesures conceptuelles qui doivent être conçues sur cette base pour être utilisées dans le tatouage vidéo numérique [84].

## 4.7 Présentation d'une technique de tatouage vidéo basée sur la décomposition en valeurs singulières (SVD) et sa version multi-résolution (MR-SVD)

Dans cette section, nous décrivons une technique de tatouage vidéo basée sur la combinaison de la SVD et la MR-SVD. Nous prenons la taille de la marque binaire égale à la partie approximative de la décomposition de premier niveau de l'image vidéo originale, obtenue en appliquant la MR-SVD.

### 4.7.1 Procédure d'insertion

Les étapes du processus d'insertion de la marque peuvent être résumées comme suit:

1. La vidéo originale est partitionnée en $k$ trames.

2. Chaque trame est convertie de l'espace colorimétrique $RGB$ vers l'espace $YC_bC_r$.
3. La MR-SVD à un seul niveau est appliquée sur la luminance $Y$ de chaque trame pour obtenir une composante d'approximation $\{\emptyset\}$ et des composantes de détails telle que : $\{\varphi_1, \varphi_2, \varphi_3\}$.
4. La SVD est appliqué à la composante $\{\emptyset\}$ de la luminance $Y$ pour chaque trame de la vidéo originale.

$$\emptyset(k) = U_\emptyset(k) \cdot S_\emptyset(k) \cdot V_\emptyset^T(k) \quad (4.3)$$

avec $k = 1, 2 \ldots N$, $N$ est le nombre de trames.

5. La marque binaire $w$ est ajoutée à la matrice $S_\emptyset(k)$ de chaque trame de la vidéo telle que :

$$E(k) = S_\emptyset(k) + \alpha \cdot w \quad (4.4)$$

$\alpha$ est la force d'insertion de la marque.

6. La SVD est appliquée sur chaque matrice $E(k)$ de chaque trame.

$$E(k) = U_w(k) \cdot S_w(k) \cdot V_w^T(k) \quad (4.5)$$

7. La SVD inverse est appliquée à la matrice des valeurs singulières modifiées $S_w(k)$ et aux $U_\emptyset(k)$ et $V_\emptyset(k)$ (obtenues de l'équation (4.3)) pour construire la partie d'approximation modifiée de chaque trame.
8. La MR-SVD inverse est appliquée sur la partie d'approximation $\{\emptyset'\}$ modifiée et sur $\{\varphi_1, \varphi_2, \varphi_3\}$ de chaque trame pour obtenir la partie de luminance modifiée $Y'$.
9. Reconstruire la trame de la vidéo tatouée à partir des parties de luminance modifiée $Y'$ et des chrominances $C_b$ et $C_r$ de la trame originale en faisant la conversion de l'espace $YC_bC_r$ vers l'espace colorimétrique $RGB$.

### 4.7.2 Procédure d'extraction

1. La vidéo tatouée et la vidéo originale sont partitionnées en $k$ trames.
2. Chaque trame est convertie de l'espace colorimétrique $RGB$ vers l'espace $YC_bC_r$.
3. La MR-SVD à un seul niveau est appliquée sur la luminance $Y_w$ de chaque trame de la vidéo tatouée pour obtenir une composante d'approximation $\{\emptyset_w\}$ et des composantes de détails telle que : $\{\varphi_{w1}, \varphi_{w2}, \varphi_{w3}\}$.

4. La MR-SVD à un seul niveau est appliquée sur la luminance $Y$ de chaque trame de la vidéo originale pour obtenir une composante d'approximation $\{\emptyset\}$ et des composantes de détails telle que : $\{\varphi_1, \varphi_{2,}\varphi_3\}$.
5. La SVD est appliquée à la composante d'approximation $\{\emptyset_w\}$ de la luminance $Y_w$ pour chaque trame de la vidéo tatouée:

$$\emptyset_w(k) = U_W(k) \cdot S_w(k) \cdot V_W^T(k) \quad (4.6)$$

6. La SVD est appliquée à la composante d'approximation $\{\emptyset(k)\}$ de la luminance $Y$ pour chaque trame de la vidéo originale:

$$\emptyset(k) = U(k) \cdot S(k) \cdot V^t(k) \quad (4.7)$$

7. Calculer la matrice $E$ telle que :

$$E(k) = S(k) + \alpha \cdot W \quad (4.8)$$

8. La SVD est appliquée à la matrice $E$ :

$$D = U_E \cdot S_E \cdot V_E^T \quad (4.9)$$

9. Création de la matrice $E'$ telle que :

$$E' = U_E \cdot S_w \cdot V_E^T \quad (4.10)$$

10. La marque est extraite de l'image tatouée comme suit :

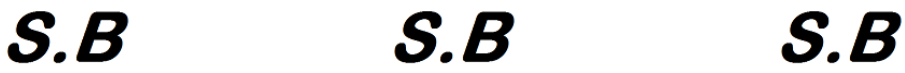
$$W' = \frac{E' - s}{\alpha} \quad (2.39) \quad (4.11)$$

