REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
ECOLE NATIONALE POLYTECHNIQUE

DEPARTEMENT D'ELECTRONIQUE

MEMOIRE DE MAGISTER
EN ELECTRONIQUE

Présenté par :

BOUCHAMA Samira

Ingénieur d'Etat en Electronique

Le tatouage des images Appliqué à l'imagerie médicale

Soutenu devant le Jury d'examen composé de:

Président :	**Mr D. BERKANI**	**Professeur**	**(ENP)**
Rapporteur :	**Mme L. HAMAMI**	**Maître de conférences**	**(ENP)**
Examinateurs :	**Mlle M. GUERTI**	**Maître de conférences**	**(ENP)**
	Mr H. BOUSBIA-SALAH	**Docteur**	**(ENP)**
	Mr M. TRABELSI	**Maître de conférences**	**(ENP)**

2007

ملخص

يمكن تعريف "رسم الصور" على أنه تقنية تسمح بإدخال معلومات رقمية في الصورة بطريقة غير مرئية ومتينة. بالإضافة إلى مهامه الأولى وهي المحافظة على حقوق المؤلف، يمكن استعمال رسم الصورفي مجال التصوير الطبي لتدعيم المحافظة على أمن الصور الموزعة عبر الشبكة في مجال الطب عن بعد.

نقوم في هذه المذكرة بدراسة طريقتين لرسم الصور، تعتمد الأولى على تقنية CDMA للإتصال (تعدد الإتجاهات بتوزيع الشفرات) وتهدف إلى التأكد من أصالة الصورة، بينما تعتمد الطريقة الثانية على مجال التشفير (cryptographie) واستعمال الحروف الثنائية الأقل دلالة (LSBs) وهذا من أجل التأكد من سلامة الصورة والحفاظ على سرية معلومات المريض.

كما نقوم بإختبار وإخضاع ثلاثة أنواع من الصور الطبية لهاتين الطريقتين، إذ تعتبر القياسات المتعلقة بنوعية الصورة ضرورية للغاية وذلك للتحقق من أن الإئلاف الحاصل بفعل تقنية الرسم لا يؤدي إلى عمليات فحص خاطئة.

مفاتيح : رسم هش، رسم متين ، التصوير الطبي، سلامة الصورة، التوثيق

Résumé

Le tatouage des images peut être défini comme étant une technique qui permet d'insérer des informations numériques dans une image de manière imperceptible et indélébile. En plus de son application initiale qui est la protection des droits d'auteur, le tatouage peut être utilisé dans d'autres domaines et en particulier dans le domaine de l'imagerie médicale pour contribuer à la sécurité des images partagées en réseau dans les applications de télémedecine. Dans ce mémoire nous étudions deux méthodes de tatouage, la première est basée sur la technique de communication CDMA (Accès Multiple par répartition de Code) et elle a pour objectif de vérifier l'authenticité d'une image. La deuxième fait appel à la cryptographie et à l'utilisation des bits les moins significatifs de l'image (LSBs) et elle a pour objectif de vérifier l'intégrité de l'image médicale et de garder la confidentialité des données du patient. Les tests sont effectués sur trois types d'images médicales, et les mesures de la qualité de l'image tatouée sont indispensables pour vérifier que la dégradation apportée par le tatouage ne conduit pas à un diagnostic erroné.

Mots clés : tatouage robuste, tatouage fragile, imagerie médicale, intégrité, authentification.

Abstract

Image watermarking can be defined as a technique that allows insertion of imperceptible and indelible digital data into an image. In addition to its initial application which is the copyright, watermarking can be used in other fields, particularly in the medical field in order to contribute to secure images shared on the network for telemedicine applications. In this report we study two watermarking methods, the first one is based on the CDMA (Code Division Multiple Access) and its aim is to verify the image authenticity whereas the second one uses cryptography and the least significant bits, and its objective is to check the integrity of the image and to keep the confidentiality of the patient data. Tests were done on three kinds of medical images and the quality measurements have been done on the watermarked image to verify that this technique does not lead to a wrong diagnostic.

Key words: robust watermarking, fragile watermarking, medical imaging, integrity, authentication.

Remerciements

Je tiens à remercier en premier lieu Mme L.Hamami qui m'a bien accueillie dans son équipe et qui m'a continuellement aidée et encouragée.

Je remercie sincèrement les membres de jury Mr D. BERKANI, Mlle M. GUERTI, Mr H.BOUSBIA-SALAH**,** Mr M. TRABELSI pour l'attention accordée à mon travail.

Je remercie particulièrement le Professeur Khelladi, Directeur du Centre de Recherche sur l'Information Scientifique et Technique (CERIST), de m'avoir autorisée et encouragée à m'inscrire en post-graduation.

Je suis également reconnaissante à Melle Z.Brahimi du Centre de Développement des Technologies Avancées (CDTA) pour son aide et ses précieux conseils.

Je remercie mes amis du labo (ENP) : Bahia, Mourad, Brahim ainsi que Lyes du CDTA.

Mes remerciements vont également aux Docteurs I. Keraghel et M. Hadj Bekkouche ainsi qu'à toute l'équipe de radiologues (CHU de Bab El Ouaed) qui m'a aidée à évaluer mes résultats.

Bien évidemment, je remercie ma mère, mon père, mon frère Nabil et mes sœurs Isma, Amel et Djazia pour leur encouragement et leur soutien.

Merci à tous ceux qui ont contribué, de près ou de loin, à réaliser ce travail.

A mes Parents

Sommaire

Chapitre 3 : Outils et algorithmes

Chapitre 4 : Confidentialité des données du patient

Chapitre 5 : Intégrité et Confidentialité des données

Liste des figures

Liste des tableaux et graphes

Abréviations

ACR	American college of Radiolog
AMR	l'Analyse Multirésolution
ASCII	American Standard/Society Code for Information Interchange
CDMA	Code Division Multiple Access
CIF	Common Intermediate Format
CT	Computerized Tomography
DICOM	Digital Image Communication in Medecine
DWT	Discrete Wavelet Transform
IRM	Imagerie par Résonance Magnétique
JPEG	Joint Photographic Experts Group
LSB	Least significant bit
LSFR	Linear Feedback Shift Register
MAE	Mean Absolute Error
MD5	Message Digest 5
MPEG	Moving Picture Expert Group
MSB	Most Significant Bit
MSE	Mean Square Error
NEMA	National Electrical Manufacturers Association
OMS	Organisation mondiale de la santé
PSNR	Peack Signal to Noise Ratio
QCIF	Quarter Common Intermediate Format
SBPA	Sequence Binaire Pseudo Aléatoire
SBPA 2D	Séquence Binaire Pseudo Aléatoire à 2 Dimensions
SNR	Signal to Noise Ratio
SVH	Système Visual Humain
wPSNR	Weighted Peack Signal to Noise Ratio

Introduction

Introduction

- **Problématique**

Le développement des technologies de l'information et de la communication en général et d'Internet en particulier a facilité le partage et le transfert des données numériques, introduisant ainsi de nouvelles formes de piratage de documents et de nouveaux défis de sécurité à relever.

En effet, bien qu'il existe aujourd'hui des techniques de protection relatives à la transmission des données numériques telle que la cryptographie, le problème de la protection du contenu d'un support numérique multimédia ne connaît pas encore de solutions satisfaisantes. Il est devenu aisé de modifier ou de reproduire un média et même de revendiquer ses droits d'exploitation.

Afin de freiner la copie des œuvres multimédias et contribuer à la protection du copyright, de nouvelles méthodes ont été développées. Il s'agit des méthodes de tatouage connues plus par "le watermarking".

Le watermarking des images consiste à insérer une information imperceptible et indélébile dans le document numérique (image, son ou vidéo), dans le but d'identifier les droits d'auteur.

En plus de la protection du copyright, l'application des techniques de tatouage s'est élargie à d'autres domaines tels que l'indexation des images, le contrôle d'intégrité des images, etc.

Le tatouage des images, trouve une application dans le domaine de l'imagerie médicale et en particulier dans le domaine de la pratique de la médecine à distance connue sous le nom de "télémédecine". En effet, la mise en place d'interfaces de visualisation à distance de données médicales connaît actuellement une forte demande. Ces interfaces permettent d'accéder aux dossiers des patients contenant des données textuelles et images. Le partage de ces données et en particulier des images sur le réseau Internet, les expose au danger de manipulations non autorisées, et ce, malgré les outils de sécurité existant tel que le contrôle d'accès.

Le tatouage a été donc proposé pour contribuer à augmenter la sécurité du partage en permettant de garder la confidentialité des données du patient et de vérifier l'intégrité des images médicales.

Depuis ces dernières années, les chercheurs s'intéressent de plus en plus au domaine du watermarking et plusieurs techniques ont déjà été proposées dans ce domaine, mais sont-elles toutes adaptables à l'imagerie médicale ?

En effet, l'image médicale a ses propres spécificités. L'image tatouée doit présenter la même lecture clinique que l'image originale, elle ne doit donc pas subir une dégradation qui affecte le diagnostic.

Il existe actuellement plusieurs techniques d'imagerie médicale telles que le scanner, l'échographie, la radiographie, l'Imagerie à Résonance Magnétique (IRM), etc. Ces images subissent-elles le même niveau de dégradation lors de l'insertion d'un tatouage ou est-ce qu'une technique de tatouage d'image médicale s'adapterait mieux pour un type d'image que pour un autre ?

Dans ce mémoire nous nous intéresserons à deux méthodes. La première traite de l'authenticité de l'image et la deuxième a pour objectif de garder la confidentialité des données du patient et de vérifier l'intégrité de l'image médicale. Nous étudierons l'apport et les limites de chaque méthode pour trois types d'images médicales : les images IRM, les images radiographiques et les images échographiques.

Les mesures objectives et subjectives de la qualité des images tatouées permettront d'évaluer les résultats.

- **Plan du mémoire**

Ce mémoire se décompose en cinq chapitres :

Dans le premier chapitre, nous présenterons des généralités sur le tatouage des images et ses différentes applications.

Nous exposerons dans le deuxième chapitre l'utilisation du tatouage dans le domaine de l'imagerie médicale et en particulier dans le domaine de la télémédecine. Nous présenterons

les spécificités de ces images et nous donnerons également un aperçu de quelques méthodes de watermarking utilisées dans le domaine médical.

Dans le troisième chapitre, nous aborderons les différents outils utilisés dans notre application, citons par exemple l'outil de communication CDMA (Code Division Multiple Access), l'outil ondelettes et quelques outils de cryptographie.

L'étude de la méthode multicouche pour la vérification de l'authenticité de l'image fera l'objet du quatrième chapitre. Cette méthode proposée par Vassaux [2] dans le cadre de la protection du copyright a pour objectif d'augmenter le nombre de bits à insérer dans une image sans pour autant la dégrader et ce en se basant sur l'outil CDMA. L'application de cette méthode sera testée dans le domaine spatial et dans le domaine de la transformée en ondelettes discrète de l'image.

Et enfin, le cinquième chapitre sera consacré à l'étude d'une méthode qui permet d'une part, de garder la confidentialité des données du patient et d'autre part, de vérifier l'intégrité de l'image médicale. Cette méthode proposée par Boucherkha [19], associe l'utilisation des bits les moins significatifs des pixels de l'image (LSB) aux outils de cryptographie. Nous adapterons cette méthode aux besoins de notre application afin d'augmenter la qualité et la sécurité de l'image.

Nous conclurons ce travail en résumant l'apport et les limites de chaque méthode étudiée et nous donnerons quelques perspectives de recherche dans ce domaine.

Chapitre 1
Généralités sur le tatouage des images

1.1 Introduction

La technique du tatouage, associée à d'autres techniques, a pour but de résoudre des problèmes variés relatifs à la sécurité des données digitales telles que la protection des droits d'auteur, la prévention de la redistribution non autorisée, l'intégrité du contenu d'une donnée, etc.

Plusieurs méthodes de tatouage existent, elles diffèrent selon l'application et les contraintes qu'elles exigent. Dans ce chapitre nous présentons des généralités sur la notion de tatouage, quelques-unes de ses applications les plus utilisées, un état de l'art sur les techniques de tatouage existantes et enfin des méthodes d'évaluation des algorithmes de tatouage en prenant en considération des mesures objectives et subjectives de la qualité de l'image tatouée ainsi que les éventuelles attaques.

1.2 La technique du tatouage

1.2.1 Définition

Le tatouage numérique est une technique qui consiste à insérer des informations numériques (marque ou signature) de manière imperceptible et indélébile dans le corps même d'un autre document numérique. Le tatouage des documents est un domaine relativement récent qui s'apparente à la stéganographie [1].

1.2.2 La cryptographie et la stéganographie

La cryptographie et la stéganographie sont des techniques qui répondent à des problèmes de sécurité. Elles sont destinées à transmettre une information à caractère confidentiel.

La cryptographie consiste à transformer un message pour qu'il devienne illisible. Seul la connaissance d'une clé et du moyen du cryptage permet de décoder le message afin de le rendre lisible. Cette technique a pour but de protéger le document pendant sa transmission.

La stéganographie consiste à dissimuler un message dans un autre. Ainsi toute personne connaissant la procédure de dissimulation peut lire le message caché. La stéganographie offre ainsi la possibilité de tenir une communication secrète entre deux ou plusieurs parties.

1.2.3 Les critères du tatouage

a) Invisibilité

Le principe fondamental du tatouage visible consiste à dissimuler la marque partiellement dans une image. Ce type de tatouage est utilisé en général pour restreindre la divulgation d'un document en fonction de l'appartenance d'un utilisateur.

En pratique, l'intérêt d'un tatouage efficace réside dans son invisibilité. Plusieurs méthodes ont été développées visant à minimiser la différence entre l'image marquée et l'originale.

b) Tatouage robuste, fragile et semi-fragile

Le tatouage robuste permet de rendre possible de déceler la marque du propriétaire de l'image malgré les différentes attaques possibles (voir la section 1.5.2). Cependant, si le contenu de l'image n'est plus exploitable après un traitement, il n'est plus nécessaire que la marque soit détectée.

Dans certains cas, il est préférable de favoriser la fragilité de la marque plutôt que sa robustesse. Un algorithme de tatouage fragile permet de vérifier que la marque est toujours présente, ce qui sous-entend que l'image n'a subi aucune modification malveillante.

Les tatouages semi-fragiles combinent à la fois les propriétés des marquages robustes et fragiles. Comme les robustes, ils tolèrent certains changements de l'image, comme des rotations, translations ou addition de bruit. Et comme les fragiles, ils sont capables de déterminer les régions ou l'image a été modifiée et celles ou elle reste authentique.

c) Capacité de marquage

La capacité de marquage est la quantité d'information que l'on insère dans la marque par rapport à la quantité d'information contenue dans le support numérique. La tendance actuelle vise à insérer une quantité d'information au moins égale à 64 bits [2].

d) Sécurité

La sécurité des techniques de tatouage se situe dans le choix d'une clé. Ainsi, la marque est indétectable par les parties non autorisées même en sachant les algorithmes d'insertion et de détection utilisés.

1.2.4 Le principe du tatouage

La figure 1.1 présente un schéma général d'implémentation de la marque. L'image originale I est tatouée de la marque W par un propriétaire possédant la clé K. L'image marquée I_w est *perceptuellement* similaire à I.

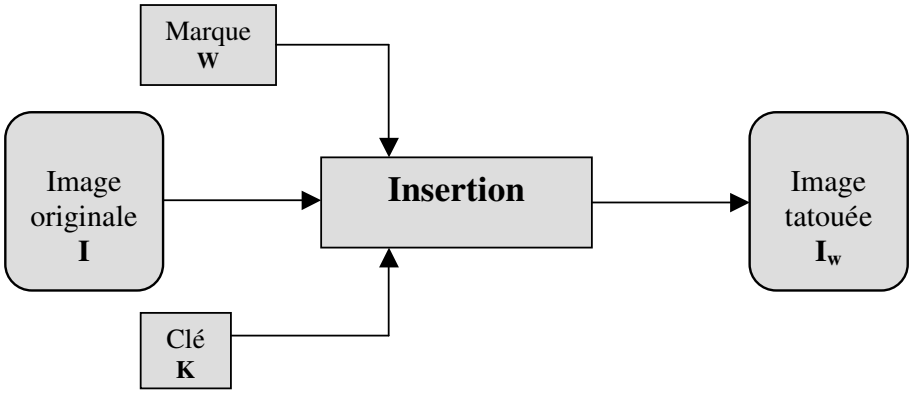


Figure 1.1 Schéma général de l'insertion d'une marque

La figure 1.2 présente un schéma général de détection de la marque. Cette phase est souvent effectuée sans utiliser l'image originale (*en aveugle*). Certains algorithmes nécessitent la connaissance de l'image originale et de la marque. A la détection, on extrait une marque W' ou bien un résultat d'une décision indiquant la détection ou non de la marque W dans l'image I_w.

