N° d'ordre :

REPUBLIQUE ALGERIENNE DEMOCRATIQUE & POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR & DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DJILLALI LIABES
FACULTE DES SCIENCES EXACTES
SIDI BEL ABBES

THESE
DE DOCTORAT

Présentée par

Mme Bekkouche Souad

Spécialité : *Informatique*
Option : *Informatique*

Intitulée

Etude et implémentation des techniques de tatouage numérique

Soutenue le ***30/04/2017***
Devant le jury composé de :

Président :	***Dr*** *Boukli Hacene Sofiane .MCA.UDL-SBA*
Examinateurs :	***Dr*** *Amar Bensaber Djamel.MCA.ESI-SBA*
	Dr *Hammou Reda Mohammed .MCA-Université Saida*
	Pr *Ali Pacha Adda -Usto-Oran*
Directeur de thèse :	***Pr*** *Faraoun Kamel Mohammed-UDL-SBA*

Année universitaire 2016 /2017

Dédicace

A mes ***chers parents*** *bien aimés*
A mon cher mari ***Hamid***
A ma chère petite fille ***Djenene.***
A mes sœurs Samira et fatna et mes frères ***Amine*** *et* ***Nassreddine****.*
A ma chère belle mère ***Chahba que son âme repose en paix.***
A mon beau père ***Maamar que Dieu le bénisse.***
A mes beaux frères Souar ***Youcef*** *et Souar* ***Mohamed.***

Remerciements

Je tiens tout d'abord à exprimer mes sincères remerciements à mon encadreur ***Mr. Faraoun Mohamed Kamel*** *qui a assumé la direction de ce travail et sa disponibilité et ses conseils m'ont permis d'accomplir ce travail dans les meilleures axes.*

Je remercie les membres de jury qui ont accepté de juger ce travail :
Dr. Boukli Hacene Sofiane*,* ***M.C.A à l'université de sidi bel abbes****, qui me fait le grand honneur d'accepter la présidence du jury.*
Dr. Amar Bensaber Djamel*.* ***M.C.A à l'université de sidi bel abbes*** *pour l'honneur qu'ils me font en acceptant de participer à ce jury.*
Dr Hammou Reda Mohammed .M.C.A-Université Saida *pour l'honneur qu'ils me font en acceptant de participer à ce jury.*
Pr Ali Pacha Adda. Professeur à l'université d'USTO Oran *pour l'honneur qu'ils me font en acceptant de participer à ce jury.*

Je réserve un remerciement chaleureux à mes chers parents.
Un grand merci à mon mari qui m'a toujours aidé, soutenu et encouragé.

SOMMAIRE

LISTE DES FIGURES

Liste des tableaux

Introduction Générale

Introduction Générale

Le développement des réseaux numériques et l'évolution rapide de la technologie informatique permettent de transmettre toutes sorte d'informations textuelles, sonores ou des images qui conduisent à la distribution illégale, la duplication et la modification facile et indétectable. Dans le domaine de la santé, la télémédecine prendre un rôle très important dans les applications médicales ou le problème reste au niveau de la transmission des données et les images médicales via l'internet ou l'apparition du tatouage est très important dans le but de sécuriser les images médicales partagées par les réseaux tout en conservant leur intégrité et leur authentification.

Ce développement et la croissance énorme des réseaux comme l'internet suivi par le développement des techniques performantes pour protéger le propriétaire des données contre l'enregistrement et la redistribution illégale. Parmi les premières techniques qui ont été réalisées pour garantir la sécurité lors de la transmission et la diffusion des données à travers le net est la cryptographie qui permet de crypter les documents et assurer les propriétés de sécurité (la confidentialité, l'intégrité et l'authentification) et permet de protéger les données seulement lors de sa transmission mais après le processus de décryptage ou déchiffrage le fichier n'est plus protégé et facilement diffusé par les utilisateurs non autorisé.

Dans les dernières décades le principe du tatouage est apparu comme l'une des méthodes pour protéger le droit d'auteur et assurer la sécurité des multimédias qui permet d'insérer une information secondaire ou une marque (logo ou nom du propriétaire) dans une image ou une vidéo ou un audio ou l'information insérée peut être extraite pour différentes buts. l'information secondaire insérée est une marque numérique qui est en général un code d'identification visible ou invisible qui peut contenir des informations sur le destinataire , le propriétaire légitime ou l'auteur , ses droits d'auteur sous la forme de données textuelles ou de l'image.

L'information pour être cachée est insérée en manipulant le contenu des données numériques, permettant à quelqu'un d'identifier le propriétaire originale. Cette marque numérique peut être détectée ou extraite plus tard pour faire une affirmation sur les données.

Les marques numériques restent intactes lors de sa transmission ou bien de sa transformation, ce qui nous permet de protéger nos droits de propriété sous la forme numérique. L'absence d'une marque dans une image précédemment marquée conduirait à la conclusion que le contenu de données a été modifié donc dans ce cas l'intégrité n'a pas été vérifiée.

Pour une protection efficace du droit d'auteur, la marque numérique doit être robuste, détectable à partir d'un document, de fournir l'information originale insérée fiable et doit être non – intrusive. Les marques robustes sont celles qui sont difficiles à éliminer à partir d'un objet dans lequel ils sont insérer malgré les variétés d'attaques possibles effectuée par des attaquants, y compris la compression tels que JPEG, mise à l'échelle, l'attaque géométrique tel que la rotation, la translation, le recadrage le bruit, le filtrage, les attaques cryptographiques et statistiques, ainsi que l'insertion d'autres marques.

Dans le but d'assurer les propriétés de sécurité, nous avons étudié le tatouage réversible qui permet de retrouver ou restaurer l'image originale, en évitant toutes les modifications possible lors de l'insertion de la marque.

L'objectif de cette thèse est d'étudier et de proposer des nouvelles méthodes de tatouage basés sur l'insertion deux types de marques (marque réversible qui est constituée à partir de l'image originale pour garantir l'authentification et l'intégrité) et la deuxième marque est un logo a crée à l'aide d'une clé secrète (pour assurer la confidentialité). Dans cette thèse, nous nous focaliserons principalement sur le tatouage réversible des images médicales et les images en niveau de gris.

Dans le chapitre 1, nous présentons un l'état de l'art sur l'aspect général de tatouage, nous y définissons la notion de tatouage selon le type d'algorithme, le champ d'application et le domaine d'utilisation. Nous présentons également les techniques de tatouage des images plus récentes et leurs applications par une description complète de différentes méthodes.

Dans le chapitre 2, nous focaliserons notre objectif sur l'étude du tatouage réversible et des différents travaux de littérature qui sont basés sur le tatouage réversible sont appliqués dans le domaine médical.

Dans le chapitre 3, nous présentons aussi les différentes méthodes dans le domaine transformé sont appliquées sur une image en niveau de gris.

Dans le chapitre 4, nous décrirons deux approches développées de tatouage réversible sont basées sur l'utilisation des images médicales en niveau de gris dans le but de réunir les trois caractéristiques de base de la sécurité (la confidentialité, l'intégrité, l'authentification) et nous présentons aussi la validation de notre approche par les mesures de l'évaluation de ses performances.

En fin nous concluons à partir les résultats de notre approche développée et nous présentons les nouvelles axes de recherche dans le domaine du tatouage réversible toujours dans le but de réunir les trois propriétés de sécurité ensemble.

Chapitre 1

Définitions et principe de tatouage numérique

Chapitre 1 *Définitions et principe de tatouage numérique*

1 Les principes et aspects généraux du tatouage

1.1 Introduction

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

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

1.2 Techniques de protection

G. Coatrieux et al **[Coa00]** ont été mentionnés que les techniques de sécurité et de protection basent sur trois propriétés : la confidentialité, l'intégrité et l'authentification.

- **Confidentialité :** sert à protéger le secret d'une donnée pour toutes personne non autorisé c'est-à-dire le fait que les données ne soient pas divulguées à d'autres que les ayants droit.
- **Authentification :** permet de vérifier l'authenticité ou l'identité des personnes.
- **Intégrité :** sert à garantir que les données ne soient ni tronquées ni modifiées notamment lors des mécanismes de stockage et de diffusion ou de transmission.

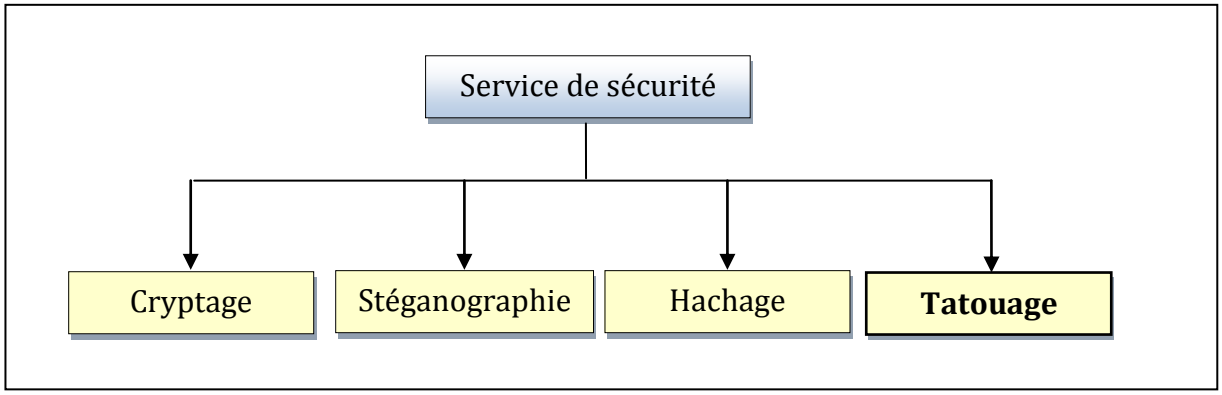


Figure 1.1 : *Service de sécurité.*

Deux méthodes de base de dissimulation d'information sont la cryptographie et la stéganographie.

La stéganographie **[Mitt99] [Fen06]** permet de cacher les données secrètes dans un canal ou dans un medium tel que l'attaque ne puisse savoir si l'information est cachée dans le canal (on parle de canal secret ou de communication secrète).

On peut aussi faire appel aux méthodes de stéganographie à clef secrète ou à clef publique sur un modèle proche de ce qui se fait en cryptologie **[Bek12]**.

La cryptographie **[Cha01] [Moe03] [Bor04]** est parmi les premières propositions pour assurer la sécurité de la transmission et le transfert de documents à travers le Net. La cryptographie est une technique largement utilisée pour protéger le contenu numérique des médias. Le message est chiffré avant la transmission et décrypté à l'extrémité de la réception à l'aide d'une clé, personne ne peut accéder au contenu sans avoir la véritable clé. Le message est appelé le texte et le message chiffré est appelé le texte chiffré. L'information est protégée avant le moment de la transmission, mais, après le décryptage, l'information devient non protégée et peut être copiée et distribuée **[Bek12]**.

a) Cryptographie

La cryptographie permet de rendre un message illisible pour garantir une parfaite sécurité (l'authentification, l'intégrité et la confidentialité,..). Elle consiste à transformer un texte en clair en un cryptogramme à l'aide d'une clé K_c *:*

$$C = E_{K_C}(M) \qquad \textbf{(1,1)}$$

Pour le décodage ou le déchiffrement du cryptogramme en texte en clair on applique la transformation inverse avec une clé K_D :

$$M = D^{K_D} \; [E^{K_C} \; (M)] \qquad \textbf{(1,2)}$$

E : Fonction de chiffrement.

D : Fonction de déchiffrement.

Les techniques de chiffrement de messages utilisent des clefs de chiffrement et de déchiffrement identiques (on appel les techniques symétriques), tel que les techniques qui sont basées sur l'utilisation des différentes clés secrètes : clé privé et clé publique (on appel les techniques asymétriques).

Parmi les techniques les plus utilisés actuellement, nous pouvons citer l'algorithme symétrique DES et l'algorithme asymétrique RSA. La représentation schématique de la cryptographie est donnée par la figure 1.2.

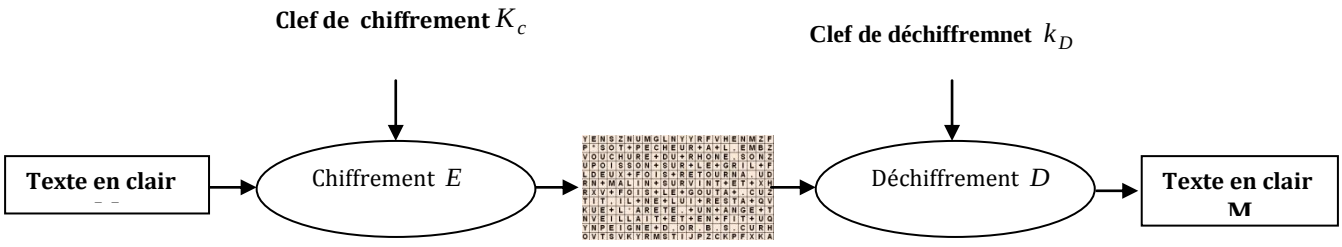


Figure 1.2 : *Schéma générique de cryptologie.*

b) Hachage

Est une fonction mathématique qui Permet de générer une empreinte quasiment unique d'une donnée ou d'un message de taille quelconque **[And93] [Pre93]** afin de s'assurer que le contenu n'a pas été modifié sinon l'empreinte serait différente.

L'empreinte peut être appelée aussi condensé, hash, ou encore somme de contrôle associé aux mécanismes d'authentification, dans certains protocoles de communication, l'échange de mails, l'échange de fichiers. Le Hachage a pour but de vérifier que le contenu n'a pas été modifié (intégrité).

L'authentification des images est réalisée en calculant le hachage de l'image reçue par l'utilisation d'une clé public pour décoder la signature numérique calculée pour révéler la

signature originale. Si les deux signatures sont identiques**,** l'image est authentifiée mais si sont différentes, l'intégrité n'est pas vérifiée.

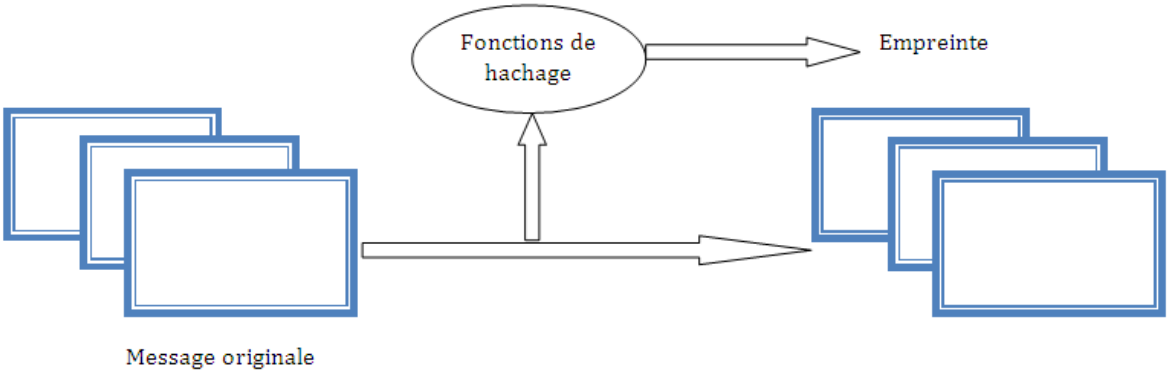


Figure 1.3 : *Principe de hachage.*

c) Stéganographie

Le terme stéganographie vient du mot Grec *steganos* signifiant *caché* et de *graphia* signifiant *écriture*, littéralement on traduit par *écriture cachée.* Dans la stéganographie, le message est inséré dans les médias numériques plutôt que de les crypter de manière que personne, sauf l'expéditeur et le destinataire peut savoir qu'il y'a un message caché. Le contenu multimédia numérique, appelé hôte, peut être déterminé par n'importe qui; mais, le message caché dans un média hôte peut être détecté que par la personne qui possède la clé secrète.

Ainsi la stéganographie reliée à des communications point-à-point entre deux parties. C'est pourquoi les méthodes stéganographique ne sont généralement pas robustes contre la modification des données, ou seulement une robustesse limitée. Le concept de tatouage numérique est dérivé de la stéganographie.

1.3 Tatouage des images numériques

1.3.1 Peu d'historique

Parmi ces premières publications traitant ce sujet de watermarking sont apparus au début des années 90 avec l'article de Tanaka sur une méthode qui permet de cacher une information dans une image hôte **[Tan90].**

Le terme digital watermark (tatouage numérique) fut utilisé pour la première fois par Andrew Tirkel et Charles Osborne **[Tir93]** en 1992. Tirkel et Osborne est originaire du Japon ont utilisé le terme: denshi sukashi qui se traduit en anglais par "electronic watermark".
Depuis 1995, le tatouage numérique a occupé une place importante dans les recherches scientifiques et a évolué très rapidement, plusieurs travaux ont été développés et implémentés dans ce domaines de recherches comme Cox a implémenté des techniques d'étalement de spectre pour le tatouage numérique **[Rua98]**. L'invention des systèmes de re-synchronisation **[Cox98]** en 1998 marquait la discipline de même que le tatouage avec information adjacente **[Koc95]** (side information channel) en 1995.

1.3.2 Définitions

Le tatouage d'image, 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 de faire une affirmation sur l'image.

En général, tout système de marquage se compose de trois parties suivantes:

- La marque et/ou la clé.
- Le processus d'insertion qui permet d'insérer la marque dans les médias hôtes.
- Le processus d'extraction qui permet d'extraire et de vérifier la présence de la marque.

a) La marque

Dans les algorithmes de tatouage des images, deux types de la marque sont utilisés : marque binaire (0 ou 1) ou sous forme une image (un logo), si l'algorithme est appliqué sur les images en niveau de gris alors la marque doit être la même nature que les images utilisées c'est à dire les images en niveaux de gris pour les algorithmes de tatouage des images en niveaux de gris, et des images couleurs pour les images couleurs.

b) Taille des données insérées (marque)

L'insertion des données dépend de l'application de tatouage, y'a des applications qui repose sur l'ajout des données comme l'insertion de nom de l'auteur, et d'autres sont basés sur l'insertion d'une partie significative d'une petite image dans une image plus grande, plus la capacité de l'algorithme s'adapte mieux aux caractéristiques de l'image hôte plus l'invisibilité est vérifiée.

c) L'utilité de la clé

Les techniques de cryptographies sont basées sur l'utilisation des clés pour vérifier si les utilisateurs ayant l'accès autorisés aux données et aussi on peut utiliser cette clé dans le système du tatouage pour générer la signature (la marque) aléatoirement.

Voici par la suite quelques définitions de tatouage a été présentées dans la littérature :

- **Miller et Cox 1997**

Le tatouage numérique signifie l'intégration d'un signal invisible ou imperceptible dans un contenu ou dans un document comme une vidéo, un audio ou une image, le tatouage est essentiellement motivé par un besoin de fournir une protection du droit d'auteur, du contenu numérique (audio, vidéo et image), de l'identification du propriétaire, de l'empreinte digitale et pour déterminer si les données ont été modifiées par rapport à l'originale **[Cox97] [Bek12].**

- **Kundur et Hatzinakos 1998**

Le processus de tatouage numérique inclut la modification des données multimédias originales pour insérer un watermark contenant des informations clés telles que les chiffres d'authentification ou de droit d'auteur, tout en conservant l'invisibilité des données originales, mais d'exiger des modifications qui peuvent être détectées à l'aide d'un algorithme d'extraction. Les types de signaux à tatouer sont des images, des sons, des vidéos et des textes **[Kun98] [Bek12]**.

- **Anderson et Kuhn 1999**

Le tatouage numérique désigne l'incorporation d'une information dans un document numérique de manière à ce que cette information soit imperceptible ou invisible pour un observateur humain, mais elle est facilement détectée par l'ordinateur en utilisant un algorithme informatique **[Pet99] [Bek12]**.

- **Christian REY et Jean-Luc DUGELAY 2001**

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (i. e, invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc.)**[Rey01][Bek12]**.

- **Chun-Shien Lu 2004**

Le tatouage numérique est un signal intégré de façon permanente dans les données numériques qui peut être détectée ou extraite plus tard par l'exécution d'un algorithme informatique afin de faire des affirmations sur les données. Le tatouage est caché dans le document hôte de telle manière qu'il est inséparable des données et qu'il est résistant à de nombreuses opérations, sans dégrader la qualité du document hôte **[Chu05] [Bek12]**.

Dans **[Zhe07]** Zheng et al ont classifiés le tatouage numérique selon les données hôtes pour l'insertion de la marque : en tatouage numérique des images, en tatouage numérique des vidéos et en tatouage numérique des sons.

1.3.3 Schéma générale de l'implémentation de tatouage

Le tatouage comporte deux phases fondamentales:

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

a) phase d'insertion de la signature ou de la marque

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

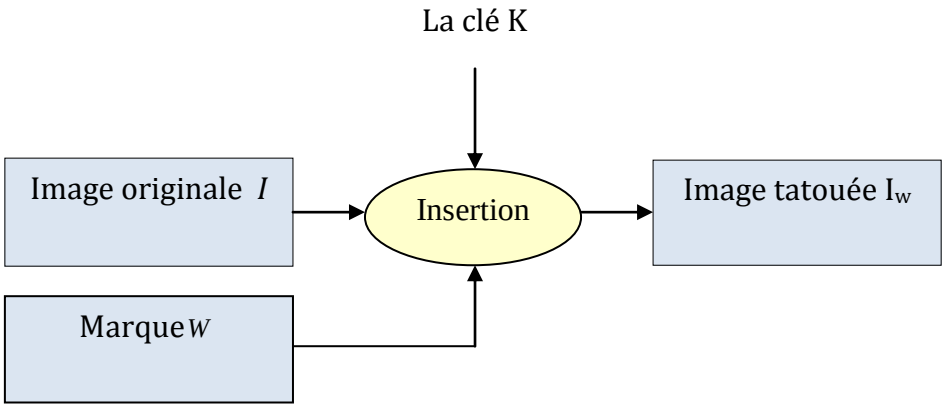


Figure 1.4 : *Schéma général de l'insertion d'une marque.*

La figure 1.4 présente le schéma général de l'insertion de la marque W à l'aide d'une clé K. L'image originale I est tatouée de la marque W par la propriétaire possède de la clé K. L'image marquée I_w est visuellement équivalente à I.

b) Phase d'extraction /détection de la signature ou de la marque

Dans le processus de l'extraction les entrées sont les données tatouées, la clé de sécurité et les données originales et / ou la marque originale en fonction de la technique utilisée, si l'extracteur ne nécessite pas la disponibilité de la copie originale, le schéma de tatouage est appelé « tatouage aveugle », si l'extracteur nécessite l'image originale, il est appelé « tatouage non aveugle » (voir la figure 1.5). Si l'image originale est utilisée, la marque peut être extraite sous sa forme exacte (si l'image n'est pas corrompue ou attaquée). S'il s'agit d'une extraction aveugle, on peut déterminer si un signal spécifique de tatouage donné est présent dans une image ou non (voir la figure1.7).Dans le schéma semi aveugle la connaissance de l'image originale et la marque ne sont pas nécessaires mais quelque informations supplémentaires de celle-ci (voir figure 1.6).

Ensuite, l'étape suivante consiste habituellement à la comparaison de la marque extraite avec la marque originale et le résultat pourrait être comme une sorte de mesure qui représente la possibilité de la présence de la marque originale dans le document ou non utilisant une fonction de corrélation. Pour certains algorithmes de tatouage, la marque extraite peut être encore décodé pour obtenir le message incorporé à des diverses buts telles que la protection du droit d'auteur et l'authentification. La marque est considéré comme robuste si elle est incorporée de manière que la marque peut rester robuste et stable même si les données tatouée passé par différentes traitements. La procédure de l'extraction est indiquée par la formule (1,3) comme suit :

$$W' = D(I_w^*, K') \qquad \textbf{(1,3)}$$

La marque W′ doit être détectée à partir de I_w^* avec/ou sans la connaissance de l'image originale I. Si I_w n'est pas modifiée (attaquée), alors W′ correspond exactement à W. Les figures 1.5, 1.6 et 1.7 présentent le schéma général de l'extraction de la marque.

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

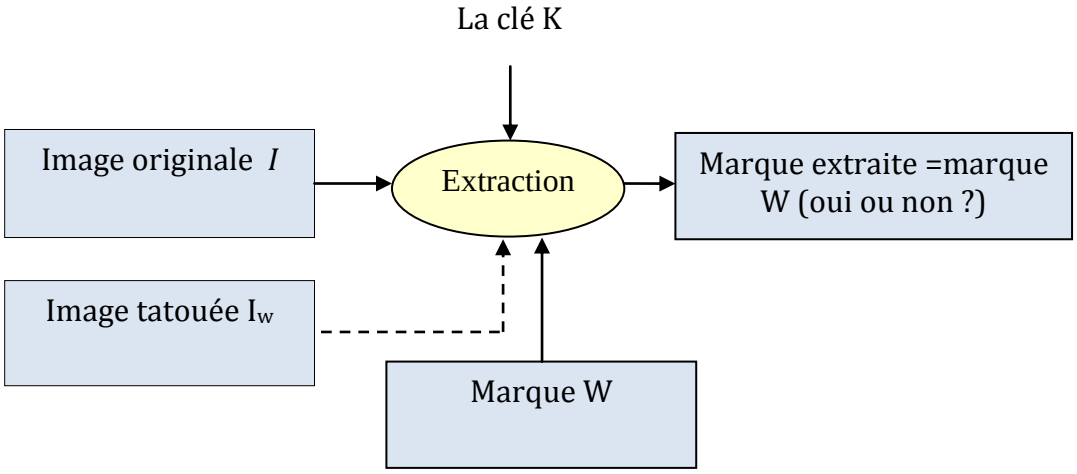


Figure 1.5 : *Schéma général d'extraction non aveugle d'une marque.*

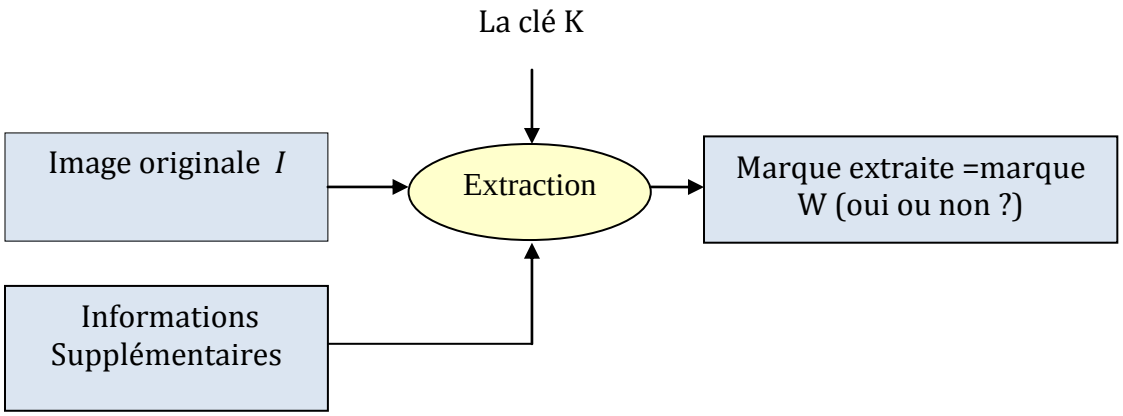


Figure 1.6 : *Schéma général d'extraction semi aveugle d'une marque.*

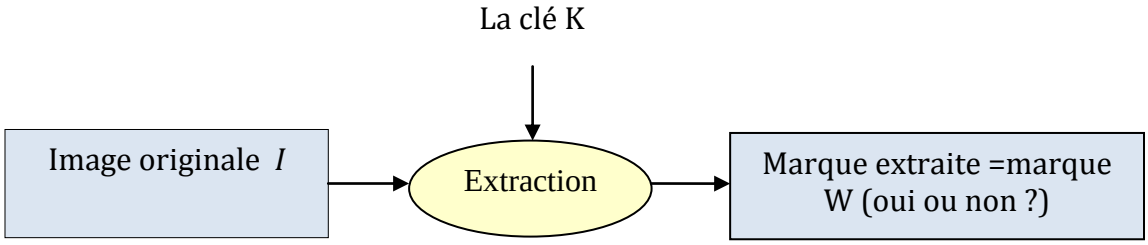


Figure 1.7 : *Schéma général d'extraction aveugle d'une marque.*

1.3.4 Propriétés de système de tatouage

L'augmentation de la force de la marque peut augmenter la robustesse, mais il diminue l'invisibilité. Il doit y avoir un compromis entre les exigences et les propriétés de tatouage en fonction de ses applications. Dans la suite, ces propriétés seront étudiées. Les propriétés principales de la marque sont la robustesse, l'invisibilité ou l'imperceptibilité et la capacité.

a) L'imperceptibilité

Est une préoccupation majeure pour les types des marques invisibles. L'imperceptibilité signifie que la quantité de la dégradation provoquée par la marque est imperceptible.

Certains algorithmes de tatouage utilisent la propriété de masquage visuel du système visuel humain (HVS) pour insérer la marque dans les régions imperceptibles dans l'objet hôte.

La perception humaine est également utilisée comme critère pour classer les techniques de tatouage en : **les marques visibles et invisibles**, Ce critère repose sur l'idée que l'insertion de tatouage n'influence pas sur la qualité visuelle de l'image pour deux raisons: pour ne perdre pas la qualité de l'image et aussi pour qu'il ne pourrait pas être détruite facilement par les pirates ou attaques. Cox et al **[Cox02]** définissent l'invisibilité comme une similitude visuelle

entre l'image originale et l'image tatouée **[Bek12]**. Les logos sont des exemples de marques visibles qui indiquent le propriétaire du contenu.

Un inconvénient des marques visibles est qu'il peut être facilement retirée de l'image numérique hôte. Les marques invisibles modifient les médias de manière qu'ils sont imperceptibles et qu'ils ne peuvent être détectés en utilisant un processus de détection approprié. Ils identifient le propriétaire des médias numériques.