### 4.7.3 Résultats expérimentaux

Dans cette section, nous évaluons les performances de la technique de tatouage vidéo proposée en termes d'imperceptibilité et de robustesse. Nous utilisons trois séquences vidéo différentes: xylophone et tennis de résolution $240 \times 320$ et avec une cadence de 30 trames par seconde et la séquence de vidéo foreman de résolution $352 \times 288$. La marque insérée pour les deux premiers vidéos est une image binaire de taille $120 \times 160$ et pour la troisième vidéo elle est de taille $256 \times 256$. Ici, nous avons pris le facteur d'échelle $\alpha = 9$. (**figure 4.5**)

$(a)$

$(b)$




$(c)$

**Figure 4.5** (a) Des trames de vidéos de test, (b) leurs trames tatouées et (c) les marques extraites

#### 4.7.3.1 Performances d'imperceptibilité

La transparence de la marque est estimée par le PSNR, est mesuré en décibels (dB) comme suit:

$$PSNR = 10 \cdot log_{10}\left(\frac{Max\,(I(i,j))^2}{EQM}\right) \quad (412)$$

$$EQM = \frac{1}{M \cdot n}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|I_0(i,j) - I_r(i,j)|^2 \quad (4.13)$$

Le $PSNR$ de toutes les images de la vidéo est donné par:

$$psnr = \frac{\sum_{i=1}^{k} PSNR\,(i)}{k} \quad (4.14)$$

avec $k$ le nombre total des trames.

Le PSNR entre la vidéo originale et la vidéo tatouée a des valeurs comprises entre 49 et 52 dB. Ces valeurs élevées de PSNR prouvent l'imperceptibilité de la méthode proposée.

#### 4.7.3.2 Performance de robustesse

Pour vérifier la robustesse de notre technique de tatouage, différents types d'attaques ont été mis en œuvre tels que la compression JPEG, l'ajout de bruit, la compression MPEG…
La comparaison entre la marque originale et la marque extraite des images vidéo tatouée et attaquées a été mesurée en utilisant le facteur de corrélation NC.

Les **tableaux 2.4** et **2.5** confirment la relation entre la force et les performances du tatouage. En effet nous constatons qu'il y a une proportionnalité remarquable entre le NC et $\alpha$ qui se traduit par une augmentation de robustesse à chaque fois que la force du tatouage augmente. Toutefois nous remarquons une proportionnalité inverse entre le PSNR et $\alpha$ qui s'interpréte par une diminution de l'imperceptibilité à chaque fois que cette force de tatouage augmente.

| $\alpha$ | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|
| **PSNR** | 56.8781 | 54.4501 | 52.4673 | 50.8162 | 49.4404 | 48.2598 |
| **NC** | 0.9931 | 0.9940 | 0.9946 | 0.9953 | 0.9957 | 0.9960 |

**Tableau 4.2** Mesures des PSNR et NC pour différentes valeurs de $\alpha$ pour la vidéo de xylophone.

| $\alpha$ | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|
| **PSNR** | 58.7235 | 56.0644 | 54.0855 | 52.4660 | 51.0627 | 49.8149 |
| **NC** | 0.9917 | 0.9949 | 0.9968 | 0.9978 | 0.9985 | 0.9990 |

**Tableau4.3** Mesures des PSNR et NC pour différentes valeurs de $\alpha$ pour la vidéo de foreman.

Le tableau suivant montre les marques extraites après l'exécution des différentes attaques.

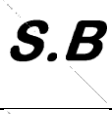
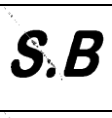
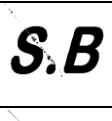
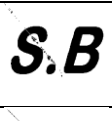
| Attaques | Marques extraites | NC |
|---|---|---|
| **La compression JPEG 70%** |  | 0.983 |
| **Salt and pepper** |  | 0.982 |
| **Le bruit poisson** |  | 0.982 |
| **Le filtre Median** |  | 0.9702 |
| **La compression MPEG2** |  | 0.9813 |
| **La compression H.264** |  | 0.9809 |
| **Cropping** |  | 0.9739 |

**Tableau 4.4** Marques extraites et valeurs de NC après différentes attaques.

#### 4.7.3.3 Comparaison avec des techniques existants

Afin d'étudier les performances de la méthode proposée, nous la comparons avec des méthodes existantes utilisant la combinaison DWT –SVD [92-93].

| Attaques | [92] | [93] | Méthode proposée |
|---|---|---|---|
| Compression JPEG | 0.869 | / | 0.983 |
| Salt and pepper | 0.694 | 0.654 | 0.976 |
| Le filtre Median | 0.921 | 0.577 | 0.970 |
| Cropping | / | 0.680 | 0.973 |