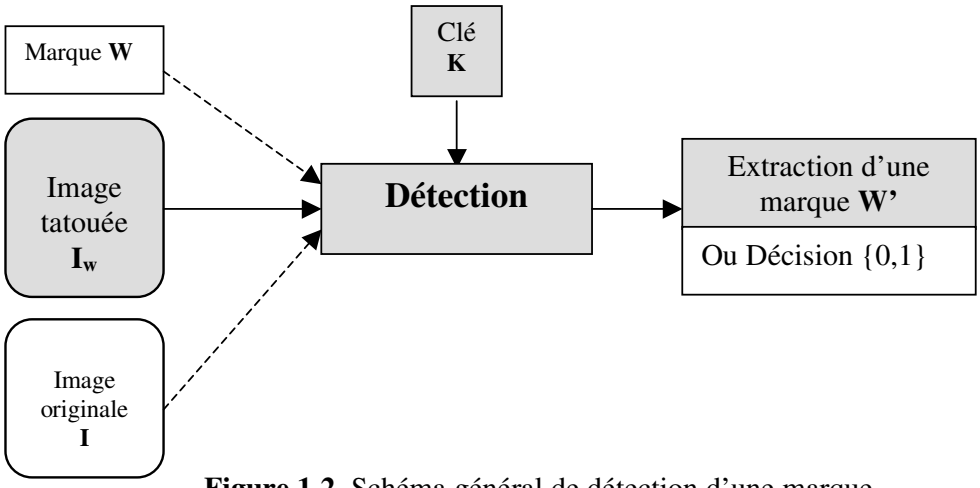


Figure 1.2 Schéma général de détection d'une marque

1.3 Quelques Applications du tatouage

Le tatouage numérique est considéré depuis quelques années comme une solution pour de nombreuses applications telles que la protection des droits d'auteur, l'intégrité des données multimédias, la prévention de la redistribution non autorisée, l'indexation et le renforcement du contenu. Dans ce qui suit, nous donnons un bref aperçu sur ces différentes applications.

1.3.1 La protection des droits d'auteur

La protection des droits d'auteur (*le copyright*) a été la première application envisagée pour le tatouage (en anglais le « Watermarking[1] ») de document. Le but du tatouage consiste ici en l'insertion d'une signature numérique qui atteste de l'identité du dépositaire du document. Cette signature ne doit être connue que de la personne ou de l'organisme qui a inséré le tatouage. Elle dépend donc d'une clé secrète qui permet son insertion et sa détection.

1.3.2 L'intégrité des données multimédias

La marque permet également de s'assurer que le contenu du document est *authentique* : il s'agit d'une marque fragile qui subit des distorsions si le document a été altéré. Elle est conçue de manière à se détériorer dès que le document est modifié.

1.3.3 La prévention de la redistribution non autorisée

Dans le but de contribuer à diminuer l'utilisation non autorisée des données digitales, le tatouage offre la possibilité d'identifier l'origine d'une copie illégale, en attribuant à chaque acheteur un numéro de série personnel (*le fingerprint*).

1.3.4 L'indexation des images

L'indexation des images consiste à classer de manière automatique des images selon leur contenu, en facilitant ainsi la recherche dans la base de donnée.

Le tatouage des images est aussi utilisé dans l'indexation. Il permet d'insérer une information décrivant le contenu de l'image ou bien un pointeur renvoyant vers une description plus complète.

[1] Le mot « Watermarking » recouvre plus précisément un tatouage invisible et robuste appliqué au service des droits d'auteur [3]

1.3.5 Le renforcement du contenu

Contrairement à un stockage simple d'informations dans l'en-tête du fichier associé à un document (image, video ou son), le tatouage est intimement lié aux données et donc théoriquement indépendant du format utilisé. Le tatouage de document rend aussi possible la transmission de plusieurs informations différentes dans un même canal.

1.4 Méthodes de tatouage existantes

Les algorithmes de tatouage d'images numériques dépendent des contraintes imposées par l'application (robustesse, degré de visibilité, temps de calcul, etc.). Nous pouvons distinguer les algorithmes les uns des autres selon les points suivants [2], [3]:

- Le type de schéma d'insertion de la signature ou la manière de mélanger intimement le message avec le signal hôte (modulation);
- La stratégie utilisée pour mettre en forme l'information à cacher ;
- Le choix de l'espace de travail.

1.4.1 Le type de schéma d'insertion de la signature

P.Bas [1] classifie les schémas de tatouage selon la façon dont la marque est inscrite dans l'image. Il distingue « les schémas additifs » qui consistent principalement à ajouter un "bruit" à l'image et "les schémas substitutifs"qui consistent à substituer la maque à des composantes de l'image. A. Manoury [4] utilise la terminologie de schémas "virtuels " au lieu de "substitutifs" en considérant que la marque n'est pas substituée, mais modifie les caractéristiques de quelques composantes de l'image.

1.4.2 La stratégie sur la marque

C'est la manière de transformer la signature (ou le message) en marque numérique et sa mise en forme par rapport à l'image à tatouer.

L'utilisation du modèle psychovisuel permet d'exploiter le système visuel humain (SVH) pour renforcer l'invisibilité du message à insérer. La méthode la plus facile est de tenir compte de l'activité de l'image : Les dégradations provoquées par le message à insérer seront faibles dans les zones homogènes de l'image et plus intenses dans les zones texturées pour lesquelles l'œil ne sera pas capable de faire la différence entre le signal provenant de l'image et celui provenant de la marque [4].

1.4.3 Le choix de l'espace de travail

La marque peut soit être insérée dans le domaine spatial, soit dans le domaine fréquentiel. Il existe aussi quelques méthodes originales pour l'insertion de la marque telle que la méthode basée sur les fractales.

a) Le domaine spatial

Les méthodes basées sur le domaine spatial consistent à insérer la marque directement dans l'image, en modifiant la luminance des pixels de l'image. Elles ont l'avantage d'être facilement implantables mais sont généralement peu robustes aux attaques.

Exemples de méthodes spatiales

- L'un des premiers algorithmes consiste à insérer la marque dans les bits de poids faibles ou les bits les moins significatifs (LSB) de la luminance de l'image. Cette technique, facile à implanter, a l'avantage de pouvoir insérer une grande quantité d'information au sein de l'image sans pour autant la dégrader, cependant, la marque insérée est très facile à enlever [5].

- La méthode du Patchwork proposée en 95 par Bender *et al.* [6], consiste tout d'abord à sélectionner, selon une clé secrète, une séquence de n pairs de pixels (A_i, B_i). Ensuite on augmente a_i de 1 et on diminue b_i de 1, avec a_i et b_i les valeurs de luminance respectives des pixels Ai et Bi. La somme S des différences donnera un résultat proche de 2n.

$$S = \sum_{i=0}^{n-1} (a'_i - b'_i) = \sum_{i=0}^{n-1} (a_i - b_i) + 2 \cdot n \qquad (1.1)$$

avec $a'_i = a_i + 1$ *et* $b'_i = b_i - 1$

Pour le pirate qui ne connaît pas les 2n paires choisies, la somme des différences pour 2n paires quelconques donnera, pour n assez grand, un résultat proche de 0.
Si l'image ne contient pas de marque, la somme S est également proche de 0.

- La méthode de l'étalement spectral permet de voir le problème du tatouage comme un problème de communication. L'image hôte est considérée comme un canal de transmission, la marque comme le message à transmettre et les attaques comme un bruit.

Hartung *et al.* proposent de construire une marque composée d'autant de blocs qu'il y a de bits à insérer. Chaque bloc est une séquence binaire pseudo aléatoire *S* composée de +1 ou –1. Pour insérer un 1 on ajoutera +*S*, cas échéant, on ajoutera –*S* [2].

Pour détecter la signature, il suffit donc de calculer l'intercorrélation de la marque W avec l'image marquée I_w . En effet, l'intercorrélation de la marque avec l'image I est négligeable par rapport à l'autocorrélation de marque.

$$<I_w,W> = <I+W,W> = <I,W> + <W,W> = \varepsilon + <W,W> \qquad (1.2)$$

Pour une marque différente W_1, on aurait $<I_w,W_1> = <I,W> + <W_1,W> = \varepsilon + \varepsilon$ (1.3)

b) Le domaine fréquentiel

Le principe des méthodes basées sur le domaine fréquentiel a été introduit par plusieurs auteurs tels que Cox *et al.* [7] et Koch *et al*. [8]. Il consiste à insérer la marque non pas directement dans l'image mais dans le domaine des transformées. Pour retrouver l'image marquée, on effectue la transformée inverse. Les auteurs de ces méthodes espèrent prévenir les attaques liées aux compressions avec perte [9].

Exemple de méthode fréquentielle

L'insertion du tatouage en utilisant la transformée en cosinus discrète (DCT) se fait en appliquant cette transformée à toute l'image et en insérant la signature dans les basses fréquences, c'est-à-dire dans les composantes les plus significatives. On applique la DCT inverse pour obtenir l'image tatouée. L'opération de détection est duale à celle de l'insertion.

c) Autres approches

- **Utilisation de la transformée en ondelettes**

L'intérêt de cette transformée est l'optimisation du choix des emplacements et la force du marquage de la signature dans l'image ainsi que son aspect multi-échelle qui offre une répartition plus robuste au tatouage [2].

L'outil "ondelettes" est présenté dans la section 3.2.2. Nous retrouvons un exemple de son utilisation dans la section 4.3.

- **Utilisation de la compression fractale**

Un objet fractal est une structure géométrique qui se reproduit sans fin à toutes les échelles. La compression d'images utilisant les fractales est une méthode de compression dans laquelle

les similarités au sein de la même image à différentes échelles, seront utilisées pour la compression [1].

Le tatouage basé sur l'utilisation de la compression fractale a été proposé en 1996 par J.Puate *et al*, l'objectif est de mettre à profit certaines propriétés d'invariance propres aux fractales afin de pouvoir prévenir certaines attaques tel que le zoom, et récupérer la marque sans recourir aux documents originaux [4].

1.5 Evaluation des algorithmes de tatouage

Il est difficile d'évaluer un algorithme de tatouage vu les multiples applications envisagées et les critères qui rentrent en jeu. Il est néanmoins possible d'identifier quelques éléments qui influencent l'évaluation du tatouage telles que la qualité de l'image et les attaques.

L'image tatouée doit être de la même qualité que l'image originale (imperceptibilité du tatouage), de plus, les attaques auxquelles doit être robuste le tatouage doivent conserver la qualité de l'image. Dans ce qui suit, nous présentons quelques métriques utilisées pour la mesure de la qualité de l'image tatouée ainsi que quelques exemples d'attaques.

1.5.1 Mesure de la qualité de l'image

Il n'existe aucun algorithme capable sans une image de référence de mesurer la qualité (ou le degré de dégradation) absolue d'une image. Cette mesure est basée sur la comparaison de pixels entre l'image originale et l'image tatouée. Parmi ces mesures nous retrouvons : l'entropie relative, l'erreur quadratique moyenne, l'erreur moyenne absolue et le rapport signal sur bruit.

a) L'entropie

L'entropie mesure la quantité d'information présente dans l'image. L'entropie relative ou bien la distance Kullback-Leibler [10], normalise l'entropie d'une image Im' en considérant l'image originale Im. Son expression mathématique est représentée par la formule (1.4):

$$m_c = p_k \sum_k \log_2 (p_k / q_k) \qquad (1.4)$$

Où p et q sont les densités de probabilité discrètes de Im' et Im respectivement sur k intensités de pixels.

Soit Im une image et Im' l'image marquée, m_c est supposée être faible dans le cas de similarité entre les deux images (S'il s'agit de la même image, m_c s'annule). m_c est élevée si les deux images diffèrent significativement.

b) L'erreur quadratique (MSE)

L'erreur quadratique compare deux images pixel par pixel. Son expression est :

$$m_s = \frac{1}{M\,N} \sum_i \sum_j \left(I(i,j) - I_w(i,j) \right)^2 \qquad (1.5)$$

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. Cette mesure nous donne une indication sur la dégradation introduite au niveau du pixel. Plus le MSE est grand, plus le niveau de dégradation est élevé.

c) L'erreur moyenne absolue (MAE)

L'erreur moyenne absolue est donnée par :

$$m_a = \frac{1}{M\,N} \sum_i \sum_j \left| I(i,j) - I_w(i,j) \right| \qquad (1.6)$$

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

d) 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 Signal to Noise Ratio), elles sont définies respectivement par les formules (1.7) et (1.8).

$$(SNR)_{dB} = 10 \log_{10} \left(\sum_{i,j} I^2(i,j) \;/\; \sum_{i,j} \left(I(i,j) - I_w(i,j) \right)^2 \right) \qquad (1.7)$$

$$(PSNR)_{dB} = 10 \log_{10} \left(MN \max_{i,j} I^2(i,j) \;/\; \sum_{i,j} \left(I(i,j) - I_w(i,j) \right)^2 \right) \qquad (1.8)$$

Deux images identiques produiront une valeur infinie de ces rapports.

e) Le PSNR pondéré

Aucune des mesures mentionnées ci-dessus ne prend en charge les différences du point de vue HVS (Système Visuel Humain). Ces mesures mathématiques sont basées sur une

comparaison pixel à pixel, alors que le système visuel humain tient compte du voisinage. La figure 1.3 représente deux images compressées par des techniques différentes. Elles ont la même valeur du PSNR mais possèdent des dégradations différentes [11].

Image compressée par Ondelettes- PSNR = 28,66 Image compressée par JPEG- PSNR = 28,65

Figure 1.3 Comparaison d'images avec le même PSNR [11]

Des mesures de la qualité visuelle des images ont été proposées ces deux dernières décennies, elles sont basées sur la modélisation du système visuel humain.

Le modèle de Watson a été conçu pour fournir une mesure qui représente la dégradation de l'image telle que perçue par le système visuel humain. Son but est de comparer les coefficients de la DCT dans un bloc d'image au seuil de sensibilité correspondant. Ce seuil est une fonction composée de sensibilité[2], masque de luminance et masque de contraste [10].

Voloshynovski *et al.* [1] ont définit une mesure appelée wPSNR (PSNR pondéré). Dans ce cas, l'erreur quadratique est pondérée par la variance de l'image de référence. L'expression du wPSNR est donnée par la formule (1.9):

$$w(\mathrm{PSNR})_{\mathrm{dB}} = 10 \log_{10} \left(MN \max_{i,j} \mathrm{I}^2(i,j) \Big/ \sum_{i,j} \left[\frac{\mathrm{I}(i,j) - \mathrm{I_w}(i,j)}{(1+ \mathrm{var_I}(i,j))} \right]^2 \right) \qquad (1.9)$$

f) Les mesures subjectives

En plus des méthodes précédentes, il serait aussi intéressant d'utiliser les critères subjectifs pour la mesure de la qualité des images. Les images, modifiées et originales sont présentées à

[2] La fonction de sensibilité est la dérivée de l'intensité de la dégradation. Cette dernière est définie dans [13] comme un rapport de variance de l'image sur la variance du bruit.

un groupe d'observateurs composé d'experts. La distance de présentation requise est de quatre fois la hauteur de l'écran. Le tableau 1.1 présente les appréciations possibles de la qualité de l'image [4], [12].

Note	Qualité
5	Excellente
4	Bonne
3	Assez Bonne
2	Médiocre
1	Mauvaise

Tableau 1.1 Appréciations possibles de la qualité de l'image

1.5.2 Les attaques

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors de son extraction [14]. Parmi ces types d'attaques citons:

a) Les attaques classiques

Les attaques classiques peuvent être simplement réalisées par un utilisateur de bonne foi lors de manipulations ou par des utilisateurs malveillants. Parmi ces attaques nous retrouvons [3]:

- L'addition de bruit;
- Le filtrage ;
- La compression avec pertes essentiellement JPEG et MPEG;
- La transformation géométrique (décalage, rotation, zoom, découpage);
- La conversion analogique / numérique;
- La composition de plusieurs images ;
- L'attaque « copier /coller » dans une image ;
- etc.

b) Les crackers [15]

C'est l'ensemble des attaques qui perturbe et désynchronise l'image et rende la marque très difficile à détecter sans recourir à l'image originale. Ainsi, le détecteur de la marque ne la retrouve pas au endroits attendus et conclu son absence. Parmi les outils actuellement disponibles qui réalisent une telle perturbation, le logiciel Stirmark[3].

[3] *Stirmark* est le premier et le plus célèbre des bancs de test. Il consiste à combiner plusieurs attaques pour tester la robustesse du tatouage.

c) La signature multiple [16]

La présence de plusieurs signatures sur l'image conduit à une ambiguïté dans la détection du propriétaire de l'image. Considérons l'exemple suivant :

Alice[4] a une image I, elle la marque avec une signature S et génère ainsi l'image I_w qu'elle rend publique. Bob marque à son tour l'image I_w avec une signature S' et obtient ainsi I'_w. Dans ce cas, Alice et Bob peuvent réclamer la paternité de cette image. Si Alice possède l'image I_w, elle peut montrer que cette image contient sa marque alors qu'elle ne contient pas la marque de Bob. Ce dernier par contre ne possède aucune image qui ne contient pas la marque de Alice, à condition que le tatouage d'Alice soit robuste.

d) D'autres attaques [11]

L'attaque de « collusion » a lieu lorsque plusieurs utilisateurs sont en possession de la même image qui contient des marques différentes (cas du fingerprint, section 1.3.3). La mise en commun de ces images permet de nombreuses opérations statistiques, et l'image résultante contiendra toutes les marques avec des amplitudes diminuées. Dans ce cas la détection sera perturbée.