Contrairement aux marques visibles, les marques invisibles ne pourraient pas être enlevées par les médias parce qu'ils sont devenus une partie intégrante du contenu après avoir été tatouée. Cependant, elles peuvent être indétectables par quelques manipulations et des déformations qui sont appelées « attaques ».

b) Robustesse

Ce critère représente la résistance ou non de la marque après des modifications subis par les attaques. Aussi Cox et al **[Cox02]** définissent la robustesse comme capacité de détecter le watemark après des opérations de modifications(traitements), par exemple, plus la qualité d'information dans l'image augmente, plus la signature sera visible ou perceptible et donc la robustesse diminue.

c) Capacité

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

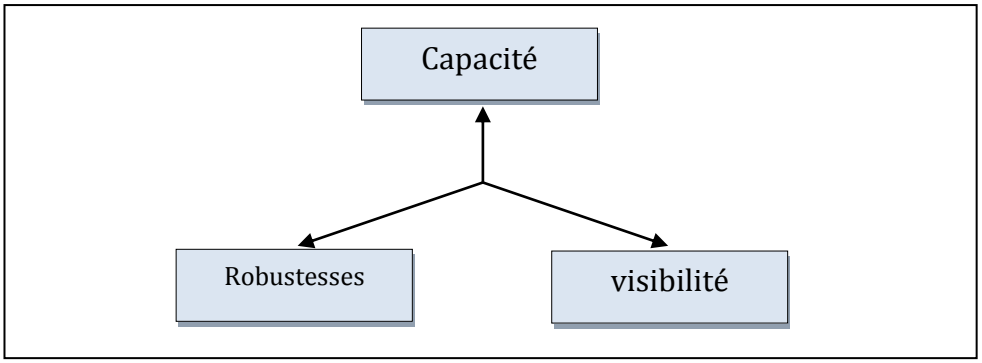


***Figure 1.8** : Compromis entre robustesse, capacité et visibilité.*

1.3.5 Taxonomie des techniques du tatouage numérique

Plusieurs travaux et publications ont présentés la taxonomie des techniques de tatouage numérique qui permet de donner un modèle générale des différents domaines de tatouage basant sur différentes critères, les techniques de tatouage peuvent être classées selon le domaine d'application, le type de document et la perception humaine **[Mil97] [Kat00]**. Comme on peut aussi classer les techniques de tatouage en fonction de type d'algorithme utilisée, le champ d'application et en fonction de domaine d'insertion.

La Figure 1.9 présente un organigramme de cette classification.

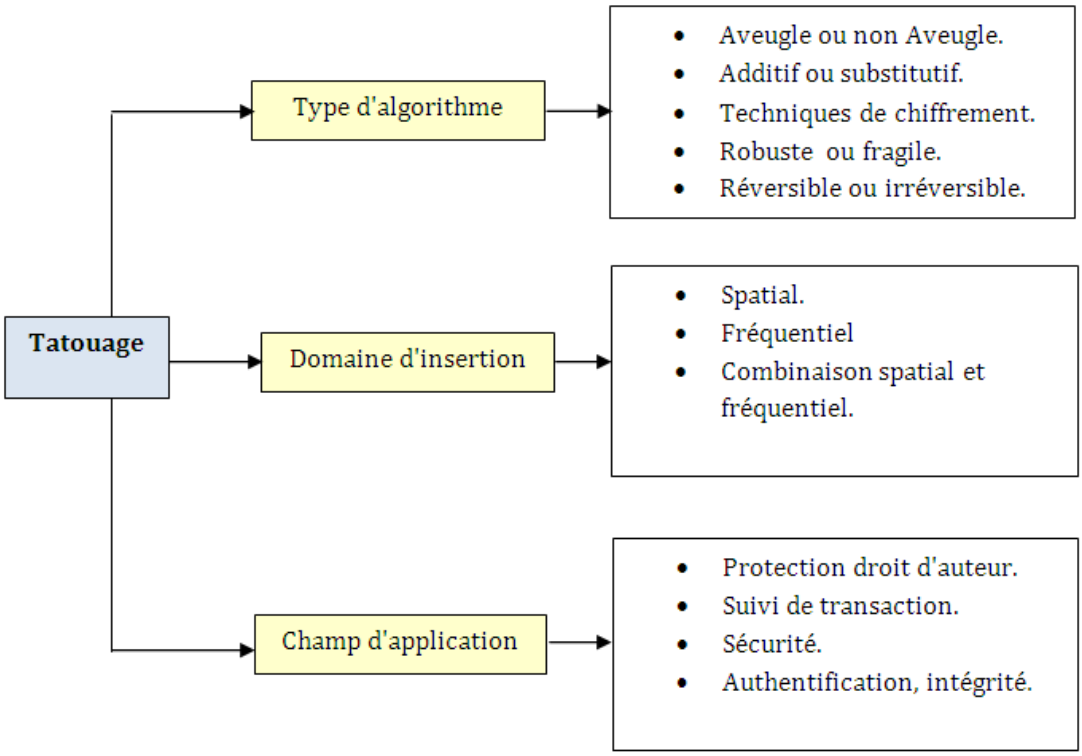


Figure 1.9 : *Taxonomie des techniques de tatouage numérique.*

1.3.5.1 Selon le type d'algorithme utilisé

Cette classification est basée sur le regroupement des techniques de tatouage en fonction de degré de la robustesse contre les attaques (**Robuste, fragile et semi fragile**), les algorithmes de l'extraction (**Aveugle, semi aveugle et non aveugle**), les techniques de l'insertion (**Additif ou substitutif)**, en fonction de préservation de l'image originale (**réversible ou irréversible**) et le type des techniques de chiffrement utilisées (**symétrique ou asymétrique**).

En terme de robustesse, Il existe trois classes de schémas de tatouage : robuste, fragile et semi fragile.

A) Tatouage robuste

Ce schéma de tatouage permet de protéger les documents et les données contre les attaques, C'est une autre propriété plus difficile à vérifier qui permet de trouver la marque ou l'information insérée dans l'image tatouée malgré que celle-ci ait enduré des attaques (supprimer ou modifier) de la part de l'attaquant.

Aussi Cox et al **[Rey01]** définissent la robustesse comme capacité de détecter le watemark après des opérations de modifications(traitements), par exemple, plus la qualité d'information dans l'image augmente, plus la signature sera visible ou perceptible et donc la robustesse diminue. Ce type de tatouage sert à garantir la protection des droits d'auteurs **[Chu05] [Zhe07] [Bek12].**

Les algorithmes robustes permettent de trouver la marque après d'éventuelles distorsions telles que la compression, le filtrage et le bruit. Cependant, les marques fragiles sont utilisés pour détecter s'il ya une manipulation ou une modification sur le contenu numérique.les marques fragiles peuvent être utilisés pour l'authentification des contenus.

B) Tatouage fragile

Ce schéma de tatouage permet de vérifier l'authentification et l'intégrité c'est à dire permet de vérifier si l'image n'a pas été modifiée mais dans ce type de tatouage, la marque insérée est sensible et fragile et ils ne doivent pas résister aux modifications de l'image tatouée. Nous citons, par exemple, les techniques qui sont décrites dans **[Cox02] [Mil97] [Kat00]**.

C) Tatouage semi fragile

Ce schéma de tatouage est utilisé pour réserver l'authentification et il 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 **[Mae06].**

On peut aussi classifier les techniques de tatouage selon l'algorithme de l'extraction :

a) Non aveugle: si l'utilisation de l'image originale et la clé sont nécessaires.

b) Semi aveugle : le schéma de l'extraction n'a pas besoin forcement de l'utilisation de l'image originale mais seulement de quelques caractéristiques de celle-ci.

c) Aveugle: le schéma de l'extraction s'effectue sans l'utilisation de l'image originale et la marque.

On peut aussi classifier les techniques de tatouage selon la clé utilisée **: Asymétrique et Symétrique**

Le tatouage asymétrique **[Won01] [Kim03]** ou le tatouage à clé publique est basé sur l'utilisation de deux clés : une clé K_s privée pour l'insertion et une clé K_p publique pour l'extraction. N'importe quel utilisateur peut détecter la marque en connaissant la clé publique K_p, mais seule la connaissance de K_s permet d'enlever ou modifier la marque **[Sol99]**.Dans le tatouage symétrique ou le tatouage à clé privé, l'insertion et l'extraction sont faites à l'aide de la même clé **[SAA01] [Bek12]**.

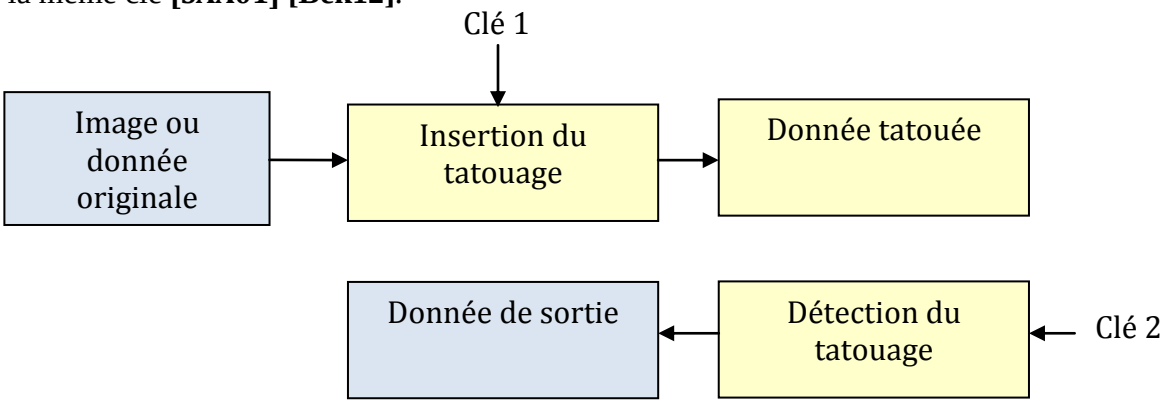


Figure 1.10 : *L'utilisation des clés.*

On peut aussi classifier les techniques de tatouage selon l'algorithme de l'insertion : r**éversibilité ou irréversibilité**

Les techniques de tatouage peuvent être classées en deux catégories, réversible et irréversible. Le tatouage réversible permet de restaurer l'image original à partir de l'image tatouée en appliquant une transformation inverse sans produire des changements et permet d'éviter toutes distorsion irréversibles dans l'image originale, contrairement au tatouage non réversible, il n'existe aucun moyen de retrouver l'image originale à partir de l'image tatouée. **[Bek12]**

1.3.5.2 Classification les schémas de tatouage suivant les méthodes de l'insertion (additif ou substitutif)

On distingue les techniques de tatouage selon la façon de l'insertion de la signature dans un document hôte, soit de façon additive connue par les techniques additives, ou de façon substitutive connue par les techniques substitutives.Le tableau présente la comparaison entre le schéma additif et le schéma substitutif.

	Capacité	**Insertion**	**Détection**
Additifs	faible	Par addition d'une séquence aléatoire	corrélation
Substitutifs	maximale	Par substitution des caractéristiques de l'image	Analyse de redondance

Tableau1.1 : *Comparaison entre les schémas additifs et les schémas substitutifs.*

A) Schéma additif

Les schémas additifs permettent d'ajouter la marque ou la signature à l'image hôte elle-même ou aux coefficients de transformées de celle-ci issue de transformation selon le type d'espace de transformation utilisé, la marque est générée à l'aide d'une clé k de façon pseudo aléatoire comme dans le cas de l'étalement de spectre **[Bas00] [Bas03]**.

La marque générée est directement insérée dans l'image originale. Pour le processus de détection, dans ce type de tatouage pour les techniques aveugle est effectués à l'aide des méthodes statistiques. Dans ce cas, une mesure de corrélation peut être effectuée.

Les processus d'insertion et de détection de schéma additif sont présentés dans la figure 1.15 et la figure 1.16 respectivement.

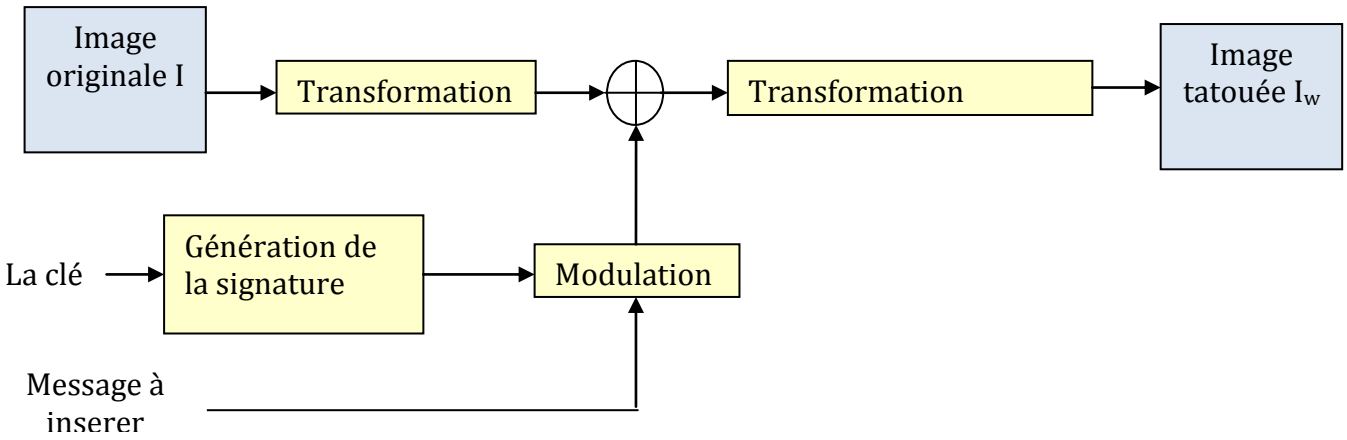


***Figure. 1.11** : Insertion de la signature pour des schémas additifs.*

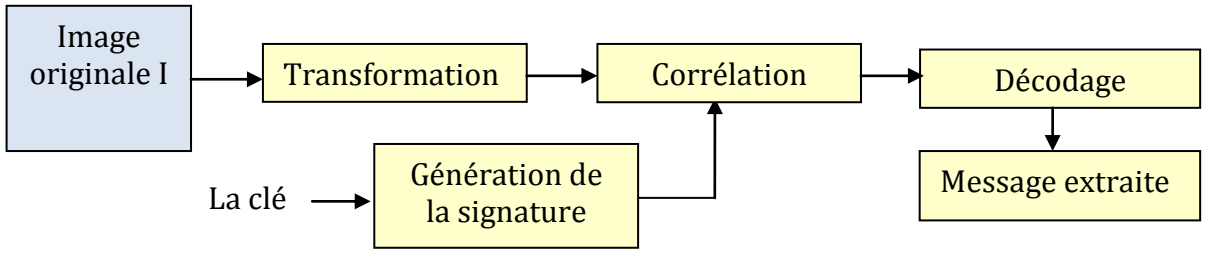


***Figure 1.12**: Extraction de la marque pour les schémas additifs.*

B) Schéma substitutif

La marque n'est pas ajoutée mais substituée à des composants de l'image (pixel, coefficient de transformés,....) sélectionnés à l'aide 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. **[Gru95] [Car95][Bek12].** Le processus d'insertion et de l'extraction de schéma substitutif sont présentés par la figure 1.18 et la figure 1.19 respectivement.

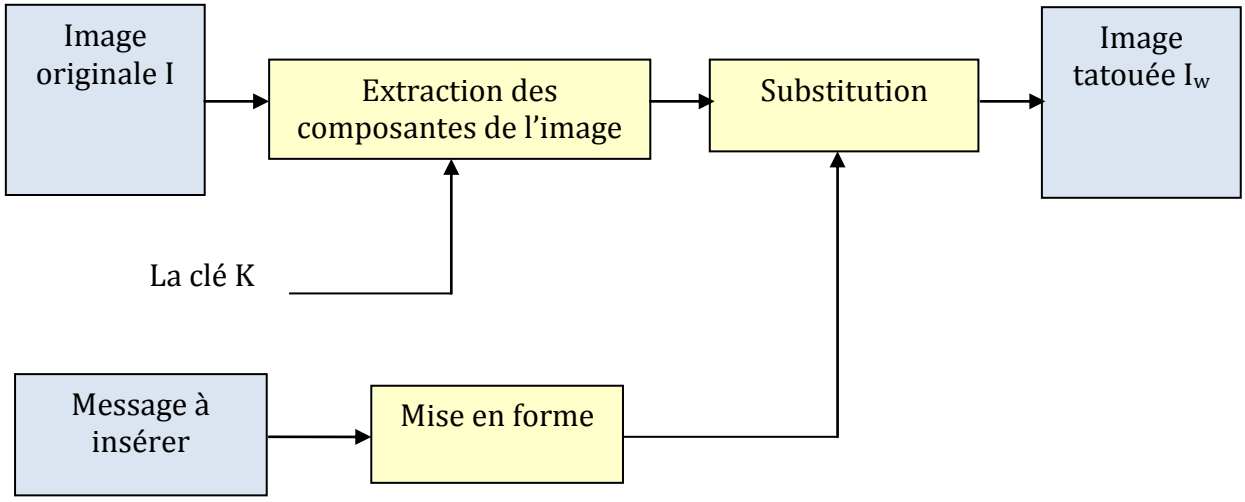


Figure. 1.13 *: Principe de l'insertion par substitution.*

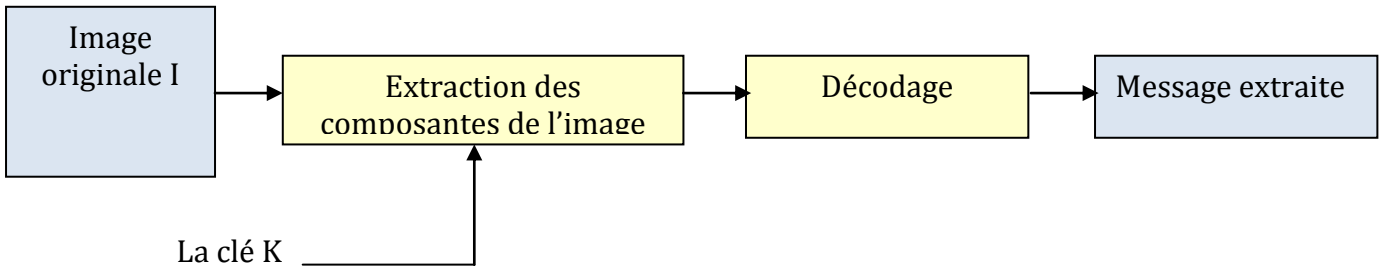


Figure. 1.14 : *Extraction et lecture de la signature par substitution.*

- ***Exemple sur les schémas*** **substitutifs**

a) Tatouage réversible RCM (Reversible Contrast Mapping) [Col05] [Meh01] [Bek12]

La plupart des approches proposées de tatouage réversible sont basées sur une étape de compression de données sans perte **[Din07]**, **[Fri02]**, **[Ala04]**. L'utilisation de cette étape de compression de données augmente la complexité mathématique du tatouage. Le tatouage RCM : la cartographie contrastée réversible est l'une de ces méthodes substitutives basée sur l'idée que la signature substitue les LSB's, elle permet de vérifier l'intégrité des images médicales et l'authentification des données relatives au propriétaire (médecin ou patient). RCM est une transformée simple définie sur des paires de pixels dans le domaine spatial. Le tatouage RCM est parfaitement réversible, même si les bits les moins significatifs (LSBs) de la transformée des pixels sont perdus **[Bek12]**.

1) Phase de l'insertion

L'algorithme de l'insertion s'effectué comme suit:

1. Décomposition de l'image originale en paires de pixels en colonnes et en lignes.

2. Pour chaque paire (x, y) :

a- Si $(x, y) \in D_c$ tel que $D_c \in [0..255]$ n'est pas composé des valeurs de pixels paires, on transforme la paire en utilisant l'équation (1,10), mettre les LSB de x' à 1 et on considère le LSB de y' disponible pour l'insertion de la marque.

$$x' = 2x - y, y' = 2y - x \qquad \textbf{(1,10)}$$

b- Si $(x, y) \in D_c$ tel que $D_c \in [0..255]$ est composé des valeurs de pixels paires, on met le LSB de x à 0 et on considère le LSB de y disponible pour l'insertion de la marque.

c- Si $(x, y) \notin D_c$, on met LSB de x à 0 et sauvegarder la valeur vrai.

3. Répéter l'algorithme jusqu'a atteindre toutes les paires de pixels.

4. La carte est une collection des paires de pixels transformées et non transformées.

- **Exemple [Bek12]**
  - Décomposition l'image originale en paires de pixels:

10	**12**						**.....**
5	**3**						**.....**
. .							

On considère la marque W=1001

- Si la paire (x_1, y_1) =(5,3)$\in$ [0,255], les valeurs de pixels ne sont pas paires, on transforme par l'équation (1,10): $x' = 2\times5-3=7$ et $y' = 2\times3-5=1$,

  Donc (x', y')=(7,1).

- On met LSB(x')=1 et LSB (y')=1 (le premier bit de W).
- Si la paire (x', y')=(10,12)$\in$ [0,255], les valeurs de pixels sont paires, on met LSB(x)=1 et LSB(y)=0 (le deuxième bit de W).

- Si (x, y)= (256,256) $\notin$ [0, 255], on met LSB de x à 0 et on sauvegarder la valeur de x=256.

2) Phase de l'extraction [Bek12]

Pour extraire la marque et restaurer les paires originales, il faut que chaque paire de pixels transformée soit correctement identifiée, les LSB de premier pixel de chaque paire sont utilisés pour indiquer si la paire est transformée ou non, 1 si paire est transformé et 0 sinon.

L'algorithme de l'extraction est s'effectué comme suit:

1- Partitionner l'image tatouée en paires de pixels.

2- pour chaque paire (x', y') :

a- Si les LSB de x' est à 1, on extraire le LSB de y' et enregistrer dans la séquence de la marque détecté, mettre le LSB de x', y' à 0 et extraire les paires originales par l'équation (1,11) come suit :

$$x = [\frac{2}{3}x' + \frac{1}{3}y'], y = [\frac{1}{3}x' + \frac{2}{3}y'] \qquad \textbf{(1,11)}$$

b- Si le LSB de x' es à 0 et la paire (x', y') avec le LSB s à 1 et appartient à D_c, on extraire le LSB de y' et on enregistre dans la séquence de la marque détectée, ensuite on restaure les paires originales à 1.

c- Si le LSB de x' à 0 et la paire (x', y') avec le LSB à 1 n'appartient pas à D_c, les paires originales sont extraites par le remplacement du LSB de x' avec la valeur vrai correspondante à partir de la séquence de la marque.

- **Exemple [Bek12]**
  - La paire de pixels transformée (x', y') =(7,1) $\in$ [0, 255]

Cas (a):

- Si LSB (x', y') =1, indique que la paire est transformée et si le contenu incorporé dans le LSB (y')=1 alors on extraire le LSB de y', bit extrait =1, on récupère les paires originales par l'équation (1,12):

$$x= [\frac{2}{3}7+\frac{1}{3}1] =5,\ y=[\frac{1}{3}7+\frac{2}{3}1] = 3 \qquad \textit{(1,12)}$$

- Si le LSB de x' =0, $\notin [0,255]$ et le LSB de paire(x', y') =1, les paires originales sont extraites par le remplacement par la valeur vrai correspondante extraite à partir de la séquence de la marque.
- Si le LSB de x'=0 et $\in [0,255]$, on extraire le LSB de y', on enregistre dans la séquence de la marque extraite et on récupère les paires originales comme $x = x' = 1,\ y = y' = 1$.

C) Méthodes Psychovisuelles

L'idée des méthodes psycho visuels est basé sur le système visuel humain SVH et prendre en considération les propriétés de masquage (signature).le processus d'insertion s'effectue par l'augmentation de la force de signature sans aucune dégradation perceptuelment visible sur le masquant(image).Plusieurs travaux dans la littérature se basent sur ce modèle dans le domaine spatial **[Aut02]** et d'autres**[SAA01]** ou les auteurs F. Autrusseau et A. Saadane ont proposés une technique de masquage qui permet d'assembler les caractéristiques de l'image dans le domaine spatiale et les caractéristiques de SVH dans le domaine transformé.

1.3.5.3 Classification les techniques de tatouage selon l'espace d'insertion

L'insertion de la marque s'effectuée soit dans le domaine spatial ou dans le domaine transformé (DFT, DCT, DWT ou SVD).

A) Espace spatial

Les marques peuvent être insérées dans le contenu multimédia dans le domaine spatial ou dans le domaine fréquentiel. Les méthodes spatiales permettent d'insérer la marque directement dans l'image et ne nécessite aucune transformation. la première étape de l'insertion est la génération d'une séquence binaire pseudo aléatoire à l'aide d'une clé secrète qui est composée uniquement de +1 et de –1 ensuite la marque utilisée pour l'insertion est une modulation de message que l'on veut insérer par la séquence. En fin l'insertion s'effectue par l'addition de la marque directement à l'image hôte *I*. On trouve l'image marquée I_w par la formule suivante *:* $\boldsymbol{I_w = I + W,}$ comme montre la figure 1.10. Cette méthode montre une robustesse face aux attaques géométriques **[Sch94].**

L'extraction se faite par une fonction de corrélation qui permet de trouver la signature ou la marque W en calculant la somme de résultat de multiplication de deux images (la marque et l'image tatouée) pixel par pixel. On répète ce processus pour chaque bit inséré pour obtenir le message extrait par la formule suivante :

$$\mathbf{<Iw,W> = <I+W,W> = <I,W> + <W,W>} \qquad \textit{(1,4)}$$

- **Exemple sur les Méthodes Fragiles irréversibles de Tatouage d'Images dans le domaine spatial**

Plusieurs travaux sont basés sur ce type d'insertion ont été réalisés **[Chu05]** :

Coltuc et al **[CHA05]** ont proposés des techniques qui sont basées sur la modification d'histogramme qui permet de mettre toutes les composantes de l'histogramme à 0 tel que la clé et la séquence qui décrivant les composantes seront aussi mis à 0. Ces méthodes sont robustes aux attaques géométriques tel que la translation, le fenêtrage, la rotation et le changement d'échelle, mais elles sont fragile aux opérations de traitement d'images (tels que le filtrage ou la compression).

Schyndel et al **[Sch94]** ont proposés deux techniques l'une permet de remplacer les LSB's par les PN séquences pseudo aléatoire et la deuxième permet d'ajouter cette dernières aux LSB, utilisent la méthode de patchwork pour insérer le message dans le canal de la luminance qui est basé sur la différence entre deux ensembles de pixels constitués à l'aide d'une clé.

D'autres travaux permettent de décomposer l'image qui est codé sur 8 bits en 8 plans. L'insertion des données dans les bits de poids faible LSB (least significatif bits) de l'image

s'effectuée par la suppression des bits de poids faible de l'image originale et en les remplaçant par les données que l'on veut insérer, 0 ou 1 suivant la séquence de la signature.

Cette méthode donne des bons résultats en terme d'invisibilité ceci est dû à l'insignifiance des bits de poids faible à fin que l'image marquée n'est pas perceptuellement dégradée mais reste faible en terme de robustesse parce que n'importe quel simple traitement peut modifier les LSB's, ce qui rend l'extraction impossible pour cette raison cette technique est classifiée parmi les schémas de tatouage fragile. Toutefois, Tirkel et al **[Tir93]** proposent de combiner cette méthode avec une procédure de l'étalement de spectre.

Cette méthode permet d'améliorer la robustesse face au bruit, comparée à la méthode simple de tatouage qui est basé sur les LSB's. Celle-ci réduit, bien sûr, le ratio de l'invisibilité, mais augmente la robustesse de la marque.

Une autre méthode a été implémentée par Wong et Celik **[Won98] [Meh01]** qui permettent d'insérer la signature dans une partie de l'image et qui n'empêche pas la partie diagnostique de celle-ci, ce qui assure l'intégrité des images médicales.

Les auteurs proposent une méthode basée sur l'insertion de la signature générée à l'aide d'une fonction de hachage MD5 ou SHA-256 qui est insérée dans les LSB's (les bits significatifs de poids faible). La phase de l'extraction basée sur la comparaison entre la signature insérée et la signature recalculée.

Wong **[Won98]** propose de décomposer l'image hôte en blocs ensuite, il calcule un résumé pour chaque bloc, la marque insérée qui est le résultat de Ou exclusif entre chaque résumé et chaque bloc d'un logo binaire qui est insérée dans les emplacements des LSB's.

La phase de l'extraction est basée sur le calcul de résumé des blocs de l'image tatouée qui sont ajoutées aux LSB's par OU exclusif, pour retrouver le vrai logo dans le cas où l'image n'a pas été altérée.

Cette méthode montre une fragilité contre l'attaque de Holliman et Memon qui permet de remplacer un bloc de l'image tatouée par une autre image marquée ce qui permet d'extraire un faux résumé .Ce problème est très important dans le domaine d'imagerie médicale qui est facile d'ajouter ou remplacer un signe pathologique dans une image par un autre.

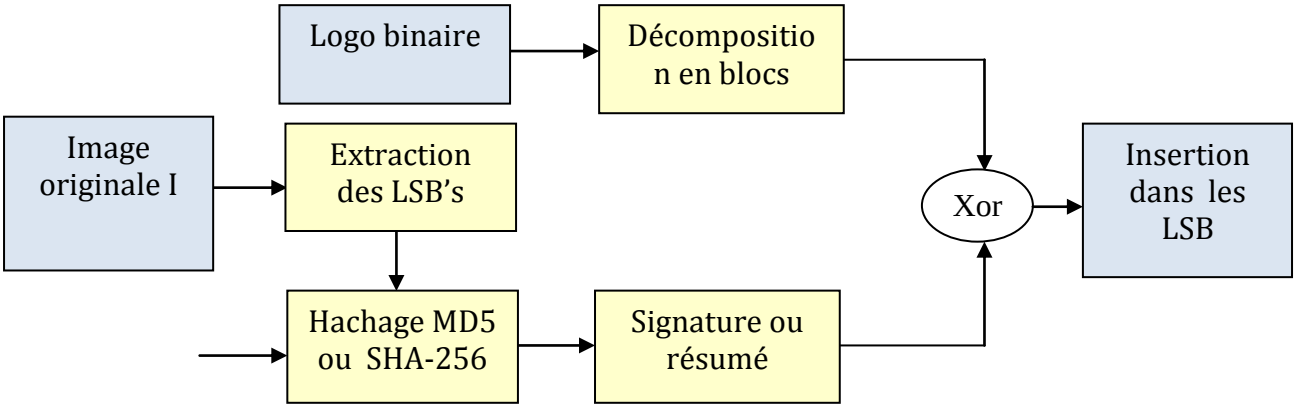


Figure 1.15 : *phase d'insertion de la technique de Wong.*

Celik **[Meh01]** a proposé de calculer le résumé sur une grande bande de blocs, la première étape est la décomposition de l'image en blocs multi niveau, l'insertion de la signature (ensemble des bits de bloc supérieur et le résumé de bloc lui même) s'effectuée dans les blocs de petite taille.