**Figure 4.5** Comparaison en termes de NC entre la méthode présentée et d'autres méthodes existantes.

## 4.8 Conclusion

Dans ce chapitre, Nous avons présenté le contexte technique qui entoure le domaine du tatouage de la vidéo qui est très différent de celui de l'image fixe. En effet, un flux vidéo possède ses propres caractéristiques qui différent de ceux de l'image. Ces propriétés sont exploitées pour le tatouage afin d'avoir des schémas assez robustes puisque les techniques de tatouage d'images présentent des limites et sont fragiles par rapport aux attaques spécifiques à la vidéo. La plupart des méthodes s'appliquent dans un domaine compressé. Seules, quelques techniques insèrent directement leur signature dans la vidéo décompressée. Nous avons aussi présenté un schéma de tatouage vidéo image par image, basée sur les transformées SVD et MR-SVD. La marque est invisible et cette méthode est robuste contre les différentes attaques appliquées.

# *Conclusion générale*

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes de la sécurité des fichiers multimédia dont les images fixes et la vidéo. La sécurisation des images stockées ou transmises est généralement effectuée par des techniques de tatouage dont leur développement est devenu un grand challenge dans ces dernières années. Après une étude bibliographique approfondie des techniques de tatouage d'images basées sur les transformées discrètes, nous avons constaté qu'elles ne sont pas très robustes aux attaques. Le projet que nous avons abordé avait pour objectif de renforcer la robustesse des techniques de tatouage basées sur les transformées discrètes et d'améliorer la qualité visuelle des images tatouées.

Dans cette thèse, nous avons présenté nos principales contributions de notre travail de doctorat qui se résument en deux méthodes de tatouage d'images fixes et une de tatouage vidéo, basées sur les transformées discrètes. Ce sont des techniques qui offrent une forte robustesse face aux différentes attaques de traitement du signal usuellement appliquées aux images et à la vidéo, et assurent particulièrement une meilleure résistance à la compression JPEG.

La première contribution est une technique aveugle et pouvant être très sécurisante par l'utilisation de plus d'une clé secrète puisque elle est basée sur la transformée de Fourier discrète paramétrique qui possède plusieurs paramètres indépendants qui peuvent être alors utilisés comme des clés supplémentaires.

La deuxième contribution est une approche hybride de tatouage des images fixes, aveugle et robuste contre la plus part des attaques telles que la compression JPEG, l'ajout de bruit et le filtrage. Elle s'article sur l'exploitation de la méthode de diffusion anisotrope de Perona-Malik, bien connue et appliquée au dé-bruitage d'images, dans le domaine de tatouage des images fixes. Cette dernière est utilisée pour la sélection des blocs significatifs pour l'insertion de la marque binaire, ce qui assure l'aspect HVS (Human Visual System). Après l'application de la DCT sur les blocs sélectionnés, la SVD est effectuée sur chacun de ces blocs transformés afin de modifier quelques éléments de la matrice $U$ ($U_{31}$ et $U_{41}$) en fonction de certaines conditions définies. Pour mieux montrer l'efficacité de cette technique et pour renforcer les résultats expérimentaux, nous avons exploité cette approche dans le tatouage de plusieurs images de test en niveaux de gris et en couleur.

Notre troisième apport est l'application d'un algorithme hybride de tatouage vidéo grâce à l'utilisation de la combinaison entre la SVD et la MR-SVD. Cet algorithme, initialement développé et utilisé pour le tatouage d'images, a été étendu à la vidéo puisque cette dernière est une succession d'images fixes. Dans ce contexte le tatouage a été réalisé sur des trames de plusieurs vidéos de test et les résultats expérimentaux montrent l'efficacité et la robustesse de cet algorithme contre la plupart des attaques.

Les résultats de simulation pour l'évaluation de la robustesse et de la perceptibilité du tatouage, en réalisant des mesures objectives sur les images et les vidéos tatouées soumises aux différentes attaques, montrent clairement l'efficacité des algorithmes proposés dans cette thèse.

Dans notre travail de doctorat, nous nous sommes concentrés beaucoup plus sur le tatouage des images fixes. Alors, nous nous sommes fixés comme perspectives l'extension des ces algorithmes, et plus particulièrement celui utilisant la technique de Pérona- Malik comme système HVS, au tatouage des fichiers vidéo.

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes de la sécurité des fichiers multimédia dont les images fixes et la vidéo. La sécurisation des images stockées ou transmises est généralement effectuée par des techniques de tatouage dont leur développement est devenu un grand challenge dans ces dernières années. Après une étude bibliographique approfondie des techniques de tatouage d'images basées sur les transformées discrètes, nous avons constaté qu'elles ne sont pas très robustes aux attaques. Le projet que nous avons abordé avait pour objectif de renforcer la robustesse des techniques de tatouage basées sur les transformées discrètes et d'améliorer la qualité visuelle des images tatouées.