L'attaque du « copiage » consiste à recopier une marque pour l'insérer dans une image non marquée. Cette dernière pourra être considérée alors comme l'image authentique. On retrouve ce problème- par exemple- dans les systèmes de télémédecine (voir section 2.2). Un médecin peut accéder à un serveur pour diagnostiquer une image de radiographie partagée sur le réseau Internet. Le médecin a besoin de vérifier l'origine de l'image (l'authenticité) à travers l'existence d'une marque déposée par des personnes autorisées.

1.6 Conclusion

L'objectif de ce chapitre était d'introduire quelques notions sur la technique de tatouage de documents numériques et des images en particulier. Les applications de cette technique sont multiples, et les contraintes qu'elle impose varient selon l'application envisagée. Les contradictions existantes entre ces contraintes rendent impossible la conception d'un algorithme universel adaptable à toutes les applications.

[4] Les prénoms Alice et Bob sont souvent utilisés en sécurité au lieu des lettres A et B.

Dans notre travail, nous nous intéressons à l'application du tatouage dans le domaine médical, et plus précisément, dans le domaine de la télémédecine. Nous présentons dans le chapitre suivant l'apport du tatouage pour les images médicales, les spécificités de ces dernières et les contraintes qui s'imposent notamment lors de la mise en réseau des images.

Chapitre 2
Le tatouage dans le domaine médical

2.1 Introduction

La télémédecine est la pratique de la médecine à distance. Elle comporte de nombreux avantages, en particulier pour les établissements de santé éloignés ou ruraux. Toutefois, elle comporte aussi des risques sur le plan de la sécurité et de la protection des données.

L'un des problèmes que peut rencontrer une image médicale transférée par Internet est sa manipulation non autorisée. A cet effet, le tatouage a été proposé pour augmenter la sécurité, l'intégrité des images médicales ainsi que la confidentialité des données du patient. Cependant, l'invisibilité de la marque pose un problème pour ce type d'images, car l'œil humain est très sensible aux contrastes dans les gris de faibles intensités. Les schémas de tatouages classiques ne s'adaptent donc pas tous aux images médicales étant donné que celles-ci ne doivent pas perdre d'information lors de l'insertion de la marque pour ne pas conduire à un diagnostic erroné. L'image tatouée doit rester visuellement identique à l'image originale.

L'objectif de ce chapitre est de présenter d'une manière succincte les problèmes de sécurité rencontrés lors de l'utilisation des images médicales numériques ainsi que l'apport de la technique de tatouage dans ce domaine.

2.2 Définition de la télémédecine

- **Définition 1** [17]

La télémédecine est un concept général qui couvre différentes applications en rapport avec la santé. Elle constitue un domaine nouveau en plein développement qui s'appuie sur plusieurs technologies pour mettre en oeuvre des approches médicales nouvelles. Selon l'Organisation mondiale de la santé (OMS), la télémédecine couvre l'utilisation d'informations et des techniques de communication dans les systèmes de santé qui ont recours à des soins donnés directement ou indirectement. Le plus grand avantage de la télémédecine réside dans l'accès aisé à des informations médicales n'importe où et n'importe quand. Un concept de base est le transfert d'informations à l'endroit où une décision ou une action est prise (on déplace donc l'information et pas le patient).

- **Définition 2** [13]

" L'essence de la télémédecine est l'échange d'information à distance, que l'information soit de la voix, une image, des éléments d'un enregistrement médical, ou les commandes d'un

robot chirurgical. Il est raisonnable de penser que la télémédecine est la communication à distance d'une information pour faciliter la pratique clinique."

2.3 La sécurité des données médicales

Le renforcement de la qualité et de l'efficacité médicale peut être effectué à travers le partage de l'information tout en prenant en charge la sécurité de l'information digitale. A cet effet, nous devons considérer essentiellement les points suivants[18] :

- **Confidentialité**

Les données privées relatives aux patients ou aux médecins ne doivent être révélées qu'aux personnes autorisées. Ceci nécessite l'utilisation de plusieurs techniques relatives à la sécurité (pare feu, cryptographie des flux, contrôle d'accès, tatouage des images, etc.)

- **Authentification ou Fiabilité**

Il s'agit de l'association d'une double vérification : l'intégrité et l'authenticité des données. L'image ne doit pas avoir été modifiée (*intégrité*) et doit être en adéquation avec l'identité du patient (*authenticité*).

- **Disponibilité**

Il s'agit de la surveillance et de la maintenance du système permettant de partager l'information médicale. Cette dernière doit donc être disponible à l'utilisateur autorisé.

2.4 Le rôle du tatouage au sein des applications de Télémédecine

L'image joue un rôle important et même vital dans le domaine médical et en particulier dans le domaine de la télémédecine. Que ce soit pour permettre un diagnostic, faciliter une intervention chirurgicale ou approfondir les connaissances d'une manière générale. De nombreuses techniques d'imageries différentes et complémentaires sont utilisées, citons à titre d'exemple: imagerie par résonance magnétique (IRM), scanner, échographie, rayons-X, scintigraphie, etc.

Une grande partie des applications liées à la télémédecine est basée sur l'utilisation d'un site web qui permet de faciliter d'une part, la communication entre les médecins ou entre le médecin et le patient à travers des moyens synchrones (discussion en ligne appelée *chat*) ou asynchrones (forums, e-mails) et d'autre part, de faciliter le partages des images médicales.

Plusieurs solutions informatiques existent pour assurer la sécurité dans les techniques de contrôle d'accès mais cette sécurité reste insuffisante devant des tentatives inlassables des pirates pour accéder aux sites web.

Le tatouage des images permet de contribuer à la sécurité des images médicales partagées, en offrant :

- la possibilité de vérifier l'intégrité et l'authenticité des données médicales,
- La possibilité de garder la confidentialité des données relatives au patient ou au médecin. En effet, cette confidentialité est aussi importante que l'intérêt de garder ces informations avec l'image.

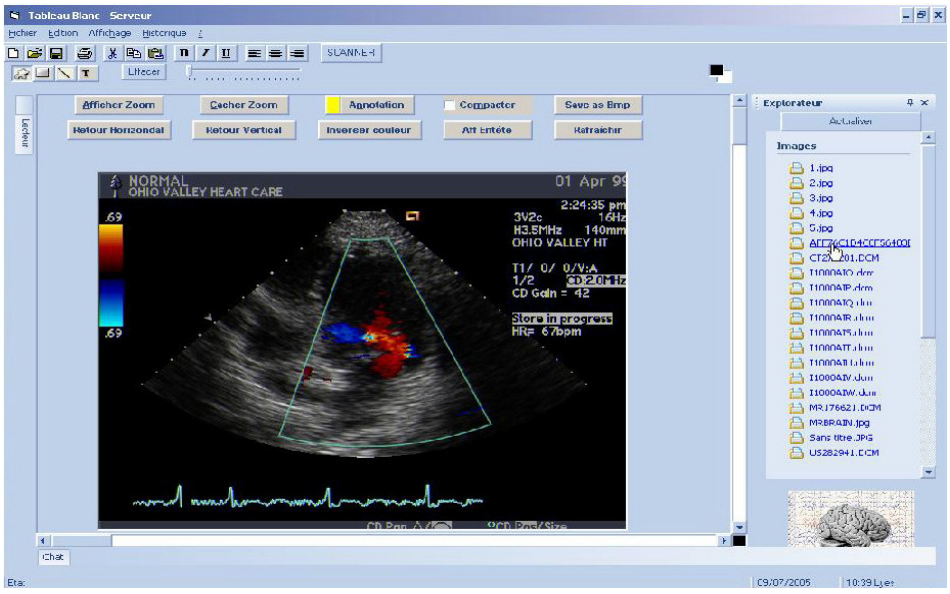


Figure 2.1 Interface offrant le partage d'images médicales
à partir d'un site web
Projet Télé-médecine- CDTA[1]

[1] Centre de Développement des Technologies Avancées (Alger)

2.5 Recommandations techniques pour les systèmes de télémédecine

L'ACR(American College of Radiologists) a fixé quelques recommandations techniques pour les systèmes de télémédecine visant à améliorer l'affichage de l'image médicale, parmi ces recommandations [13]:

1. Images de petit format – CT (image de scanner), IRM, ultrasons, médecine nucléaire et fluorographie[2] :
- Acquisition ou numérisation : au moins 500 x 500 pixels, définition sur 8 bits,
- Affichage : au moins 500 x 480 pixels, définition sur 8 bits.

2. Images de grand format - films radiographiques :
- Acquisition ou numérisation : une résolution spatiale minimum de 2,5 paires de lignes/mm et une acquisition en 1024 niveaux de gris (10 bits),
- Affichage : une résolution spatiale minimum de 2,5 paires de lignes/mm et une acquisition en 256 niveaux de gris (8 bits).

Il est recommandé que la téléconférence supporte le format vidéo CIF6 (Common Intermediate Format) de taille 352 x 288 pixels ou le format QCIF7 (Quarter CIF) de taille 72x88 pixels quand une faible qualité est acceptée.

2.6 L'utilisation des standards médicaux

Les standards médicaux permettent l'interopérabilité entre les systèmes et offrent la possibilité d'associer à l'image d'autres informations relatives au patient ou au médecin.

Dans les services de radiologie par exemple, où la production d'image est importante, il y a risque de perte des informations (nom du patient, diagnostic, etc.). Les formats standards, tel que le DICOM, permettent d'enregistrer les images médicales sur support numérique ainsi que toutes les informations textuelles associées

La norme DICOM (Digital Image Communications in Medicine) a été développée en 1992 par l'ACR et NEMA (National Electrical Manufacturers Association) afin de faciliter l'interconnexion des systèmes d'imagerie médicale aux réseaux.

[2] Voir Annexe: Les types d'images médicales

2.7 Exemple de méthodes de tatouage utilisées dans le domaine de l'imagerie médicale

2.7.1 Le tatouage multiple [19]

Le tatouage multiple consiste, d'une part, en l'insertion de données « d'annotation » cryptées qui contiennent généralement des renseignements sur le patient, la signature du médecin et éventuellement des commentaires et ceci en utilisant un tatouage robuste afin de sécuriser ces données et garder la confidentialité du patient, et d'autre part, en l'insertion d'une marque qui est effacée à la moindre manipulation du fichier, il s'agit d'un tatouage fragile.

La marque fragile est insérée au centre de l'image originale en utilisant la méthode des bits de poids faibles ou LSB (voir section 5.2). Dans cette méthode, la marque va couvrir toute l'image, à l'exception des bordures. Ces dernières sont laissées pour la marque robuste afin de minimiser la dégradation de l'image. La figure 2.2 présente un schéma d'insertion général de cette méthode de tatouage.

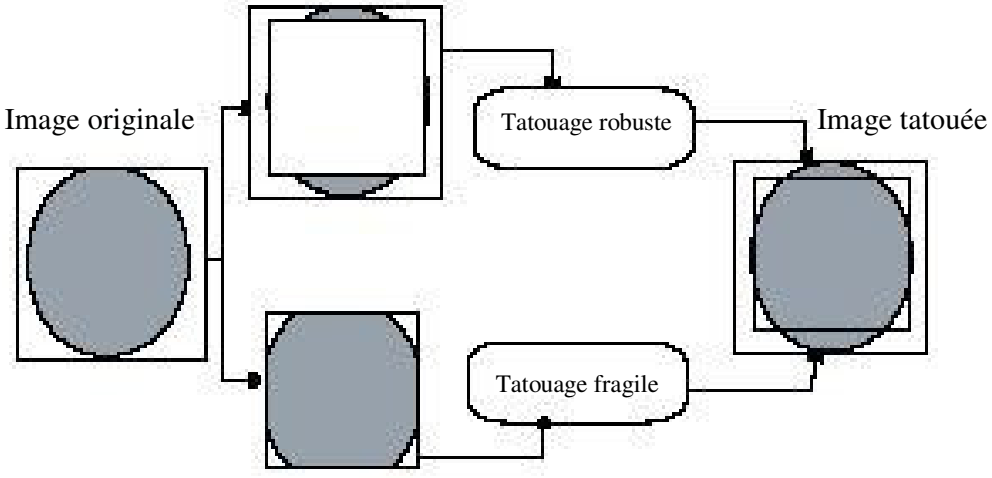
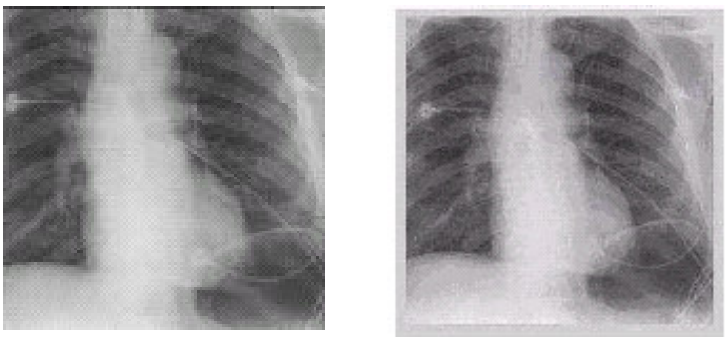


Figure 2.2 Schéma d'insertion d'un tatouage multiple [19]

Pour la marque d'annotation, elle est arrangée sous forme d'un cadre qui s'adapte à la bordure de l'image (voir figure 2.3), on l'insère ensuite d'une manière additive linéaire aux trois bandes les plus élevées de la transformée en ondelettes (voir section 3.2.2) appliquée sur la bordure de l'image originale, on applique ensuite la transformée en ondelettes inverse.



(a) (b)

Figure 2.3 Exemple d'image tatouée avec un tatouage multiple [19]
(a) Image originale, (b) Image tatouée

La détection des deux tatouages se fait séparément. La détection de la marque d'annotation suit quelques étapes de l'insertion. La bordure de l'image tatouée est décomposée en utilisant la transformée en ondelettes (DWT), la valeur de la corrélation est calculée en utilisant les trois coefficients passe bande les plus élevés. La marque fragile est détectée en utilisant la méthode de détection LSB.

Cette méthode permet la détection de la moindre manipulation de l'image médicale. L'insertion du tatouage d'annotation au niveau de la bordure évite la détérioration de la qualité de l'image, cependant, il reste possible de le détruire via des attaques malveillantes. Pour remédier à ce problème, il serait intéressant de tester l'insertion de cette marque au niveau des régions texturées de l'image.

2.7.2 Système d'authentification des images médicales basé sur un tatouage réversible[20]

La méthode présentée ci-dessous est la méthode de référence utilisée dans notre application pour la confidentialité des donnée du patient et la vérification de l'intégrité de l'image. Nous présentons ci-dessous les algorithmes d'insertion et de détection de tatouage ainsi que les résultats obtenus afin de pouvoir les comparer avec nos résultats.

L'objectif de cette méthode est de pouvoir :

- insérer une marque invisible dans l'image médicale. Cette marque contient généralement les données relatives au patient.
- Authentifier l'image sans ambiguïté.
- Obtenir une image marquée qui ne soit pas supérieure en taille à l'image originale.

- Récupérer l'intégrité de l'image originale à partir de l'image marquée

Cette méthode combine les outils de cryptographie avec un schéma de watermarking réversible. L'algorithme d'insertion est le suivant :

- Calculer l'empreinte de l'image pour les bits de poids forts (MSB).
- Concaténer l'empreinte de l'image avec les données du patient et crypter le résultat
- Sélectionner les LSBs de tous les pixels de l'image originale et leur appliquer la compression sans perte.
- Concaténer le résultat compressé avec les données cryptées et les réinsérer dans l'emplacement des LSBs.

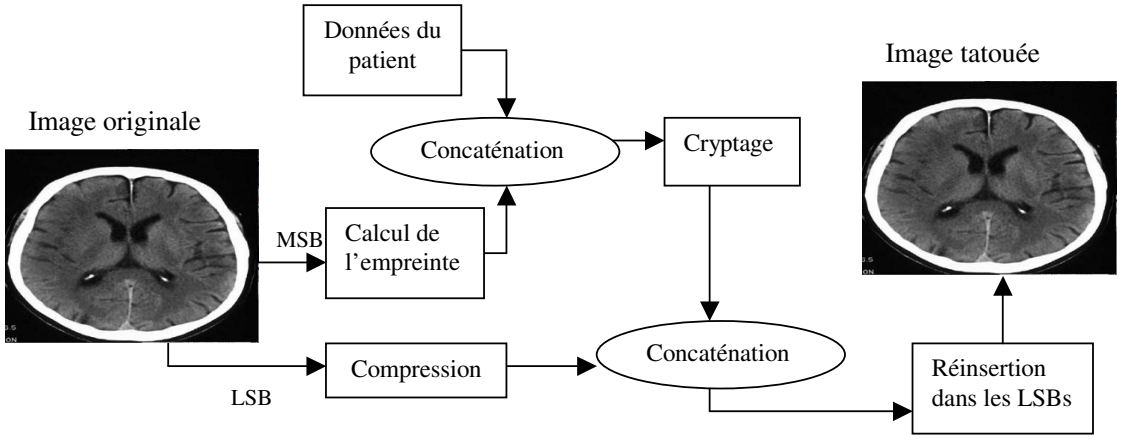


Figure 2.4 Schéma d'insertion du tatouage réversible **[20]**

- Les étapes de détection sont les suivantes :

- Extraire les données des LSBs
- Séparer les deux chaînes de caractères, contenant les LSBs compressés et la concaténation de l'empreinte avec les données du patient.
- Décompresser les données des LSBs et les remettre à leur emplacement pour récupérer l'image intégrale.
- Récupérer les données du patient et l'empreinte de l'image en appliquant un décodage de Vigenère.