- ***Exemple sur les méthodes de tatouage dans le domaine spatial***

a) Méthode de patchwork

Les auteurs **[Gru95]** ont proposés une technique qui permet de faire la différence de la luminance entre deux ensembles de points ou patchs générés à l'aide d'une clé. L'insertion s'effectuée par la modification de la luminance de ces pixels qui est donnée par :

$$\tilde{a}_i = a_i + 1 \qquad (1,5)$$

$$\tilde{b}_i = b_i - 1 \qquad (1,6)$$

Cette méthode parmi les méthodes statistiques qui sont appliquées sur les pixels d'une image qui seront indépendants et identiquement distribués qui est choisie aléatoirement et est déterminé par une clé.

$$D[S] = \sum_{i=1}^{n} D[a_i] - D[b_i] = 0 \qquad (1,7)$$

La détection s'effectuée par l'utilisation de la clef privée pour retrouver les paires de pixels utilisées par la somme des différences donnée par l'équation (1,8), cette technique possède plusieurs inconvénients d'une part manque de robustesse et elle ne permet d'insérer qu'une

faible quantité de données et d'autre part si la personne connaissant plusieurs images qui utilisent la même clé, alors il peut facilement de la décrypter.

$$S = \sum_{i=1}^{n} \tilde{a}_i - \tilde{b}_i \qquad (1,8)$$

b) Moyenne des blocs

Le principe de cette méthode **[Car95]**, **[Lan96]** est basé sur deux schémas bidirectionnels et unidirectionnels. La première étape est la division de l'image hôte en blocs, pour le codage de bit '0', ils incrémentent la moyenne de ces blocs ou leurs emplacements sont déterminés par une clé secrète. Pour le codage à un '1' ils décrémentent dans le cas de codage bidirectionnel. Si dans le codage « unidirectionnel »ils incrémentent la moyenne d'un bloc pour coder un "1" Edc xcddddddt de la laisser inchangée pour un "0". Pour le processus de détection la présence de l'image originale est nécessaire.

c) Insertion simple / Insertion multiple **[Lan97]**

La première étape est la décomposition de l'image en blocs et en ajoutant à chaque bloc des données aléatoire dans le cas de l'insertion multiple ou une seule donnée dans le cas de l'insertion simple qui est multiplié par un facteur d'invisibilité α qui permet de contrôler la force de processus de l'insertion qui donne une interprétation sur la robustesse, c'est à dire plus le facteur est grand plus la robustesse est bonne mais donne une dégradation perceptible.

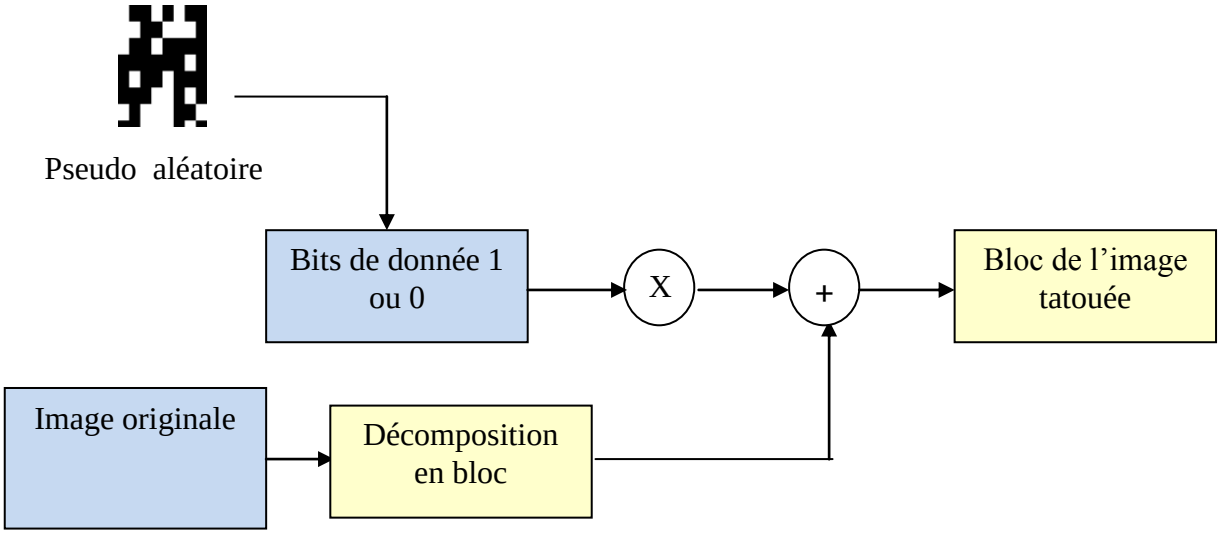


Figure 1.16: *Phase d'insertion simple.*

Le processus de détection est s'effectué par le calcul de la fonction de corrélation entre le pseudo aléatoire et les différentes blocs.

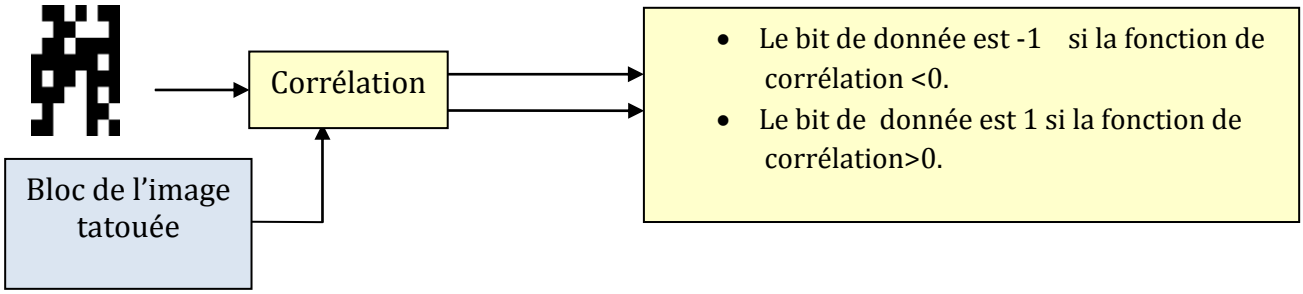


Figure 1.17 *: Phase d'extraction simple.*

- ***Exemples sur le schéma de tatouage additif dans le domaine spatial***

a) Etalement de spectre

Parmi les premières publications qui ont été basés sur les techniques de tatouage additif ; la méthode d'étalement de spectre par Cox **[Cox96]**, qui permet de rendre la marque robuste au bruit, au filtre linéaire et ainsi que à la compression, le principe de cette méthode est de moduler un message M à transmettre dans un espace bruité ou l'image hôte *I* est considérée comme un canal de transmission, ou l'attaque est le bruit. Cette méthode est réalisée en modulant le message M avec une séquence pseudo-aléatoire large bande spectrale pour trouver l'image I^*_w en utilisant l'équation (1,9)

$$I^*_w = I + \alpha . W \qquad \textbf{(1,9)}$$

- ***Par exemple***

On a un message m= {0; 1}, pour générer la marque à l'aide d'une séquence pseudo-aléatoire SBPA= [1 0 1] et le spectre T= [1 0 0], on applique une modulation de fréquence, alors la marque M= [1 0 1 0 1 0 0 1 0], la taille du signal tatouée est la même que la taille de la séquence pseudo aléatoire SBPA.

Dans le processus de détection, pour retrouver le message inséré, la fonction de corrélation a été appliquée entre la partie tatouée et la séquence pseudo-aléatoire, la réponse est positive dans le cas ou le bit est 1 ou à 0 dans le cas ou le résultat est négatif. La première étape est la

génération de la marque de la même manière que la phase d'insertion, la deuxième étape est la décomposition de l'image tatouée en blocs conformément au nombre de bits du message.

En troisième lieu, une fonction de corrélation s'effectue entre chaque bloc de séquence et chaque bloc de l'image marquée pour la détection ou non de la marque.

Winkler **[Win99]** a proposé une méthode différente de l'étalement de spectre dans le domaine spatial, cette technique permet d'insérer très peu de données et d'étaler chaque bit de cette dernière sur toute image, basée sur l'utilisation des fonctions de modulation large bande de même taille que l'image originale.

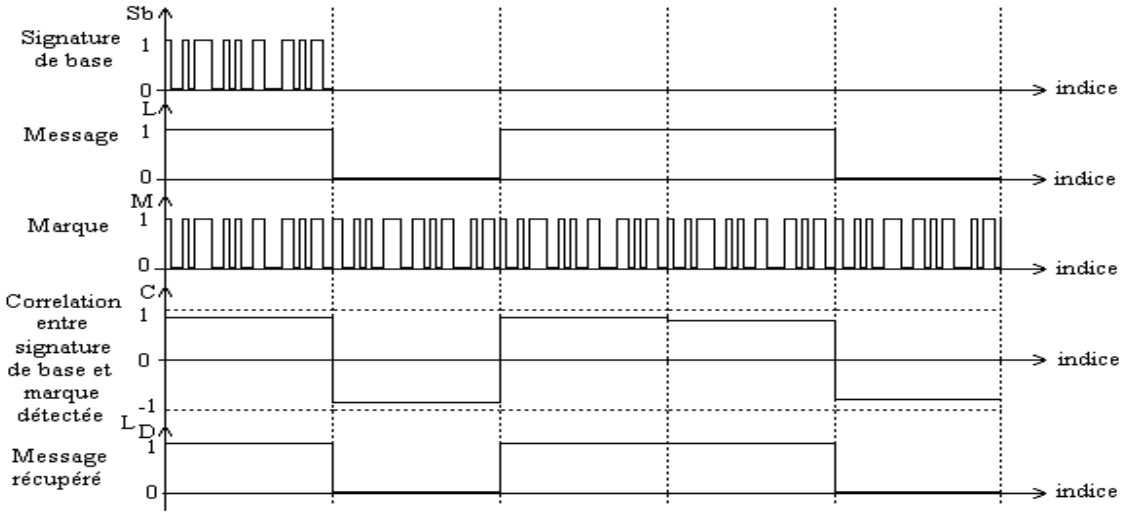


Figure 1.18 : *Principe de l'étalement de spectre.*

b) CDMA dans le domaine spatial CDMA-SD [45]

La technique CDMA (Code Division Multiple Access) est une technique de référence implémentée par Vassaux en 2000. Elle se base sur le principe d'insertion de la marque dans un document ou dans une image sans la dégrader perceptuellement selon le schéma additif dont le but est de garantir la confidentialité des données du patient et de vérifier l'intégrité de l'image médicale.

1) Phase d'insertion

L'étape d'insertion s'effectue dans le domaine spatial. Tout d'abord la première étape consiste à partitionner l'image originale en blocs de même taille, la deuxième étape génère la séquence pseudo aléatoire à l'aide d'une clé secrète K , la marque que l'on veut ajouter est une série de blocs +SBPA et –SBPA (+SBPA si les bits sont à 1, -SBPA si les bits sont à 0)

pondérée avec le coefficient de visibilité α , l'insertion de la marque s'effectue directement sur l'image originale I pour produire l'image tatouée I_w **[Bek12]**.

2) Phase d'extraction

Dans la phase d'extraction, on utilise des fonctions de corrélation pour le décodage. La première étape consiste à générer la marque de la même manière que la phase d'insertion, la deuxième étape permet de décomposer l'image tatouée en blocs conformément au nombre de bits du message. En troisième lieu, une fonction de corrélation s'effectue entre chaque bloc de séquence et chaque bloc de l'image marqué pour la détection ou non de la marque.

La méthode de CDMA-SD permet d'insérer un nombre de bits du message dans l'image. Le problème se pose lorsque le nombre de bits du message est grand, ceci rend la détection de la marque plus difficile. Comme solution, il est aussi proposé d'insérer plusieurs couches CDMA ou plusieurs marques et le résultat de leur addition constitue la marque définitive pour l'insertion **[Bek12]**.

Plusieurs travaux qui ont été réalisés sont basés sur des algorithmes robustes face aux quelques attaques géométriques dans le domaine spatial par exemple celles publiés dans **[Cox00]**, **[Fab00]**.Mais le tatouage dans le domaine spatial ne donne pas une garantie parfaite de la robustesse contre toute type d'attaques.

Pour cette raison les chercheurs ont proposés de travailler dans l'axe qui se base sur l'utilisation d'autres domaines robustes fréquentielle ou transformés.

B) L'espace transformé ou fréquentiel

les méthodes de tatouage dans le domaine fréquentiel peuvent utiliser plusieurs transforme différents , tels que la transformation discrète en cosinus (DCT)**[Cha05][Koc95]**,la transformation discrète en Fourier (DFT)**[Sol00]** , la transformation discrètes en ondelettes (DWT)**[Har09][Kha06]** et la décomposition des valeurs singulières (SVD)**[Yong05][Sve01]**, etc. Dans la littérature, il a été affirmé que les techniques du domaine fréquentiel sont plus robustes que les techniques du domaine spatial. Parmi les travaux qui ont en relation avec ce domaine sont décrit en détail dans le chapitre 3.

- ***Exemple sur le schéma de tatouage additif dans le domaine fréquentiel***

a) CDMA dans le domaine fréquentiel DWT (Discret Wavelet Transform) CDMA-DWT [Chr02] [Bek12]

C'est une technique a été proposée par Chris Shoemaker **[Chr02]**, elle permet d'insérer la signature pas directement dans l'image hôte mais aux coefficients (horizontaux, verticaux, diagonaux) de transformés obtenus après une décomposition par la transformée de DWT.

1) Phase d'insertion

La première étape est la génération de la séquence de pseudos aléatoires à l'aide d'une clé secrète K , la marque est un résultat du produit de la séquence par un facteur α , ce dernier est utilisé pour ajuster ou adapter la marque aux caractéristiques de l'image originale. Le facteur α est un coefficient de visibilité pour régler l'intensité de l'image ou bien pour augmenter l'intensité de la marque pour satisfaire le critère d'invisibilité et rendre la marque moins perceptible.

La deuxième étape consiste à ajouter la marque aux coefficients de transformées issus de décomposition par la DWT de l'image originale donnant l'image approximative I_A et trois détails horizontale DH, verticale DV et diagonale DD. Ces derniers sont des informations relatives à l'image (texture, contours, ...).

$$DH'=DH+\alpha W$$

$$DV'=DV+\alpha W$$

$$DD'=DD+\alpha W$$

Pour calculer l'image tatouée, on calcule la transformée inverse DWT^{-1} de l'image approximative et les trois détails modifiés par la marque pondérée par le facteur α .

$$I_w = DWT^{-1}(I_A, DH', DV', DD').$$

2) Phase d'extraction

La phase d'extraction permet de faire la décomposition en DWT de l'image tatouée I_w , ensuite on calcule la fonction de corrélation entre la marque utilisée lors de la phase d'insertion et les

coefficients de transformée en DWT de l'image tatouée tel que le décodage sera selon le signe de corrélation **[Chr02] [Bek12]**.

Dans la littérature, les résultats expérimentaux montrent que le domaine d'ondelette est un meilleur environnement pour l'application du système de tatouage numérique qui donne une invisibilité parfaite par rapport au domaine spatial. La technique de CDMA-DWT donne de bons résultats pour une insertion d'une signature de grande taille et facilite la récupération de la marque même si l'image tatouée a subi des manipulations malveillantes comme le bruit et la compression.

Dans la littérature, les résultats expérimentaux qui ont été réalisés par Chris Shoemaker **[Chr02]** et aussi par vassaux **[Vas00]** montrent que la méthode CDMA dans le domaine spatial est robuste contre l'attaque de bruit et la compression JPEG avec une restauration parfaite de la signature insérées. Chaque marque dans chaque couche est générée à l'aide d'une clé secrète donc le nombre de clés utilisées est égal au nombre de couches utilisées. Par conséquent, plus le nombre de clés est grand plus la technique est robuste face aux attaques cryptographiques.

L'inconvénient de ce schéma de tatouage est la dégradation visuelle avec l'insertion des signatures de grande taille ainsi que le temps de calcul qui augmente avec l'augmentation de la taille des marques **[Bek12]**.

Le tableau récapitule la comparaison entre les méthodes qui ont été implémentées dans le domaine médical (sur les images IRM) :

1.3.5.4 Classification des techniques de tatouage selon le domaine d'application

Les systèmes de tatouage numérique sont développés en fonction de différents domaines d'applications. Voici les applications courantes de tatouage :

a) La protection du droit d'auteur

L'une des principales applications de tatouage est la protection du droit d'auteur. Les informations sur le propriétaire du droit d'auteur sont insérées dans les données originales pour empêcher d'autres personnes de prétendre être les propriétaires légaux des données. Les marques utilisées à cette fin sont censés être très robuste contre diverses attaques permettant à éliminer la marque. Dans l'imagerie médicale les images médicales doivent être protégées avant leur diffusion, la protection est assurée par l'insertion d'une marque ou du copyright de propriétaire ou d'un organisme. Cette marque est insérée et extraite à l'aide d'une clé secrète de chiffrement /déchiffrement de la signature **[Cox02] [Bek12]**.

b) L'intégrité et l'authentification de contenu

Afin d'être en mesure de valider le contenu, tout changement ou manipulation avec le contenu doivent être détectées et consiste de vérifier que l'image n'a pas été modifiée ou détectée par rapport à l'image originale en cours de route en adéquation avec l'identité du patient ou du médecin. **[Cox02][Gol10][Bek12].**

Ceci peut être réalisé grâce à l'utilisation de la marque fragile ou de semi- fragile qui a une faible robustesse aux modifications de l'image hôte. Le tatouage semi- fragile peut également servir l'objectif de la mesure de la qualité. La marque extraite peut non seulement informer l'altération possible de l'image hôte, mais aussi de fournir plus d'informations sur la dégradation de celle-ci.

c) Suivi des transactions

Cette application permet d'insérer une marque dans l'image dont cette marque contient des informations relatives au propriétaire (patient ou médecins), à sa destination et de la façon de son utilisation **[Cox00] [Bek12]**.

d) Contrôle de copie

Les utilisateurs peuvent avoir le privilège différent (contrôle de la lecture / copie) sur l'objet en raison de paiement différent pour cet objet. Il est prévu dans certains systèmes d'avoir un mécanisme de copie et de contrôle de l'utilisation pour vérifier la copie illégale du contenu ou de limiter le nombre de fois de la copie. Le watermark peut être utilisé à cette fin. **[Din07][Win99]**.

e) Indexation et les liens descriptifs

Le tatouage permet d'insérer une signature dans l'image pour rendre l'indexation plus simple. La signature générée par un créateur est une collection d'informations avec un sommaire ou un descripteur ou un lien vers une autre information pour faciliter le classement et la recherche rapide dans une base de données **[Col05] [Ala04] [Bek12]**.

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

1.4 Les attaques

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

Selon S. Voloshynovskiy et al. **[Vol01]** les attaques sont regroupées en quatre classes principales : les attaques d'effacement ou de suppression, les attaques géométriques, les attaques cryptographiques et les attaques de protocole.

Selon les auteurs Cox et al **[Cox02]** les attaques sont classées en deux types : les attaques sur la robustesse et les attaques sur la sécurité.

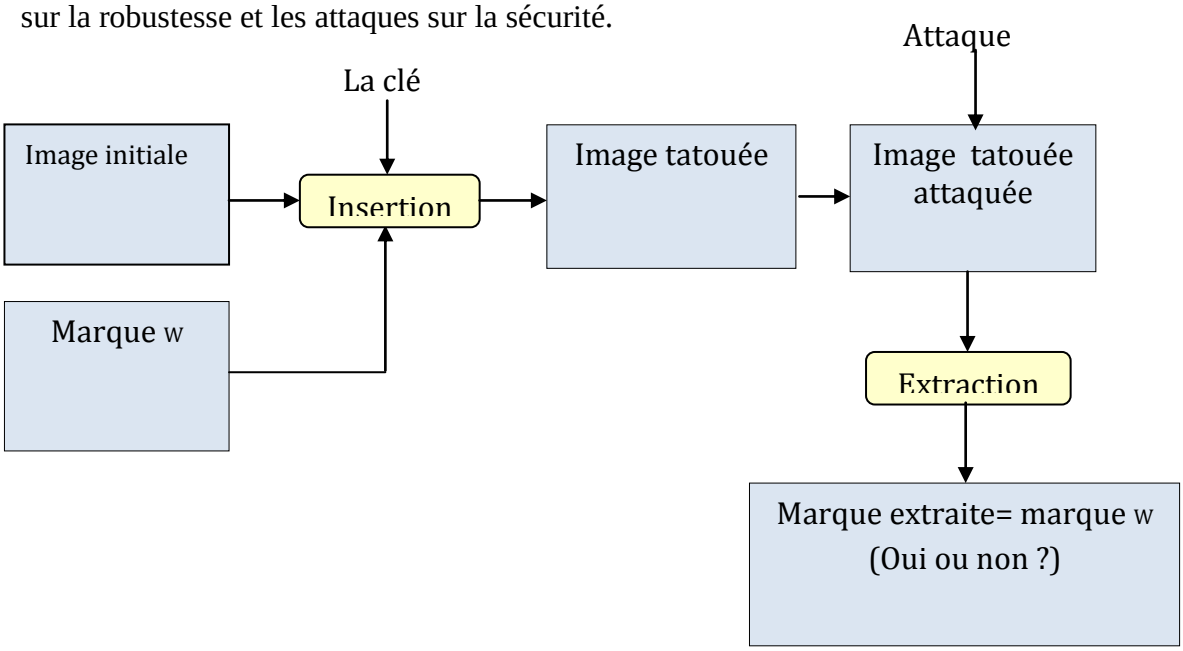


Figure. 1.19: *Exemple d'un schéma général d'un système de tatouage subi de l'attaque.*

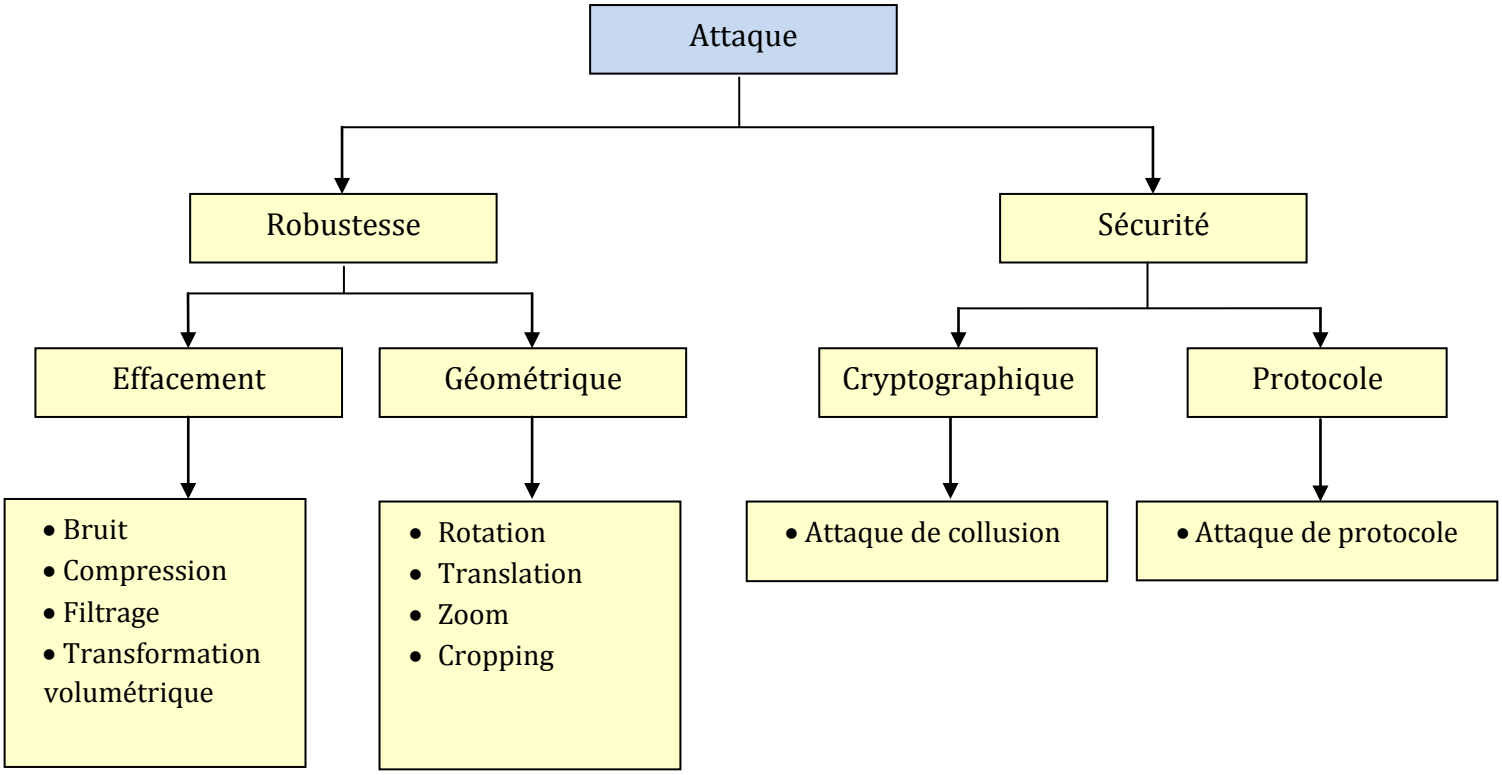


Figure. 1.20 : *Classification des attaques [**Vol01**].*

1.4.1 L'attaque d'effacement ou les attaques de traitement d'image

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

a) Attaque de bruitage

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

b) Compression avec perte JPEG

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

c) Filtrage et le lissage

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

d) Transformations volumétriques

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

1.4.2 Les attaques géométriques

Permettent de déformer ou déplacer l'image tatouée pour empêcher la détection de watermark telle que la translation, la rotation, l'agrandissement, la réduction, contrairement aux attaques de suppression, les attaques géométriques ne fait pas enlever le watermark inséré, mais tentent de déformer la synchronisation de l'extracteur de la marque insérée. Les informations de watermark insérées peuvent être récupérées si la synchronisation parfaite est retrouvée. Les attaques géométriques permettent de déformer ou déplacer l'image tatouée ce qui rend la détection de watermark ou la signature difficile, parmi les transformations géométriques les plus usuelles : la translation, la rotation, l'agrandissement, la réduction,...

a) Rotation

Des petits angles de rotation appliqués, peuvent rendre le watermark non détectable.

b) Stirmark

Est une succession de distorsions géométriques aléatoires appliquées dans des plusieurs points ou pixels d'une image d'une façon global ou local.

c) C*ropping* (rognage)

Sert à supprimer ou couper une partie d'une image.

d) 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.

1.4.3 Les attaques sur la sécurité

Parmi les attaques sur la sécurité nous citons:

a) Les attaques cryptographiques

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

b) Les attaques de protocole

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

Craver et al.**[Vol01]** ont mentionnés une attaque, comme l'attaque d'inversion de watermark ou l'attaque IBM, qui produit un faux schéma de tatouage qui peut être appliqué sur une image tatouée qui permet à créer un doute sur ce qui a été inséré en premier ,l'attaque de copier est un autre type d'attaque de protocole, dans ce cas, la marque est prédite en utilisant un ensemble de données tatouées, ce watermark prévu est inséré dans une autre donnée en adaptant les caractéristiques locales pour satisfaire son imperceptibilité.

1.5 Mesures d'évaluations visuelles de la qualité des images

Pour vérifier le critère d'invisibilité, l'image marquée doit être la même qualité que l'originale c-à-dire que l'image tatouée et l'originale soient perceptuellement similaires.

Les mesures visuelles de qualité de l'image sont effectuées sur le calcul de proximité de l'image tatouée par rapport à l'image originale ou le niveau de distorsion ou niveau de dégradation introduite par d'autres traitements sur l'image. Parmi ces mesures, on trouve des métriques basées sur la comparaison des pixels entre l'image hôte et l'image tatouée.

Parmi les métriques qui sont basées sur la différence des pixels, on cite: PSNR, MSE, MAE, SNR.

a) L'erreur quadratique (MSE) [Aia01]

L'erreur quadratique moyenne (Mean Square Error) compare deux images pixel par pixel. Elle est représentée par la formule (1,13)

$$m_s = \frac{1}{MN}\sum_i\sum_j (I(i,j) - I_w(i,j))^2 \qquad \textbf{(1,13)}$$

Où $I(i,j)$ est la valeur de la luminance du pixel (i,j) de référence et $I_w(i,j)$ celle de l'image à tester, les deux images étant de taille (MxN). La MSE renseigne sur la dégradation ou niveau de la distorsion introduite au niveau du pixel entre l'image hôte I et l'image marquée I_w. Plus la MSE est grande, plus le niveau de distorsion est élevé, une MSE de valeur faible est mieux appréciée **[Bek12]**.

b) L'erreur moyenne absolue (MAE)

L'erreur moyenne absolue (Mean Absoluate Error) est donné par la formule (1,14) **[Mot03]** :

$$m_a = \frac{1}{MN}\sum_i\sum_j \left|I(i,j) - I_w(i,j)\right| \qquad \textbf{(1,14)}$$

Cette équation quantifie les moyennes des différences absolues entre I et I_w.

c) Le rapport signal sur bruit

Les mesures de distorsion les plus populaires en traitement d'image sont, le rapport signal sur bruit "SNR" (Signal to Noise Ratio), et le "PSNR" (Peack Signl to Noise Ratio) **[Aia01]**.

Le PSNR mesure la proximité de l'image tatouée par rapport à l'image originale ou il mesure la distorsion introduite entre l'image tatouée et l'image originale au niveau du medium, Le rapport signal sur bruit SNR est un indicateur sur la qualité de la transmission d'une image, il permet de comparer le niveau d'un signal désiré au niveau du bruit.

Il est défini comme le rapport de puissance de signal sur la puissance de bruit **[Bek12]**.

SNR et PSNR sont définies respectivement par les formules (1,15) et (1,16).

$$\mathrm{SNR} = \frac{\sum_1^M\sum_1^N \mathrm{I}^2}{\sum_1^M\sum_1^N (\mathrm{I_w} - \mathrm{I})^2} \qquad \textbf{(1,15)}$$

$$PSNR = 10.\log_{10}\frac{Xmax^2}{MSE} = \frac{255^2}{MSE} \qquad \textit{(1,16)}$$

Où X est la valeur maximum possible au niveau de Pixel, il est codé sur 8 bits, X=255.Une valeur de PSNR inferieure à 30db signifié que l'image contient des dégradations visuelles ou perceptibles.