Dans cette thèse, nous avons présenté nos principales contributions de notre travail de doctorat qui se résument en deux méthodes de tatouage d'images fixes et une de tatouage vidéo, basées sur les transformées discrètes. Ce sont des techniques qui offrent une forte robustesse face aux différentes attaques de traitement du signal usuellement appliquées aux images et à la vidéo, et assurent particulièrement une meilleure résistance à la compression JPEG.

La première contribution est une technique aveugle et pouvant être très sécurisante par l'utilisation de plus d'une clé secrète puisque elle est basée sur la transformée de Fourier discrète paramétrique qui possède plusieurs paramètres indépendants qui peuvent être alors utilisés comme des clés supplémentaires.

La deuxième contribution est une approche hybride de tatouage des images fixes, aveugle et robuste contre la plus part des attaques telles que la compression JPEG, l'ajout de bruit et le filtrage. Elle s'article sur l'exploitation de la méthode de diffusion anisotrope de Perona-Malik, bien connue et appliquée au dé-bruitage d'images, dans le domaine de tatouage des images fixes. Cette dernière est utilisée pour la sélection des blocs significatifs pour l'insertion de la marque binaire, ce qui assure l'aspect HVS (Human Visual System). Après l'application de la DCT sur les blocs sélectionnés, la SVD est effectuée sur chacun de ces blocs transformés afin de modifier quelques éléments de la matrice $U$ ($U_{31}$ et $U_{41}$) en fonction de certaines conditions définies. Pour mieux montrer l'efficacité de cette technique et pour renforcer les résultats expérimentaux, nous avons exploité cette approche dans le tatouage de plusieurs images de test en niveaux de gris et en couleur.

Notre troisième apport est l'application d'un algorithme hybride de tatouage vidéo grâce à l'utilisation de la combinaison entre la SVD et la MR-SVD. Cet algorithme, initialement développé et utilisé pour le tatouage d'images, a été étendu à la vidéo puisque cette dernière est une succession d'images fixes. Dans ce contexte le tatouage a été réalisé sur des trames de plusieurs vidéos de test et les résultats expérimentaux montrent l'efficacité et la robustesse de cet algorithme contre la plupart des attaques.

Les résultats de simulation pour l'évaluation de la robustesse et de la perceptibilité du tatouage, en réalisant des mesures objectives sur les images et les vidéos tatouées soumises aux différentes attaques, montrent clairement l'efficacité des algorithmes proposés dans cette thèse.

Dans notre travail de doctorat, nous nous sommes concentrés beaucoup plus sur le tatouage des images fixes. Alors, nous nous sommes fixés comme perspectives l'extension des ces algorithmes, et plus particulièrement celui utilisant la technique de Pérona- Malik comme système HVS, au tatouage des fichiers vidéo.

# Bibliography


[1] V. Martin, “Contribution des filtres LPTV et des techniques d’interpolation au tatouage numérique,” Thèse PhD, Ecole doctorale : Informatique et Télécommunications, Spécialité : Signal, Image, Acoustique et Optimisation, 2006.

[2] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia. Image Processing,” *IEEE Transaction on image processing*, Vol. 6, No. 12, pp. 1673–1687, December 1997.

[3] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for images, audio and video,” *Proceedings of the International Conference on Image Processing*, pp. 243–246, 1996.

[4] C.-C. Chang, P. Tsai, C.-C. Lin, “SVD-based digital image watermarking scheme”, *Recognition Letters*, vol. 26, no. 10, pp. 1577–1586, 2005. DOI:10.1016/j.patrec.2005.01.004.

[5] K.-L. Chung, W.-N. Yang, Y.-H. Huang, S.-T Wu, Y.-C. Hsu, “On SVD-based watermarking algorithm”, Applied *Mathematics and Computation*, vol. 188, no. 1, pp. 54-57, 2007. DOI: 10.1016/j.amc. 2006.09.117.

[6] M.-Q. Fan, H.-X. Wang, S.-K. Li ‘’Restudy on SVD-based watermarking scheme’’, *Applied Mathematics and Computation*, vol. 203, no 2, pp. 926–930, 2008. DOI:10.1016/j.amc.2008.05.003.

[7] C.-C. Lai, “An improved SVD-based watermarking scheme using human visual characteristics”, *Optics Communication*, vol. 284, no. 4, pp. 938-944, 2011. DOI: 10.1016/j.optcom.2010.10.047.

[15] J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, ‘’Digital Watermarking and Steganography ‘’, *Second Edition* Ingemar, vol. 624, November 2007.