Le contrôle de l'intégrité de l'image se fait en calculant l'empreinte de l'image et en la comparant avec l'empreinte extraite de l'image.

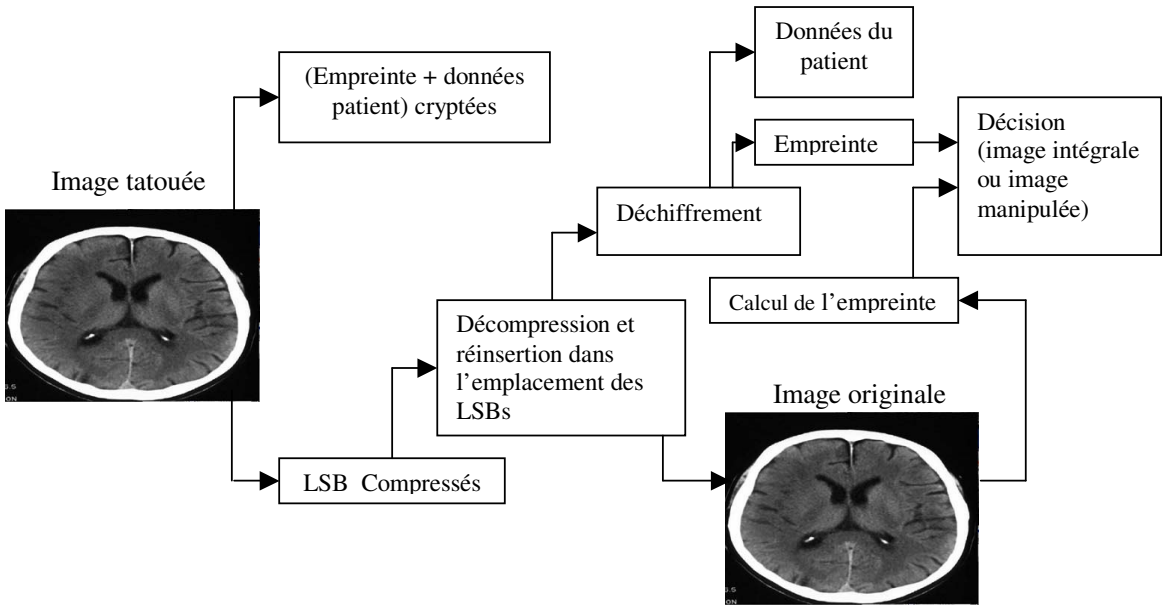


Figure 2.5 Schéma de détection du tatouage réversible **[20]**

- Résultats :

-Le format des données insérées

Données	**Nombre de caractère**
Nom	14
Prénom	14
Age	3
Sexe	1

Tableau 2.1 Format des données du patient (le tatouage réversible) **[20]**

- Calcul du PSNR

	Dimensions	**PSNR (dB)**
Image 1	256 x 256	39,72
Image 2	400 x 268	53,27
Image 3	512 x 512	41,33

Tableau 2.2 Taille des images de test et dégradation introduite par le tatouage réversible[20]

Figure 2.6 Images échographiques utilisées pour les tests
du tatouage réversible [20]

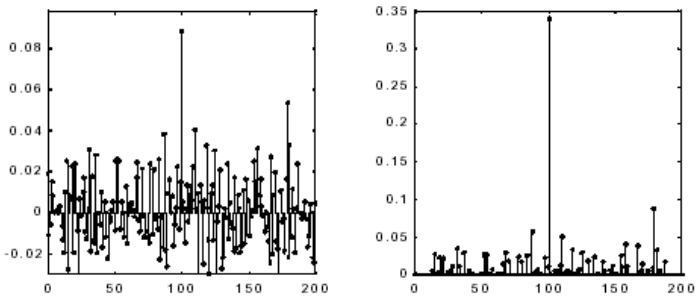
2.7.3 Tatouage des images médicales utilisant la transformation de Gabor [21]

La transformation de Gabor (voir section 3.2.2.b) est aussi utilisée pour obtenir une marque robuste et invisible.

Dans cette méthode, l'image est transformée en plusieurs blocs de coefficients de Gabor. La marque utilisée est un bruit gaussien pseudo aléatoire généré par une clé.

Tous les blocs de coefficients, à l'exception du premier, sont altérés selon la règle multiplicative connu dans la transformation de Gabor. Ceci conduit à un nombre important de coefficients ce qui facilite le processus de détection. Malgré ca, l'image garde une bonne qualité car le premier bloc qui n'est pas altéré contient une quantité d'information importante de l'image.

Il existe deux méthodes pour effectuer la détection, une méthode basée sur le calcul de la corrélation et une méthode basée sur le diagramme de similarité. Cette 2eme méthode s'adapte mieux à l'utilisation de la transformation de Gabor.



(a) (b)

Figure 2.7 Comparaison de détecteurs [21]
(a) Simple détecteur de corrélation
(b) Détecteur basé sur le diagramme de similarité

2.8 Conclusion

Le tatouage des images trouve une application dans la sécurité de l'image médicale numérisée, en particulier dans les applications de télé-médecine.

Plusieurs méthodes ont été proposées pour l'application du tatouage dans le domaine de l'imagerie médicale. Ces méthodes tentent de prendre en compte les spécificités de l'image médicale et adoptent différentes stratégies d'insertion de tatouage dans le but de minimiser sa dégradation, et ce en faisant appel à divers outils telles que la transformée de Gabor, la transformée en ondelettes, la compression sans perte et la cryptographie.

Dans le cadre de notre travail, nous nous intéressons essentiellement à l'authentification de l'image médicale et à la confidentialité des données du patient. Les différents outils auxquels nous ferons appel sont présentés dans le prochain chapitre.

Chapitre 3

Outils et algorithmes

3.1 Introduction

L'objectif de ce chapitre est de présenter les différents outils auxquels nous faisons appel dans les chapitres suivants afin d'insérer un tatouage dans l'image médicale. Dans la première méthode que nous décrirons ultérieurement (voir chapitre 4), nous utilisons l'outil de communication CDMA. Cette méthode vise à vérifier l'authenticité de l'image médicale. Nous utiliserons également l'outil Ondelettes pour étudier cette méthode dans le domaine de la transformée en ondelettes discrète (DWT) de l'image.

Dans une autre méthode (voir chapitre 5) utilisée dans le but de vérifier l'intégrité de l'image et d'assurer également la confidentialité des données de la source (patient ou médecin), nous empruntons du domaine de la cryptographie l'algorithme de Vigenère pour chiffrer les données ainsi que l'algorithme MD5 (Message Digest, version 5) pour calculer l'empreinte d'un message.

La présentation de ces outils n'est pas exhaustive. Il est recommandé de consulter des références plus spécialisées pour de plus amples détails.

Nous retrouvons les points abordés dans ce chapitre dans [22] et [2] pour la CDMA, [23], [4] et [24] pour les ondelettes, et enfin [25] et [26] pour la cryptographie.

3.2 Outils

3.2.1 La technique CDMA

L'Accès Multiple par Répartition de Codes ou CDMA (Code Division Multiple Access), est une technique de multiplexage utilisée initialement dans la communication numérique dans le cadre d'applications militaires.

Dans cette technique d'accès multiple, les utilisateurs partagent le même espace fréquentiel et transmettent sur les mêmes intervalles temporels.

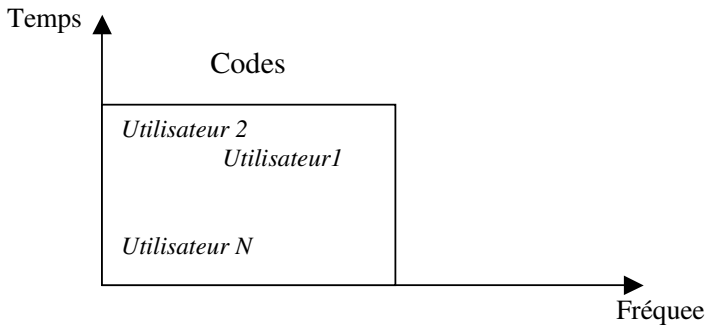


Figure 3.1 Schéma d'un multiplexage par code (CDMA)[2]

Il s'agit, dans ce cas, d'affecter à chaque émetteur un code, appelé aussi signature, qui lui permet de transmettre des informations en évitant d'interférer avec les messages provenant d'autres utilisateurs. La réduction des interférences d'accès multiples n'est obtenue que dans le cas de l'utilisation de séquences de codes strictement orthogonaux.

Le CDMA permet aux différents utilisateurs de transmettre leurs données sur n'importe quelle fréquence et sans nécessiter de synchronisation entre eux. La capacité de multiplexage du CDMA n'est limitée que par la capacité à générer un maximum de séquences de codes, celles-ci étant choisies de manières à minimiser les Interférences d'Accès Multiple

Dans cette technique, chaque bit de message à transmettre est modulé au niveau de l'émetteur par une séquence pseudo aléatoire [-1, 1, 1,-1, ….] ou son complément. Cette séquence correspond au code associé à chaque émetteur, chaque séquence étant orthogonale avec chacune des autres.

Le signal qui est transmis dans le canal est composé de la somme de signaux de chaque utilisateur. En réception, la corrélation avec les différents codes permet d'extraire les différents messages.

Les séquences aléatoires sont souvent représentées par « les *m-séquences* » (maximum length shift register sequence) . Ces séquences sont de longueur $L = (2^m - 1)$ bits et sont générées à partir de m registres à décalage avec bouclage (LFSR : Linear Feedback Shift Registers) comme illustré sur la figure 3.2. Les registres qui sont bouclés dépendent des coefficients de polynômes ″premiers″. Ces séquences sont périodiques de période *L*. Elles contiennent chacune (2^{m-1}) éléments égaux à (+1) et $(2^{m-1}-1)$ éléments égaux à (-1).

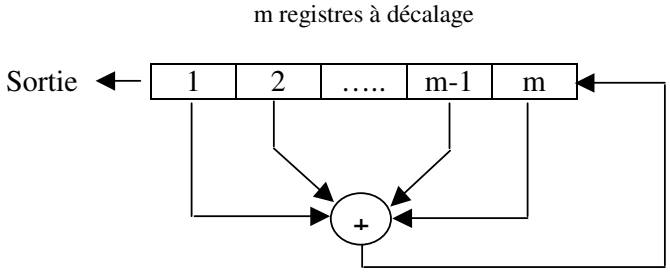


Figure 3.2 Génération d'une m-séquence [2]

Les m-séquences possèdent une bonne propriété de corrélation, la fonction d'autocorrelation vaut L en 0 et –1 partout ailleurs.

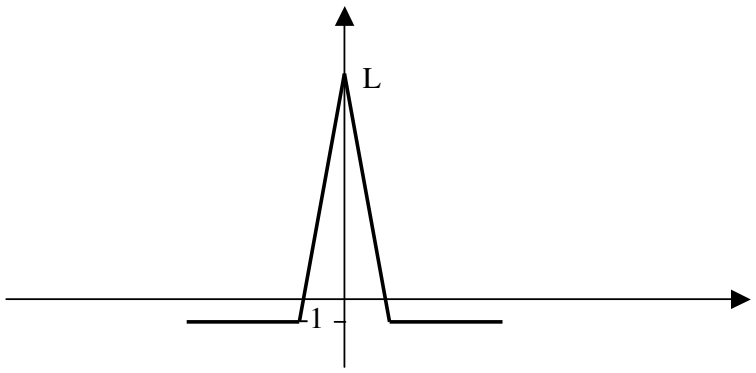


Figure 3.3 Fonction d'autocorrelation d'une m-séquence

3.2.2 Les ondelettes

a) La transformée de Fourier

La transformée de Fourier consiste à analyser une fonction ***f*** à l'aide d'exponentiels complexes. On note F la transformée de Fourier et $\overline{F}$ la transformée inverse.

$L^2(\Re)$ est l'espace des fonctions réelles à énergie finie sur l'ensemble des réels $\Re$.

Pour $f \in L^2(\Re)$; sa transformée de Fourier est définie par :

$$\hat{f}(\omega) = (Ff)(\omega) = \int_{\Re} f(t)\, e^{-2i\pi\omega t}\, dt \quad , \quad \omega \in \Re \qquad (3.1)$$

La transformée de Fourier inverse est définie par :

$$f(\omega) = (\overline{F} f)(t) = \int_{\Re} \hat{f}(\omega)\, e^{+2i\pi\omega t}\, d\omega \quad , \quad t \in \Re \qquad (3.2)$$

Le principe d'Heisenberg stipule qu'on ne peut obtenir à la fois une résolution infiniment bonne en temps et en fréquence : il y a un compromis à réaliser entre les deux.

On définit :

- La durée utile de la fonction *f*

$$\Delta t^2 = \frac{\int t^2 \, |f(t)|^2 \, dt}{\int |f(t)|^2 \, dt} \qquad (3.3)$$

- La bande utile de la fonction *f*

$$\Delta \lambda^2 = \frac{\int \omega^2 \, |\hat{f}(\omega)|^2 \, d\omega}{\int |\hat{f}(\omega)|^2 \, d\omega} \qquad (3.4)$$

Le principe d'incertitude donne la relation suivante entre ces deux quantités

$$\Delta t \, . \, \Delta \lambda \geq \frac{1}{4\pi} \qquad (3.5)$$

La localisation en temps (mesurée par Δt) se fait au détriment de la localisation en fréquence (mesurée par $\Delta\lambda$), et réciproquement. Le meilleur compromis autorisé par le principe d'Heisenberg ($\Delta t \, . \, \Delta\lambda = 1/4\pi$) est réalisé par une gaussienne.

La transformée de Fourier consiste à analyser une fonction à l'aide de sinusoïdes, or le support de cette fonction est infini, et de plus, ne privilégie aucun intervalle de temps. Toute information temporelle sur la fonction *f* (t) analysée est donc perdue. On dit que la transformation de *Fourier* est une transformation intégrale à caractère global.

b) La transformée de Gabor

Pour avoir des informations temporelles sur notre signal, une idée consiste à analyser le signal par morceaux. On applique la transformée de Fourier sur un intervalle [-A, A] du signal *f* (t); on peut donc situer ce qu'on analyse à une précision A. C'est le principe de la transformée de Fourier à fenêtre glissante appelée aussi la transformée de Gabor.

La transformée de Gabor revient à multiplier la fonction *f* par une fenêtre que l'on va déplacer sur toute la fonction. Prendre la fenêtre $w = \mathbf{1}_{[-A,A]}$ revient à *couper* simplement le signal en morceaux de taille 2A. *w* est définie ici comme une fenêtre réelle et symétrique, normalisée, de taille 2A.

On définit :

$$w_{\omega,t}(t)=w(t-b)e^{+2i\pi\omega t} \quad , \qquad \omega, b \in \Re \tag{3.6}$$

La transformée continue de Gabor s'exprime alors par la formule suivante :

$$G f(\omega,b) = \int_{\Re} f(t)\ \overline{w_{\omega,b}(t)}\ dt \quad , \quad \omega, b \in \Re \tag{3.7}$$

Ici, la fonction *f* est analysée à l'aide de la famille de fonction $w_{\omega,b}$ (t) . b désigne le point autour duquel l'analyse (de précision A) est faite, et donne donc une information temporelle ; ω donne la localisation fréquentielle, sa précision est proportionnelle à (1 / A) .

Bien que délivrant une information temporelle, la transformée de Gabor s'avère toutefois insuffisante pour certaines applications. Si l'on veut repérer, par exemple, l'apparition d'un choc, ou d'une singularité, dans un signal, on ne pourra être plus précis que la résolution 2A de la fenêtre : l'enveloppe est rigide.

c) La transformée continue en ondelettes

Une ondelette est une fonction ψ de $L^2(\Re)$ qui vérifie la condition d'admissibilité :

$$\int_{\Re+} \frac{|\psi(\omega)|^2}{|\omega|} d\omega = \int_{\Re-} \frac{|\psi(\omega)|^2}{|\omega|} d\omega < +\infty \tag{3.8}$$

L'ondelette mère ψ, génère une famille d'ondelettes constituée de ses dilatées et de ses translatées :

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\ \psi\left(\frac{t-b}{a}\right) \quad , \quad a \in \Re^+ \ , \ b \in \Re^- \tag{3.9}$$

La transformée en ondelettes continue d'une fonction $f \in L^2(\Re)$ est donnée par la formule :

$$C_f(a,b) = \int_{\Re} f(t)\ \overline{\psi_{a,b}(t)}\, dt = (f, \psi_{a,b})_{L^2} \quad , \quad a \in \Re^{+*}, b \in \Re \tag{3.10}$$

$C_f(a,b)$ est la famille des coefficients d'ondelette.

b est le paramètre de translation, l'ondelette ayant été déplacée pour être centrée sur b : c'est donc le point autour duquel l'analyse se fait. a est le paramètre d'échelle, il décide de la finesse de l'analyse ; plus a est grand, plus $\psi_{a,b}$ est dilatée, et plus l'analyse se fait sur une large zone de f.