La corrélation normale (NC) est aussi utilisée pour évaluer la qualité de l'extraction de la marque insérée entre la marque originale W et la marque extraite Wˆ ; Cette corrélation est calculée par la formule (1.17)

$$NCC = \frac{\sum_i \sum_j W(i,j).W^*(i,j)}{\sum_i \sum_j W(i,j)^2} \qquad \textit{(1,17)}$$

Ou W (i, j) est la valeur de pixel à la position (i, j) de l'image hôte, et W* (i, j) est la valeur de pixel à la position (i, j) de l'image tatouée.

1.6 Conclusion

Dans ce chapitre nous avons étudié l'aspect général de tatouage, nous avons présentés des notions générales de tatouage tels que les critères pour la tatouage numérique être performant, les différentes attaques et comment évaluer les techniques de tatouage perceptuellement.

Nous avons aussi présentés les phases de conception du tatouage (phase d'insertion et phase d'extraction) et la classification selon différentes contraintes (le champ d'application et l'espace d'insertion dans le domaine spatial ou dans le domaine transformé tel que la DCT, la DWT, la DFT et la SVD, et en fonction de type d'algorithme utilisé (robuste ou fragile, additif ou substitutif, aveugle ou non aveugle), les techniques de chiffrement (asymétrique ou symétrique) et selon la restauration de l'image hôte (réversible ou irréversible).

Le tatouage réversible est utilisé pour assurer l'intégrité de l'image qui permet de retrouver ou restaurer l'image originale à partir de l'image tatouée en appliquant une transformation inverse sans produire des changements perceptuel et permet aussi d'éviter une distorsion irréversible dans l'image originale en appliquant des techniques capable d'extraire l'image

originale, Par contre le tatouage non réversible, il n’existe aucun moyen de retrouver l'image originale à partir de l'image tatouée. Ce critère sera étudié en détail dans le chapitre suivant.

Chapitre 2

Tatouage numérique réversible dans le domaine spatial

Chapitre 2 *Tatouage numérique réversible dans le domaine spatial*

2.1 Introduction

Grâce à des techniques de tatouage appropriés, la protection des données peut être assurée et que l'on peut savoir si le contenu reçu a été altéré ou non.

Toutefois, le tatouage peut causer des dommages aux informations sensibles présentes dans le support hôte, et donc à la réception, la récupération exacte de celle-ci ne peut pas être possible. Dans certaines applications, même la moindre distorsion dans les images hôtes est intolérable.

Par exemple, dans le domaine de l'imagerie médicale, si une image médicale est modifiée par le tatouage fragile, un léger changement peut affecter l'interprétation de manière significative, par conséquent le médecin puisse faire un faux diagnostic. De même, en cas d'application militaire, les changements en raison de l'insertion d'information secrète peuvent modifier sensiblement l'image originale et par conséquent, la décision prise peut considérablement être coûteuse. Par conséquent, il est nécessaire de restaurer le travail hôte à sa forme originale.

Le tatouage réversible, aussi connu sous le nom de tatouage sans perte, qui permet de l'extraction complète de l'information insérée avec une restauration complète du support hôte. Le tatouage réversible peut donc être considéré comme un cas particulier de tatouage.

En plus**,** le tatouage réversible gagne plus d'attention pour les quelques dernières années en raison de ses applications de plus en plus dans le domaine de communication militaire et dans le domaine sanitaire.

2.2 Principe du tatouage réversible

Le tatouage réversible se base sur l'insertion de la marque dans l'image d'une façon réversible, il est aussi capable de restituer l'image hôte âpres la phase de l'extraction et la vérification de l'intégrité.

Les méthodes de tatouage réversible sont basées sur l'utilisation de la compression comme une base ; le rôle principal de la compression est de réduire l'espace dans le support et de minimiser la quantité de données pour garder la qualité visuelle de l'image.

Les méthodes irréversibles sont basées sur l'insertion des données par la modification des bits les moins significatifs LSB. Pour garantir la réversibilité, il faut donc coder ces LSB's et les compresser pour les réinsérer dans leurs emplacements **[Fou98]**. Le schéma de ce type se divise en deux phases : phase d'insertion et phase d'extraction.

a) Phase d'insertion

Cette phase permet de représenter les étapes d'insertion d'une signature invisible générée à l'aide d'une clé k, l'insertion peut s'effectuer dans l'espace spatial ou dans l'espace fréquentiel comme la transformée de DCT, DWT, DFT ou SVD. Soit $\boldsymbol{I}$ une image hôte, $\boldsymbol{W}$ une marque générée à l'aide d'une clé $\boldsymbol{K}$ tel que le résultat obtenue est une image tatouée $\boldsymbol{I_W}$.

— ***Les étapes d'insertion de tatouage réversible*** **[Fou98] :**

- On transforme l'image hôte selon le domaine d'insertion spatial ou fréquentiel.
- On choisi les composantes de l'image soit les pixels (dans le domaine spatial) ou bien les coefficients de transformée (dans le domaine fréquentiel) pour l'insertion de la marque.
- Ensuite on applique une fonction de hachage sur les composants de l'image.
- On concatène le résultat de hachage avec les données de l'utilisateur pour obtenir une signature.
- On Reconstruit l'image marquée ou tatouée par le processus d'insertion qui s'effectue par l'ajout de la signature aux composants de l'image choisis dans l'étape 2.

b) Phase d'extraction

La phase d'extraction se base sur deux étapes : la première étape est basée sur l'extraction de la marque insérée et la deuxième est basée sur le calcul de taux de similitude entre les données initiales originales et les données extraites pour prendre une décision si l'intégrité est garantie ou non.

Les étapes d'extraction de tatouage réversible **[Fou08] :**

- Transformer l'image tatouée selon le domaine d'insertion (spatial ou transformé).
- Extraire les composantes marquées.
- Inverser la phase d'insertion pour trouver les composantes de la signature.
- Appliquer une fonction de hachage sur l'image tatouée.
- Faire une comparaison entre la marque extraite avec la marque originale obtenue par la fonction de hachage.
- Prendre la décision si l'intégrité est vérifiée ou non. si l'intégrité est vérifiée alors on passe à la reconstruction de l'image hôte. Si l'image est altérée, donc elle sera rejetée.

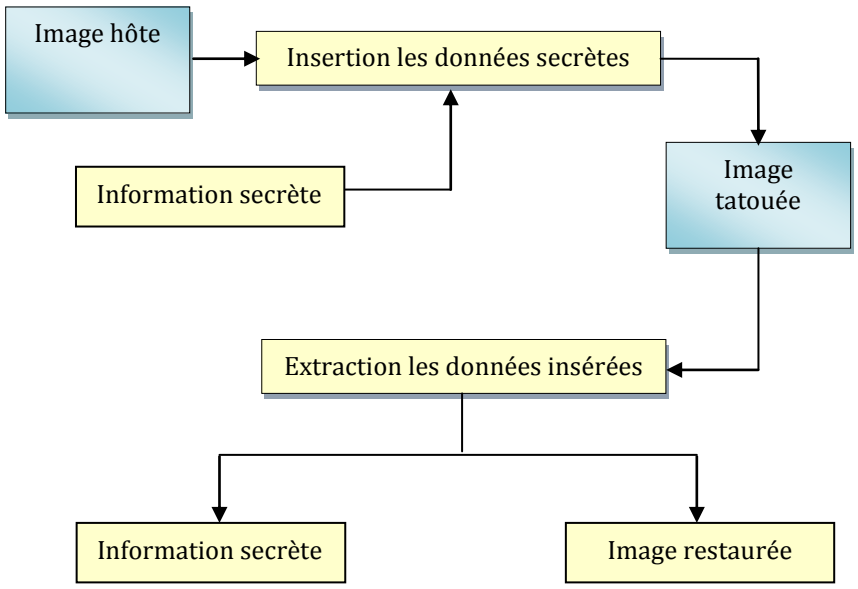


***Figure2.1** : Principe de tatouage réversible.*

2.3 Les méthodes du tatouage réversible

Le tatouage réversible se base sur la compression des données qui se diffère selon le type des données initiales et qui permet d'avoir un plus d'espace dans l'image tatouée tel que dans le domaine médical la compression est utilisée pour éviter toute distorsion qui donne une fausse interprétation qualitative de l'image médicale contrairement aux méthodes irréversibles peut se faire par la modification par exemple les LSB's.

Pour assurer la réversibilité en effectuent un processus de l'insertion des données en modifient les éléments du signal hôte (les LSB's ou bien les coefficients de transformée) et les compresser pour les réinsérer dans l'image hôte et rendre la récupération des données insérées facile par l'extracteur.

L'une des premières méthodes de tatouage réversible a été présentée par Honsinger et al. [66]. Ils ont utilisés la méthode de l'addition modulo 256 pour atteindre la réversibilité dans leur technique du tatouage. L'utilisation de modulo 256 rendre cette technique fragile par rapport à l'attaque de bruit Sel and Pepper.

Macq **[Mac00]** a développé une approche de tatouage réversible par la modification de l'algorithme de patchwork et le modulo 256. Bien que, Honsinger et al. **[Hon01]** et Macq **[Mac00]** ont proposé une technique réversible ou l'imperceptibilité de leur approche ne sont pas vérifié.

Les résultats obtenus par la technique de Honsinger et al et Macq sont fragile contre l'attaque de bruit Sel et Pepper.

Jessica Fridrich[**[Bly04]** a montré deux méthodes différentes de tatouage réversible, l'une de ces méthodes est basée sur la compression sans perte.

Celik et al **[Cel02]** séparent d'abord le bloc en un bloc des bits de poids faible et en bloc de poids fort, ensuite ils ont appliqués la compression pour réduire la taille des bits de poids faible, pour retrouver l'image tatouée en assemblant les deux blocs.

Le processus de l'extraction est basé sur la division de chaque bloc en deux blocs. Pour extraire la marque insérée en utilisant la décompression pour retrouver les bits insérés et la récupération de l'image originale.

Fidirich et al **[Fri01]** ont proposé une autre technique qui se base sur la compression mais elle est fragile telle que des petites modifications peut perturber l'extraction de la marque.

Puech et al **[Pue05]** ont présenté aussi une technique qui se base sur la compression et qui permet de décomposer une image initiale en sous images, chaque sous images est composée de bits de poids fort qui sont encodés par la compression RLE (Run-Length Encoding) pour gagner un espace pour l'insertion des données réversibles. Pour obtenir l'image tatouée en assemblant les deux sous images qui seront cryptées. L'avantage de cette méthode et de réduire le temps de calcul par l'utilisation de la compression qui suit un processus unique.

La méthode qui a été proposée par Tian **[Tian03]** se base sur la présentation de l'image initiale en pair de pixels, ensuite pour chaque pair une valeur moyenne de la différence est calculée, cette différence est modifiée par les bits insérés. Ces nouvelles valeurs obtenues permettent de restaurer les pixels originaux et les données insérées.

Alattar**[Ala04]** a proposé une technique qui permet d'insérer un bit dans un vecteur de pixel au lieu d'une paire de pixel. L'avantage de cette méthode est la performance très élevée car l'insertion de plusieurs bits de la marque est s'effectué à la fois dans un vecteur de pixel.

Une autre technique aveugle de décalage d'histogramme a été introduite par Thodi et Rodriguez **[Tho07]** qui permet d'augmenter la qualité visuelle de l'image tatouée par rapport à la méthode de Tian mais elle est fragile à tous différents types d'attaques.

De Vleeschouwer et al. **[Vle03]** ont proposé une technique réversible et aveugle qui permet de découper une image en un ensemble des blocs de même taille d'une façon aléatoire ensuite un histogramme de la luminance est calculé pour chaque ensemble.

L'insertion s'effectue par un décalage de cet histogramme de la luminance tel que cette luminance est entre 0 et 255. Les résultats de cette technique montrent que cette méthode est plus robuste.

2.4 Les travaux basant sur le tatouage réversible dans le domaine médical

2.4.1 L'imagerie médicale

L'imagerie médicale regroupe l'ensemble des moyens physiques ou des techniques utilisés par la médecine pour le diagnostic mais aussi pour le traitement d'un grand nombre de pathologies pour visualiser les cellules d'un organisme (corps humain) **[Guy02]**.

Son but est de proposer une représentation visuelle perceptible d'une information ou d'une donnée à caractère médicale. Une image médicale peut être interprétée structurellement (description de la structure (forme)) ou fonctionnellement (description du fonctionnement d'un organe).Dans un cadre plus large, l'imagerie médicale englobe tous les moyens et les techniques d'acquisition, de stockage, de traitement et d'interprétation des informations médicales sous forme une image. **[Bek12]**

2.4.2 Les images numériques et le système visuel humain

1) Représentation mathématique sous forme matricielle

Une image numérique 2D est représentée par une matrice de m lignes et n colonnes ou le pixel est indiqué par un couple (i, j) où i est l'indice de ligne tel que $i \in \{0, m-1\}$, et j est l'indice de colonne ou $j \in \{0, n-1\}$, tel que n est la largeur et m est l'hauteur de l'image.

a) Numérisation des images

C'est une procédure qui permet d'acquérir, de traiter, de formater et d'enregistrer des images réelles sous une forme représentable par des valeurs numériques. La numérisation c'est toute transformation qui subie l'image originale pour pouvoir la manipuler par un système informatique. La numérisation peut être directe ou indirecte, elle permet de passer de l'image médicale intensive originale à l'image prête pour divers traitements informatiques et

ensuite être remise au patient ou au médecin demandeur sous forme de film ou sous forme numérique. **[Gol10]**

L'image numérique est découpée en de nombreuses suites de petits points appelés pixels. La qualité de l'image dépend en partie du nombre de pixels déterminé. Plus le nombre de pixels *est* élevé, plus la qualité de *l'image* obtenue *est* grande. La dimension donnée en pixel précise le format d'affichage**.** Il existe différents formats de stockage de l'image (JPEG, GIF, PNG, MNG, TIFF, BMP et PSD) **[Gol10]**.

b) Système visuel humain

La perception visuelle est très importante dans le domaine de traitement d'image, la perception visuelle est un dispositif qui repose sur la spécification du SVH (système visuel humain).le SVH est un système compliqué qui est crée sur des éléments visuels et rendre la vision par l'ordinateur et la vision humaine semblent avoir la même fonction.

Les applications qui reposent sur la protection des droits d'auteurs et la sécurité des données sont basée sur l'utilisation de system visuel humain (HVS) parmi eux la compression et le tatouage qui nécessite d'insérer la marque tel que l'invisibilité et la robustesse soient présente.

Beaucoup de recherches dans les techniques de tatouage d'images sont basées sur les propriétés de perception du système visuel humain (HVS) et ont été réalisées pour améliorer la robustesse et la capacité des données à dissimiler.

Le développement et l'amélioration de la précision des modèles visuels humains aident à la conception et la croissance des masques perceptuels qui sont utilisés pour mieux dissimuler la marque insérer dans l'image originale (hôte) en augmentant sa sécurité et en récupérant les données insérées **[Gol10]**.

2.4.3 Nécessité de La sécurité des données et des images médicales dans la télémédecine

L'imagerie médicale est un domaine où la protection de l'intégrité et la confidentialité du contenu est une question cruciale en raison des caractéristiques spéciales provenant de l'éthique stricte, législatives et les implications diagnostiques. Il est très important pour prévenir la manipulation non autorisée et l'appropriation illicite de ces images numérisées.

Les risques sont accrus lorsqu'il s'agit d'un environnement ouvert comme l'internet. Les images devraient être sauvegardés intactes en toute circonstance et avant toute opération. Avec la numérisation, la télémédecine ou la transmission des images et des dossiers médicaux entre des professionnels de santé et des organisations des soins à travers les réseaux est devenue possible **[Che05] [Bek12]**.

Dans ces applications, l'mage joue un rôle vital pour permettre un diagnostic, faciliter une intervention chirurgicale ou approfondir les connaissances d'une manière générale. Ainsi aujourd'hui, il est possible dans certains centres occidentaux que le médecin demandeur reçoit à distance l'examen radiologique de son patient en temps réel à travers les réseaux connectant différents types des systèmes d'informations médicaux (SIM).

Les infrastructures les plus courantes sont les Hospital Information System (HIS),les Radiology Information System(RIS),et les PACS (Pictures Archiving and Communication Systems).Toutes ces applications ont pour objectifs de faire circuler plus vite, en plus grand nombre les flux d'informations entre différents services de l'infrastructure et particulièrement les dossiers médicaux, souvent complexes, des patients **[Che05][Bek12]**.

En effet l'image médicale est rarement transmise seule, elle doit souvent être mise en perspective avec les autres éléments plus conventionnels du dossier médicale : l'historique du malade, ses antécédents, sa pathologie et ses traitements actuels, sans oublier les informations administratives permettant d'identifier d'une façon univoque les patients et les données.

Les patients considèrent les informations liées à leur état de santé comme étant les plus privées. Pour encourager la confiance des patients et minimiser les risques organisationnels, les établissements de santé doivent impérativement protéger les données et les images collectées **[Che05][Bek12]**.

Le mode de circulation d'information soulève de sérieuses questions de sécurité relatives aux dossiers médicaux, particulièrement face aux exigences des aspects éthiques et légaux propres au domaine médical.

Les problématiques soulevées par la généralisation de la numérisation des images médicales sont encore nombreuses et ne peuvent être considérées comme totalement résolues à l'heure actuelle. Les principaux aspects de sécurité concernant les dossiers médicaux sont :

- La confidentialité, qui assure que les informations médicales transmises à travers les réseaux ou stockées pour l'archivage ne sont accessibles que par les parties concernées. Les atteintes à la confidentialité sont alors la divulgation d'information secrète et le re-routage par les parties non autorisées.

- L'authentification sert à prouver que les dossiers reçus ont bien été émis par la partie déclarée et qu'ils n'ont pas été altérés en cours de route. Une partie non -autorisée peut avoir inséré une fausse image médicale ou un faux document dans le système d'information.

- L'intégrité assure que les informations médicales n'ont pas été altérées accidentellement ou frauduleusement pendant leur transfert sur le canal de communication, permet de détecter toutes modifications provenant par les utilisateurs non autorisés. parmi les premières méthodes proposées pour garantir l'intégrité des images sont basées sur le tatouage fragile **[Yu08] [Pue04]** qui permet d'insérer une marque sous forme un logo dans l'image hôte de telle façon que les modifications qui sont portées à l'image, et à la marque. La présence de la marque indique la vérification de l'intégrité.

En plus de l'intégrité, l'avantage de ce dernier est de retrouver l'image originale. Les applications du tatouage réversible seront donc celles généralement développées pour sécuriser les transmissions non fiables ou le choix de la méthode est basé sur la préservation et particularités des images médicales.

2.5 Méthodes de tatouage réversible dans le domaine médical

Aujourd'hui; les systèmes de gestion de données modernes de l'Hôpital (HDMSs) sont appliquées dans un réseau informatique; en plus des équipements médicales produisent des images médicales sous forme numérique.

HDMS doit stocker et échanger les images dans un environnement sécurisé pour assurer l'intégrité de l'image et la vie privée des patients. Les techniques de tatouage réversibles peuvent être utilisées pour fournir l'intégrité et la confidentialité. Dans **[Bek11]**, une technique de sécurité est basée sur le tatouage et le cryptage a été proposé pour être utilisé dans l'imagerie médicale et de la communication en médecine (DICOM). Il fournit l'authentification du patient, et l'intégrité des informations sur la base de tatouage réversible. La valeur de hachage et de l'identité du patient sont concaténés pour former une marque. Cette dernière est chiffrée en utilisant l'une des techniques de cryptage, enfin, la signature est insérée dans l'image médicale.

Pour la plupart des applications, certaine distorsion dans le contenu de l'image pourrait être acceptable, mais pour des applications médicales, les images doivent être conservés parfaitement sans aucune perte d'information, ce qui ‘il faut le tatouage ne doit pas introduire des distorsions visibles dans l’image.

Des différents schémas de tatouage ont été proposés pour résoudre les problèmes de protection à la fois la confidentialité médicale et l'authentification des données .le tatouage robuste contenant la signature numérique du médecin pour vérifier l'authentification, et le tatouage fragile dans le but de contrôler l'intégrité des données.

Dans **[Bou04]** un nouveau paradigme de tatouage sert à garantir l’authentification des données et l’intégrité des images par l’insertion d'une marque réversible dans l'image hôte, ce qui permet la récupération exacte de l'image originale lors de l'extraction de la signature incorporée. Cette propriété correspond exactement aux exigences imposées par la manipulation des images médicales.

Les auteurs ont présenté un travail, ils combinent les outils cryptographiques(le chiffrement) et la MAC (Message authentification Code) obtenue par la fonction de hachage, pour fournir la confidentialité et l'authentification en même temps et de façon réversible. La confidentialité est obtenue par la concaténation de la forme cryptée de l'information du patient avec l’image médicale correspondante tandis que l'authentification est obtenue par l’insertion de condensé du message.

Dans le processus de vérification, on extraire la MAC et les informations du patient en le comparant avec celle calculer à partir de l’image originale pour authentifier l’image sans ambiguïté. Si l'image est altérée en quelque sorte, le programme de vérification sera alerté par l’utilisateur (le médecin). Il existe plusieurs avantages de tatouage réversible d'une image médicale, de telle façon:

— Un patient ne veut pas nécessairement sa / son image médicale ouvert au public (image médicale est considéré comme propriétaire de ce patient).

— Parfois, le lien entre l'image et le patient est perdu, donc, l’insertion de l'information de patient dans l'image pourrait être une mesure utile de la sécurité.

- ***Exemple de tatouage réversible***

Cette approche permet d'insérer les données des patients incluses (N° d'identification, Signature, Dossier du patient, adresse, signature de l'hôpital, diagnostic médical, les données de médecin) dans un ensemble de différents types d'images médicales (IRM, échographie, Radiographie ...).

Toutes les données doit être cachées, protégées et correctement transmises lors de partage et la diffusion de l'image. Un système de tatouage qui se base sur le tatouage réversible permet de retrouver l'image originale après l'extraction de la signature à partir de l'image tatouée.

Dans **[Bou04]** cette méthode de littérature a été présentés par Boucherkha .S et Benmohamed pour le but de garantir l'authentification des données et l'intégrité des images médicales relatives au patient. Nous présentons ci-dessous les étapes de l'insertion et de l'extraction de tatouage réversible.

1) Phase d'insertion

L'algorithme d'insertion est le suivant :

- Sélectionner les LSB's (les bits de poids faible) et les MSB's (les bits de poids forts) de l'image originale.
- Calculer l'empreinte des bits de poids forts (MSB) de l'image.
- Concaténer l'empreinte de l'image avec les données du patient et de crypter le résultat.
- Appliquer la compression sans perte au LSB's de l'image originale.
- Concaténer le résultat compressé avec les données cryptées et les réinsérer dans l'emplacement des LSB's pour obtenir une image tatouée ou marquée. La figure 2.2 représente le schéma de l'insertion de tatouage réversible.

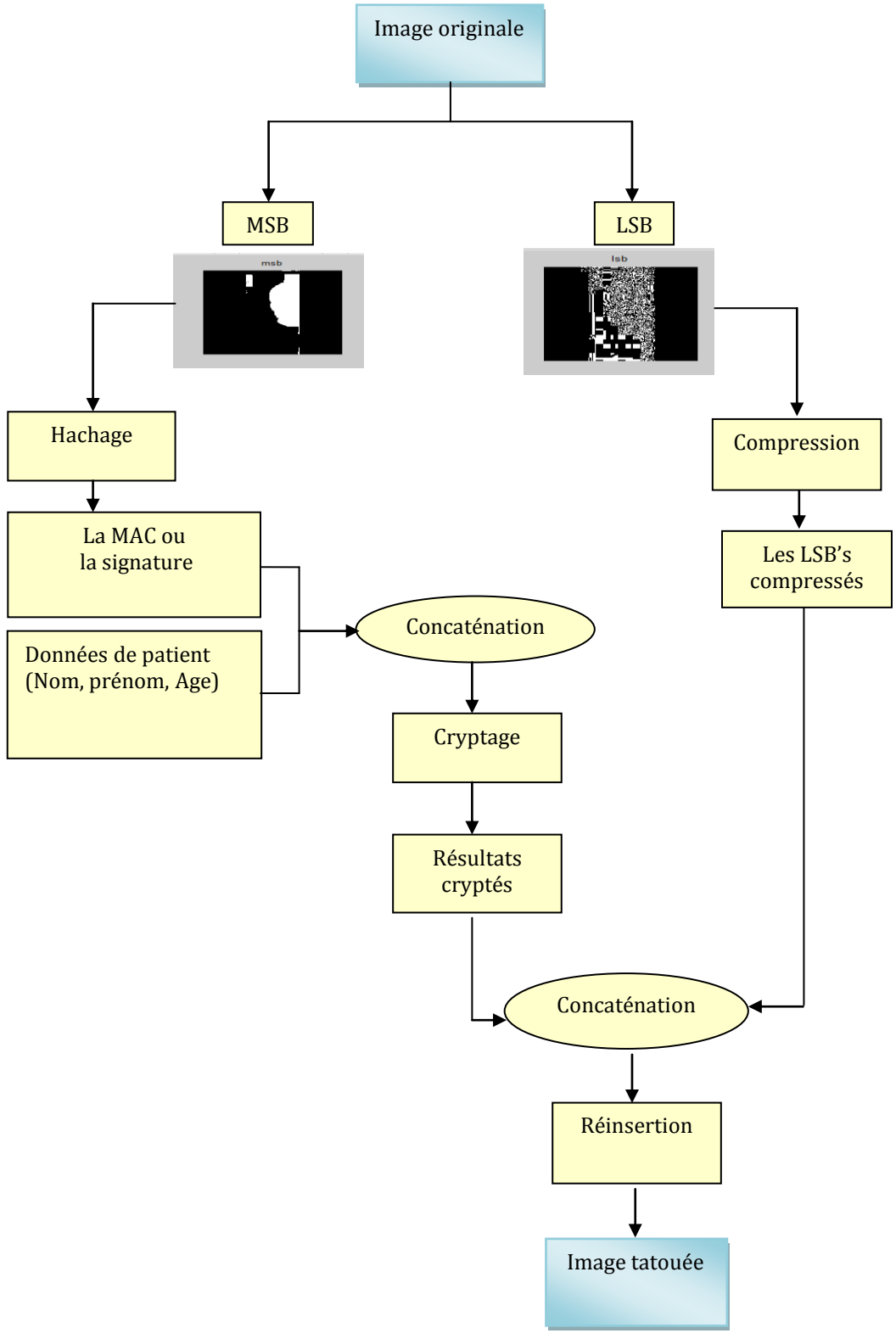


Figure 2.2 : *Schéma d'insertion du tatouage réversible* ***[Bou04].***

2) Phase d'extraction

L'algorithme d'extraction est le suivant :

— Extraire les données des LSB's.

— Séparer les deux chaînes de caractères, la première chaine contenant les LSB's compressés et la deuxième chaine c'est la concaténation de l'empreinte avec les données du patient.

— Décompresser les LSB's et les remettre à leur emplacement pour récupérer l'image originale.

— Récupérer les données du patient et l'empreinte de l'image en appliquant un décodage.

— Le contrôle de l'intégrité de l'image se fait en calculant l'empreinte originale MAC (Message Authentication Code) et en le comparant avec l'empreinte extraite.

La figure 2.3 illustre le processus de l'extraction de tatouage réversible. Le tatouage réversible utilise des jeux conséquents de cryptographie et la fonction de hachage, si ces algorithmes sont faibles et crackable ce qui rend cette méthode automatiquement faible **[Bek12].**

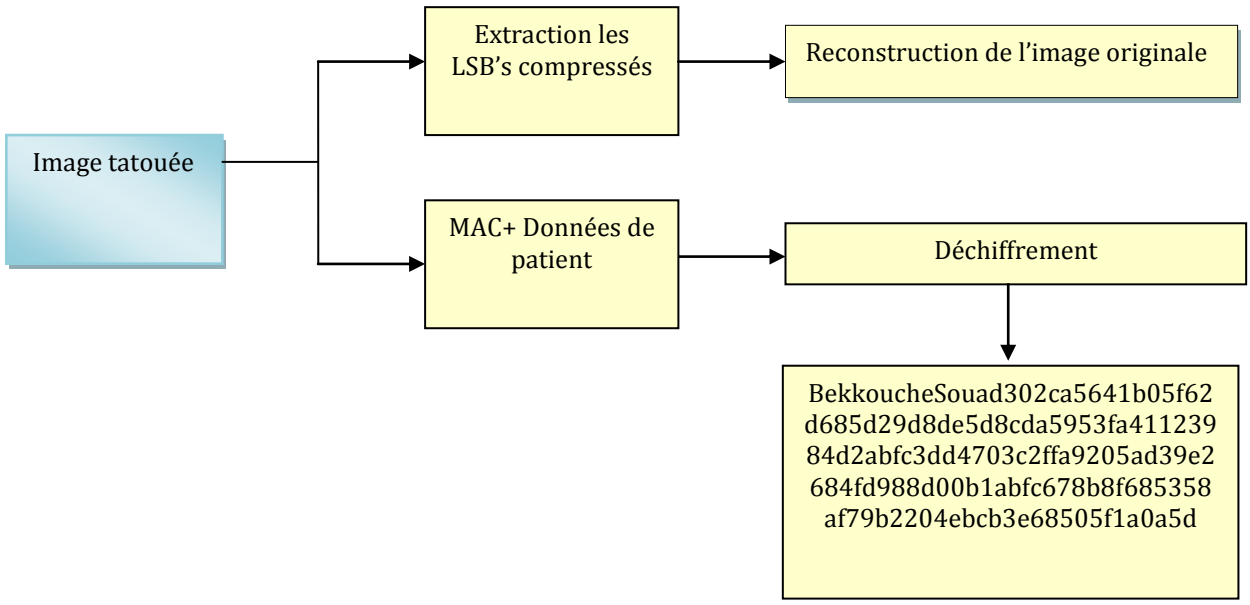


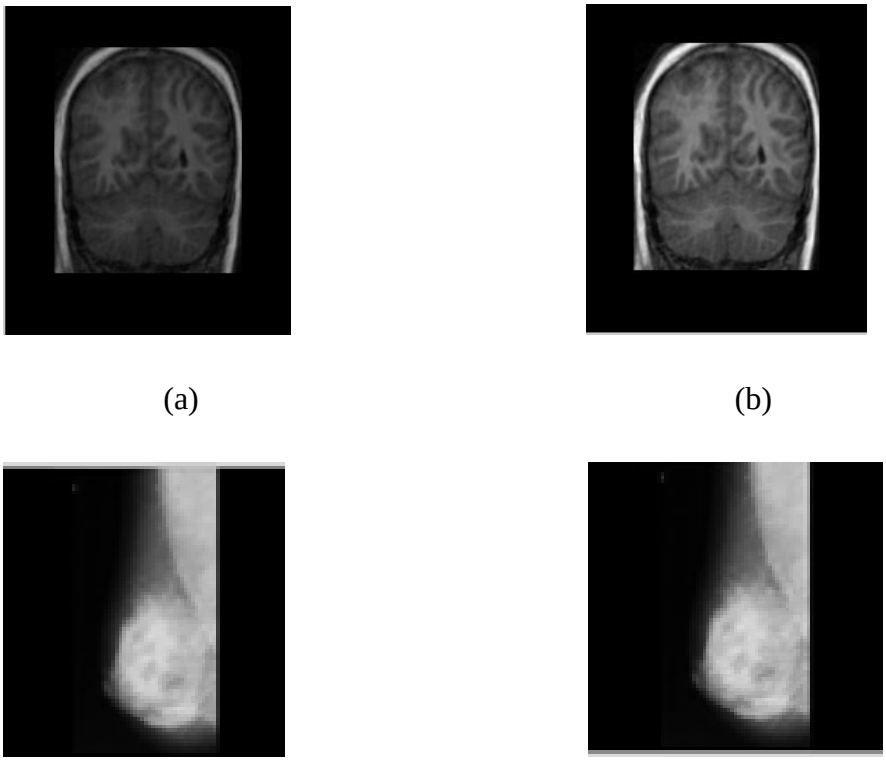
Figure 2.3 : *Schéma d'extraction du tatouage réversible* ***[Bou04].***

Données de patient	Nombre de caractères
Empreinte (signature)	128
Nom	20
Prénom	20
Age	2
Sexe	1

Tableau 2.1 : *Format des données du patient insérées par le tatouage réversible (RW)* ***[Bou04] [Bek11].***

Le nombre de bits maximaux inséré dans l'image est : (128+20+20+2+1) x 8 = 1368 bits.