[16] J. Simpson and E. Weiner, editors. *Oxford English Dictionary*. *Oxford University Press, 2000.*

[17] Dard Hunter. *Handmade Paper and Its Watermarks: A Bibliography*. B. Franklin, New York, 1967.

[18] Mathison. *Gentlemen’s Magazine*, XLIX, 1779.

[19]David Kahn. *The Codebreakers—The Story of Secret Writing*. Scribner, New York, 1967.

[20] B. Schneier, “Cryptographie appliquée : Algorithme, protocoles et codes sources en C,” *Vuibert Informatique*, deuxième édition, janvier 2001.

[21] J. Dumas, J. Roch, E. Tannier, and S. Varrette, "*Théorie des codes-compression cryptage, correction*," *Dunod*, France, 2007.

[22] M.Ali Hajjaji, ''Tatouage numérique des images: Application à la messagerie médicale'', thèse de doctorat, Université de Monastir,Tunis,2013.

[23] Hanène Trichili, ''Elaboration d'une nouvelle approche de tatouage pour l'indexation des images médicales'', PhD thesis, *Ecole nationale supérieure de télécommunications*, France, 2006.

[24] Fadoua Drira, Florence Denis, and Antilla Baskurt, ''Tatouage d'images par techniques multidirections et multirésolutions''. Liris 2004.

[25] D. Augot, J.M. Boucqueau, J.F. Delaigle, C. Fontaine, and E. Goray, ''Securebdelivery of images over open networks'', *Proc. of the IEEE*, 87 :1251–1267, July 1999.

[26] C. Fontaine, ''Contribution à la recherche de fonctions booléennes hautement non linéaires, et au marquage d'images en vue de la protection des droits d'auteur'', PhD thesis, Thèse de Doctorat de l'université Paris 6, Novembre 1998.

[27] J.O. Ruanaidh, H. Petersen, A. Herrigel, S. Pereira, and T. Pun ''Cryptographic copyright protection for digital images based on watermarking techniques'', Theoretical *Computer Science*, 226 :117–142, September 1999.

[28] I. Farah, I. Ismail, and M. Ahmed, ''A watermarking system using the wavelet technique for satellite image'', *World academy of science, engineering and technology*, 2006.

[29] S. Bekkouche, ''Etude et implémentation des techniques de tatouage numérique '', thèse de Doctorat, Université de Djillali Liabes, Faculté des sciences exactes, Sidi Bel Abbes, 2017.

[30] Gael Chareyron, ''Tatouage image : une approche couleur'', PhD thesis, Université Jean Monnet, Saint-Etienne, France, 2005.

[31] Gouenou Coatrieux and Henri Maitre. ''Images médicales, sécurité et tatouage annals of telecommunications'', pages 782–800, 2003.

[32] M. George, J.Y. Chouinard, and N. Georganas. "Spread spectrum spatial and spectral watermarking for images and video". In *IEEE Canadian Workshop on Information Theory*, Kingston, Canada, :119,122, juin 1999.

[33] G. Doerr et J. Luc Dugelay, ''Problématique de la Collusion en Tatouage Vidéo Collusion Issue in VideoWatermarking ''.

[34] G. Doerr et J.-L. Dugelay. ''A guide tour of video watermarking''. S*ignal Processing : Image Communication*, Special Issue on Technologies for Image Security, 18(4) :263–282, April 2003.

[35] K. Su, D. Kundur, et D. Hatzinakos. ‘’A novel approach to collusion resistant video watermarking’’. *Security and Watermarking of Multimedia* Contents IV, volume 4675 de Proceedings of SPIE, pages 491–502, January 2002.

[36] G. Do¨err et J.-L. Dugelay. ‘’Collusion issue in video watermarking dans Security, Steganography and Watermarking of Multimedia’’, *Proceedings of SPIE,* Contents VII, , volume 5681, pages 685–696, January 2005.

[37] Y. Terchi, ‘’Développement de nouvelles techniques fréquentielles de tatouage du signal audio’’, thèse de Doctorat, département d’électronique, Université Ferhat Abbes, Sétif,2018.

[38] M.A. Akhaee, N. Khademi Kalantari, F. Marvasti, ‘’Robust audio and speech watermarking using Gaussian and Laplacian modeling’’, Signal Processing. 90 (2010) 2487–2497. doi:10.1016/j.sigpro.2010.02.013.

[39] Sondes Ajili. tatouage des images médicales : ‘’Approche basée sur dct’’. Thèse de master, *Ecole Nationale d’Ingenieurs de Sousse,* Tunisie, 14 juillet 2012.

[40] B. Patrick and C. Jean Marc. ‘’Tatouage couleur adaptatif fondé sur l’utilisation d’espaces perceptifs uniformes’’. *Laboratoire des Images et des Signaux*, Saint Martin d’Hères , France, juin 2004.