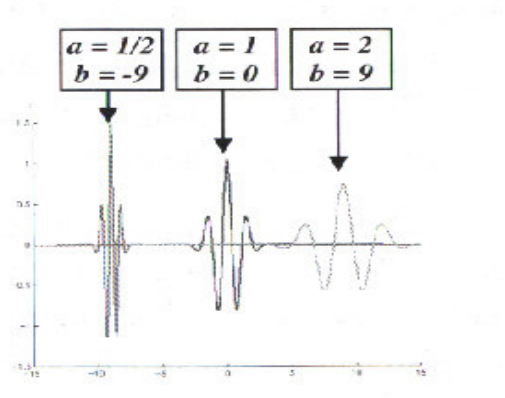


Figure 3.4 Translation / dilatation d'une ondelette [23]

- **Exemples d'ondelettes**

L'ondelette de Haar

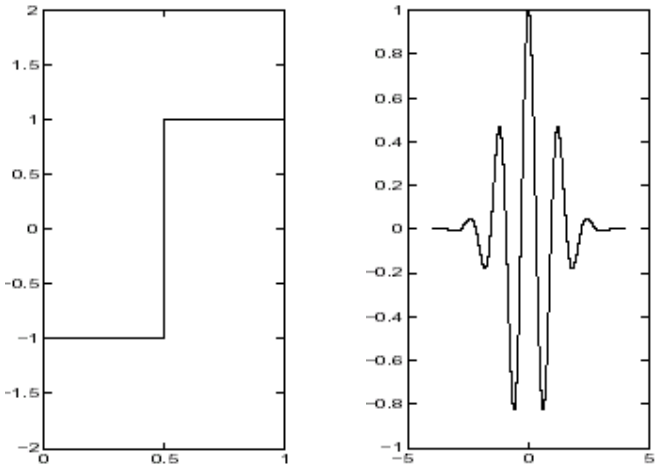
C'est la plus simple des ondelettes : définie sur l'intervalle [0,1] (ou parfois sur [-1/2 , 1/2]), c'est la fonction H constante par morceaux qui vaut :

$$H(x) = \begin{cases} 1 \quad si \quad x \in [0, 1/2] \ , \\ -1 \quad si \quad x \in [1/2, 1] \end{cases} \qquad (3.11)$$

L'ondelette de Morlet

Il s'agit de la gaussienne modulée

$$\psi(t) = e^{-\pi t^2} e^{2i\pi k_0 t} \qquad (3.12)$$



(a) (b)

Figur

$$\hat{f}(\omega) = (Ff)(\omega) = \int_{\mathbb{R}} f(t)\, e^{-2i\pi\omega t}\, dt \quad , \quad \omega$$

d) La transformée discrète en ondelettes

On considère :

$$a \in \{a_0^p\} \text{ et } b \in \{n a_0^p b_0\}_{p,n \in Z} \text{ avec } a_0 > 1, \quad b_0 > 0 \qquad (3.13)$$

La famille d'ondelettes $\Psi_{a,b}(t)$ devient :

$$\Psi_{p,n}(t) = a_0^{-p/2}\, \psi(a_0^{-p} t - n b_0) \qquad p, n \in Z \qquad (3.14)$$

La transformée discrète en ondelettes de la fonction *f*, avec $f \in L^2(\Re)$ est donnée par la formule :

$$C_f(p,n) = \int_{\Re} f(t)\, \overline{\psi_{p,n}(t)}\, dt = (f, \psi_{p,n})_{L^2} \quad , \quad p, n \in Z \qquad (3.15)$$

La transformée en ondelettes dyadique est obtenue en posant $a = 2^j$, $j \in Z$

La transformée en ondelettes discrète peut être obtenue par l'analyse multirésolution abordée dans le point suivant.

e) L'analyse multirésolution

Une analyse multirésolution (AMR) de l'espace des signaux d'énergie finie de $L^2(\Re)$ consiste en une suite de sous espaces fermés emboîtés $(V_j)_{j=-\infty \ldots +\infty}$ ($\ldots \subset V_2 \subset V_1 \subset V_0 \subset V_{-1} \subset \ldots$)

de $L^2(\Re)$, dont l'intersection est réduite à {0} et l'union dense dans de $L^2(\Re)$. Ces espaces sont déduits de l'espace V_0 par contraction (pour j<0) ou dilatation (pour j>0) :

$$f(t) \in V_j \Leftrightarrow f(2t) \in V_{j-1} \quad \text{pour} \quad j \in Z$$

Et enfin, Il existe une fonction φ de V_0 qui engendre V_0 :

$$V_0 = \{ f \in L^2(\Re) \mid f(t) = \sum_{k \in Z} e_k \varphi(t-k) \ , \ (e_k) \in l^2(Z) \}$$

$l^2(Z)$ est l'espace des suites de carré sommable.

Les {*Vj*} servent d'espace d'approximation.

j s'appelle la résolution et représente le niveau d'analyse de la fonction *f*; l'approximation dans V_j de *f* est deux fois plus fine que celle dans V_{j-1}, mais deux fois moins bonne que celle dans V_{j+1}.

A l'opposé de l'espace d'approximation {*Vj*}, on définit l'espace de détails {*Wj*}, ou *Wj* est le supplémentaire orthogonal dans V_{j-1} :

$$V_j = V_j \oplus Wj \quad \text{et} \quad V_j \perp Wj$$

Les *Wj* contiennent l'information de détails nécessaires pour passer d'une approximation d'une résolution à une approximation de résolution supérieure. Le signal est la somme de ces détails.

Les *Wj* forment une base orthonormée d'ondelettes de $L^2(\Re)$, ils sont engendrés par $\{\psi_{j,k}\}_{k \in Z}$ et V_j sont engendré par les $\{\varphi_{j,k}\}_{k \in Z}$.

Dès la fin de 1980, un algorithme de décomposition/ reconstruction rapide a été proposé par Mallat. Il établit le lien entre les bases orthonormées d'ondelettes et les bancs de filtre classiques en traitement de signal.

Selon l'algorithme rapide de Mallat, quatres filtres sont utiles pour calculer les coefficients : deux sont associés à la fonction d'échelle φ et les deux autres sont associés à la fonction ψ.

La suite h détermine les filtres associés à φ et la suite g détermine ceux associés à ψ.

$$\varphi_{j+1,0} = \sum_{k \in Z} h_k \ \varphi_{j,k} \quad , \quad \psi_{j+1,0} = \sum_{k \in Z} g_k \ \psi_{j,k} \qquad (3.16)$$

f) Généralisation à deux dimensions

En traitement d'image, les ondelettes orthogonales sont très utilisées car elles conduisent à des calculs rapides.

Dans le cas de signaux d'une dimension (1D), on dispose des deux fonctions φ et ψ et des deux filtres associés. Le signal est décomposé en une approximation et un détail. En deux dimensions (2D), l'image est décomposée en une approximation et trois détails ((horizontal, diagonal et vertical). La fonction d'échelle et les trois ondelettes agissent sur le plan :

$\varphi(x,y) = \varphi(x)\,\varphi(y)$, permet de définir les approximations

$\psi_1(x,y) = \psi(x)\,\varphi(y)$, permet de définir les détails horizontaux

$\psi_2(x,y) = \psi(x)\,\psi(y)$, permet de définir les détails diagonaux

$\psi_3(x,y) = \varphi(x)\,\psi(y)$, permet de définir les détails verticaux

Les deux filtres (basse et haute fréquence) utilisés en 1D sont utilisés également en 2D en les appliquant successivement sur les lignes puis les colonnes de la matrice associée à l'image.

Dans la figure 3.6, les approximations, indexées par niveau (L1,L2 et L3), représentent des versions de plus en plus grossières d'une image médicale radiographique.

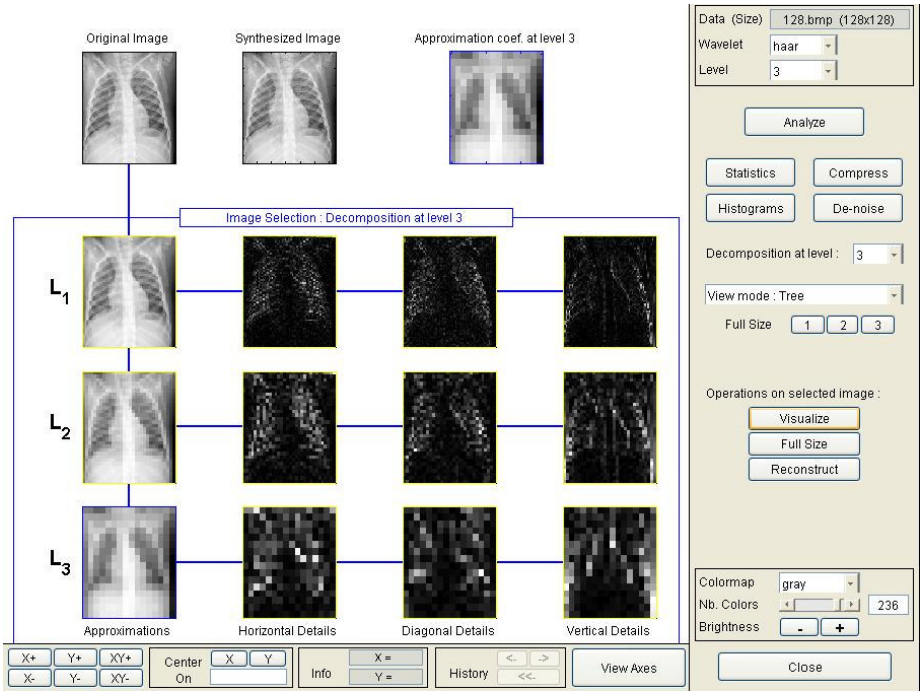


Figure 3.6 Décomposition en ondelettes d'une image médicale par l'ondelette de Haar

3.2.3 Cryptographie

a) Les algorithmes de chiffrement

Le chiffrement est l'application de transformations à un message pour le rendre incompréhensible. Le *déchiffrement* est l'action qui permet de reconstruire le *texte en clair* à partir du texte chiffré.

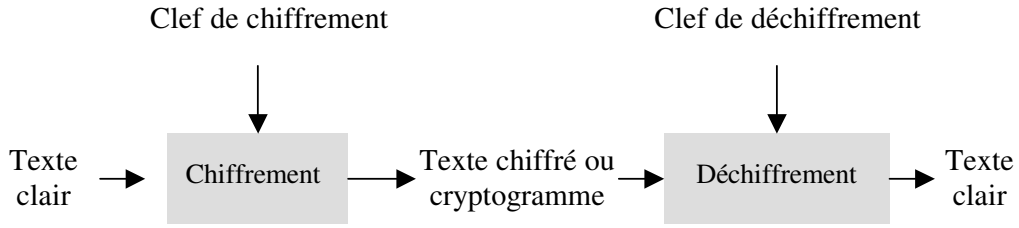


Figure 3.7 Principe de base de la cryptographie

Voici un exemple des algorithmes de chiffrement :

L'algorithme de Vigenère est un algorithme de chiffrement inventé par le français Braise de Vigenère. Un message est dissimulé par cet algorithme en utilisant un tableau appelé « le carré de Vigenère ».
Le carré de Vigenère est composé de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder (voir figure 3.8).

Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire. On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé. Pour coder, on regarde dans le tableau l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé.

Exemple: chiffrons le texte "TATOUAGE DES IMAGES" avec la clef "CRYPTO" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair). Pour coder la lettre T avec la clef C, on regarde dans le tableau l'intersection de la ligne donnée par T, et de la colonne donnée C, on retrouve la lettre V.

Texte Clair	T	A	T	O	U	A	G	E	D	E	S	I	M	A	G	E	S
Clef	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T
Texte codé	V	R	R	D	N	O	I	V	B	T	L	W	O	R	E	T	L

Tableau 3.1 Exemple d'un chiffrement de Vigenère

En supposant que le mot clé contienne un nombre m de lettres distinctes, un caractère alphabétique du texte clair peut être transformé en m caractères différents. Un tel procédé est dit poly-alphabétique. En général, il est impossible d'utiliser une analyse statistique simple pour retrouver le texte clair.

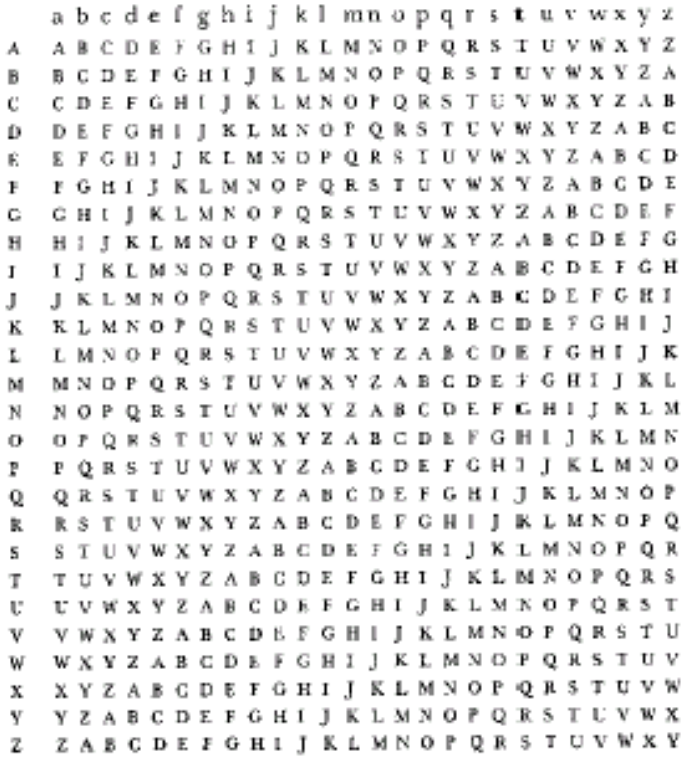


Figure 3.8 Le carré de Vigenère

b) Les fonctions de Hachage

Une fonction de hachage, aussi appelée fonction de condensation, est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe ; la chaîne résultante est appelée *empreinte* (*digest* en anglais).

Dans le cas d'une fonction de hachage à sens unique, il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile d'engendrer des chaînes à partir d'une empreinte donnée, et donc de déduire la chaîne initiale à partir de l'empreinte. La fonction de hachage est dite sans collision, c'est à dire qu'il est impossible de trouver deux messages ayant la même empreinte.

Voici un exemple des fonctions de hachage :

L'algorithme MD5 (Message Digest, version 5) est une fonction de hachage cryptographique qui permet d'obtenir pour chaque message une empreinte numérique avec une probabilité très forte que, pour deux messages différents, leurs empreintes soient différentes.
L'empreinte du fichier est une valeur de 128 bits correspondant à une somme de contrôles calculée à partir du fichier et qui permet la vérification de l'intégrité des données téléchargée.

MD5 travaille avec un message de taille variable. Le message est divisé en blocs de 512 bits, on applique un remplissage (*padding*) de manière à avoir un message dont la longueur est un multiple de 512. Le remplissage se présente comme suit :

- on ajoute un '1' à la fin du message
- on ajoute une séquence de '0' (le nombre de zéros dépend de la longueur du remplissage nécessaire)
- on écrit la taille du message, un entier codé sur 64 bits

Après un traitement initial, MD5 manipule le texte d'entrée par blocs de 512 bits divisée en 16 sous-blocs de 32 bits. La sortie de l'algorithme est un ensemble de 4 blocs de 32 bits (A, B, C et D) qui, joints ensemble, forment une seule empreinte de 128 bits.

La boucle principale a 4 rondes. Chaque ronde consiste en 16 exécutions d'une opération. Chaque opération calcule une fonction non linéaire de trois des variables A, B, C et D. Ensuite elle ajoute au résultat la quatrième variable, un sous bloc du texte à chiffrer et une constante. Ce nouveau résultat est ensuite décalé circulairement vers la gauche d'un nombre

variable de bits et ensuite ajouté à l'une des variables A, B, C ou D. Enfin, ce dernier résultat remplace l'une de ces variables pour les opérations suivantes.