Nous avons effectué des tests sur deux types d'échantillons d'images médicales format BMP (image IRM de taille 256 x256 et une image Mammographie de taille 166 x166) .Un échantillon de 10 images est pris pour chaque type d'image **[Bek11] [Bek12]**.La figure2.4 montre les images tatouées IRM et Mammographie



(a) (b)

(a') (b')

Figure 2.4 : *(a) image originale, (b) image tatouée par la technique* ***[Bou04].***

Le tatouage réversible (RW) est adapté pour mettre et incorporer les données de patient cryptées dans l'image d'une manière réversible qui utilise la compression sans perte et permet d'un coté de restaurer parfaitement l'image originale qui peut être authentifiée sans ambigüité et d'un autre coté sauvegarde et transmis les données du patient d'une manière confidentiel. Les résultats expérimentaux montrent que la performance de système du tatouage qui est basé sur le tatouage réversible **[Bou04]** dépend de la force et la résistance des outils cryptographiques utilisés qu'il faut devrait donner une sécurité complète **[Bek11]**.

2.6 Conclusion

Comme nous venons de le voir, le principal inconvénient des méthodes de tatouage réversible dans le domaine spatial est la faible robustesse face aux attaques et notamment face aux attaques géométriques.

Les techniques de tatouage réversible telle que celle que nous venons de découvrir peuvent tout aussi bien être adaptées au domaine fréquentiel.

Les domaines transformés les plus fréquemment exploités pour les applications de tatouage d'image sont le domaine de Fourier DFT (Transformation en Fourier Discrète) et le domaine DCT (Transformation en Cosinus Discrète), la SVD (la décomposition de valeur singulière) et la DWT (la décomposition en Ondelette Discrète). Ce domaine sera étudié en détail dans le chapitre suivant.

Chapitre 3

Tatouage numérique des images dans le domaine fréquentiel

Chapitre 3 *Tatouage numérique des images dans le domaine fréquentiel*

3.1 Introduction

Le domaine transformé est un espace dans lequel l'image est représentée sous la forme d'un ensemble de fréquences de différentes amplitudes**.**

Les algorithmes dans le domaine transformé sont basés sur l'insertion de l'information dans l'image hôte par opposition au domaine spatiale. L'insertion dans l'espace fréquentiel s'effectue par l'utilisation de différentes transformations TFD (Transformée de Fourier Discrète), TCD (Transformée en Cosinus Discrète), DWT (Transformé Ondelette Discrète) et SVD (Single Value Decomposition).

L'utilisation de la transformée par TCD, SVD ou DWT se mis en œuvre par la transformation de l'image en différents coefficients de différentes priorités suivant le système visuel humain.

Pour insérer plus d'informations dans l'image hôte sans produire aucune déformation perceptuelle visible il faut que la transformation soit plus proche aux propriétés de SVH (système visuel humain).Généralement les algorithmes de tatouage dans le domaine fréquentiel sont plus robustes contre la compression telle que JPEG, car le même espace transformé utilisé, permet le codage de l'image.

3.2 Le domaine de la transformée en Cosinus Discrète (DCT)

La transformée en cosinus discrète DCT a été réalisée en 1974 par Ahmed.N, elle est présentée dans l'article sous le titre "Traitement d'Image et La transformation en cosinus discrète" .Cette technique est effectuée par l'utilisation de codage de l'image pour insérer le watermark **[Bou04]** ce qui le rend plus robuste face à une compression JPEG, la compression la plus utilisée parmi les transformations existantes. L'avantage de cette transformation est d'exploiter les méthodes psychovisuelles qui sont basés sur l'utilisation des zones où l'insertion de la marque reste imperceptible par contre les techniques d'insertion par la modification des coefficients de la DCT. Ce qui les rend très fragile aux opérations géométriques **[Bou04]**.

Les techniques qui sont basées sur la transformée de DCT permet de séparer les hautes fréquences des basses fréquences. Les basses fréquences contient l'information de l'image entière tel que les hautes fréquences contient les détails de cette dernière .Si l'insertion s'effectue dans les hautes fréquences la technique sera robuste mais la marque sera invisible par contre si l'insertion s'effectue dans les basses fréquences, la marque sera invisible mais la technique ne sera pas robuste ; donc il faut trouver un compromis entre les deux propriétés (invisibilité /robustesse) par l'insertion de la marque dans les moyennes fréquences.

Lorsque la DCT est effectuée sur une matrice carrée M×M de pixels le résultat est une matrice carrée M× M de coefficients de fréquence. A cause de la difficulté rencontrée durant l'application de la DCT sur la matrice entière, celle-ci est décomposée en blocs de taille 8 × 8 pixels.

Les équations (3,1) et (3,2) donnent respectivement la transformée en cosinus discrète directe et la transformée en cosinus discrète directe inverse de l'image MxN.

La transformée Directe :

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \Lambda(u)\Lambda(v)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} I(i,j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right].\cos\left[\frac{\pi.v}{2.M}(2j+1)\right] \quad \textbf{(3,1)}$$

Et l'inverse de la transformation DCT (IDCT) est défini comme suit :

$$I(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(u)\Lambda(v)F(i,j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right].\cos\left[\frac{\pi.v}{2.M}(2j+1)\right] \quad \textbf{(3,2)}$$

Avec :

$F(u,v)$: Les coefficients de DCT de l'image.

$I(u,v)$: Valeur d'un pixel de l'image.

La première étape est basée sur la division de l'image en bloc 8x8 de pixels ensuite la transformation donnée par la formule (3,3) est appliquée sur les blocs de l'image.

$$F(u,v) = \frac{\Lambda(u).\Lambda(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} I(i,j).cos\left[\frac{\pi.u}{16}(2i+1)\right].cos\left[\frac{\pi.v}{16}(2j+1)\right] \quad \textbf{(3,3)}$$

Pour donner un bon compromis entre la qualité de l'image et le temps de calcul il faut éviter d'appliquer la DCT sur l'image entière qui prenait plus de temps donc il suffit d'appliquer la DCT sur les blocs de taille fixe de 8x8 pixels [85].

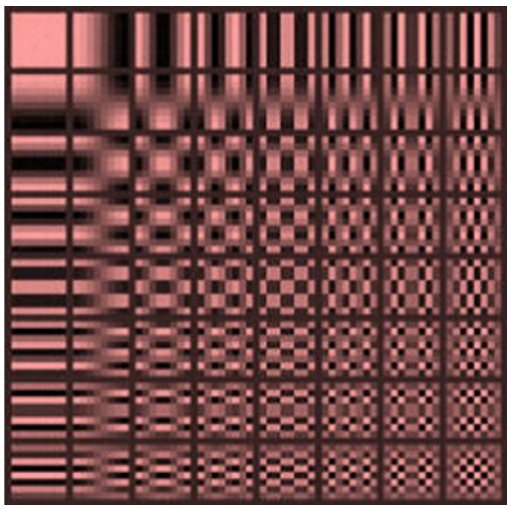


Figure 3.1 : *Représentation des 64 composantes fréquentielles formant la base de décomposition en DCT 8x8 (les moyennes fréquences obtenues par DCT []).*

Cox et al. (1997)**[Kil97]** ont suggérés que la marque numérique est insérée dans les zones visuellement significatives des coefficients de DCT dans un mode non linéaire. Autrement dit, les marques devraient être insérées dans la composante significative du système de vision humain (HVS) par contre la plupart des techniques de compression tentent de réduire la redondance des images. Cox et al (1997) ont montré la robustesse de cette technique contre de multiples attaques.

Plus tard, les chercheurs ont suggéré de modifier les techniques proposées par Cox et al. (1997) en raison de sa revendication de robustesse. Pour augmenter la capacité de l'information et de la détection, certains travaux proposés sont basé sur la division de l'image en blocs puis d'appliquer la DCT sur chacun de ces blocs, comme il est montré dans la compression JPEG **[Kil97]**.

Hsu et al. (1999) **[Hsu99]** étaient en désaccord avec Cox et al. (1997) et ont proposé une technique qui montre que la marque est un seulement certains nombres de coefficients de moyenne fréquence dans le but d'avoir une distorsion minime et par conséquent il permet de donner une haute qualité visuelle des images.

Hsu et al. (1999)**[Hsu99]** ont utilisé la DCT et la relation entre les blocs voisins pour insérer la marque. Ils ont suggéré d'insérer la marque par la sélection des coefficients intermédiaires modifiés afin de satisfaire la transparence et la robustesse. Ils ont également proposés que la marque numérique doive être un pseudo aléatoire changée avant de l'insérer dans l'image hôte.

Dans son papier, Hsu a expliqué qu'après la transformation par la DCT de l'image originale, les coefficients de la moyenne fréquence en ordre de zigzag des blocs transformés sont sélectionnés pour insérer la marque numérique. Dans leurs résultats expérimentaux, ils ont également noté que la technique d'insertion pourrait survivre face à l'attaque de cropping, et la compression avec perte **[Hsu99]**.

Une autre méthode non aveugle a été proposée par Suhail **[Suh03]** qui est proche de la technique de Cox 97. Elle est basée sur la décomposition de l'image en blocs où la marque est une séquence aléatoire qui est insérée dans les moyennes fréquences de chaque bloc. Les résultats de cette méthode donnent des meilleures caractéristiques par rapport aux résultats de Cox97 **[Kil97]**.

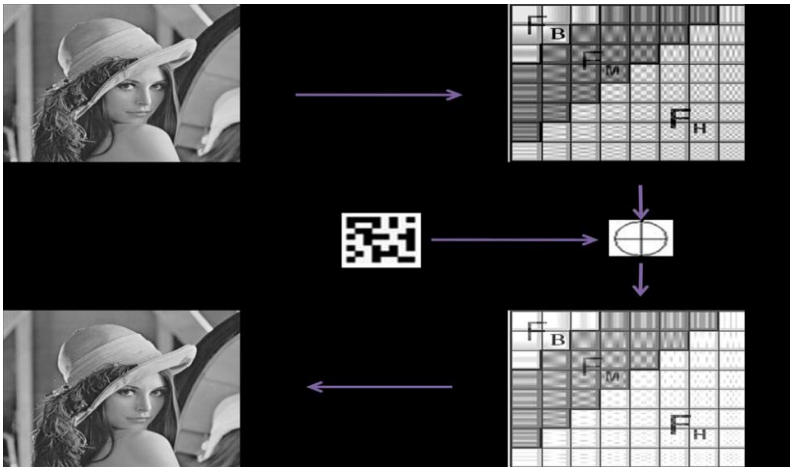


Figure 3.2 : *Exemple d'insertion dans les fréquences moyennes de DCT.*

Koch98 **[Koc89]** a proposé une autre méthode de tatouage qui se base sur l'insertion de la marque dans le domaine fréquentielle DCT qui permet de décomposer l'image en blocs de 8x8, ensuite ils calculent la DCT sur chacun de ces blocs. L'insertion s'effectue à partir des coefficients de DCT qui se trouvent dans les blocs de moyennes fréquences qui sont quantifiés suivant une table de quantification.

L'insertion dans le domaine de la transformée en modifiant les coefficients DCT offre de nombreux avantages, notamment la robustesse contre les attaques intentionnelles de traitement d'image tels que la luminosité et le réglage du contraste, correction gamma, filtrage etc, elle montre également la résistance à la compression. Cependant, la plupart des approches fondées sur la DCT ne garantis pas complètement la robustesse contre les attaques géométriques comme le recadrage et le redimensionnement.

3.3 Domaine d'ondelettes

La transformé de DWT est une technique qui se base sur la transformation de l'image du domaine spatiale vers le domaine transformé, 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 **[Bar12]**.

La DWT représente l'image sous forme de quatre sous bandes de résolution minimale pour une décomposition à un seul niveau, les trois sous bandes représentent les détails de l'image (horizontale, verticale, et diagonale) et la quatrième est une image d'approximation. Pour reconstruire l'image, on calcul l'inverse de DWT à partir des quatre sous bandes d'ondelette **[Dub98]**.

Il ya différents types de familles d'ondelettes (Haar, Daubechies, Coiflet, Symlet, Biorthogonal etc) dont les qualités varient en fonction de plusieurs critères.

La DWT sépare une image en quatre parties qui sont le détail d'approximation de résolution inferieur (LL), horizontale (HL), vertical (LH) et diagonale (HH). La sous-bande LL est le résultat de filtre passe-bas filtrer à la fois les lignes et les colonnes et contient une description approximative de l'image.

La sous bande HH est un filtre passe-haut qui contient les composantes à haute fréquence. Les images HL et LH sont des résultats de filtrage passe-bas et de filtrage passe-haut respectivement **[Rio91]**.

Après que l'image est traitée par la transformée en ondelettes, la plupart des informations de l'image originale est contenue dans le détail LL. Le détail LH contient les informations de détail vertical qui correspond aux bords horizontaux. Le détail HL représente les informations de détail horizontal correspond aux bords verticaux. Le processus peut être répété pour calculer plusieurs niveaux de décomposition en ondelettes comme il est illustré dans les figures 3.3 et 3.4 **[Rio91]**.

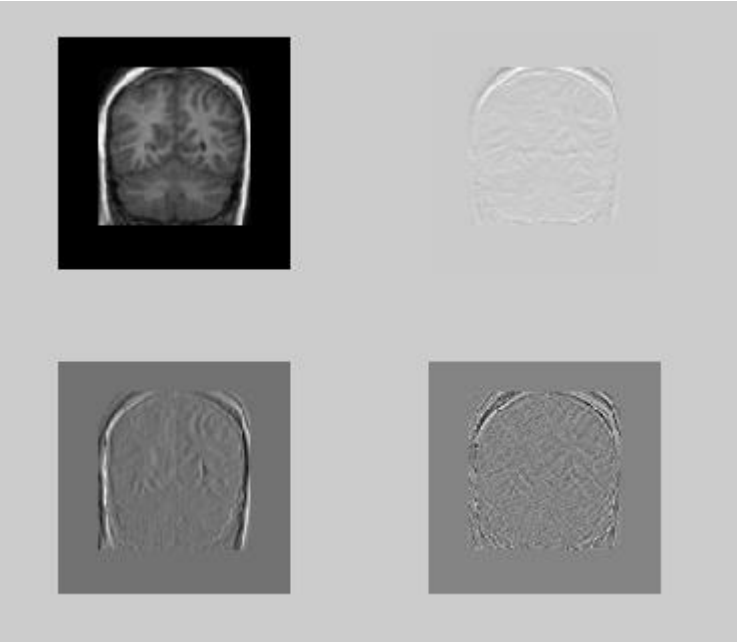


Figure 3.3*: Décomposition par la transformée en ondelettes de l'image médicale IRM.*

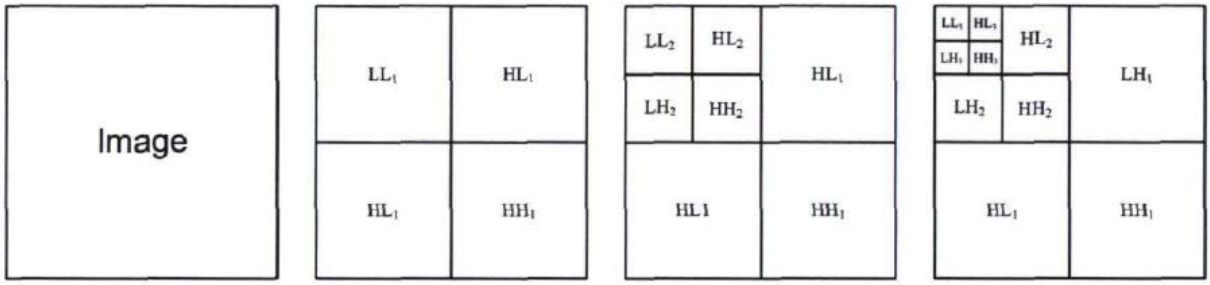


Figure 3.4 *: La représentation à échelles séparés d'une décomposition successive par la transformée en ondelettes discrète.*

Dans **[Kun97]** Kunder et Hatzinakos ont proposé un algorithme de tatouage d'images qui est basé sur le modèle du SVH (système visuel humain) se base sur la transformation de l'image initiale et celle de la marque (une image logo) en ondelette discrète, l'insertion est s'effectuée selon une mesure qui représente la visualité de pixel, les coefficients de la transformé de la marque sont ajoutés aux coefficients de la transformée correspondante aux points de la plus grande mesure calculée de l'image hôte.

Xia et al. (1998) **[Xie98]** ont présenté un schéma de tatouage non aveugle où l'image hôte et la clé secrète étaient nécessaire dans le processus de l'extraction.

La méthode proposée permet d'insérer la marque (codes pseudo-aléatoires) aux grands coefficients de haute fréquence moyenne de la DWT d'une image. Des considérations

perceptuelles ont été prises en compte par le réglage de la quantité des modifications proportionnelles à l'intensité du coefficient lui-même.

Kim & Moon (1999) **[Kim99]** ont proposés d'utiliser les coefficients DWT de tous les sous bandes. L'image d'approximation est utilisée pour insérer la marque (séquence aléatoire) distribuée dans l'ensemble de l'image qui a été basée sur les travaux de Cox (1997) dans le domaine DCT.

Dans **[Kun98]** Kunder et Hatzinakos ont proposé une méthode de tatouage fragile où la marque est une séquence binaire qui est insérée dans les coefficients de détail de l'image initiale à l'aide d'une clé qui est générée aléatoirement, la clé a une valeur 1 (le nombre de chiffres de 1 doit être plus grand ou égale à la taille de la marque) ou 0 si les coefficients sont tatouée ou non respectivement.

D'autres chercheurs ont travaillé sur le tatouage basé sur la DWT sont Chen et al. 2003**[Che03]** qui ont présenté un algorithme de tatouage aveugle qui est basé sur l'algorithme de variable de quantification. Maity et al. (2004) **[Mai04]** ont proposé d'utiliser le schéma de tatouage qui est basé sur le Spread Spectrum par l'insertion dans le détail d'approximation et les sous-bandes diagonales du deuxième niveau de décomposition par ondelette.

La transformée en ondelette discrète est nécessaire dans le domaine de tatouage numérique à cause de son utilisation qui est basé sur la compression JPEG et sa robustesse face aux attaques, en plus cette transformée permet de développer des masques psychovisuels par la décomposition de l'image en détail fréquentiel.

3.4 La décomposition en valeurs singulières SVD

La SVD est un outil de factorisation des matrices très important dans le domaine de traitement d'images, grâce à ses propriétés algébriques il est plus utilisé dans le tatouage numérique.

Parmi les propriétés principales de SVD, cette transformée ne change pas significativement même après des modifications introduite par l'insertion de la marque dans l'image. La transformée en SVD permet de mettre toute l'énergie maximale de l'image dans les valeurs singulières minimales.

3.4.1 Définition

Toute matrice A, de taille m×n, peut se décomposer en produit de trois matrices de la façon Suivante :

$$A=U\times S\times V^t$$

Où

S : est une matrice diagonale de taille nxn constituée de valeurs singulières.

U et V sont des matrices orthogonales, de dimensions mxm et nxn respectivement,

On a:

$$U^t\times U=I \quad et \quad V^t\times V=I$$

Tel que t est l'operateur de transposition.

3.4.2 Schéma de tatouage SVD

Pour insérer les bits de la marque dans l'image hôte on utilise la matrice S obtenue après la transformée en SVD de l'image originale. Tel que :

- I : représente l'image originale.
- W : représente la marque.
- I_w représente l'image tatouée.

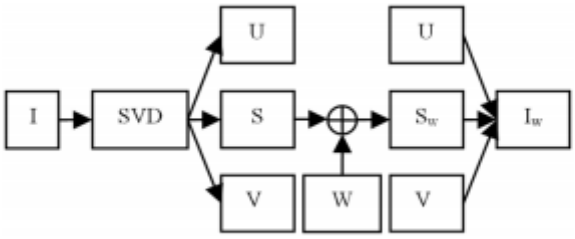


Figure3.5*.Schéma de tatouage SVD.*

3.4.3 Les algorithmes de tatouage basés sur l'utilisation de la transformée SVD

La transformée par la SVD est un outil mathématique très nécessaire dans le traitement d'images et plus utilisé dans le tatouage d'image numérique qui donnent des bons résultats en terme de l'invisibilité et de la robustesse. Dans la littérature plusieurs algorithmes sont basés

sur la SVD : Les algorithmes qui appliquent la SVD sur toute l'image (Global –SVD) et les algorithmes qui appliquent la SVD sur des blocs de cette dernière (SVD-bloc)

Dans ce qui suit on présente quelques algorithmes de tatouage qui sont basés sur cette transformée.

A) Algorithme Global-SVD de Chandra

D.V. Satish Chandra [99] a proposé une technique non aveugle qui permet d'appliquer la transformée SVD sur l'image initiale entière (Global –SVD) et sur la marque, ensuite les SV's obtenues sont multipliées par un scalaire puis on les ajoutes aux SV's de l'image initiale.

Dans la phase de l'extraction on a besoin d'utiliser les trois matrices qui sont la matrice diagonale de l'image originale et les matrices orthogonales de la marque originale.

Une autre méthode proposée par Chandra c'est celle de Bloc-SVD tel que l'image initiale est décomposée en blocs. L'insertion est s'effectuée par l'ajout de bit de la marque qui est multiplié par un facteur ou par un scalaire à la grande valeur de SV's du bloc correspondant de l'image.

L'algorithme de l'insertion et de l'extraction sont présentés ci-dessous :

a) Algorithme d'insertion

Entrées :

– I : image hôte de taille n × m.

– W : marque originale de taille n × m.

Sorties :

–I_w: image tatouée.

– Les matrices :

- S : matrice diagonale de l'image hôte.
- U_w et V_w: Les matrices orthogonales de la marque originale.

— ***Les étapes d'insertion sont comme suit:***

1. La décomposition de l'image initiale I en valeurs singulières :

$$I=U\times S\times V^t$$

2. La décomposition de la marque *W* en valeurs singulières :

$$W=U_w\times S_w\times V_w{}^t$$

3. Construction d'une nouvelle matrice diagonale S_x tel que les valeurs diagonales sont λ_{xi}

selon la formule suivante :

$$\lambda_{xi} = \lambda_i + \alpha\times\lambda_{wi}$$

Où α est un scalaire choisit pour garder la qualité visuelle de l'image tatouée, λ_i sont les éléments diagonaux de S obtenue par la SVD de l'image hôte *I* et λ_{wi} sont les éléments diagonaux de *Sw* obtenue par la SVD est appliquée sur la marque.

4.Reconstruction de l'image tatouée I_w en utilisant S_x et les matrices orthogonales (U,V) de l'image originale comme suit :

$$I_w=U\times S_x\times V^t$$

b) Algorithme d'extraction

Entrées :

- I_w^* : image tatouée et éventuellement attaquée.
- Les matrices :

– *S* : matrice diagonale de l'image hôte.

– U_w *et* V_w : matrices orthogonales de la marque originale.

Sortie :

– La marque W^*.

Etapes :

1. La décomposition de l'image I_w^* en valeurs singulières :

$$I^*_w=U^*\times S^*\times V^{*t};$$

2. Le calcul de la matrice diagonale S^*_w

$$S^*_w=(S^*-S)/\alpha\ ;$$

3. Reconstruction de la marque W^* en utilisant : S^*, U_w, V_W

$$W^*=U_w\times S^*_w\times V_w^{\ t}\ ;$$

B) Algorithme Bloc-SVD de Chandra [Cha02]

Cet algorithme est basé sur la décomposition de l'image hôte en blocs B de taille L x L ensuite la SVD est appliquée sur chaque bloc. Le principe de l'insertion est comme suit :

a) Algorithme d'insertion

Entrées :

– I : image hôte de taille $n\times m$.

– Taille du bloc : $L\times L$

– W : la marque originale de taille n.

Sortie :

–I_w: image tatouée.

— ***Les étapes d'insertion sont comme suit:***

1. La décomposition de l'image hôte I en blocs B_j de taille $L\times L$;

2. Pour chaque bloc B_j faire :

- Décomposition de B_j en valeurs singulières :

$$B_j=U_j\times S_j\times V_j^t\ ;$$

- Insertion d'un bit de la marque(W_j) dans la plus grande SV's du bloc Bj comme suit :

$$\lambda_w=\lambda_j^1+\alpha\times w_j$$

Tel que λ_w est la plus grande valeur de SV's du bloc tatoué B_{wj}.α est un scalaire choisit pour augmenter la qualité de l'image tatouée, Sw est la matrice diagonale, le premier S_j est le premier élément a remplacé parλ_w. Cette matrice est utilisée pour construire le bloc tatoué B_{wj} comme suit :

$$B_{wj}=U_j\times S_w\times V_j^t$$

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

b) Algorithme d'extraction

Entrées :

- I : image hôte de taille $n\times m$.
- I_w: image tatouée et probablement attaquée.
- Taille du bloc : $L\times L$

Sortie :

- W^*: la marque extraite.

Etapes :

1. Décomposition de l'image tatouée I_w^* en blocs B^*_j de taille L×L.

2. Décomposition de B^*_j en valeurs singulières :

3. Pour obtenir Le bit W_j de la marque en utilisant la plus grande SV's du bloc tatoué (λw^*) et celle du bloc originale λ_j^1 comme suit :

$$W_j^* = \lambda w^* - \lambda_j^1 /\alpha$$

3. Retrouver la marque W^*à partir des bitsW_j^* ;

C) Algorithme de R.Liu et T.Tan[Liu02]

Les auteurs R.Liu et T. Tan ont proposé une technique de tatouage non aveugle qui permet d'ajouter la marque multipliée par un scalaire ou un facteur (pour régler la qualité visuelle de l'image) aux SV's de l'image originale.

Les deux matrices orthogonales de l'image hôte sont utilisées pour obtenir l'image tatouée. Le processus de l'extraction besoin de la connaissance de trois matrices comme il est déjà

montré dans l'algorithme précédent. Cette méthode montre une robustesse contre plusieurs attaques par exemple l'attaque de compression JPEG, l'attaque de rotation et l'attaque de cropping.

Le principe de l'insertion et de l'extraction de l'algorithme est présenté comme suite :

a) Algorithme d'insertion

Entrées :

- I : image hôte de taille n×m.
- W: la marque originale de taille n×m.

Sorties :

- I_w : image tatouée.

Les matrices :

- S : matrice diagonale de l'image hôte.
- U_w , V_w: matrices orthogonales de la marque originale.

Les étapes d'insertion sont comme suit:

1. La décomposition de l'image hôte I en valeurs singulières :

$$I=U\times S\times V^t$$

2. La marque W est ajoutée à la matrice S comme suit :

$$D=S+\alpha\times W$$

3. La décomposition de D en valeurs singulières :

$$D=U_w\times S_w\times V_w$$

4. L'image tatouée I_w est obtenue en utilisant les SV's modifiées (S_w) de l'image originale :

$$I_w=U\times S_w\times V^t$$

b) Algorithme d'extraction

Entrées :

I_W^*: L'image tatouée et probablement attaquée.

Les matrices

- S : matrice diagonale de l'image hôte ;
- U_w, V_w : matrices orthogonales de la marque originale.

Sorties :

- W^*: la marque extrait.

Etapes :

1. La décomposition de l'image I_{w^*} en valeurs singulières :

$$I_W^* = U^* \times S^* \times V^* ;$$

2. Le calcul de la matrice D^* qui contient la marque en utilisant U_W et V_W comme suit :

$$D^* = U_w \times S^* \times V_w^* ;$$

3. La marque W^* est obtenue en utilisant S comme suit :

$$W^* = (D^* - S)/\alpha \quad ;$$

1.5 La combinaison des domaines

Dans la littérature les techniques de tatouage ont été proposées, qui reposent sur la combinaison de différentes types de domaine d'insertion (spatial et fréquentiel) ou la combinaison des transformés.

Nous indiquons par exemple la méthode montrée par **[Lef01]** et la méthode montrée par **[Kur08]** qui permettent de combiner les techniques de DWT et CDMA (Code Division Multiple Access).

Dans **[Gan04]**, **[Yav04]**, **[Fen06]**, **[Liu04]** et **[Gan04]** un schéma de tatouage a été présenté qui consiste de combiner la transformée en ondelette discrète DWT et la décomposition en valeur singulière SVD, la première étape se base sur la décomposition de l'image hote par la DWT en quatre sous bandes, ensuite la SVD est appliquée à chacun de ces

bandes, enfin l'insertion de la marque s'effectue par la modification des valeurs singulières SV's.