[41] M. D. Adams and F. Kossentni. ‘’Reversible integer to integer wavelet transforms for image compression : Performance evaluation and analysis’’. *IEEE Transactions on Image Processing archive*, 9 :1010, 1024, June 2000.

[42]I.F. Jafar, K.A. Darabkh, R.T. Al-Zubi, R.R. Saifan, ‘’An efficient reversible data hiding algorithm using two steganographic images’’, *Signal Processing*. 128 (2016) 98–109. doi: 10.1016/j.sigpro.2016.03.023.

[43] J. Zhou, W. Sun, L. Dong, X. Liu, O.C. Au, Y.Y. Tang, ‘’Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation’’, *IEEE Trans. Circuits Syst. Video Technol*. 26 (2016) 441–452. doi:10.1109/TCSVT.2015.2416591.

[44] Z. Guoliang. ‘’Face recognition with singular value decomposition’’. *CISSE Proceeding*, 2006.

[45]X. He-Huan L. Li, C. Chin-Chen, and M. Ying-Ying. ‘’A novel image watermarking in redistributed invariant wavelet domain’’. *Journal of Systems and Software*, 84 :923–929, 2011.

[46] A. NINASSI, O. LE MEUR, P. LE CALLET, D. BARBA, and A. TIREL. ‘’Task impact on the visual attention in subjective image quality assessment’’. *European Signal Processing Conference*, Florence, Italy, September, 2006.

[47]H. Guan, Z. Zeng, S. Zhang. "A new dct-based digital image watermarking algorithm", *International Conference on Automatic Control and Artificial Intelligence, ACAI*, pp.166-169, March 2012.

[48]Nasrin M. Makbol and Bee Ee Khoo. ''Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition''. *International Journal of Electronics and Communications* (AEU), 67 :102,112, 2013.

[49] Khalil I. Al saif, Sundus Khaleel Ebraheem, and Ghada Thanon Yuonis. ''Copyrightauthentication by using karhunen-loeve transform''. *Journal of university of anbar for pure scienc*, 6 :1,8, 2012

[50] Khalil I. Al saif, Sundus Khaleel Ebraheem, and Ghada Thanon Yuonis. ''Copyright authentication by using karhunen-loeve transform''. *Journal of university of anbar for pure scienc*, 6 :1,7, 2013.

[51] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding secret information into a dithered multilevel image. IEEE Military Communications Conf. USA, 1 :216,220, 1990.

[52] Y. Park, H. Kang, K. Yamaguchi, and K. Kobayashi. ''Watermarking for tamper detection and recovery''. *IEICE Electronics Express*, 5 :689,696, 2008.

[53] S.Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, and J. Su. ''Attacks on DigitalWatermarks : Classification, Estimation-based Attacks and Benchmarks''. *IEEE CommunMag*, 39(9) :118–126, 2001.

[54] I. Nouioua, ''Développement et Implémentation d'Algorithmes de Tatouage Numérique des Données Multimédia'', thése de doctorat, département d'électronique, Université Ferhat Abbes, Sétif, 2019.

[55] M. Ben Halima, W. Boussella, M. Charfi, A. Alimi, " Restauration des images couleurs de documents arabes anciens basé sur les EDPs," in *Laurence Likforeman-Sulemroc*, pp. 103-108, September, 2006

[56] A.-B. Watson, "Image Compression Using the Discrete Cosine Transform", *Mathematica Journal*, vol. 4, no. 1, pp. 81-88, 1994. DOI: 10.1007/978-3-322-96658-2_5.

[57]M. Aurélie. Représentations parcimonieuses adaptées à la compression d'images. PhD thesis, Université Européenne de Bretagne, France, 2 Avril 2010.

[58] T. Bekkouche, ''Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes'', thèse de Doctorat, département d'électronique, Université Ferhat Abbes, Sétif, 2018.

[59] S. Bouguezel and al., "New Parametric Discrete Fourier and Hartley Transforms, and Algorithms for Fast Computation," *IEEE Trans. on Cir. and Syst.,* Vol. **58**, no.3, pp. 562-575,

2011.

[60] S. Bouguezel, M. O. Ahmad, and M. N. S. Swamy, "A new class of reciprocal-orthogonal parametric transforms," *IEEE Trans. Circuits Syst I. Reg. Papers.*, Vol.**56**, no. 4, pp. 795-805, 2009.

[61] C. C. Tseng, "Eigen values and eigenvectors of generalized DFT, generalized DHT, DCT-IV and DST-IV matrices," *IEEE Trans. Signal Process*., Vol. **50**, no. 4,pp. 866-877,2002.

[62] J. Guo, Z. Liu, and S. Liu, "Watermarking based on discrete fractional random transform," *Opt.commun.*, Vol. **272**, no. 2, pp. 344-348, 2007.