Les fonctions non linéaires utilisées pour chaque ronde :

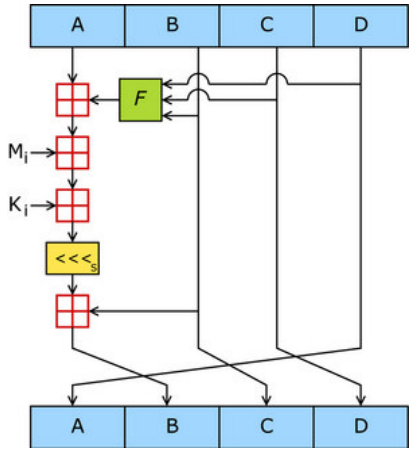


Figure 3.9 Une opération de MD5

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

$\oplus, \wedge, \vee, \neg$ symbolisent respectivement les opérations booléennes XOR, AND, OR et NOT.
Les quatre opérations des quatre rondes sont comme suit :

- R1 (A,B,C,D,Mi,Ki) équivaut à A = B + ((A + F(B,C,D) + Mi + Ki) <s)
- R2 (A,B,C,D,Mi,Ki) équivaut à A = B + ((A + G(B,C,D) + Mi + Ki) <s)
- R3 (A,B,C,D,Mi,Ki) équivaut à A = B + ((A + H(B,C,D) + Mi + Ki) <s)
- R4 (A,B,C,D,Mi,Ki) équivaut à A = B + ((A + I(B,C,D) + Mi + Ki)<s)

Mi représente le ième sous bloc du message (i allant de 0 à 15).
<s représente le décalage circulaire à gauche de s bits
Ki représente les différentes constantes.
Les variables A, B, C et D sont initialisées par les valeurs :
A= 0x67452301
B= 0xEFCDAB89

C= 0x98BADCFE

D= 0x10325476

Exemples:

- La valeur de l'empreinte de l'image représentée dans la figure 3.10, par l'algorithme MD5 est : 6B2295E255DCC7239C01F5CCAE89331B

- La valeur de l'empreinte de la chaîne de caractère «TatouageDesImagesMédicales » est : 9DAA4C9FD4508D9F3B994A135E384D3C

En changeant la lettre « M » du mot « Médicales »par un « m » en minuscule, on obtient une valeur de l'empreinte suivante : E6EB8D7251E79AAA7B97AEC908177D58
Cette valeur – toujours calculée par le MD5- est très différente de la valeur précédente malgré qu'il y a eu changement d'un seul caractère.

Figure 3.10 Exemple d'une image radiographique,
format BMP, codée sur 8 bits,
de dimensions 512 x 512

3.3 Conclusion

Dans ce chapitre nous avons présenté quelques outils utiles dans notre application. En effet, l'outil CDMA et les séquences pseudo-aléatoires seront utilisés pour l'insertion d'un tatouage robuste utile pour la vérification de l'authenticité de l'image, quant aux outils de cryptographie, ils seront utilisés pour renforcer la sécurité des données à travers l'insertion d'un tatouage fragile qui vise d'une part, à préserver la confidentialité des données de la source (patient ou médecin) et d'autre part, à vérifier l'intégrité de l'image. Ces deux méthodes sont présentées dans les prochains chapitres.

Chapitre 4
Authenticité de l'image

4.1. Introduction

La méthode proposée par Vassaux [2] vise à augmenter le nombre de bits du message à insérer dans l'image sans pour autant la dégrader visuellement. Cette méthode, appelée « méthode multicouche » est basée sur le principe du CDMA (voir section 3.2.1). Elle est robuste aux attaques de traitement d'image (filtrage, compression, rééchantillonnage, etc.) et à la compression jusqu'à un taux de 50%.

Dans ce chapitre nous présentons cette méthode et son application à l'image médicale dans le but d'identifier l'origine d'une image médicale à travers la signature de "l'établissement de santé" ou du médecin. La méthode sera testée dans le domaine spatial et dans le domaine de la transformée en ondelettes discrete.

Notre objectif est d'insérer dans l'image médicale une marque de 64 bits, suffisante pour vérifier l'authenticité de l'image, sans pour autant la détériorer et en déduire l'applicabilité de cette méthode, initialement conçue pour la protection du copyright, dans le domaine de l'imagerie médicale.

Les tests seront effectués sur trois types d'images médicales, des images IRM (Images par Résonance Magnétique), radiographiques et échographiques, codées sur 256 niveaux de gris, format BMP.

Les mesures de la qualité de l'image nous permettront de faire une étude comparative quant à l'adaptabilité de cette méthode à ces trois types d'images.

4.2. Description de la Méthode Multicouche

4.2.1 Principe de la méthode

L'insertion et la détection dans le domaine spatial suivent les étapes citées ci-dessous:

a) Découpage de l'image en blocs

L'image est découpée en blocs selon le nombre de bits du message à insérer. Pour insérer, par exemple, 8 bits dans l'image, on la découpe en 8 blocs.

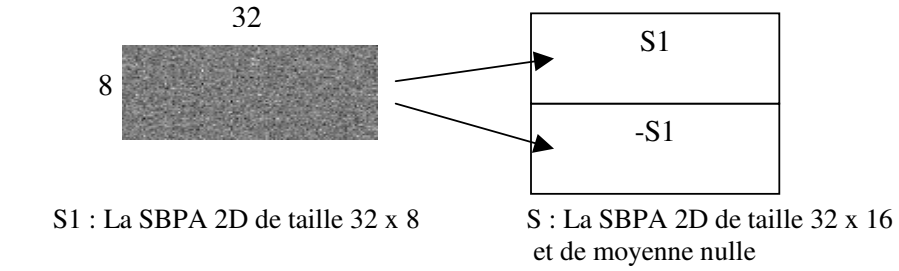
b) Génération d'une Séquence Binaire Pseudo Aléatoire (SBPA)

Une SBPA est générée à l'aide d'une clé secrète. Cette séquence est composée uniquement de +1 et de –1 et a une moyenne nulle.

La SBPA est d'abord transformée en une séquence à deux dimensions. Par exemple, pour une SBPA 2D de taille 32 x 16, on génère une SBPA de taille 512 échantillons et ensuite on remplit la première ligne de la marque par les 32 premiers échantillons, la deuxième par les 32 suivants et ainsi de suite jusqu'à la 16 ème ligne.

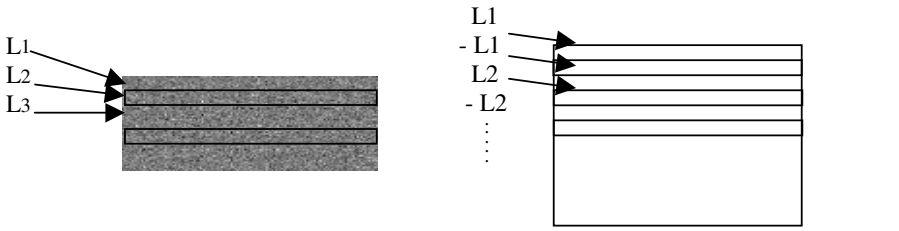
Pour générer une SBPA 2D de taille 32 x 16, de moyenne nulle, qu'on appelle S, on génère une SBPA 2D de taille 32 x 8 (S1) et on remplit la deuxième moitié par –S1 comme illustré dans la figure 4.1 (a).

Une deuxième méthode consiste à créer une SBPA 2D (S1) de taille 32 x 8 et à remplir ensuite les lignes paires de S par les « Li » lignes de S1, les lignes impaires de S seront remplies par «-Li » comme illustré dans la figure 4.1 (b).



S1 : La SBPA 2D de taille 32 x 8 S : La SBPA 2D de taille 32 x 16 et de moyenne nulle

(a)



S1 : La SBPA 2D de taille 32 x 8 S : La SBPA 2D de taille 32 x 16 et de moyenne nulle

(b)

Figure 4.1 Génération d'une SBPA 2D de moyenne nulle

c) Modulation du message à insérer

Les blocs obtenus suite au découpage de l'image sont remplis par S. Si un bloc correspond au bit « 1 » du message, on le remplit par + S et s'il correspond au bit « 0 », on le remplit par -S.

d) Ajout de la marque à l'image

La marque est insérée à l'image selon le schéma représenté dans la figure 4.2.

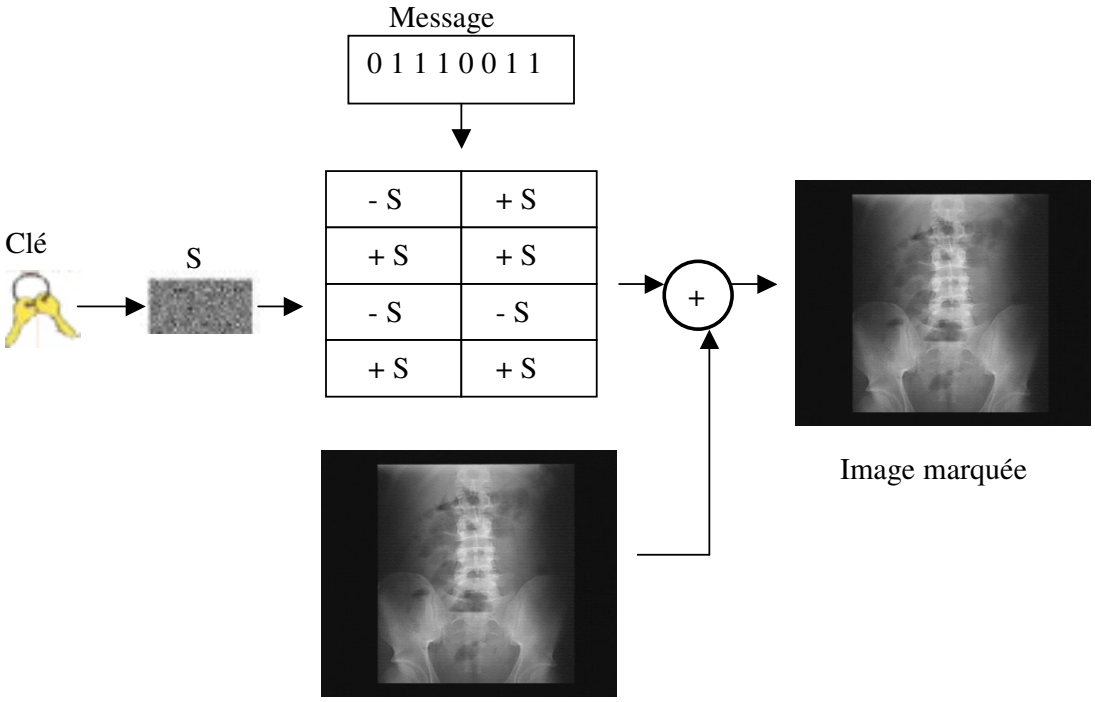


Figure 4.2 Insertion du tatouage par un découpage en blocs

e) Masques psychovisuels

Le masque psychovisuel est utilisé pour pondérer la signature selon les propriétés de masquage local de l'image. Dans notre cas nous utilisons le calcul de la variance locale : pour chaque pixel p(x,y) de l'image, on calcule la variance sur un bloc *B* de taille 3x3, centré sur le pixel :

-	-	-
-	p(x,y)	-
-	-	-

La variance d'un bloc B_i :

$$VarB_i(x,y) = \frac{1}{9}.\sum_{u=x-1}^{x+1}\sum_{v=y-1}^{y+1}\left(B_i{}^2(u,v) - (\frac{1}{9}.\sum_{u_1=x-1}^{x+1}\sum_{v_1=y-1}^{y+1}B_i(u_1,v_1))^2\right)$$

La variance est normalisée en la divisant par la valeur maximale des variances et multipliée ensuite à la SBPA 2D.

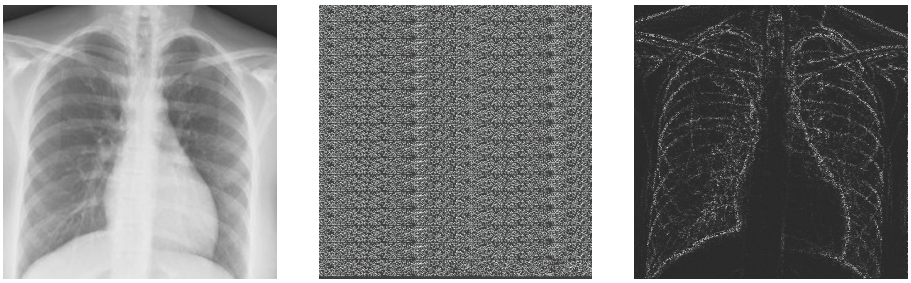


Image originale Marque sans masque Marque avec masque

Figure 4.3 Utilisation du masque psychovisuel

f) Visibilité du tatouage

La dernière étape consiste à multiplier la SBPA 2D par un facteur α qui permet de régler la puissance de la signature. La marque ainsi formée peut être insérée dans le domaine spatial (directement dans l'image) ou dans le domaine DWT.

g) La détection de données insérées

Pour détecter les données sur l'image marquée, on effectue la corrélation de S avec chaque bloc de l'image marquée. La marque ayant une moyenne nulle, on peut considérer que l'intercorrélation de la marque avec l'image est négligeable par rapport à l'autocorrélation de la marque. Pour détecter la signature, il suffit donc de calculer l'intercorrélation de la marque avec l'image marquée. Si le résultat est positif on considérera que le bit associé à ce bloc est 1, dans le cas contraire on choisira 0.

Soit :

I l'image originale, W la marque, W_1 une marque différente,

I_w l'image marquée , $I_w = I + W$

En supposant que la taille de ces images soit m x n, la détection suit alors l'étape suivante :

Calcul de l'intercorrélation: $<I_w,W> = <I+W,W> = <I,W> + <W,W>$

$$= \varepsilon + m \times n \quad (\text{avec } \varepsilon << (m \times n)) \tag{4.1}$$

Pour une marque différente on aurait $<I_w,W_1> = <I,W> + <W_1,W>$

$$= \varepsilon + \varepsilon << <I_w,W> \tag{4.2}$$

rappelons que le calcul de corrélation en 0 entre deux images I(m,n) et J(m,n) avec $1 \leq m \leq M$ et $1 \leq n \leq N$, est :

$$<I, J> = \sum_{m=1}^{M} \sum_{n=1}^{N} I(m,n) \times J(m,n) \tag{4.3}$$

4.2.2 L'apport de la technique CDMA

Dans la méthode de référence citée ci-dessus, les dimensions de la SBPA 2D sont inversement proportionnelles au nombre de bits à insérer, et plus les dimensions de la SBPA 2D sont petites, plus il devient difficile de détecter les différents bits du message.

La technique CDMA en communication propose de mélanger plusieurs signaux à l'émission pour différencier les différents signaux à la réception, la détection se fait par un calcul de corrélation. A partir de là, Vassaux [2] a proposé « la méthode multicouche » dans le but d'augmenter le nombre de bits à insérer sans pour autant dégrader l'image. En effet, au lieu d'insérer le message sur une seule couche, il est étalé sur plusieurs couches en superposant plusieurs marques pour former la marque définitive.

Dans le cas où la même SBPA 2D est affectée à deux couches une erreur de détection pourrait en suivre si la SBPA 2 D d'un bloc est retranchée avec le second, c'est la raison pour laquelle on affectera pour chaque couche une SBPA 2D dépendante d'une clé unique.