Hu et al **[Hu11]** ont proposé un schéma de tatouage hybride qui se base sur la combinaison de DWT et DFT par l'insertion d'un modèle dans les moyennes fréquences pour résoudre le problème de désynchronisation relié avec les attaques géométriques.

- ***Exemple des algorithmes qui sont basés sur l'hybridation des transformées***

1) La méthode DWT-DCT-SVD appliquée sur les images en niveau de gris

Dans **[Awa13]** les auteurs ont proposé une technique de tatouage robuste qui se base sur la transformée en ondelette discrète, la transformée en cosinus discrète et la décomposition en valeur singulière : les étapes de l'insertion et de l'extraction sont présentées comme suit :

a) Algorithme d'insertion

1. La décomposition de l'image hôte *I* de la taille 512 x 512 par la DWT en quatre sous bandes LL, HL, LH, HH tel que la taille de chaque sous bande est de 256x256.
2. Choisir la sous bande LL puis la diviser en 2*2 blocs carrés, ensuite la DCT est appliquée à chaque bloc.
3. Recueillir la valeur DC de chaque matrice de coefficient C obtenue par la DCT et les combiner pour obtenir une nouvelle matrice DC de taille 128×128.
4. Ensuite, la SVD est effectué à la nouvelle matrice DC par la formule suivante $DC=U_1\times S_1\times V_1^t$ pour obtenir U_1, S_1 et V_1.
5. Prenez la marque W de taille 128×128, Puis modifier S_1 avec la marque W comme suit :

$$S_m = S_1 + \alpha \times W ;$$

6. L'application de SVD aux valeurs singulières modifiées, pour obtenir U_2, V_2 et S_2 par :

$$SVD(S_m)=U_2\times S_2\times V_2^t ;$$

7. Calculer la matrice DC modifiée $DC_M=U_2\times S_2\times V_1^t$ qui contiennent les informations de la marque.

8. Changez chaque valeur DC de chaque matrice C (coefficient de DCT) dans l'étape ci-dessus par DC_M, pour obtenir la nouvelle matrice de coefficient C_M.
9. L'inverse de DCT est appliquée à chaque C_M pour produire la bande de fréquence tatouée LL_M.
10. Enfin, l'inverse de DWT est effectuée aux LL_M, HL, LH et HH pour obtenir l'image tatouée I_w.

b) Algorithme d'extraction

Le processus d'extraction est la suivant :

1. La DWT est appliquée à l'image tatouée I_W, pour obtenir les détails LL_W, HL_w, LH_w et HH_w.
2. Choisir la sous-bande LL_W, puis la diviser en 2 ×2 blocs carrés et ensuite la DCT est effectuée à chaque bloc.
3. Recueillir la valeur DC de chaque coefficient C_W de la matrice DCT et de les combiner pour obtenir une nouvelle matrice DC_w de taille 128×128.
4. Appliquer la SVD à DC_W : $DC_w=U_w\times S_w\times V^t_w$, pour obtenir les matrices U_w, S_w et V_w
5. Combiner S_w avec U_2, V_2 pour obtenir la matrice E :

$$E=U_2\times S_w\times V^t_2 \ ;$$

6. Extraire la marque par l'équation :

$$E_w=(E-S_1)/\alpha \ ;$$

2) La méthode DWT-SVD a été appliquée sur les images médicales

Dans **[Hu11]** Nilesh Rathi et Ganga Holi ont proposés une méthode qui est basé sur la combinaison de la transformée par DWT et la SVD ,tout d'abord l'image hôte est décomposée en quatre sous bandes de fréquences : LL (détail approximative) qui représente les détails de basses fréquences et HL (détail horizontale) et les détails LH qui représentent les fréquences moyennes et HH (détail diagonale)qui représente les hautes fréquences, dans cette technique les auteurs ont choisit le détail HH pour l'insertion des données car il contient les données les plus importantes.

Le schéma proposé permet de remplacer les valeurs singulières de la bande HH par les valeurs singulières de la marque.

Les étapes de l'insertion et de l'extraction sont présentées comme suit :

a) Algorithme d'insertion

1. Décomposition par la SVD de la marque W :

$$W=U_w\times S_w\times V_w^{\,t}\ ;$$

2. Appliquer la DWT pour décomposer l'image médicale hôte en quatre sous bandes: LL, HL, LH et HH.

3. Appliquer la SVD à la sous bande HH :

$$SVD\ (HH) = U_H\times S_H\times V_H^{\,t}\ ;$$

4. Remplacez les valeurs singulières de la bande HH par les valeurs singulières de la marque.

5. Appliquer l'inverse de SVD pour obtenir la sous bande HH modifiée.

$$HH' = U_H\times S_W\times V^t_{H\ ;}$$

6. Appliquer l'inverse de DWT pour reconstruire l'image médicale tatouée I_w.

b) Algorithme d'extraction

1. Décomposition de l'image tatouée par la DWT en quatre sous-bandes: LL_w, HL_w, LH_w et HH_w.

2. Appliquer la SVD à la sous bande HH_w.

$$SVD\ (HH_W) = U_{HW}\times S_{HW}\times V^t_{HW};$$

3. Extraire les valeurs singulières de la sous bande HH_w.

4. Construire la marque utilisant la matrice S_{HW} et les matrices orthogonales U_w et V_w obtenues par la SVD qui est appliquée à la marque originale.

$$W^*=U_w\times S_{HW}\times V_w^{\,t};$$

5. Retrouver l'image médicale par l'inverse de DWT appliquée aux sous bandes HH_w et les autres sous bandes de l'image tatouée.

3) La méthode DWT-DCT-SVD a été appliquée sur les images médicales [Rat14]

Cette méthode s'effectue par l'utilisation des trois transformées DWT, DCT et SVD, la première étape est basée sur la décomposition de l'image hôte en quatre sous bandes, ensuite la DCT est appliquée sur l'une de sous bande choisie, le résultat est une matrice B tel que l'insertion s'effectuée par le remplacement des valeurs singulières de la matrice B par les valeurs singulières de la marque.

L'image médicale tatouée peut être obtenue par l'inverse de DWT utilisant le détail HH_w de l'image tatouée et les restes de sous bandes de celle-ci. Les étapes de l'insertion et de l'extraction sont présentées comme suit :

a) Algorithme d'insertion

1. W : La marque est décomposée en utilisant la SVD

$$W=U_W\times S_W\times V^t_W \ ;$$

2. La DWT est effectué pour décomposer l'image médicale hôte en quatre sous-bandes: LL, HL, LH et HH.
3. La DCT est appliquée à la sous bande HH pour obtenir la matrice B, ensuite on décompose par la SVD cette dernière :

$$B=U_B\times S_B\times V_B{}^t \ ;$$

4. Remplacement les valeurs singulières de B par les valeurs singulières de la marque W.
5. L'inverse de la SVD et de l'inverse de DCT sont effectuée pour obtenir la sous bande HH modifiée.

$$B'=U_B\times S_W\times V_B^t$$

6. L'inverse de DWT est appliqué pour trouver l'image médicale tatouée.

b) Algorithme d'extraction

1. La décomposition de l'image tatouée en quatre sous-bandes: LL_w, HL_w, LH_w et HH_w.

4. La DCT est effectué à la sous bande HH_w qui donne une matrice B_W, ensuite la SVD est appliquée à cette dernière.

$$B_W=U_{BW}\times S_{BW}\times V_{BW}{}^t \ ;$$

5. L'extraction des valeurs singulières.
6. Construire la marque en utilisant les valeurs singulières et les matrices orthogonales U_w et V_W obtenus par la SVD effectue sur la marque originale et la matrice S_B

$$W^* = U_W \times S_B \times V^t_W$$

7. Reconstruire l'image médicale par le calcul de l'inverse de la DCT et l'inverse de DWT en utilisant la bande originale HH et le reste des sous bandes de l'image tatouée.

3.6 Conclusion

Dans ce chapitre nous avons présentés un état de l'art sur les techniques de tatouage numérique appliqué dans le domaine fréquentiel ou transformé DWT, DCT et SVD pour vérifié une ou l'autre des propriétés de sécurité.

Ce chapitre présente des œuvres dans le domaine de tatouage en utilisant diverses techniques de différents domaines qui ont été bien documentés.

Les avantages des schémas qui utilisent le domaine fréquentiel comme domaine d'insertion peuvent être robustes face aux opérations de compression puisqu'ils utilisent le même domaine. D'autre part, le calcul de la transformée d'une image est devenu moins coûteux grâce aux algorithmes de transformation qui sont rapides.

La suite de notre travail visait à présenter l'approche développée et analyser les performances de cette méthode face à un ensemble d'attaques et montrer leurs résultats de comparaison entre la méthode qui est discutés au par avant **[Awa13]**.

Chapitre 4

Approche proposée et résultats expérimentaux

Chapitre 4 *Contribution proposée et résultats expérimentaux*

4.1 Introduction

Dans le domaine de tatouage des images, beaucoup des travaux ont été réalisés pour augmenter la robustesse et la capacité des données à dissimuler.

Nous présentons dans ce chapitre la méthode développée dans le but de satisfaire les trois propriétés de sécurité et de chercher à trouver un compromis entre la sécurité, l'imperceptibilité et la robustesse.

Nous avons présentée une méthode de tatouage des images en niveau de gris dans le domaine transformé et sa robustesse face aux différentes attaques ensuite une étude comparative est effectuée sur les images médicales IRM.

Finalement on discute les résultats obtenus de comparaison de notre contribution avec la technique présentée dans **[Awa13]**.

4.2 La méthode proposée(R-DWT-DCT-SVD) [Bek15]

Les schémas de tatouage qui utilise le domaine fréquentiel comme un espace de travail est intéressant pour les opérations de compression tant que le même domaine est utilisé pour le codage de l'image, et par conséquent, elles permettent aussi un traitement plus rapide.

D'après **[Bek11]** et **[Bek12]**, on remarque aussi que la combinaison dans le domaine fréquentielle DWT reste plus robuste contre les attaques le bruit et le rotation et aussi plus rapide en temps de calcul, cela a encouragée de terminer les travaux dans le domaine transformée.

Dans le schéma proposé, une combinaison de trois transformées DCT, DWT et SVD sont utilisés pour obtenir une robustesse optimale.

Dans ce chapitre nous présentons un système de tatouage d'image sécurisé, réversible et robuste qui utilise la combinaison des transformations : DWT, DCT et la SVD pour accroître l'intégrité, l'authentification et la confidentialité. Le schéma proposé utilise deux différents types de marques de tatouage: une marque réversible W_1, qui est utilisée pour garantir les

propriétés de sécurité : L'intégrité et l'authentification ; et la deuxième marque W_2, qui est définie par une image logo pour fournir la confidentialité.

La première étape est basée sur la transformation de DWT pour décomposer l'image hôte en quatre sous bandes LL, LH, HL, HH. Les deux marques sont ensuite insérées dans le détail LL et HH de l'image hôte ensuite, la DCT est appliquée sur le détail LL et HH pour obtenir D et D3 qui subira chacun une transformée par la SVD pour donner les trois matrices : la matrice diagonale S et les deux matrices orthogonaux U et V pour D_1 et la matrice diagonale S_3 et les matrices orthogonaux U_3, V_3 pour D_3. La première étape de l'insertion consiste à générer à la fois les deux marques W_1 et W_2.

Une transformée DWT est appliquée sur les deux marques qui produisent quatre niveaux (LL_1, HL_1, LH_1, HH_1) et (LL_2, HL_2, LH_2, HH_2) pour W_1 et W_2, respectivement. Nous effectuons ensuite la transformation par la DCT sur LH_1 et LH_2 pour donner D_2 et D_1, ensuite la transformée par SVD est appliquée sur D_1 et D_2 pour donner les matrices (U_2, S_2, V_2) et (U_1, S_1, V_1), respectivement.

L'insertion de la marque W_1 est effectuée en ajoutant les deux matrices diagonales S et S_2 qui étaient préalablement multipliée par un facteur α pour obtenir S_{33}. L'insertion de la marque W_2 est réalisée en additionne les deux matrices diagonales S et S_2 qui est multipliés par un facteur pour obtenir S_{32}. Enfin la SVD est effectuée sur S_{32} pour obtenir W_{img}, les tableaux récapitulent le processus de génération les deux marques W_1 et W_2 et les étapes d'insertion

Entrée	**Transformations utilisées**	**Sortie**
Image hôte	DWT, DCT et SVD	Matrices orthogonale : U_1, V_1 Matrice diagonale : $S_{1(}$(représente la première marque W_1)

***Tableau 4.1** : Génération de la marque W_1.*

Entrée	Transformations utilisées	Sortie
Image(Logo)	DWT, DCT et SVD	Matrices orthogonale : U_2, V_2 Matrice diagonale : S_2 (représente la première marque W_2)

***Tableau4.2** : Génération de la marque W_2.*

Entrée	Transformations utilisées	Sortie
Image hôte I	DWT(I)	LL, LH, HL, HH
LL	SVD(LL)	Matrices orthogonale : U, V Matrice diagonale : S
HH	SVD(HH)	Matrice orthogonale : U_3, V_3 Diagonale : S_3
	Processus d'insertion de la marque W_1 :	$S_{33}=S+\alpha\times W_1$
	Processus d'insertion de la marque W_2 :	$S_{32}=S3+\alpha\times W_2$
S_{32}	SVD	Matrices orthogonale : U_5, V_5 Matrice diagonale : S_5
S_{33}	SVD	Matrices orthogonale : U_6, V_6 Matrice diagonale : S_6
U3 ,S5,V3	U3×S5×V3'	Wimg
W_{img}	IDCT	B
U,S6,V	U×S6×V'	W_{img2}
B,LH,HL,Wimg2	IDWT	Image tatouée I_w

***Tableau 4.3 :** Processus de l'insertion de la marque W_1 et de la marque W_2.*

Dans les sections suivantes, nous présentons les étapes détaillées de processus de l'insertion et de l'extraction de l'approche développée, qui utilise la DCT, DWT et la SVD. Les performances de l'approche proposée sont évaluées dans la section suivante.

a) Processus d'insertion

Afin d'assurer les aspects principaux de la sécurité, qui sont l'authentification, l'intégrité et la confidentialité, nous proposons l'utilisation d'une nouvelle approche de tatouage réversible qui a été effectué par l'insertion de deux différents types de marques :

- Une marque réversible W_1, qui est utilisé pour vérifier l'authentification des données et de l'intégrité de l'image. Elle est définie par le chiffrement RSA des données d'un bloc composé d'une combinaison de résultat de la fonction de hachage SHA-512 des bits les plus significatifs (MSB) avec la compression RLE des bits les moins significatif (LSB);

- Une deuxième marque W_2 qui est créée par le chiffrement d'un logo à l'aide d'une clé secrète qui permet à l'utilisateur de vérifier sa confidentialité et sa l'intégrité.

Le système de tatouage proposé prend l'image hôte *I* et les deux marques générée W_1 et W_2 comme entrée pour donner en sortie une image tatouée I_w.

Les différentes étapes de l'insertion et de l'extraction des deux marques sont présentées dans les sections suivantes, le schéma complet de l'approche proposée est illustré dans les figures 4.3 et4.4.

— ***La matrice S1 représentant la matrice de la marque W_1 qui est générée selon les étapes suivantes:***

1. On Extraire les MSBs de l'image hôte et on calcule le message correspondant (Code d'Authentification MAC par la fonction de hachage SHA-512;
2. On concatène la signature obtenue (la MAC) avec les données du patient, ensuite on crypte la chaine résultante ;
3. On sélectionne les LSB's(les bits de poids faible) et les compressée en utilisant la compression RLE (Run Length Encoding);
4. On Concatène la chaîne compressée avec celle cryptée;
5. On Convertit les caractères d'une chaîne obtenue à une matrice binaire A;
6. On applique la DWT à la matrice résultante A pour obtenir: LL_1, HL_1, LH_1 et HH_1;
7. On applique la transformée de DCT au détail LH_1 pour obtenir une nouvelle matrice D_1;
8. On décompose par la SVD la matrice D_1 pour obtenir les SV's: $U_1.S_1.V_1$ '.

- La matrice obtenue S_1 représente la marque W_1 qui doit être inséré dans l'image hôte *I*.

La marque W_1 est calculée à partir de l'image initiale pour respecter l'intégrité et l'authentification (comme illustré dans la Figure 4.1).

Le tableau récapitule les matrices obtenues lors de la génération de la marque W_1

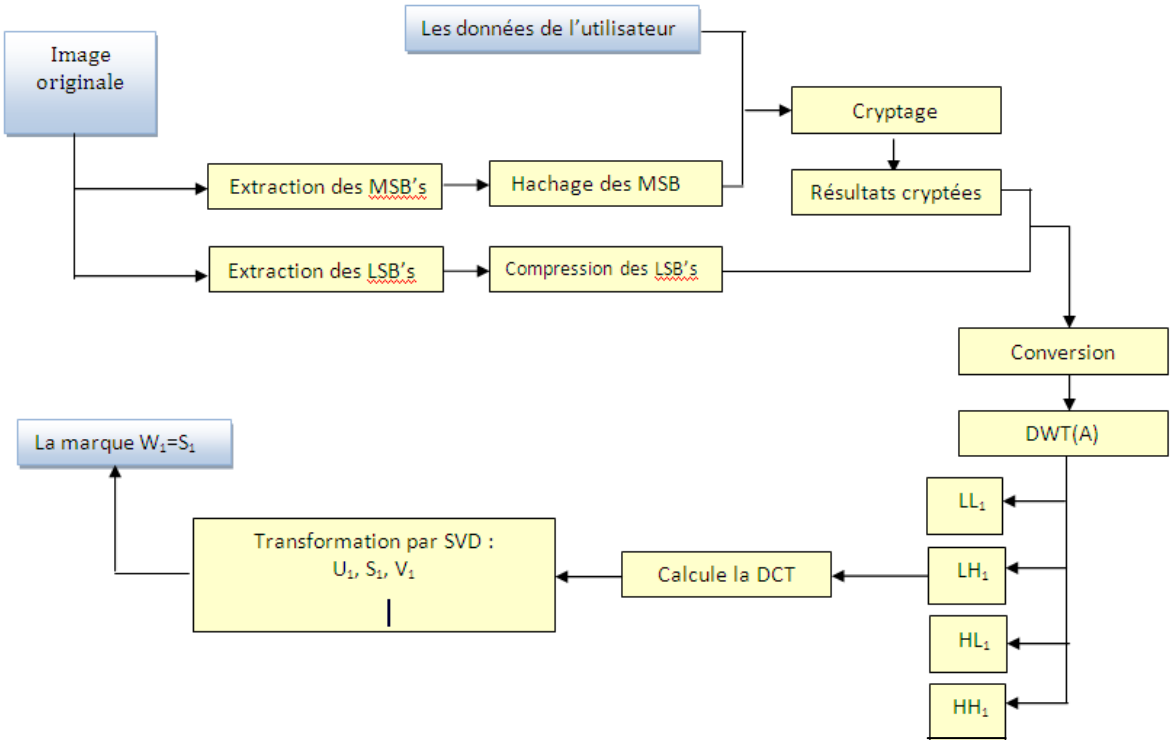


Figure 4.1 : *Génération de la marque W_1.*

— ***La matrice S_2, qui représente la marque W_2, est alors générée en fonction des étapes suivantes:***

1. Lire le message et le rendre sous forme un vecteur;
2. Une séquence pseudo aléatoire est ensuite générée à l'aide d'une clé secrète en utilisant le chiffrement ;
3. On convertit le texte chiffré résultant à une matrice, ensuite on applique la DWT sur cette dernière pour obtenir: L_{L2}, H_{L2}, L_{H2} et H_{H2};
4. On applique la DCT au détail LH_2 pour obtenir la nouvelle matrice D_2;
5. On décompose D_2 en valeurs singulières pour obtenir les SV's:

$$SVD\ (D_2) = U_2.S_2.V_2^t.$$

- La matrice obtenue S_2 représente la marque W_2 qui doit être insérée dans l'image hôte *I*. La marque W_2 est calculée à partir de l'image (logo) qui permet de garantir la confidentialité (comme illustré la Figure 4.2).

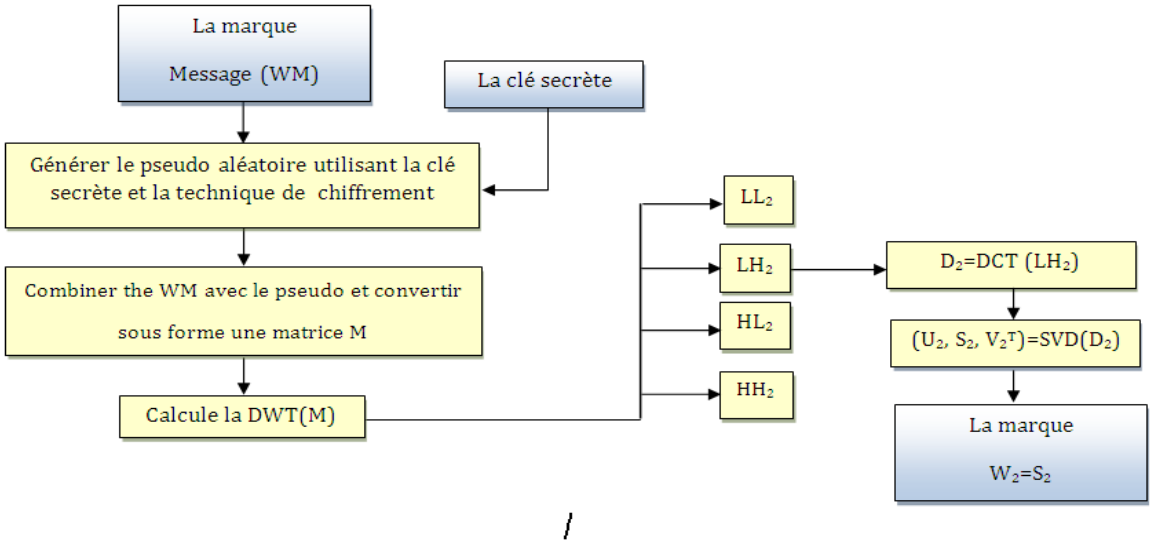


Figure 4.2 : *Génération de la marque W_2.*

Après la génération les deux marques W_1 et W_2, on montre le processus de l'insertion dans la section suivante :

— ***Le processus pour insérer la marque W_1 est effectué comme suit :***

1. On applique la DWT pour décomposer l'image hôte en quatre sous-bandes;
2. On effectue la SVD au détail LL de l'image hôte pour obtenir les SV's:

$$SVD\ (LL) = USV';$$

3. On insère les valeurs singulières de la marque S_1 à la matrice S pour obtenir S_{33}:

$$S_{33} = S + \alpha * S_1;$$

4. On effectue la SVD à la matrice S_{33} pour obtenir les SV 's:

$$SVD\ (S_{33}) = U_6.S_6.V_6^t;$$

5. Enfin, on calcule la matrice tatouée W_{img2} en utilisant U, V, et S_6:

$$W_{img2} = U.\ S_6.V^t$$

Après cela, la marque W_2 est insérée dans l'image tatouée comme montre-le processus suivant :

— ***Le processus pour insérer la marque W_2 est effectué comme suit :***

1. On applique la DCT à la sous-bande HH de l'image hôte pour obtenir la nouvelle matrice D_3;
2. On effectue la SVD à la matrice D_3:

$$SVD\ (D_3) = U_3.S_3.V_3^t;$$

3. On Ajoute le contenu de S_2 de la marque W_2 à la matrice diagonale S_3 pour obtenir la nouvelle matrice S_{32} *:*

$$S_{32} = S_3 + \alpha \times S_2\ ;$$

4. On effectue la SVD à la S_{32} pour obtenir U_5, V_5^t et S_5 et de reconstruire la matrice W_{img} utilisant S_5, U_3 et V_3:

$$W_{img} = U_3.\ S_5.V_3^t.$$

5. On applique l'inverse de DCT pour reconstruire la matrice B en utilisant W_{img};

6. On Obtient l'image tatouée I_w en effectuant l'inverse de DWT utilisant B_2 et les trois coefficients de DWT: W_{img2}, HL_2, B et HH_2.Le processus détaillé de l'insertion de la marque W_2 est illustrée à la figure 4.3.

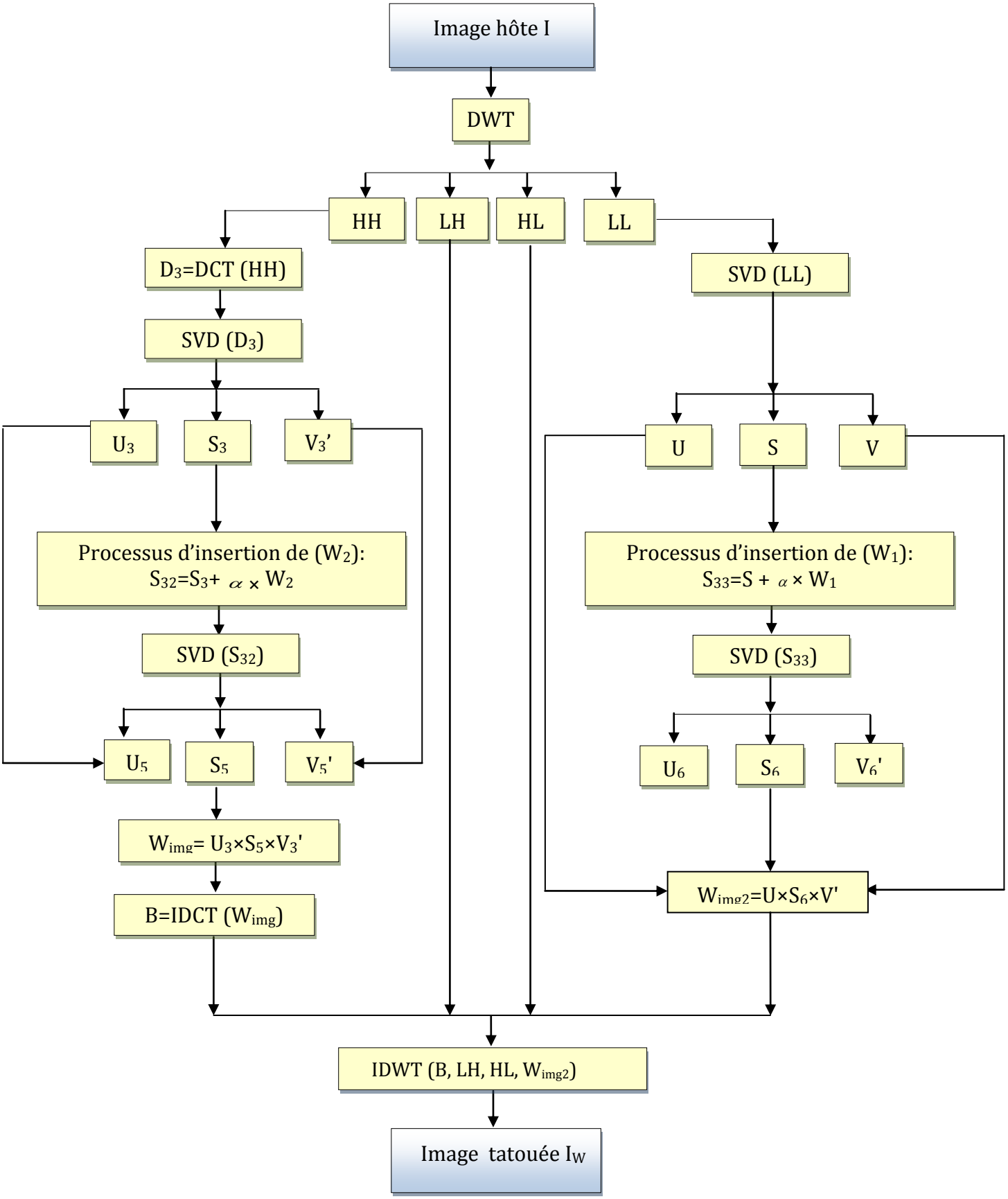


Figure 4.3 : *processus d'insertion de l'approche développée.*

b) Processus d'extraction

La phase d'extraction se décompose en deux phases de l'extraction de la marque W_1 et celle de la marque W_2.La première étape consiste à décomposer par la DWT de l'image tatouée I_w, qui donnent quatre composantes détaillées: LL^*_W, LH^*_W, HL^*_W et HH^*_W (qui peut être corrompu). Le détail LL^*_W est utilisé pour extraire la marque W_1, tandis que le détail HH^*_W est utilisé pour extraire la marque W_2.

— ***Les différentes étapes d'extraction de la marque W_1 sont explicitement expliquées comme suit:***

1. L'image tatoué I_W * (qui peut être attaquée) est décomposé par la transformé DWT en quatre coefficients: LL^*_W, LH^*_W, HL^*_W et HH^*_W;
2. On applique la SVD sur LL^*_W pour obtenir:

$$SVD\ (LL^*_w) = U_w{}^* \times S_w{}^* \times Vw{}^{*t};$$

3. La marque corrompu est obtenue par: $Sr = (S\text{-}S_w{}^*) / 4$;
4. La matrice contenant la marque est calculée par: $D^* = U_1.S_r.V_1^t$;
5. La marque extraite W_1^* est obtenu par le calcul de l'inverse de DWT en utilisant les coefficients originales: LL_1, HL_1, LH_1, et la matrice D^*.

— ***Les différentes étapes d'extraction de la marque W_2 sont explicitement présentées comme suit:***

1. On transforme par la DCT le détail HH^* pour obtenir T_w;

2. On transforme par SVD le résultat T_w pour obtenir:

$$SVD\ (T_w) = U_{ww} \times S_{ww} \times V_{ww}{}^t;$$

3. La marque corrompu est obtenue par:

$$S_{r1} = (S_3 - S_{ww}) / \alpha\ ;$$

4. La matrice contenant la marque est calculée par:

$$D_{22}{}^* = U_2 \times S_{r1} \times V_2^t;$$

5. La transformation inverse de DCT est appliquée à $D_{22}{}^*$;

6. La marque W_2 *extraite est obtenue en effectuant l'inverse de DWT en utilisant les coefficients originales de W_2: LL_2, HL_2, LH_2 et la matrice D_{22} *.

Le processus détaillé de l'extraction de la marque est illustré dans la figure 4.4.