[63] J. M. Vilardy and al., "Digital images phase encryption using fractional Fourier transform, " *Proc. Conf. Electron. Robot. Automo.Mech, Morelos, Mexico*, pp. 15–18, Sep 2006.

[64] I. Nouioua, N. Amardjia, S. Belilita, "A novel Blind and Robust Video Watermarking Technique in Fast Motion Frames Based on SVD and MR-SVD'', *Security and Communication Networks*, p 17, November 2018. DOI: 10.1155/2018/6712065.

[65] L. Cao, "Singular Value Decomposition Applied To Digital Image Processing", Division of Computing Studies, Arizona Arizona State, University Polytechnic Campus, Mesa, Arizona 85212, pp. 1-15.

[66] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", *Digital Signal Processing*, vol. 21, no. 4, pp. 522-527, 2011. DOI: 10.1016/j.dsp.2011.01.017.

[67] Megalingam, R.K. ; Nair, M.M. ; Srikumar, R. ; Balasubramanian, V.K. ; Sarma, V.S.V., "Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques," *International Conference on Signal Acquisition and Processing*, 2010. ICSAP '10.

[68] S. Belilita, N. Amardjia, T. Bekkouche and I. Nouioua, '' Combining SVD-DCT Image Watermarking Scheme Based on Perona-Malik Diffusion'', Elektronika ir Elektrotechnika journal, Vol. 25 No 4, Augest 2019, DOI: https://doi.org/10.5755/j01.eie.25.4.23973.

[69] S.-l. Jia, "A novel blind color images watermarking based on SVD", *Optik – Int. Light Electron Opt*, January 23-27, 2014. DOI: 10.1016/j.ijleo.2014.01.002.

[70] J. Weickert, "Anisotropic diffusion on image processing", *ECMI Series*, 1998.

[71] A. Atlas, F. Karami, D. Meskine, "The Perona-Malik inequality and application to image de-noising", *Nonlinear analysis: Real World Applications*, vol. 18, pp. 57-68, August 2014. DOI: 10.1016/j.nonrwa.2013.11.006.

[72] De-noising using variations of Perona-Malik model with different edge stopping functions",

*Procedia Computer Science*, vol. 58, pp. 673-682, 2015, DOI: 10.1016/j.procs.2015.08.087.

[73] P. Perona, J. Malik, "Scale-space and edge detection using anisotropic diffusion", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.12, no 7, pp. 629-639, 1990. DOI: 10.1109/34.56205.

[74] L. C. Evans, "Partial Differential Equations", *Graduate Studies in Mathematics*, vol. 19, American Mathematical Society, Providence, Rhode Island, 1998. DOI: 10.1090/gsm/019

[75] S. Deb, " Video Data Management and Information Retrieval", IRM Press pp. 321-346, IRM Press, 2005

[76] D.A. Cook, "A history of narrative film," second Edition, p2 W.W. *Norton & Compnay Inc*. New York, 1990.

[77] T. Wiegand , "Digital Image Communication Digital," Course at Technical University of Berlin,2003.

[78] G.J. Sullivan, J.R. Ohm; W.J. Han; T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard," *IEEE Transactions on Circuits and Systems for Video Technology*, 2013

[79] https://www.youtube.com/yt/about/press/ access 17/02/2019.

[80]Glossary of video terms and acronyms : www.tektronix.com

[81] D. Ghosh, and K. Ramakrishna, "Watermarking Compressed Video Stream over Internet," *The 9th Asia-Pacific Conference on Communications 2003 (APCC2003)*, Vol.2, pp.711-715, 2003.

[82] A. Bouderbala, ''Implémentation d'un algorithme de tatouage Vidéo robuste dans Le domaine compressé'', thèse de Magister, Faculté des sciences de l'ingénieure, Université Mentouri Constantine.

[83] G. Doërr, "Security issue and collusion attacks in video watermarking," doctoral thesis, 2005.

[84] G. Doërr and J.L. Dugelay, "A Guide Tour of Video Watermarking", *Signal Processing: Image Communication*, vol.18, no.4,pp. 263-282, 2003

[85] W.H Chen, C.H. Smith, and S.C. Fralick, "A fast computational algorithm for the discrete cosine transform," *IEEE Trans. Commun*., vol. COM-25, pp. 1004-1009. 1977.

[86] E.T.Lin, and E.J. Delp,"Temporal synchronization in video watermarking," *IEEE Transactions on Signal Processing* ,vol.52 ,pp. 3007-3022,2002.

[87] A. BOUDERBALA, "Implémentation d'un algorithme de tatouage Vidéo robuste dans Le domaine compressé, " thèse de magister.

[88] L. E. A. SAUERBRONN, M. A. DREUX, “Transparent Digital Watermark, ” *In Monografias do Departamento de Informática da PUC-Rio*, 2000, Rio de Janeiro, 2000.