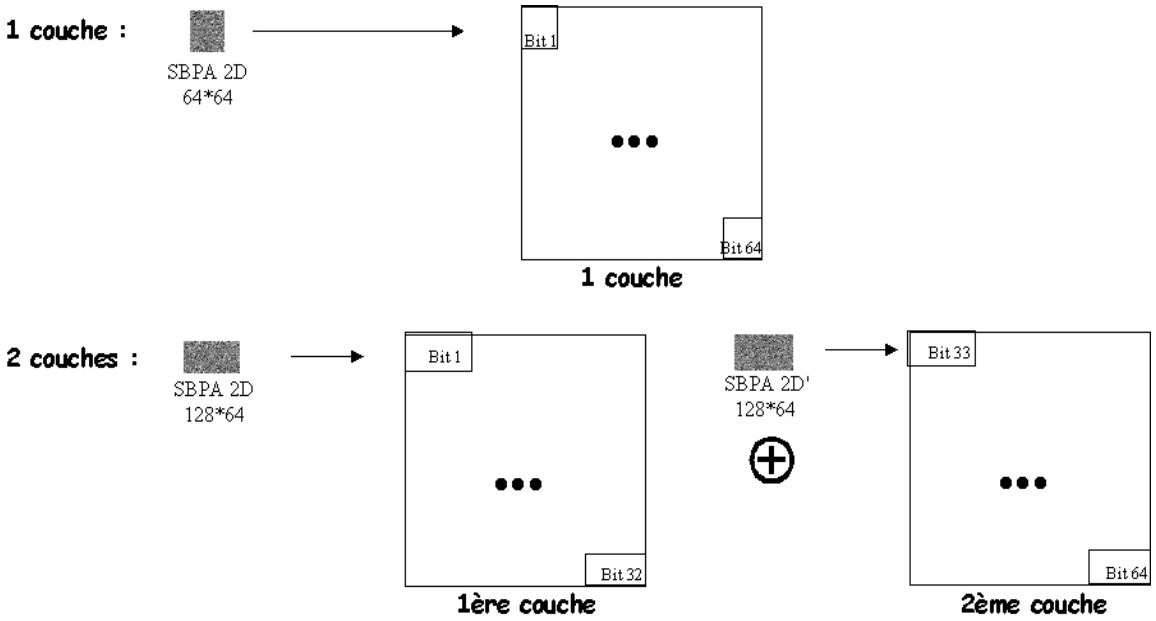


Figure 4.4 Construction de la marque dans un schéma multicouche à une et à deux couches avec 64 bits insérés [2]

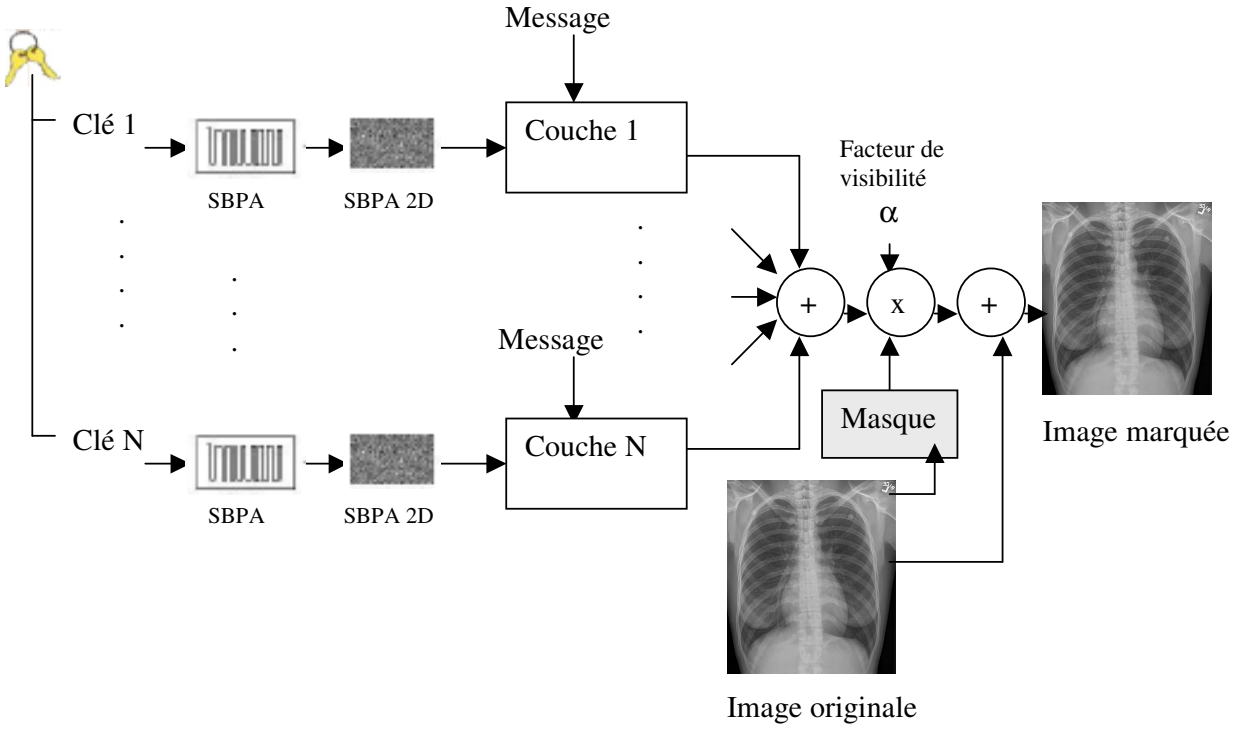


Figure 4.5 Schéma d'insertion de la méthode multicouche

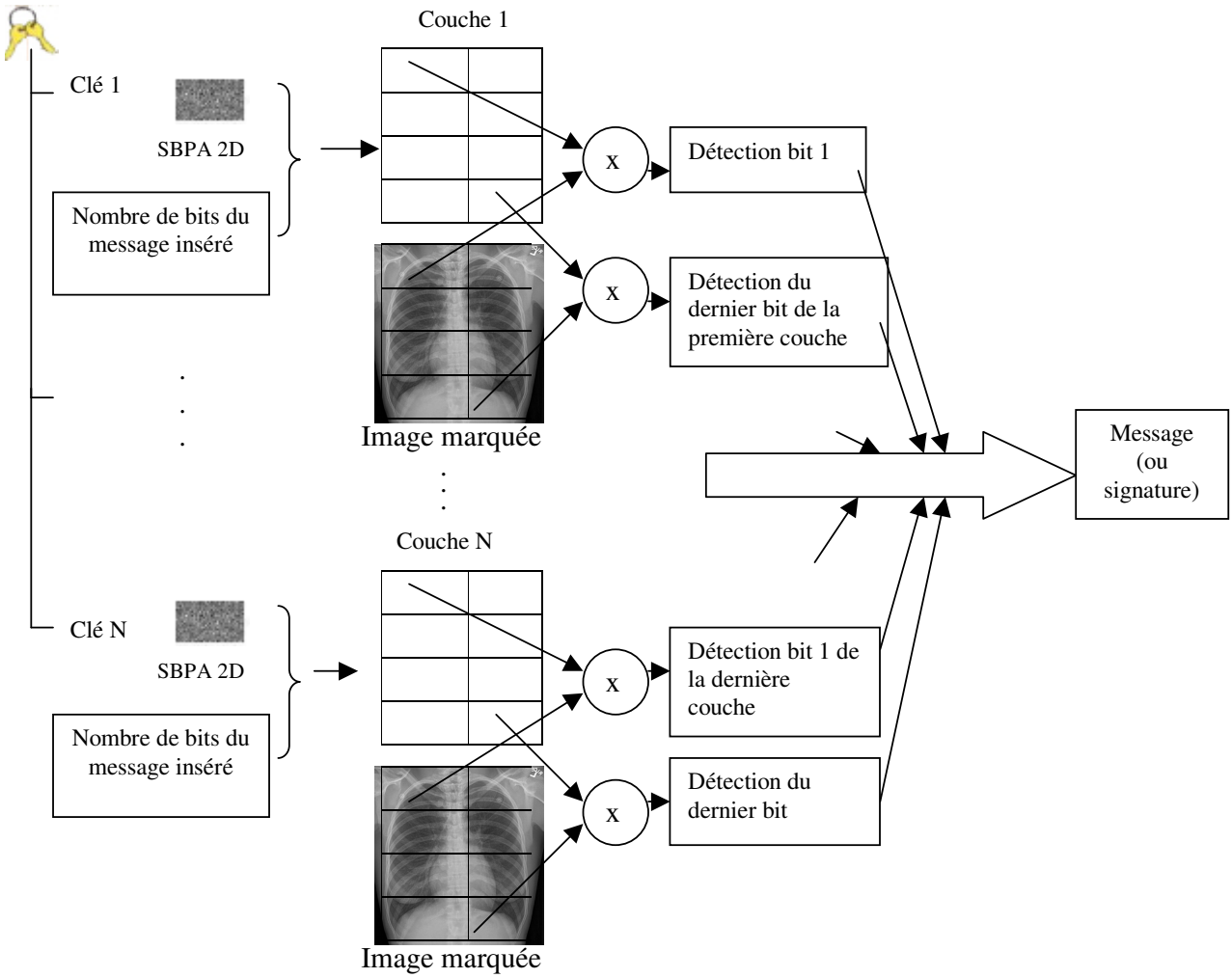


Figure 4.6 Schéma de détection de la méthode multicouche

4.3 Application de la méthode multicouche dans le domaine DWT

Le schéma d'insertion est un schéma additif. Les étapes d'insertion restent les mêmes, cependant l'insertion se fera dans les détails horizontaux, verticaux et diagonaux de l'image (voir section 3.2.2.f) après sa décomposition par la transformée en ondelettes discrète.

4.3.1 Algorithme d'insertion

L'algorithme d'insertion est le suivant

- Génération de la séquence multicouche à l'aide d'une clé K.
- Génération de la marque W.
- Décomposition de l'image par DWT en un niveau de résolution.

$$DWT\ (I) = (IA,DH,DV,DD),$$

avec IA : image approximative, DH: détail horizontal, DV: détail vertical et DD: détail diagonal.

- Insertion de la marque dans les 3 détails de l'image décomposée (diagonal, vertical et horizontal). La marque est pondérée par le coefficient α. Nous obtenons les trois détails marqués :

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

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

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

Remarquons que la marque doit avoir la même taille que les détails.

- Reconstruction de l'image décomposée qui donnera l'image marquée I', à l'aide de la transformée en ondelettes discrète inverse IDWT :

$$I' = IDWT\ (IA,DH',DV',DD').$$

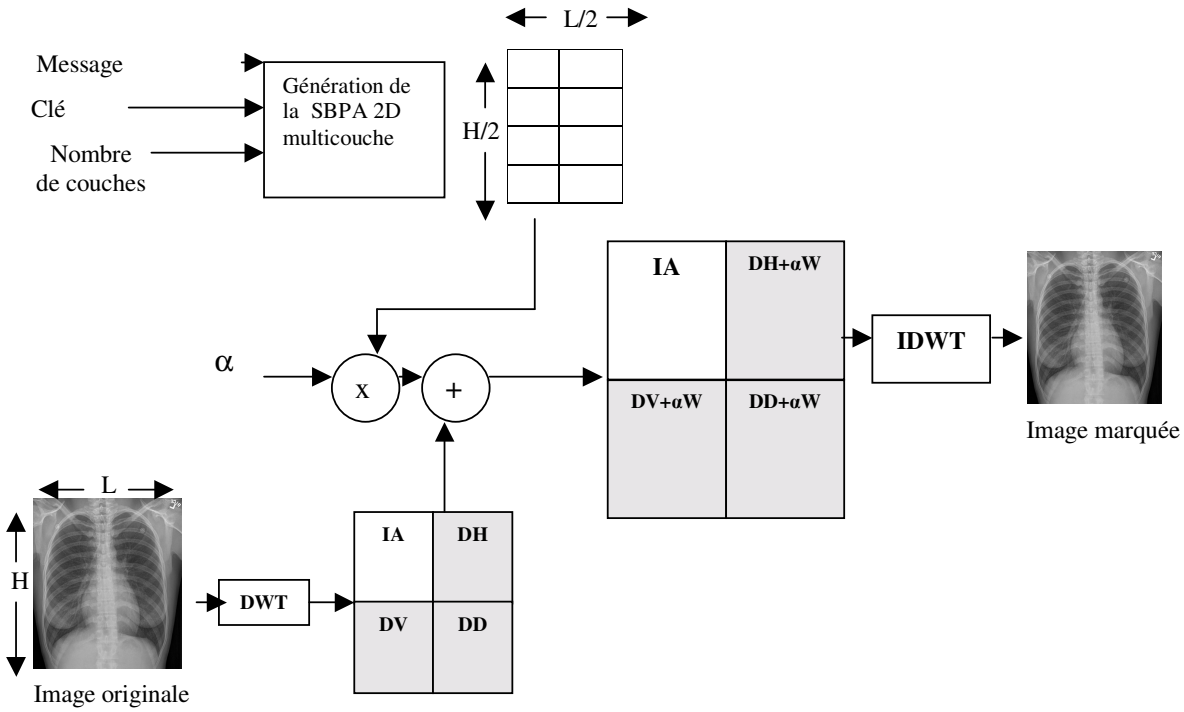


Figure 4.7 Schéma d'insertion dans le domaine DWT (méthode multicouche)

4.3.2 Algorithme de détection

La détection de la marque se fait de la même manière que dans le domaine spatial, mais le calcul de corrélation se fait entre la séquence multicouche et chaque détail de l'image décomposée.

L'algorithme de détection est le suivant :

- Génération de la séquence multicouche avec la même clé d'insertion K.
- Décomposition de l'image par la DWT en un seul niveau de résolution.
- Calcul de la corrélation entre la séquence multicouche et les trois détails de l'image décomposée puis le message est décodé selon le signe de la corrélation.

Les données recherchées sont donc extraites trois fois ce qui nous permet de les vérifier et éventuellement de les corriger.

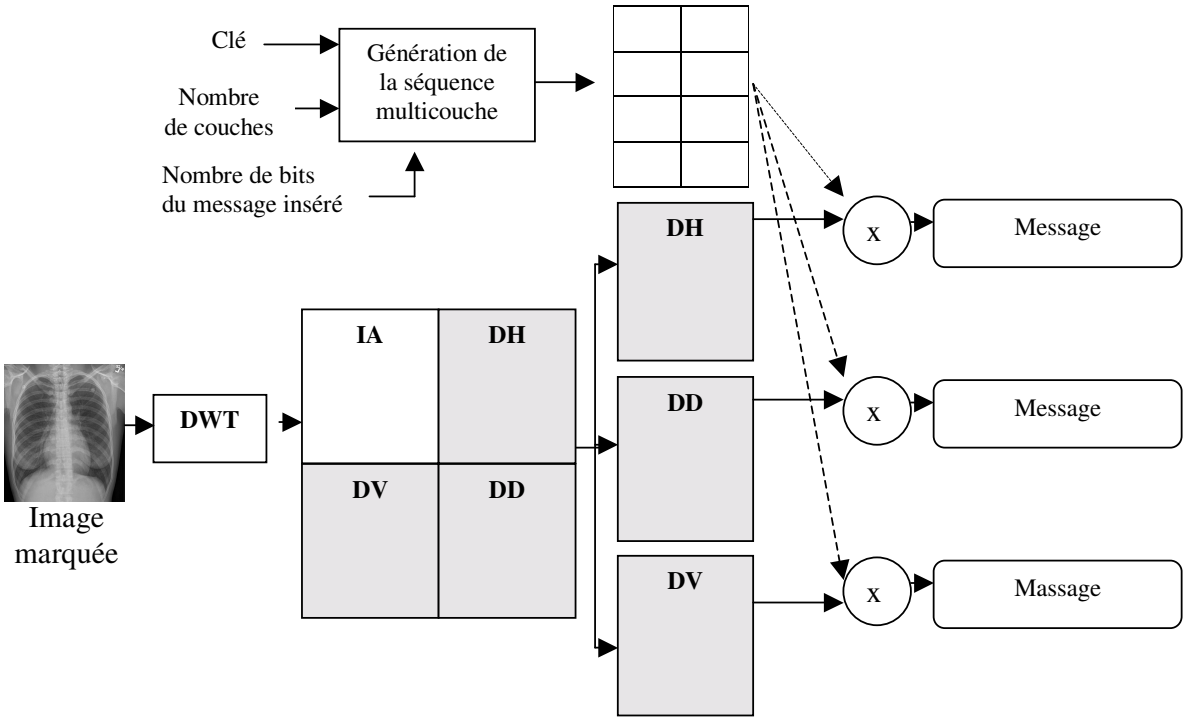


Figure 4.8 Schéma de détection dans le domaine DWT (méthode multicouche).

4.4. RESULATS

4.4.1 Résultats obtenus dans le domaine spatial

Les tests ont été effectués sur trois types d'images médicales (IRM, radiographie, échographie) codées sur 256 niveaux de gris, format BMP, de taille 512 x 512.

L'algorithme a été implémenté en C++ sur une machine P IV cadencée à 2 Ghz, 256 Mo de RAM sur un système d'exploitation Windows XP.

a) Exemples des images utilisées pour les tests

Nous avons effectué les tests sur trois types d'échantillons d'images médicales :

Echantillon 1 : 10 images radiologiques

Echantillon 2 : 10 images échographiques

Echantillon 3 : 10 images IRM

La figure 4.9 présente quelques unes de ces images.