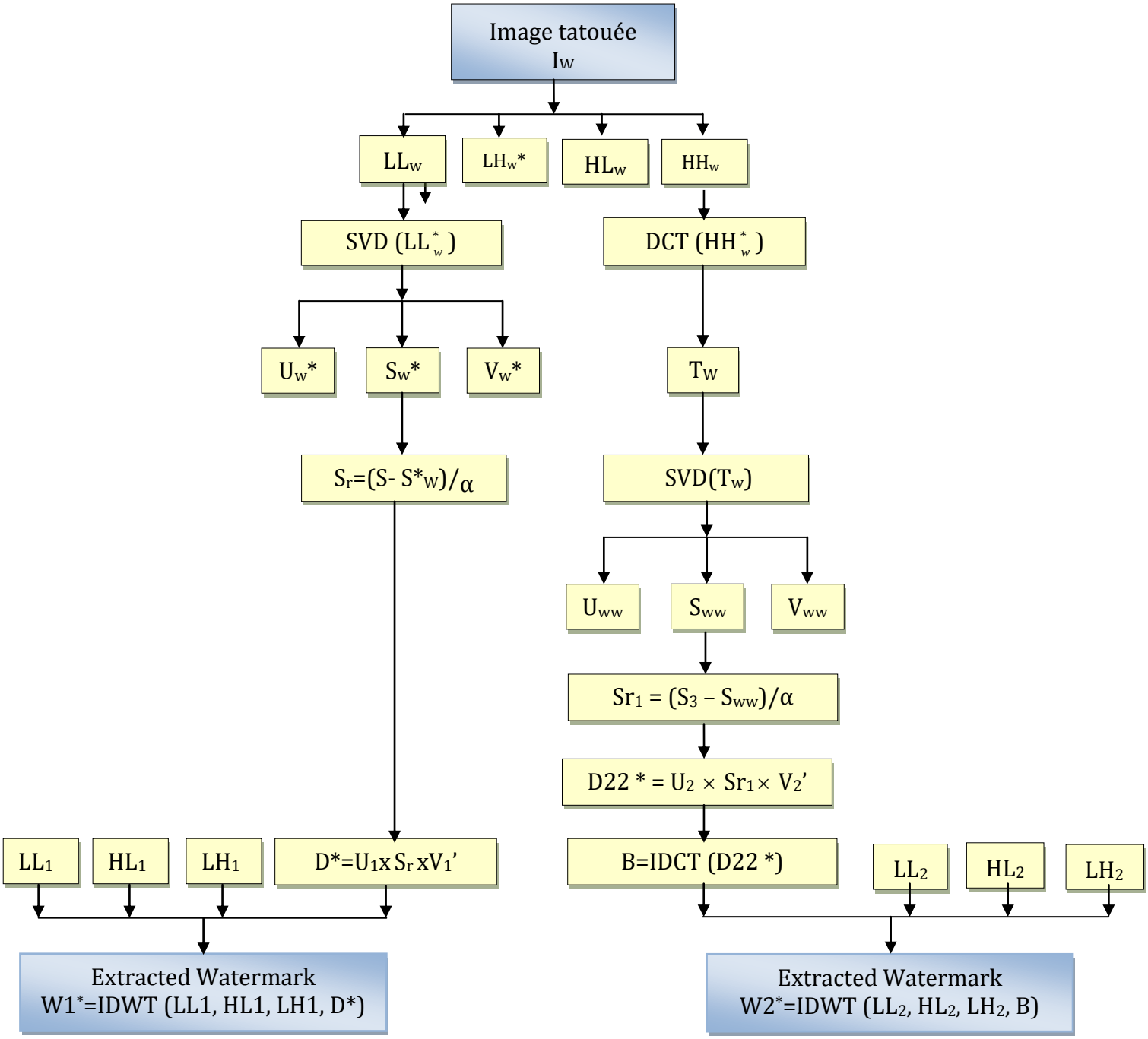


Figure 4.4 : *Processus d'extraction de l'approche développée.*

4.3 Résultats et interprétation:

4.3.1 Réalisation avec Matlab 7

Dans cette section nous allons exposer les résultats auxquels nous sommes parvenus en appliquant respectivement l'approche développée présentées auparavant. Les résultats de qui seront présentés dans ce chapitre sont réalisés avec l'outil de développement Matlab 7b. Ce dernier qui est un environnement informatique conçu pour le calcul matriciel, c'est un outil puissant permettant de résolution de nombreux problèmes, sa facilité d'emploi avec des nombres complexes et ses possibilités d'affichage graphique en font un outil intéressant pour beaucoup d'autres.

4.3.2 Présentation de l'application

L'application réalisé dans le cadre de notre travail permet de tatouer les images médicales de type IRM en niveau de gris, de format BMP et de résolution 256x256. Deux types de données peuvent être insérés dans les images médicales :

- Les informations médicales regroupent les informations du patient (nom, prénom, date de naissance, sexe, profession), les informations concernant le médecin traitant (Nom, Prénom), la date d'acquisition de l'image médicale et le diagnostic. Les données médicales de différents patients sont insérées dans l'image médicale de diagnostic correspondante et sont transmises à travers les centres hospitaliers.
- Le logo (image monochrome) qui peut être la signature du médecin ou logo d'un hôpital.

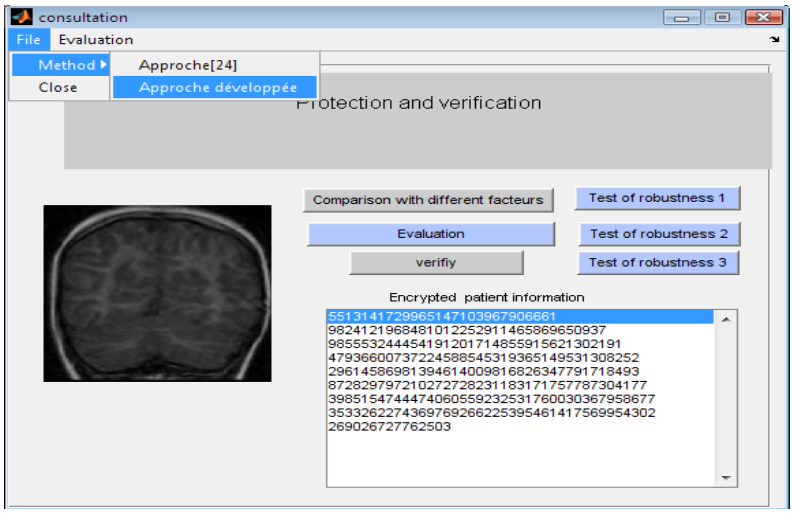


Figure 4.5 : *Interface pour l'image IRM.*

4.3.3 Format des données et des images de test

- L'empreinte ou la signature obtenue par le hachage SHA-512 bits.
- Le nom et le prénom codés sur 20 caractére, chacun.

Données de patient	Nombre de caractères
Empreinte (signature)	128
Nom	20
Prénom	20
Age	2
Sexe	1

Tableau 4.4 : *Format des données du patient insérées par le tatouage réversible (RW)* ***[Bou04] [Bek11]****.*

4.3.4 Le nombre de bits maximal inséré dans l'image est :

(128+20+20+2+1) x 8 = 1368bits.

Nous avons effectué des tests sur un échantillon d'images médicales format BMP (IRM de taille 256 x256.Un échantillon de 10 images est pris pour chaque type d'image.

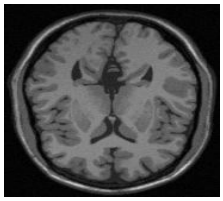


Figure 4.6: *Image IRM originale.*

4.3.5 Calcul l'empreinte par SHA-512

L'intérêt de la fonction de hachage est permet de produire deux empreintes totalement différentes pour deux textes ou images dont la différence est minime de l'ordre d'un bit. Bien entendu, plus la taille de la clé (128, 256,512) est grande, plus la sécurité est robuste.

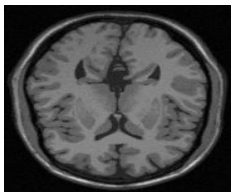
Type de l'image	L'empreinte de l'image par SHA-512 en caractères
Image IRM 	433f0b857dca78e7c36ff92f4bcd4b201732d69092df732 be8a9116c3cf9136e7beba8404e5ce262f4b4047342c381 46aabac44b7d9023756216b237e42dcde3.

Tableau 4.5 : *Calcule d'empreinte par SHA-512.*

4.3.6 Insertion et l'extraction des données

- Pour insérer la signature, l'utilisateur doit remplir les champs de saisie suivants :

— La signature.

— La clé.

Lors de l'insertion, l'utilisateur récupère le nombre de bits de la signature. Cette donnée est nécessaire pour la phase d'extraction.

- Pour détecter les données du patient, l'utilisateur doit avoir :

— L'image marquée.

— La clé.

— Le nombre de bits insérés ou la signature.

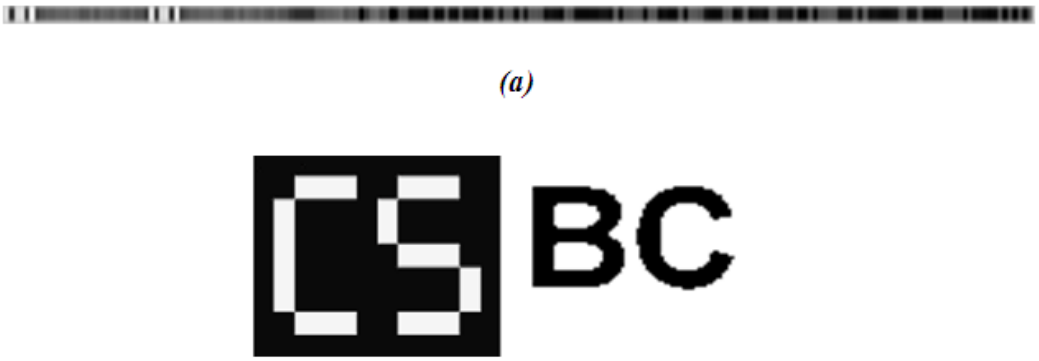


Figure 4.7 : (a) *la marque réversible* W_1, ***(b), (c) et (d) :*** *la marque* W_2.

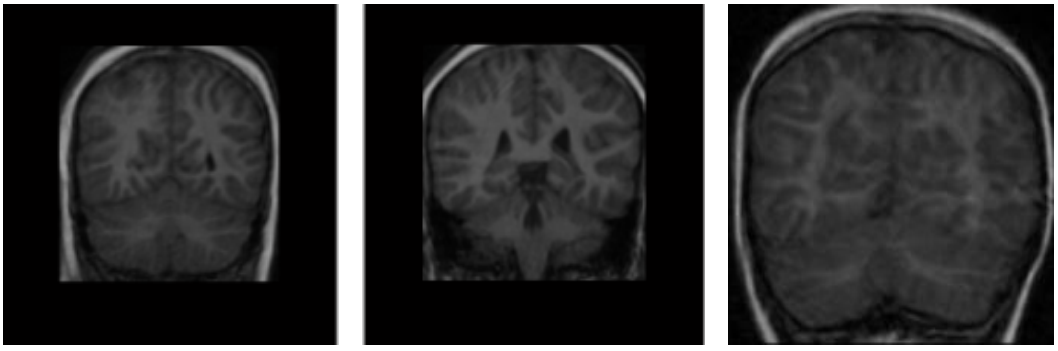


Figure 4.8:Image originale : (a) *image IRM_31,* ***(b)*** *image IRM_32 et* ***(c)*** *image IRM_33.*

Les performances de la méthode proposée ont été analysées en utilisant la mesure de corrélation (NC), qui exprime la qualité de la marque extraite qui doit être la mesure de la similitude entre la marque originale et la marques extraite W^*.

Selon **[Hsi01]**, la NC est définie par l'équation (1,17) dans le chapitre 1, où W (i, j) sont les valeurs de pixel à la position (i, j) de l'image originale, et W^*(i,j) sont les valeurs de pixels de la marque W à la position (i, j) de l'image tatouée.

L'analyse comparative des six algorithmes de tatouage a été faite selon les paramètres de mesure de qualité PSNR, SNR et MAE, MSE **[Aia01]**, La valeur de PSNR obtenue entre les

images hôtes (images originales) et les images tatouées, en décibels (dB) est utilisée pour mesurer la distorsion introduite par le tatouage entre ces deux images. Ce ratio est souvent utilisé comme mesure de la qualité visuelle de l'image originale par apport à l'image tatouée. Plus le PSNR est élevé plus la qualité visuelle de l'image tatouée est bonne. La MSE renseigne sur la dégradation ou la distorsion introduite au niveau de pixel. Plus la valeur du MSE faible, mieux l'image tatouée est appréciée. Les résultats obtenus sont montrés dans les tableaux 4.3 et 4.4 pour l'image IRM.

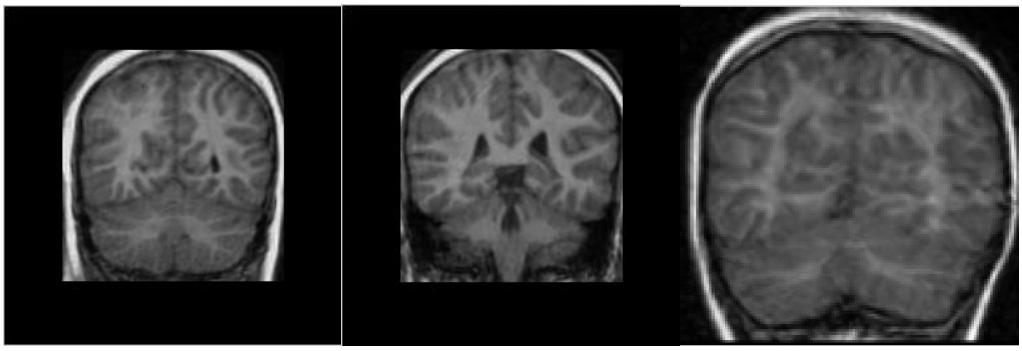
Afin d'évaluer le schéma proposé, nous avons utilisé trois images médicales en niveau de gris: IRM_31, IRM_32, et IRM_33 (illustré dans la Figure 4.8 (a), (b) et (c)).la marque réversible W1 a une taille de 1x206, pour la marque W_2 on utilise deux images de différentes tailles (CS) de taille 106 x 143 et (BC) de taille 91×72 comme illustre la figure 4.7.

4.4 Simulations et résultats expérimentaux

Les résultats expérimentaux sont basés sur deux phases pour évaluer notre approche la première est consacrée sur l'invisibilité et la deuxième est consacrée sur la robustesse contre les attaques.

a) En termes d'invisibilité

L'image tatouée obtenue par l'approche développée utilisant la marque réversible W_1 et la marque W_2 (logo CS). Comme illustre la figure 4.9.

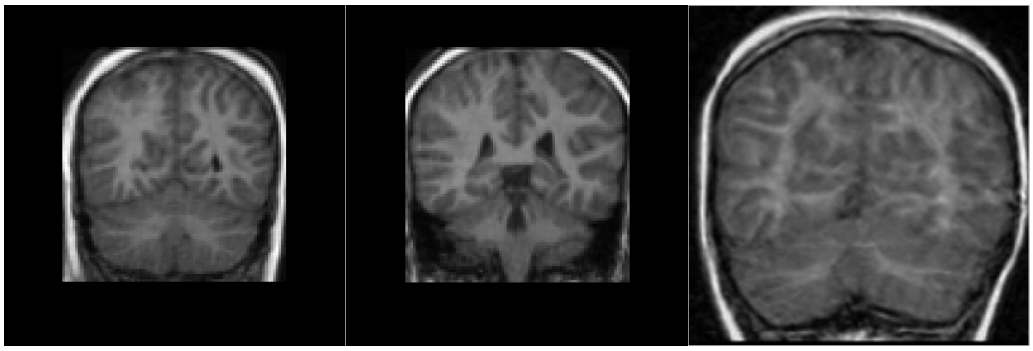


(b) ***(b)*** ***(c)***

***Figure 4.9** : Image tatouée par la marque W1 et la marque W2(CS) :*

(a) IRM_31, ***(b)*** IRM_32, ***(c)*** IRM_33.

L'image tatouée obtenue par l'approche développée utilisant la marque réversible W_1 et la marque W_2 (logo BC). Comme illustre la figure 4.10.



(a) ***(b)*** ***(c)***

Figure 4.10 : *Image tatouée par la marque W1 et la marque W2(BC) :*

(a) *image IRM_31,* ***(b)*** *IRM_32,* ***(c)****IRM_33.*

A partir de ces figures, on peut voir qu'il est difficile de faire la différence entre les images originales et leurs images tatouées. Le tableau 4.6 suivant présente les résultats de notre approche avec différentes marques (CS et BC) :

Type de la marque	**CS**		**BC**	
	PSNR	**SNR**	**PSNR**	**SNR**
IRM_31	44.0275	27.9576	44.1584	28.0885
IRM_32	45.5016	28.7166	45.6836	28.8986
IRM_33	47.2310	33.4748	47.5236	33.7674

Tableau 4.6 *: Résultats d'évaluation de l'approche proposée avec différentes marques (Facteur α=0.6).*

Le tableau 4.7 suivant présente les résultats de comparaison entre la méthode proposée et l'approche **[Awa13]** avec l'insertion de la marque réversible W_1 et la marques W_2 (CS, BC).

Type de la marque	**CS**		**BC**	
Approche proposée	**PSNR**	**SNR**	**PSNR**	**SNR**
IRM_31	44.15	28.08	44.15	28.08
IRM_32	45.67	28.89	45.68	28.89
IRM_33	47.23	33.47	47.52	33.76
Type de la marque	**CS**		**BC**	
Approche **[Awa13]**	**PSNR**	**SNR**	**PSNR**	**SNR**
IRM_31	35.45	19.38	35.45	19.38
IRM_32	36.21	19.43	36.21	19.43
IRM_33	35.01	21.26	35.01	21.26

***Tableau 4.7** : Résultat de comparaison entre l'approche proposée et la méthode* selon NCC *après l'insertion de la marque réversible W1et la marque W2 (CS et BC).*

Le tableau 4.6 suivant présente les résultats de comparaison entre la méthode proposée et l'approche **[Awa13]** selon le paramètre NCC avec l'insertion de la marque réversible W_1 et la marque W_2 (CS).

	Approche [Awa13]				**Approche proposée**				
	PSNR	**SNR**	**NCC**	**Run time**	**PSNR**	**SNR**	**NCC1**	**NCC2**	**Run time**
IRM_31	36.24	20.17	0.999	8.42	44.01	27.93	0.996	0.999	23.66
IRM_32	36.40	19.61	0.999	8.72	45.58	28.80	0.998	0.997	21.57
IRM_33	35.61	21.85	0.999	8.81	47.30	33.55	0.998	0.998	25.81

***Tableau 4.8** : Résultat de comparaison entre l'approche proposée et la méthode* selon NCC (*avec le facteur α=0.1) après l'insertion de la marque réversible W_1et la marque W_2(CS).*

Les figures 4.11, 4.12 et 4.13 suivantes illustrent les marques extraites à partir des images *Iw* tatouées avec le facteur α=0.1

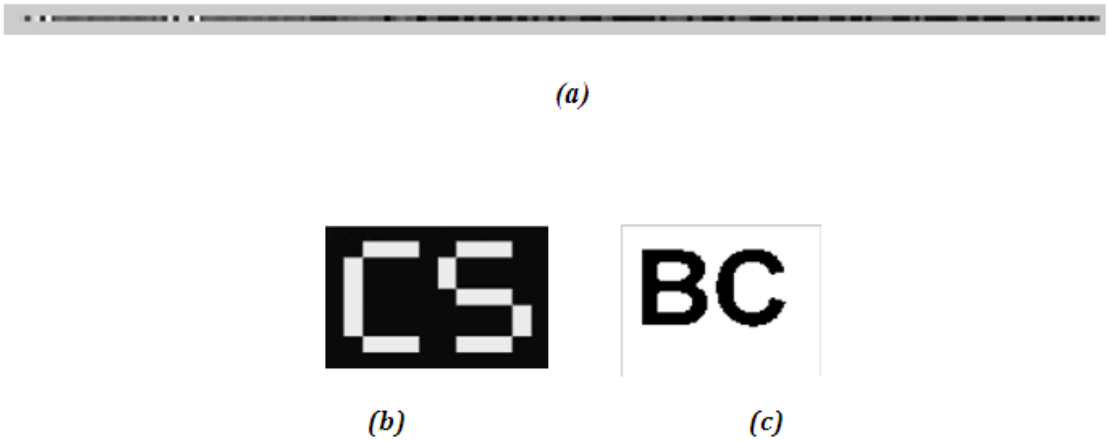


Figure 4.11 :(a), (b), (c) *Les marques extraite à partir de l'image tatouée IRM_31 tatouée* (α=0.1).

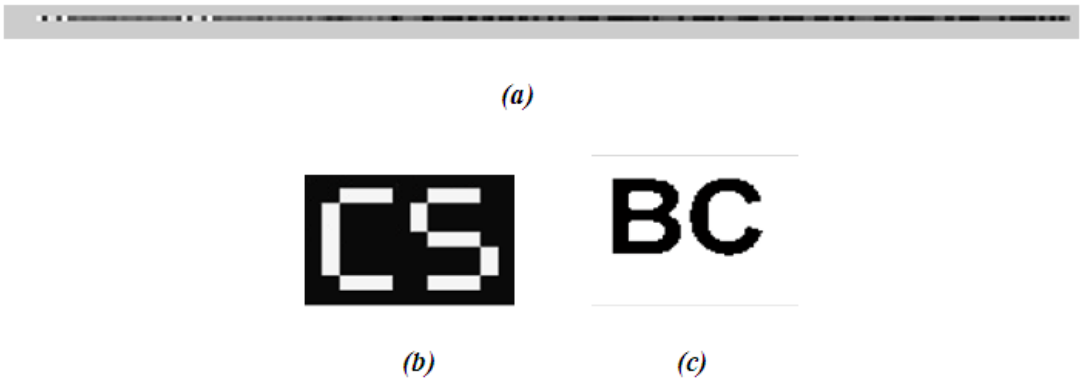


Figure 4.12 : (a), (b), (c) : *Les marques extraite à partir de l'image tatouée IRM_32.*

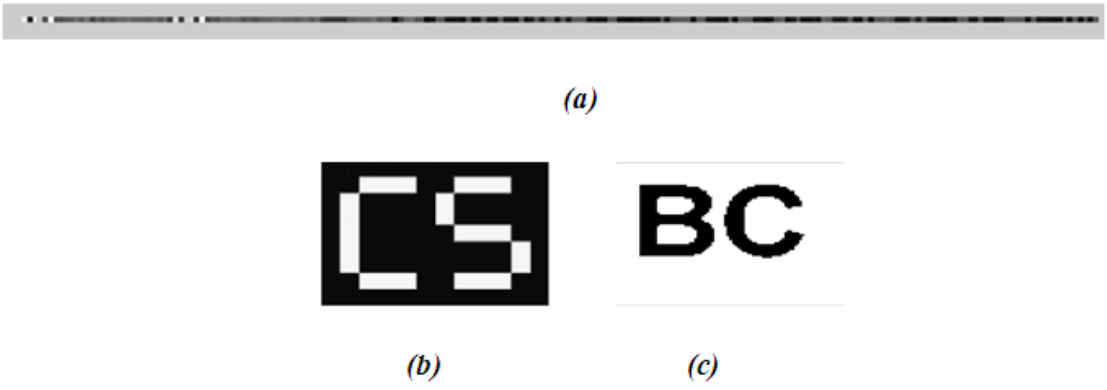


Figure 4.13 *: **(a), (b), (c)** : Les marques extraite à partir de l'image tatouée IRM_33.*

Après l'extraction de la marque, le coefficient de corrélation est calculé en utilisant la marque originale et celle extraite

b) En termes de robustesse

Pour valider la robustesse de notre approche on test sa robustesse contre les attaques. Pour étudier la robustesse par rapport aux attaques de tatouage communes, nous avons appliqué sur l'image tatouée une compression JPEG (avec un facteur de qualité égal à 10%), un bruit sel & Pepper (avec un facteur de qualité 0,02), et l'attaque de rotation avec angles (90 °, 180 ° et 270). La figure 4.14 illustre les images tatouées attaquée

Le tableau 4.6 illustre les résultats de performances obtenues en terme de NCC. Cette mesure a été appliquée entre la marque insérée originale et celle extraite à partir de l'image tatouée attaquée.

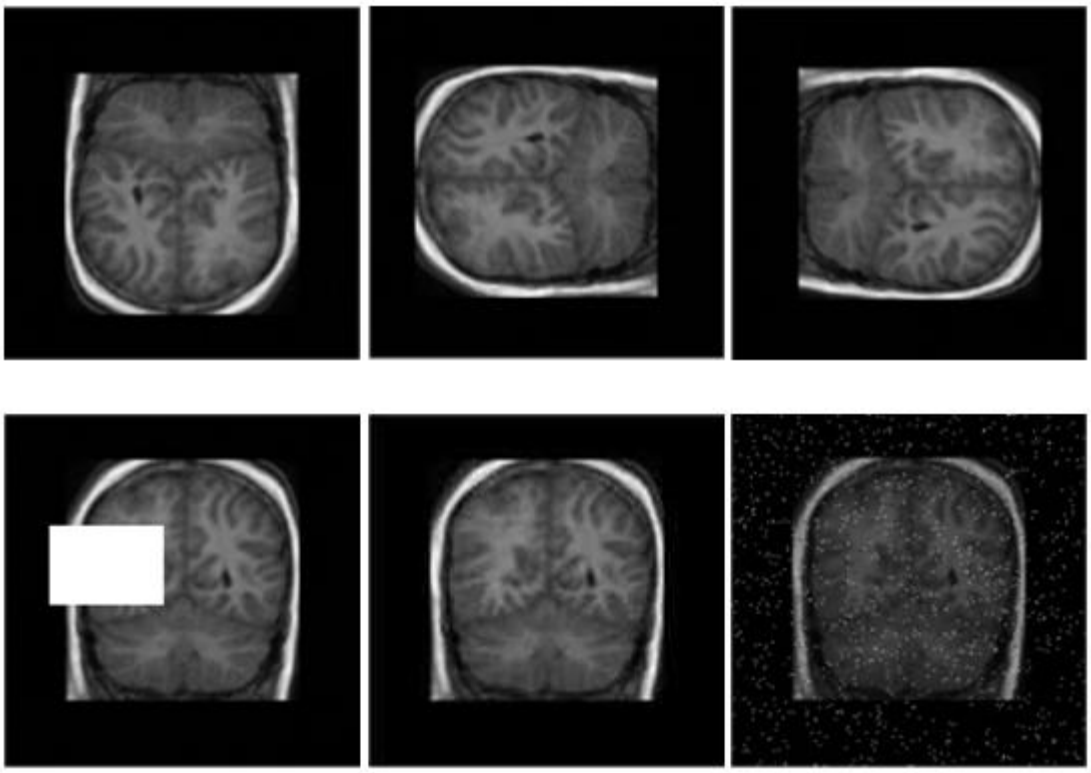


Figure 4.14: *Image IRM_31 tatouée attaquée : (a) la Rotation (90°), (b) la Rotation (c)la Rotation (270°) d) le cropping, (e) la compression JPEG, (f) le bruit.*

- **Robustesse de l'approche proposée à l'attaque** de bruit

Pour évaluer les performances de notre approche, on utilise le bruit conventionnel Salt & Pepper. Les attaques sont, par conséquent, appliquées sur l'image tatouée sont basée sur l'idée que l'attaquant n'a pas l'accès à l'image originale ou à la signature insérée. L'attaquant n'a aucune idée si l'attaque fait son effet ou pas donc les résultats ne sont pas connus par l'attaquant.

Avec l'ajout de bruit conventionnel avec un facteur 0.02, la performance du tatouage est testée. Comme illustre la figure 4.14 (f)

- **Robustesse de l'approche proposée à l'attaque de rotation**

L'attaque de rotation est l'un des types les plus populaires de l'attaque géométrique appliquées sur des images numériques. Trois niveaux de rotations ont été mises en œuvre. Premièrement la rotation de l'image originale tatouée de degré de 90 °, puis de 180 ° et enfin l'image est mise en rotation par 270° dans le sens des aiguilles d'une montre, comme illustre la figure 4.14 (a, b, c).

- **Compression JPEG**

Pour vérifier la robustesse de notre méthode, on applique la compression JPEG sur l'image tatouée (avec un facteur de qualité égal à 10%), comme illustre la figure 4.14 (e).

- **Cropping**

Afin de tester la capacité de détecter les opérations de cropping on applique l'attaque de cropping sur l'image tatouée, comme illustre la figure 4.14 (f).Après l'extraction du watermark, le coefficient de corrélation NCC **[Hsi01]** est calculé en utilisant le watermark original et celui extrait à partir de l'image tatouée attaquée.

Le tableau 4.9 présente la robustesse de notre technique contre quelques types d'attaques avec divers paramètres tel que NCC_1 le coefficient de corrélation entre la marque réversible W_1 et celle réversible extraite et NCC_2 le coefficient de corrélation entre la marque W_2 (CS) et la marque extraite W_2^*.

Les tableaux 4.9 et 4.10 montrent les résultats de comparaison entre notre approche et la méthode **[Awa13]** selon le NCC et le PSNR entre l'image originale et tatouée attaquée.

			Rotation (90°)	**Rotation (180°)**	**Rotation (270°)**	**JPEG Compression**	**Cropping**	**Salt &Pepper**
IRM_31	NCC obtained in **[Awa13]**		0.99971	0.99972	0.99972	0.99971	0.99976	0.99982
	Approche proposée	**NCC_1**	**0.99959**	**0.99959**	**0.99940**	**0.99890**	**0.98698**	**0.97374**
		NCC_2	**0.99988**	**0.99988**	**0.99989**	**0.99989**	**0.99988**	**0.99773**
IRM_32	NCC obtained in [109]		0.99970	0.99970	0.99970	0.99967	0.99973	0.99990
	Approche proposée	**NCC_1**	**0.99896**	**0.99896**	**0.99896**	**0.99810**	**0.96386**	**0.97184**
		NCC_2	**0.99988**	**0.99988**	**0.99988**	**0.99989**	**0.99988**	**0.99768**
IRM_33	NCC obtained in [109]		0.99953	0.99953	0.99953	0.99959	0.99965	0.99994
	Approche Proposée	**NCC_1**	**0.99925**	**0.99931**	**0.99925**	**0.99861**	**0.98877**	**0.98792**
		NCC_2	**0.99988**	**0.99988**	**0.99987**	**0.99989**	**0.99988**	**0.99807**

Tableau 4.9 : *Comparaison des performances de la méthode de tatouage proposée et la méthode DWT-DCT-SVD selon le NCC sous l'attaque.*

	DWT-DCT-SVD					
	PSNR					
	Rotation (90°)	**Rotation (180°)**	**Rotation (270°)**	**Compression JPEG**	**Cropping**	**Salt &pepper**
Image_ 31	18.67	20.05	18.67	33.83	24.17	35.41
Image_ 32	20.57	19.62	20.57	33.77	25.53	35.68
Image_ 33	18.66	17.46	18.66	32.06	22.91	37.16
	Technique proposée					
	PSNR					
	Rotation (90°)	**Rotation (180°)**	**Rotation (270°)**	**Compression JPEG**	**Cropping (5%)**	**Salt &pepper**
Image_31	18.99	20.33	18.99	34.71	24.39	35.36
Image_32	20.75	19.82	20.75	34.87	25.68	35.72
Image_33	18.85	17.60	18.85	33.35	23.21	37.21

Tableau 4.10 : *Comparaison de la performance de la méthode de tatouage proposée et la méthode DWT-DCT-SVD selon le PSNR sous l'attaque.*

Les résultats montrent que, même avec une attaque importante qui détruit une partie du contenu de l'image, la marque peut encore être restauré ou extraite avec une qualité très satisfaisante. Pour plus d'illustration, les figures 4.11, 4.12 et 4.13 montrent la marque extraite W_1et W_2 à partir de plusieurs images attaquées. Il est clair que la qualité visuelle de la marque est très préservée même avec la présence des attaques telles que la compression et le cropping.