[89] A. Boho, G. V. Wallendael, A. Dooms, J. D. Cock, G. Braeckman, P. Schelkens, B. Preneel, and R. Van de Walle, “End-to-end security for video distribution,” *IEEE Signal Process. Mag*., vol. 30, no. 2, pp. 97–107, 2013

[90] S.Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative Encryption and Watermarking in Video Compression,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol.17, no.6, pp. 774–778, 2007.

[91] H.Park, S.H. Lee, Y.S. Moon, “Adaptive video watermarking utilizing video characteristics in 3D-DCT domain”, in: Digital Watermarking,” Springer, pp. 397– 406, 2006.

[92] O. S. Faragallah, “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain,” *AEU-International Journal of Electronics and Communications*, vol. 67, no. 3, pp.189-196, 2013.

[93] K. Niu, X. Yang, L. Xiang., “Hybrid quasi-3d dwt/dct and svd video watermarking,” in *proceedings of International Conference on Software Engineering and Service Sciences (ICSESS)*, pp. 588-591, Beijing, China, 16-18 July 2010.

**Summary**

In this thesis, we present three contributions in the field of image and video watermarking. In the first contribution, we propose a new blind watermarking method that can be very secure by using more than one secret key since it is based on the parametric discrete Fourier transform (PDFT) which provide several independent parameters that can be used as additional keys. In the second contribution, we propose a new hybrid (based on the 2D-DCT and the SVD) watermarking technique for still images that is blind and robust against most attacks such as JPEG compression, noise addition and filtering. It focuses on the exploitation of the anisotropic diffusion method of Perona-Malik, a well known process applied in image denoising, in the field of still images watermarking. The Perona-Malik method is used in the selection of significant blocks for inserting the binary mark, which ensures the HVS (Human Visual System) aspect. In the third contribution we present a robust hybrid video watermarking algorithm based on SVD and MR-SVD.

**Keywords**: Still images and video watermarking; Anisotropic diffusion of Pérona-Malik ; PDFT; 2D-DCT; SVD; MR-SVD.

**Résumé**

Dans cette thèse, nous présentons trois contributions dans le domaine du tatouage d'images et vidéo. Dans la première contribution, nous proposons une nouvelle méthode de tatouage aveugle et pouvant être très sécurisante par l'utilisation de plus d'une clé secrète puisque elle est basée sur la transformée de Fourier discrète paramétrique (PDFT) qui possède plusieurs paramètres indépendants pouvant être utilisés comme clés supplémentaires. Dans la deuxième contribution, nous proposons une nouvelle technique hybride (basée sur la 2D-DCT et la SVD) de tatouage des images fixes, aveugle et robuste contre la plus part des attaques telles que la compression JPEG, l'ajout de bruit et le filtrage. Elle s'article sur l'exploitation de la méthode de diffusion anisotrope de Perona-Malik, bien connue et appliquée au dé-bruitage d'images, dans le domaine de tatouage des images fixes. La méthode de Perona-Malik est utilisée pour la sélection des blocs significatifs pour l'insertion de la marque binaire. Ce qui assure l'aspect HVS (Human Visual System). Dans la troisième contribution nous présentons un algorithme hybride de tatouage vidéo robuste basé sur la SVD et la MR-SVD.

**Mots clés** : Tatouage d'images fixes et vidéo ; Diffusion anisotrope de Pérona-Malik ; PDFT ; 2D-DCT; SVD ; MR-SVD.

**ملخص**

في هذه الرسالة، نقدم مساهمتين في مجال صور الوشم. في المساهمة الأولى، نقترح طريقة جديدة للوشم الأعمى التي يمكن أن تكون آمنة للغاية باستخدام أكثر من مفتاح سري لأنه يعتمد على تحويل PDFT الذي يحتوي على العديد من المعلمات المستقلة التي يمكن استخدامها بعد ذلك ك مفتاح إضافي. في المساهمة الثانية ، نقترح تقنية هجينة جديدة من الوشم الصور الثابتة ، أعمى وقوية ضد معظم الهجمات مثل ضغط JPEG ، إضافة الضوضاء والتصفية. إنه يركز على استغلال طريقة الانتشار متباين الخواص Perona-Malik ، المعروفة والمطبقة في تقليل الصور ، في مجال الصور الثابتة للوشم. يتم استخدام طريقة Perona-Malik لاختيار كتلة هامة لإدراج العلامة الثنائية ، والتي تضمن الجانب HVS (النظام البصري البشري ). في المساهمة الثالثة ، نقدم خوارزمية وشم فيديو هجينة قوية تعتمد على SVD و MR-SVD.

**الكلمات المفتاحية** : وشم الصور الثابتة و الفيديو ؛ نشر متباين الخواص من Pérona-Malik ؛ PDFT ؛ 2D-DCT ؛ SVD ؛ MR-SVD.