D'autres travaux ont été menés afin de montrer la robustesse du tatouage proposé par rapport à plusieurs attaques. Pour les images tatouées attaquées, on calcule une valeur de score de la détection qui indique si la marque est réellement présente dans les images. Nous avons implémenté une technique inspirée de **[Far07]** en utilisant le coefficient de corrélation

normalisée entre la marque originale et la marque extraite. Le score est donné par la formule (4,1):

$$S = \frac{\sum_{i=0}^{M-1}(2p_i - 1)(2p'_i - 1)}{\sqrt{\sum_{i=0}^{M-1}(2p_i - 1)^2 . \sum_{i=0}^{M-1}(2p'_i - 1)^2}} = \frac{1}{M}\sum_{i=0}^{M-1}\sum_{i=0}^{M-1}(2p_i - 1).(2p'_i - 1) \qquad \textbf{(4,1)}$$

Ou p_i et p'_i sont les éléments de la marque originale et celle de la marque extraite respectivement tel que M est la taille de la marque.

Si le score S est supérieur à un certain seuil Ts, on peut dire que la marque est présente dans l'image. D'après **[Far07]**, la valeur de seuil peut être calculée en utilisant la formule (4,2) est donnée comme suit

$$T_S = 4.5\sqrt{2/M} \qquad \textbf{(4,2)}$$

Par conséquent, étant donné que la taille de la marque W_1 est 106x143, nous concluons que le seuil T_S est égal à 0,14.la figure 4.15, montre la variation du score obtenu pour la détection de la marque extraites, à partir de plusieurs images attaquées en utilisant différentes angle de rotation. Nous pouvons facilement voir que le score de détection est toujours supérieur au seuil T_s qui signifie que la marque est toujours détectée**.**

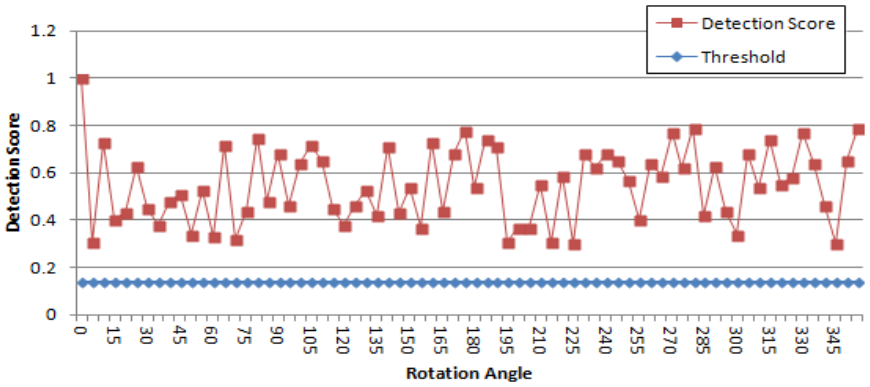


Figure 4.15 : *Score de détection de la marque extraite à partir de l'image tatouée attaquée par l'attaque de rotation avec différentes angles.*

En plus, le calcul du score de détection est effectué par rapport à l'attaque de compression JPEG. Figure 4.16 illustre l'évolution du score de détection de la marque avec plusieurs valeurs de taux de la compression. On voit que même avec des taux de compression élevés, la marque peut encore être détectée car le score de détection est au-dessus du seuil T_S. Les figures 4.15 et 4.16 sont approuves que les résultats de NCC présentées dans le tableau 4.6, et montre que la technique du tatouage proposée est robuste contre plusieurs attaques.

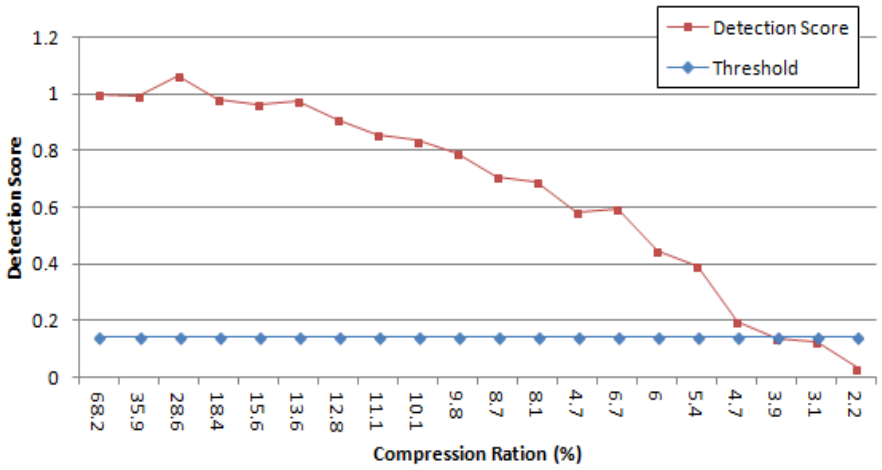


Figure 4.16 : *Score de détection de la marque extraite à partir de l'image tatouée attaquée par l'attaque de compression JPEG avec différentes facteurs.*

4.5 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle méthode de tatouage réversible des images médicales. Cette méthode est basée sur la combinaison de plusieurs types de transformations DWT, DCT et SVD afin d'insérer deux types d'images différents de marques. L'objectif de ce travail est d'augmenter la sécurité d'un système de dissimulation de données, qui peut être appliquée à la fois pour la protection du droit d'auteur et l'authentification de contenu. Les trois transformations que nous avons utilisées obtenus après la transformation de l'image hôte.

Les résultats obtenus sont satisfaisants, la méthode réversible R- DWT-DCT-SVD offre un compromis entre la capacité, l'imperceptibilité et la réversibilité que l'approche classique DWT-DCT-SVD qui a été présentée dans **[Awa13]**, les résultats obtenus montrent aussi que notre schéma de tatouage proposé peut résister à plusieurs types d'attaques y compris les attaques de transformation géométrique, l'attaque de bruit, et l'attaque de compression par JPEG.

Conclusion générale

Conclusion et perspectives

Le tatouage numérique a été réalisé comme une technique intéressante pour la sécurité des images et des données : L'intégrité, la confidentialité et l'authentification .Notre objectif est de vérifier les trois propriétés de sécurité ensemble, dans ce cas le tatouage doit trouver un meilleur compromis entre deux critères : l'imperceptibilité et la robustesse pour garantir l'authentification et la protection des images.

Au cours de cette thèse nous avons étudié la problématique liée au tatouage numérique des images. Nous avons présenté une méthode de tatouage réversible qui a permis d'assurer l'intégrité des images tout en donnant une récupération parfaite de l'image aux utilisateurs.

Dans la première partie de cette thèse nous avons étudié les services de sécurité et la problématique liée au tatouage numérique. Nous avons mis l'accent sur le tatouage réversible et nous avons présenté ses contraintes, ses caractéristiques, le processus de l'insertion et celui de l'extraction, ensuite nous avons décrit quelques méthodes de tatouage réversible dans le domaine spatial.

Le domaine spatial donne des avantages mais aussi des limitations, notre contribution est basée sur l'utilisation de critère de réversibilité dans le domaine fréquentiel, nous avons développé un système de tatouage robuste réversible R-DWT-DCT-SVD basant sur l'insertion de deux types de marques (marque réversible W_1 et la marque W_2 sous forme un logo), ensuite nous avons appliqué cette technique sur les images médicales IRM en niveau de gris de taille 256x256 pixels.

Nous avons terminé par une comparaison avec la méthode décrite dans le chapitre précédent selon les critères d'évaluation PSNR, SNR, NCC. Les résultats expérimentaux ont montré que cette technique donne une bonne qualité visuelle de l'image et une robustesse parfaite contre quelques attaques comme le cropping, la compression JPEG et aussi la rotation tout en offrant une réversibilité et une restauration complète et intacte de l'image originale.

Perspectives

Pour notre contribution nous envisagerons d'utiliser des images couleurs avec l'utilisation d'une seule marque W_3 qui est générée à l'aide de deux marques (marque réversible W_1 et la marque logo W_2) pour garantir les trois propriétés de sécurité et elle se base sur le critère de réversibilité pour garantir l'intégrité, l'authentification et la confidentialité.

Bibliographie Générale

[Aia01] B. Aiazzi, L. Alparone et S. Baronti, Near-lossless compression of 3-D optical data, IEEE *Transactions on Geoscience and Remote Sensing.* Vol. 39, n° 11, p. 2547–2557, Nov. 2001.

[Ala04] A.M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. Image Process., vol.13, no. 8, pp. 1147–1156, Aug. 2004.

[And93] RJ.Anderson ,''the Classification of Hash Functions'',Codes and Ciphers' ,proceedings of fourth IMA Conference on Cryptography and Coding ,pp83-93.1993.

[Aut02] F. Autrusseau, "Modélisation Psychovisuelle pour le tatouage des images", Signal and Image Processing. Ph. D. Thèse, Université de Nantes France, 2002.

[Awa13] Mayank Awasthi, anshi Lodhi. Robust Image Watermarking based on Discrete Wavelet Transform, Discrete Cosine Transform & Singular Value Decomposition, Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 3, Number 8 (2013), pp. 971-Research India Publications.

[Ala04] A. M.Alattar. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing, 1147–56. 96, (13- 8 Aug. 2004).

[Bar12] K.BARHOUMI. Approche par marquage pour l'évaluation de la qualité d'image dans les applications multimédias, MÉMOIRE, Novembre 2012.

[Bas03] B. Bas, P. Roue and J. M. Chassery. Tatouage d'images couleurs additif : vers la sélection d'un espace d'insertion optimal, In Coresa03, volume 1, 2003.

[Bor04] J.C.Borie.Sécurisation d'images par cryptage :application aux images méicales .thése de doctorat université de Nimes ,2004.

[Bek12] S.Bekkouche, A.Chouarfia. Tatouage des images médicales, Mémoire de magistère, Université d'USTO Oran, 2012.

[Bek11] S.Bekkouche, A.Chouarfia. Spatial and Frequency combination RW/CDMA watermarking technique, the 2nd International Conference on Multimedia Technology, Hangzhou China, 2011.

[Bek15] S.Bekkouche, M.K.Faraoun. Robust and reversible images watermarking scheme using combined DCT-DWT-SVD transforms, journal of information processing system. 2015.

[Bek12] S.Bekkouche, A.Chouarfia. Mammography Image Authentication: A Comparison of Combined Watermarking Techniques Based on Reversible Watermarking and CDMA in Frequency Domain International Journal of Network and Mobile Technologies,Volume 3, Issue 1, Hong Kong, January2012.

[Bly04] P. Blythe and J. Fridrich. Secure digital camera, Proceedings of Digital Forensic Research Workshop (DFRWS), pages 17–19, 2004.

[Bou04] J.Bourgeois, P.Michel Steve and R.B.Rubio. Watermarking, Tuteur Robert Erra, 28 janvier 2004.

[Car95] Caronni, Germano, Assuring Ownership Rights for Digital Images in Proceedings of the VIS '95, Vieweg, Wiesbaden, p. 251-263, 1995.

[Cel02] M.Celik,G.G.Sharma,A.M.Tekalp,E.Sabe,"reversible data hiding". Proceedings of the International Conference On Image Processing2002, Rochester, NY, September 2002.

[Cha01] C.Chang.M.S.Hwang and T-S Chen."A new encryption algorithm for image cryptosystems".The Journal of Systems and Software,Vol 58 pp83-91,2001.

[Cha05] G.CHAREYRON. Tatouage d'image une approche couleur, Thèse de doctorat informatique, Université Jean Monnet Saint -Étienne, Décembre 2005.

[Cha02] D.V. Chandra. Digital Image Watermarking using Singular Value Decomposition. In 45th IEEE Midwest Symposium on Circuit and Systems, Tulsa, volume 3, pages 264–267, 2002.

[Che05] Y. A .Chen. Fragile Watermark Error Detection Scheme for Wireless Video Communications. IEEE Transactions on Multimedia, 7(2):201–211, 2005.

[Che03] L. Chen and J. Lin. Mean Quantization Based Image Watermarking. Image Vision and Computing, 21(8):717–727, 2003.

[Chr02] S.R.Chris. Hidden Bits: A Survey of Techniques for Digital Watermarking,Virtual Union, Spring 2002.

[Coa00] G.Coatrieux,H.Maitre,B.Sankur,Y.Rolland,and R.Collorec. "relevance of **w**atermarking in medical imaging",Proceedings of IEEE of EMBS International Conference on Information Technology Applications in Biomedicine 2000,PP.250-255,9-10 Nov 2000.

[Col05] D. Coltuc and A. Tremeau, E. J. Delp and P. W. Wong, Eds., Simple reversible watermarking schen in Proc. SPIE: Security, Steganography, Watermarking Multimedia Contents VII, pp.561–568, 2005.

[Cox98] I. J. Cox, M.L. Miller, A.L. McKellips. Watermarking as communication with side information, IEEI Selected Areas Communication. 16(4), 587-593, May 1998.

[Cox97] I. Cox and M Miller. A Review of Watermarking and the Importance of Perceptual Modeling. In Electronic Imaging'97, 1997.

[Cox96] I.Cox, J. Kilian, T. Leighton and T. Shamoon, A secure, robust watermark for multimedia, in Proc. Workshop on Information Hiding, Univ. of Cambridge, U.K., pp.175-190, May 30 - June 1, 1996.

[Cox02] I. Cox and M. Miller. The first 50 years of electronic watermarking. EURASIP Journal on Applied Signal Processing, 2002(2):126–132, 2002.

[Cox00] I.Cox, M.L. Miller, and J.A. Bloom. Watermarking Applications and Their Properties. In IEEE International Conference on Information Technology: Coding and Computing, pages6–10, Las Vegas, 27 -29 Mars 2000.

[Cox02] I. Cox, M. Miller, and J. Bloom. Digital Watermarking: Principles & Practices. Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.

[Din07] D.Coltuc and J.M.Chassery, Very Fast Watermarking by Reversible Contrast Mapping, IEEE Signal Processing Letters, VOL. 14, No. 4, April 2007.

[DUB98] J.P.DUBUS. Analyse Multirésolution Et Psychovisuelle technique de l'ingénieur Mesures et contrôle, Vol RE1, No R632, pages 1 – 21, 1998.

[EL H12] M.EL HAJJI. La sécurité d'images par le tatouage numérique dans le domaine d'ondelette, thèse de doctorat es-sciences, La Faculté des Sciences d'Agadir, 28-01-2012.

[Fab00] Fabien A.P. Petitcolas, Stefan Katzenbeisser. "Watermarking techniques" dans Information Hiding, techniques for steganography and digital watermarking" France, p 106, 2000.

[Far07] M.K.Faraoun,A. Rabhi. "RST Robust watermarking schema based on image normalization and DCT decomposition." Malaysian Journal of Computer Science 20.1 2007.

[Fen05] J.B.Feng,H.C.Wu,CS.Tsai,and Y.Chu,"a new multisecret images shaing scheme using largrange's interpolation", Journal of systems and Software,vol .76,No.3,PP.327-339,june 2005.

[Fen06] Ke.feng he, et al: Watermarking for images using the HVS and SVD in the wavelet domain, Dans Proceedings of IEEE International Conference on Mechatronics and Automation, pp.2352- 2356, 2006.

[Fou08] E.K Fourati. Elaboration d'une approche tatouage réversible pour vérification intégrité des médicales. université de sfanx Tunisie ,2008.

[Fri02] J. Fridrich, M. Goljan, and R. Du, Lossless data embedding—New paradigm digital watermarking EURASIP J. Appl. Signal Process.,no. 2, pp. 185– in 196, 2002.

[Fri01] J. Fridrich, M. Goljan, R. Du, Invertible authentication, in: Proceedings of the SPIE Security and Watermarking of Multimedia Content, San Jose, USA, pp. 197–208,2001.

[Gan04] E.Ganic, A.M.Eskicioglu: Robust DWT-SVD domain image watermarking: embedding data in all frequencies, ACM Special Interest Group on Multimedia, pp.166-174, Magdeburg, Germany, 2004.

[Gol10] N.El-H.GOLEA. RGB color image digital watermarking, Thèse de Magistère, University Elhadj Lakhder-Batna, 2010.

[Guy02] F.Guy, D.Clara, M.Bernard . Imagerie médicale .Fondation pour la Recherche Médicale, Avril 200

[Gru95] D. Gruhl, W. Bender, and Moritomo. Techniques for data hidding. In processing of SPIE, volume 2420, page 40, february 1995.

[Har09] Harsh K. Verma1, Abhishek Narain Singh, Raman Kumar, «Robustness of the Digital ImageWatermarking Techniques against Brightness and Rotation Attack", International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

[Hon01] C.W. Honsinger, P.W. Jones, M. Rabbani, J.C. Stoffel, Lossless recovery of an original image containing embedded data, U.S. Patent No. 6,278,791, 2001.

[hsi01] M.S Hsieh, Wavelet-based Image Watermarking and Compression, Ph.D Thesis, Institute of Computer Science and Information Engineering National Central University,Taiwan, Dec. 2001.

[Hsu 99] C.T Hsu and J-L.Wu. Hidden Digital Watermarks in Images, IEEE Trans. Image Processing, Vol.8, No.1, 1999, pp.58-68.

[Hu11] Y. Hu, Z. Wang, H. Liu, G. Guo: A Geometric Distortion Resilient Image Watermark Algorithm Based on DWT-DFT. Journal Of Software, Vol. 6(9),pp. 1805-1812. 2011.

[Kat00] S. Katzenbeisser and F. Petitcolas. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 2000.

[Kha06] Y.I. Khamlichi, M. Machkour, K. Afdel, A. Moudden, ' Medical Image Watermarked by Simultaneous Moment Invariants and Content-Based for Privacy and Tamper Detection', Proceedings of the 6th WSEAS International Conference on Multimedia Systems & Signal Processing, Hangzhou, China, April 16-18, pp109-113, 2006.

[Kil97] J. Kilian I. J. Cox and T. Leighton Aand T. G. Shamoon. Secure Spread Spectrum Watermarking For Multimedia, IEEE Trans. on Image Processing 6, no. 12, 1673–1687, (1997).

[Kim03] T. Y. Kim, T. Kim, and H. Choi. Correlation-based Asymmetric Watermark Detector. In IEEE International Conference on Information Technology Coding and Computing ITCC'2003, pages 564–568, 2003.

[Kim99] Kim, J.R., and Moon, Y.S. A robust wavelet-based digital watermarking using level-adaptive thresholding. International Conference on Image Processing Proceedings, ICIP 99, vol. 2, 226–230. (October, 1999).

[Koc95] E. Koch, J. Zhao, towards robust and hidden image copyright labeling, in: Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing June 20-22, Neos Marmaras, Greece, 1995.

[Kun98] D. Kundur and D. Hatzinakos. Digital Watermarking Using Multiresolution Wavelet Decomposition.In IEEE International Conference on Acoustics, Speech and Signal Processing,Seattle, Washington, volume 5, pages 2969–2972, 1998.

[Koc95] E. Koch, J. Rindfrey, and Z. Zhao. Copyright Protection for Multimedia Data. In International Conference on Digital Media and Electronic Publishing, pages 203–213, 1995.

[Koc95] E. Koch, J. Rindfrey, and Z. Zhao. Copyright Protection for Multimedia Data. In International Conference on Digital Media and Electronic Publishing, pages 203–213, 1995.

[Kun97] D. Kundur and D. Hatzinakos. A robust Digital Image Watermarking Method Using Wavelet Based Fusion. In International Conference on Image Processing (ICIP'97), volume 1, pages 544–547, 1997.

[Kun98] D. Kundur and D. Hatzinakos. Digital Watermarking Using Multiresolution Wavelet Decomposition. In IEEE International Conference on Acoustics, Speech and Signal Processing, Seattle, Washington, volume 5, pages 2969–2972,1998.

[Kur08] R. Y. Kuraz and A. H. Modar, "Improve Watermark Security via Wavelet Transform and CDMA Techniques," Al-Rafidain Engineering, Vol. 6, pp. 39-49, 2008.

[Lan96] G. C. Langelaar, J. C. A. van der Lubbe, J. Biemond, Copy protection for multimedia data based on labeling techniques in Proceedings of the Symposium on Information Theory in the Benelux, Enschede, The Netherlands, May 1996.

[Lan97] C. Langelaar, J.C.A. van der Lubbe, R.L. Lagendijk, Robust labeling methods for copy protection of images in Proceedings of the SPIE Electronic Imaging 97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, p. 298-309, Feb. 1997.

[Lef01] F. Lefèvre, D. Guéluy, D. Delannay, B. Macq: A Print and Scan Optimized Watermarking Scheme, IEEE Multimedia Signal processing, 2001.

[Liu02] R. Liu and T. Tan. An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. In IEEE Transactions on Multimedia, volume 4, pages 121–128, March 2002.

[Meh01] U.Mehmet . Celik, S. Gaurav, A Hierarchical Image Authentication Watermark With Improved Localization And Security in Proceedings of the IEEE International Conference on Image Processing, vol. II, p. 502-505, Oct 2001.

[Mitt99] T.Mittelholzer."An Information theoretic approach to steganography an watermarking".IHW'9,Dresen,Germany,September 1999.

[Moe03] A.Moez ,M.S.Bouhlel et L. Kamoun , "Nouvelle technique de crypto-compresion pour la sécurisation de la transmission es images médicales",Sciences Electronique, "Technologies de l'information et des Télécomunications ,M.S.Bouhlel,B.Solaiman et L.Kamoun ISBN 9973-41-85-6,Mars 2003.

[Mot03] G. Motta, F. Rizzo et J. A. Storer. Compression of hyperspectral imagery. In Data Compression Conference, DCC, vol. 8, p. 333– 342. IEEE Mars 2003.

[Pet99] F. Petiscolas, R. Anderson, and M. Kuhn. Information Hiding Terminology: A Survey.IEEE Signal Processing, 78(7):1062–1078, 1999.

[Pre93] B.Preneel," Analysis an Design of cryptographie Hash Functions",thése de

doctorat,CatholicUniversity of leuven 1993.

[Pue05] G.Lo-Varco,W.Puech, and M.umas."Content Based Watermarking for securing Color Images". Journal Of Imaging Science and Technologie,Vol 49,pp.450-458,2005.

[Pue04] Puech W., Rodrigues J. : A new crypto-watermarking method for medical images safe transfer. In Proc. 12th European Signal Processing Conference (EUSIPCO'04), pp. 1481–1484. 98.2004.

[Qua04] Quan Liu and Qingsong Ai, "Combination of DCT-based and SVD-based watermarking scheme", DSP, ICSP‟04, 873-876.2004.

[Rat14] N. Rathi, H.Ganga . Securing Medical Images by Watermarking Using DWT-DCT-SVD, International Journal of Computer Trends and Technology (IJCTT) volume X Issue Y–Month 2014.

[Rey01] C. REY and J. DUGELAY. Un panorama des m´ethodes de tatouage permettant d'assurer un service d'intégrité pour les images. Traitement du Signal, 18(4) :283–295, 2001.

[Rio91] Rioul, O., Vetterli, M., Wavelets and signal processing. IEEE Signal Processing Magazine, Vol. 8, pp. 14-38, 1991.

[Rua98] J.J.K. Ó Ruanaidh and T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, Signal Processing, vol. 66, no. 5, pp. 303-317, May 1998.

[SAA01] A. SAADANE, F. AUTRUSSEAU, Tatouage perceptuel et adaptatif, Institut de Recherche en Communications et Cybernétique de Nantes (IRCCyN), La Chantrerie,BP50609, 44306 Nantes Cedex. Traitement du Signal – Volume 18 – n° 4 – Spécial 2001

[Sch94] R. Schyndel, A. Tirkel, and C. Osborne. A Digital Watermark. In IEEE International Conférence on Image, volume 2, pages 86–90, 1994.

[Sol99] K. Solachidis and I. Pitas. Circularly Symmetric Watermark Embedding in 2-D DFT Domain. pages 3469–3472, 1999.

[Sol00] V. Solachidis and I. Pitas. Self-similar ring shaped watermark embedding in 2d-dft domain. In

10th European Signal Processing Conference, EUSIPCO'00, Tampere, Finlande, pages 1977–1980, september 2000.

[Suh03] M.A. Suhail. Digital Watermarking-Based DCT and JPEG Model, IEEE Transactions on Instrument and Measurements, vol. 52(5), pp. 1640-1647, October 2003.

[Tan90] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding Secret Information into a Dithered Multilevel Image, In 1990 IEEE Military Communications Conference, pages 216–220, Monterey, Oct 1990.

[Tan03] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. 890–896, 13-8-2003.

[Tho07] Thodi D. M, Rodriguez .j: Expansion Embedding Techniques for Reversible Watermarking. IEEE Transactions on Image Processing 16, 3 (Mar.2007).

[Tir93] A.Z. Tirkel. Electronic watermark. In DICTA, Austin, Texas, pages 666–672, december 1993.

[Vas02] Vassaux B., Bas P., Chassery J.M., Tatouage d'images par étalement de spectre: Apport de la technique CDMA en mode multicouche, Journées CORESA, Poitiers, 19-20Octobre 2000.

[Vol01] 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.

[Zhe07] D. Zheng, Y. Liu, J. Zhoa, and A. Saddik. A survey of RST Invariant Image Watermarking Algorithms. ACM Computing Surveys, 39(2), 2007.

[Yav07] E. Yavuz, Z Telatar: Improved SVD-DWT based digital image watermarking against watermark ambiguity. In Proceedings of the 2007 ACM symposium on Applied computing (SAC '07), ACM, New York, NY, USA, pp. 1051-1055, 2007.

[Yon05] Y Yongdong Wu. On the Security of an SVD based Ownership Watermarking IEEE transactions o Multimedia, Vol 7. No.4, August, 2005.

[Win99] Winkler, M. Kutter, Vers un tatouage à étalement de spectre optimal utilisant le système visuel humain in Proceedings of the CORESA 99, Sophia Antipolis, France, p. 25-33, June 14-15, 1999.

[Won01] P. Wong and A. Memon. Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification. IEEE Transactions on Image Processing, 10(10):1593–1601, 2001.

[Won98] P. W. Wong, A Public Key Watermark for Image Verification and Authentication in Proceedings of the Int. Conf. Im. Proc, vol. I, p. 155-459, 1998.

[YU08] J. Yu, X.Wang, J. Li, and X. Nan. An Effective Fragile Document Watermarking Technique. In IEEE International Symposium on Electronic Commerce and Security, pages 908–911, 2008.

[Vle03] De Vleeschouwer C., Delaigle J.-F., Macq B. : Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Transactions on Multimedia 5, 1, 97–105. 96, 97, 99,105,(Mar. 2003).

Abstract

We present a secure and robust image watermarking scheme that uses a combined reversible DWT-DCT-SVD transformations to increase integrity, authentication and confidentiality. The proposed scheme uses two different kinds of watermarking image: a reversible watermark W1 used for verification (ensuring integrity and authentication aspects), and a second one W2 defined by a logo image that provide confidentiality. The proposed scheme is shown to be robust, while performances of proposed approach are evaluated with respect to the PSNR (Peak Signal to Noise Ratio), SNR (Signal noise to ratio), NCC (Normalized Correlation) and running time. Robustness of the scheme is also evaluated against different attacks including compression attack and Salt & Pepper.

Keywords - Image Security, Image Watermarking, Reversible DWT-DCT-SVD Transform

Résumé

Nous présentons un schéma de tatouage d'image sécurisé et robuste basé sur le tatouage réversible et la combinaison les transformées DWT-DCT-SVD pour accroître et satisfaire l'intégrité, l'authentification et la confidentialité. Le schéma proposé utilise deux différents types d'images de tatouage: une marque réversible W_1, qui est utilisé pour la vérification les propriétés : l'intégrité et l'authentification; et la deuxième marque W_2, qui est défini par une image logo pour satisfaire la confidentialité. Notre approche proposée se révèle être robuste, tandis que ses performances sont évaluées par le rapport du signal sur le bruit (SNR), le PSNR, NCC (métrique de corrélation) et le temps d'exécution. La robustesse de cette approche est également évaluée par rapport aux différentes attaques, y compris l'attaque de compression et le bruit Salt & Pepper.

Mots clé: sécurité de l'image, tatouage de l'image, Réversible DWT-DCT-SVD.

ملخص

في هذه المذكرة قمنا بتقديم طريقة جديدة لوشم الصور الطبية لغرض تحقيق السرية وأمن تحويلها عن طريق الشبكة, تعتمد هذه الطريقة على استعمال نمطين من الوشم الأول W1 و هو الوشم الرجعي أو العكسي لغرض تحقيق السلامة و التوثيق و الوشم الثاني W2 و هو عبارة عن صورة لغرض تحقيق السرية .

بعد إدراج الوشمين في الصورة الطبية نقوم بحساب النتائج التجريبية على أساس العوامل PSNR,SNR,TE,NCC حيث وضحت السعة للتشابه أنها تتوافق مع الصور الموشومة كما بينت أن لها مثالة عالية ضد الهجمات من بينها ضغط الصورة و هجم Salt et pepper.

الكلمات المفتاحية:

أمن الصورة،وشم الصورة،DWT-DCT-SVT العكسي.