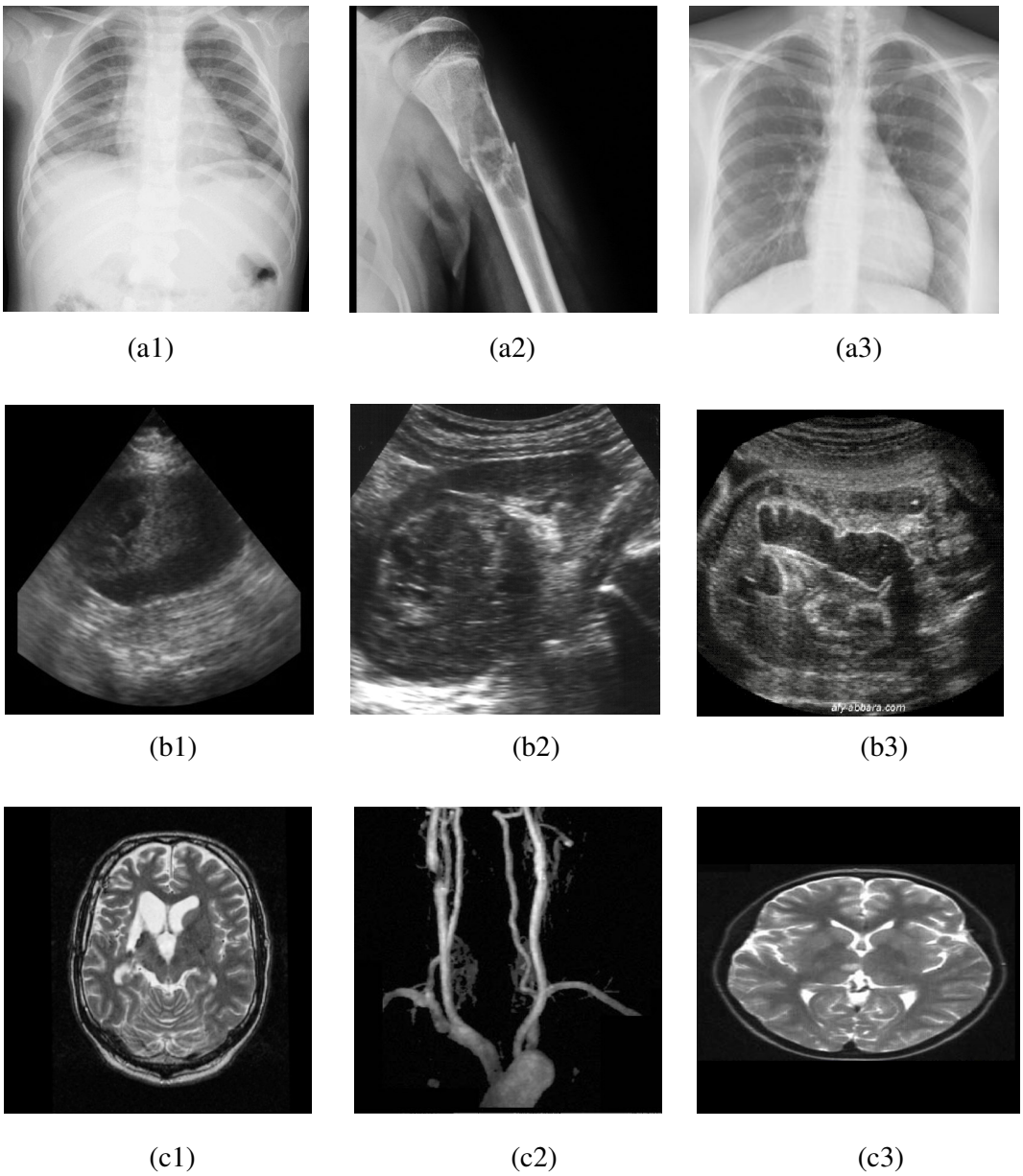
b) Insertion et détection des données

- Pour insérer la signature, l'utilisateur doit remplir les champs de saisie suivants :
  - La signature (64 bits)
  - La clé secrète
  - Le nombre de couches utilisées

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

- Pour détecter les données du patient, l'utilisateur doit avoir :
  - L'image marquée
  - La clé
  - Le nombre de couches utilisées
  - Le nombre de bits insérés

Dans le cas où les trois types d'échantillons d'images n'auraient subi aucune attaque, la détection d'une signature de 64 bits se fait avec succès dans le cas de l'utilisation de 2, 4 et 8 couches et ce en choisissant le coefficient de visibilité adéquat.



(a1) (a2) (a3)

(b1) (b2) (b3)

(c1) (c2) (c3)

Figure 4.9 Exemple d'images médicales

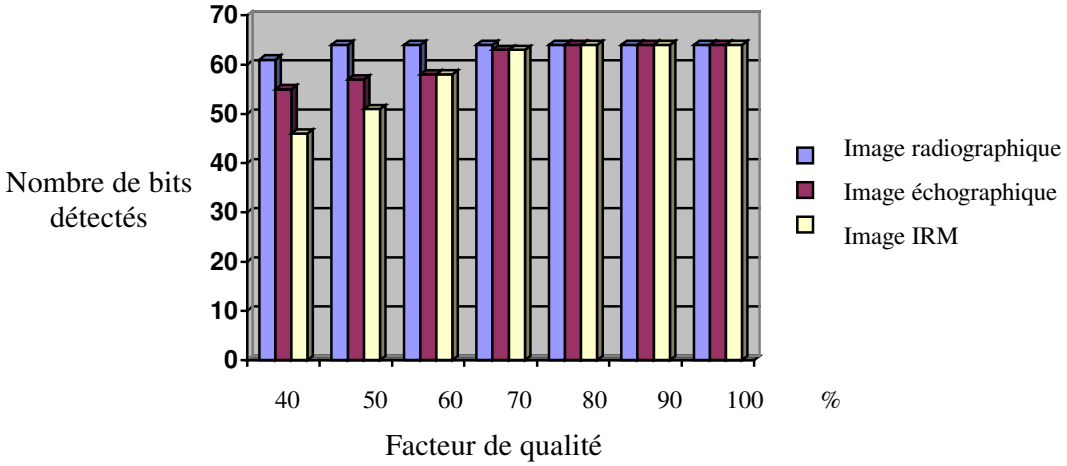
(a1), (a2) et (a3) : Images radiologiques

(b1), (b2) et (b3) : Images échographiques

(c1), (c2) et (c3) : Images IRM

c) Robustesse du tatouage à l'attaque de compression JPEG

L'attaque de compression JPEG a été testée sur les trois types d'images médicales tatouées avec un message inséré de 64 bits, 8 couches et un coefficient de visibilité de 0.3. Les tests effectués montrent que l'augmentation du taux de compression (diminution du facteur de qualité) entraîne une diminution du nombre de bits détectés. De plus, les images radiographiques semblent être plus robustes à l'attaque JPEG que les images échographiques ou IRM (graphe 4.1).



Graphe 4.1 Nombre de bits détectés en fonction du facteur de qualité de la compression JPEG

d) Qualité de l'image

Nous avons calculé le wPSNR des images tatouées en faisant varier le nombre de couches ou le coefficient de visibilité. Nous avons également comparé la qualité de l'image en insérant un tatouage avec ou sans masque. Les graphes 4.2, 4.3 et 4.4 indiquent les résultats obtenus pour les trois types d'images de la figure 4.10.

Rappelons que le wPSNR permet de quantifier numériquement la visibilité de la marque en prenant en considération la variance de l'image. Plus le wPSNR est grand, moins la marque est visible dans les zones texturées (à variance élevée) de l'image.

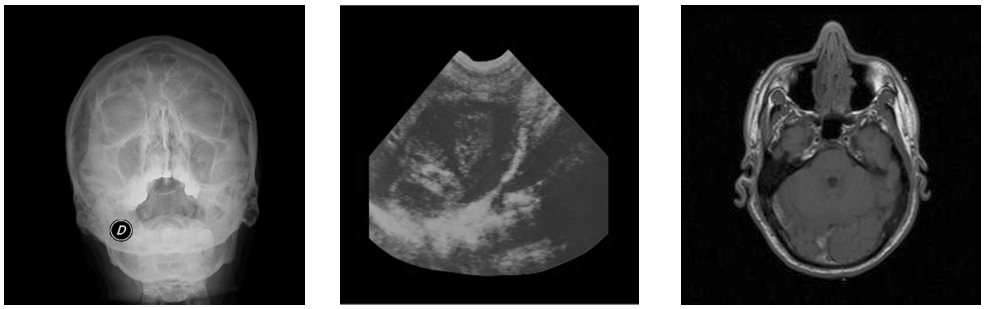
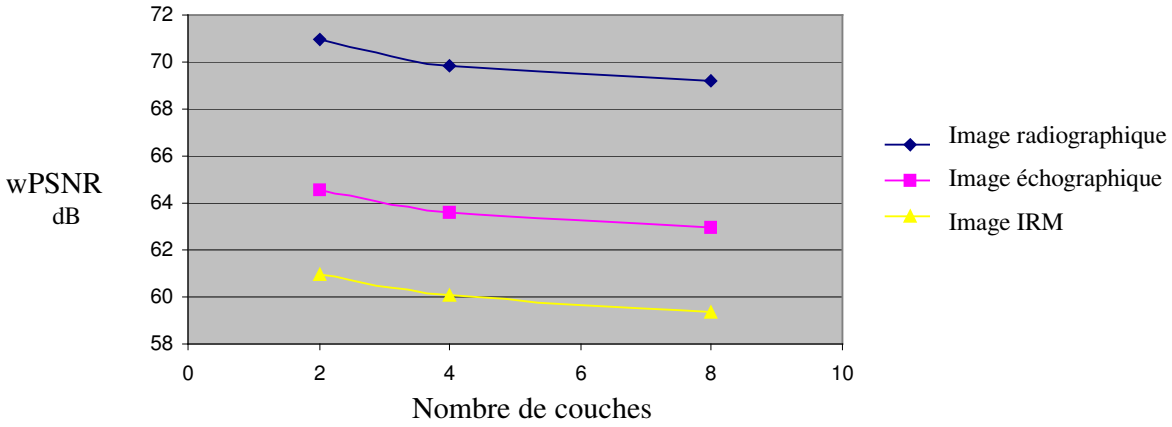
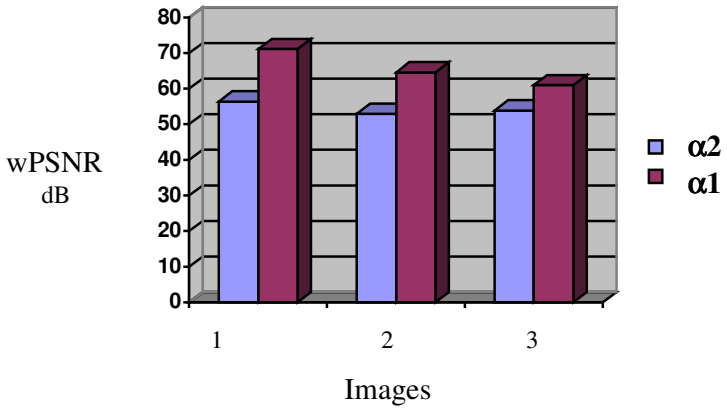


Image 1 Image 2 Image 3

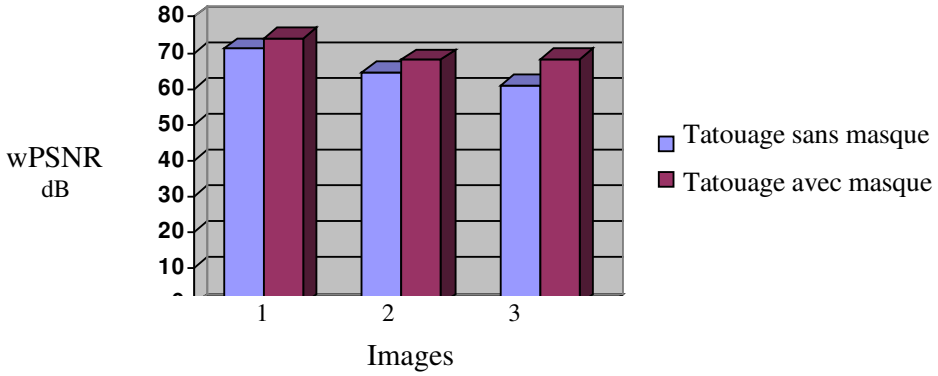
Figure 4.10 Images de test
Image 1 : image radiographique
Image 2 : image échographique
Image 3 : image IRM



Graphe 4.2 Mesure de la dégradation
pour 2, 4 et 8 couches



Graphe 4.3 Mesure de la dégradation de trois images tatouées avec deux coefficients de visibilité α1 (0.1) et α2 (0.5)



Graphe 4.4 Mesure de la dégradation de trois images tatouées avec et sans utilisation du masque psychovisuel

Nous remarquons que le wPSNR est inversement proportionnel au nombre de couches utilisées et au coefficient de visibilité. En effet, bien que l'augmentation du nombre de couches permet d'augmenter le nombre des bits à insérer et améliorer la détection, elle accentue cependant la visibilité de la marque. De même pour le coefficient de visibilité qui améliore la détection de la marque mais peut entraîner la dégradation de l'image.

Le masque psychovisuel améliore également la qualité de l'image puisqu'il diminue la valeur de la SBPA 2D au niveau des zones homogènes de l'image et l'augmente au niveau des zones texturées permettant ainsi une meilleure dissimulation de la marque.

Enfin nous avons comparé la qualité de l'image pour les trois types d'échantillons d'images médicales en fixant la valeur du coefficient de visibilité et le nombre de couches utilisées (voir tableau 4.1).

	wPSNR (dB)									
Images radiographiques	68	70	69	71	65	62	62	61	77	65
Images échographiques	59	61	61	70	66	63	65	64	62	74
Images IRM	66	60	61	63	69	61	61	68	63	68

Tableau 4.1 Valeur du wPSNR pour les trois types d'échantillons d'images médicales.
α =0.3, Nombre de couches : 8

Selon le calcul du wPSNR et l'avis des spécialistes, cette méthode donne de bons résultats pour les trois types d'images médicales et notamment pour l'image radiographique, à condition de choisir les paramètres adéquats (nombre de couche, facteur de visibilité, utilisation du masque). Ceci est probablement du à la nature texturée de l'image radiographique. En effet, si on prenait à titre indicatif l'image radiographique et l'image échographique représentées dans la figure 4.11, nous remarquons que la première est caractérisée par une variance et un wPSNR plus grands que ceux de l'image échographique.

On remarque qu'en augmentant le nombre de bits insérés jusqu'à 192 bits, on obtient des résultats proches des résultats précédents du point de vu calcul du wPSNR cependant on remarque que pour certaines images IRM et échographiques, la marque devient visible au niveau des zones où la luminosité est proche de la valeur 255 (voir figure 4.12), Ceci est causé par l'ajout de la SBPA 2D, le pixel étant codé sur 8bits, la valeur 255 bascule à 0 si on lui rajoute un « 1 ».

Image radiographique
Ecart type = 78
wPSNR = 70,32 dB

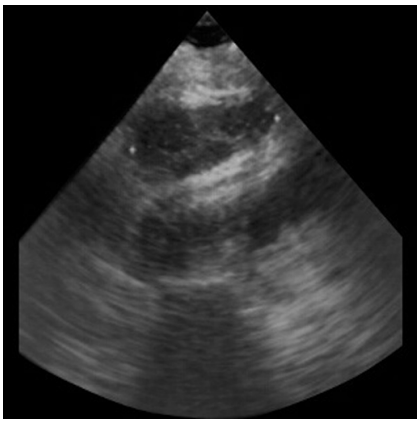


Image échographique
Ecart type= 39,44
wPSNR = 61,5 dB

Figure 4.11 Comparaison de la qualité de l'image tatouée entre deux types d'images médicales

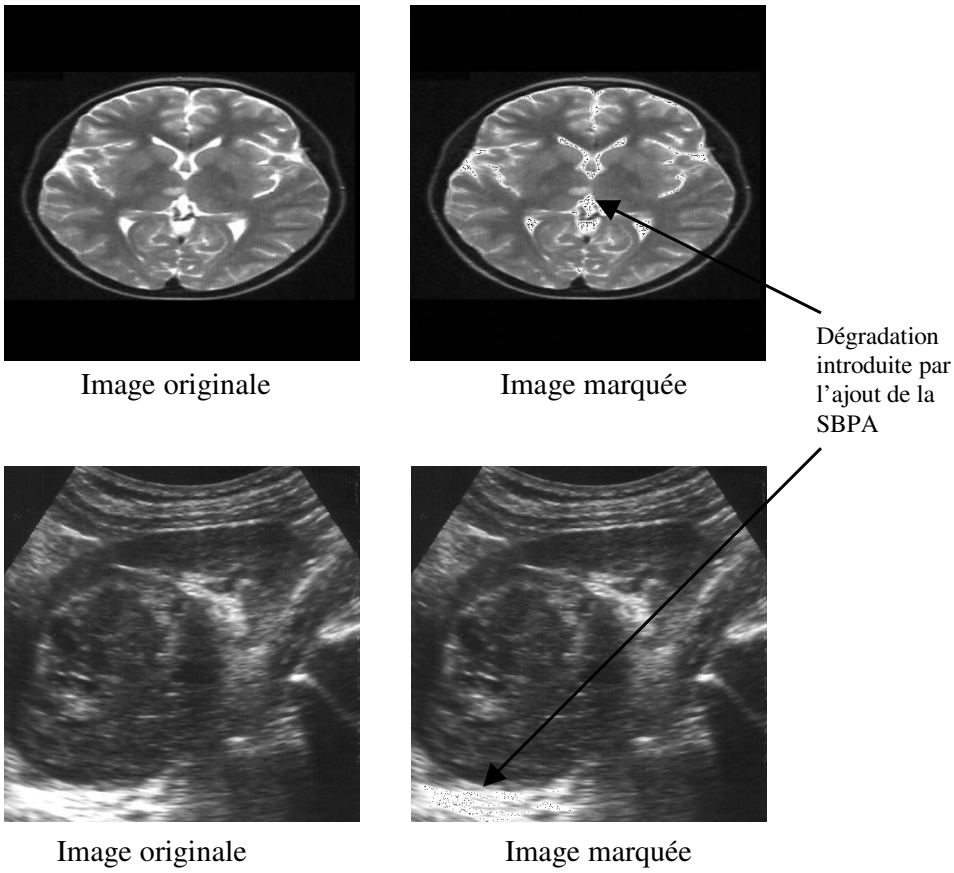


Figure 4.12 Visibilité du tatouage pour une image IRM et une image échographique

4.4.2 Résultats obtenus dans le domaine DWT

L'objectif de l'application de cette méthode dans le domaine DWT est l'étude de la qualité de l'image et de sa robustesse à la compression JPEG.

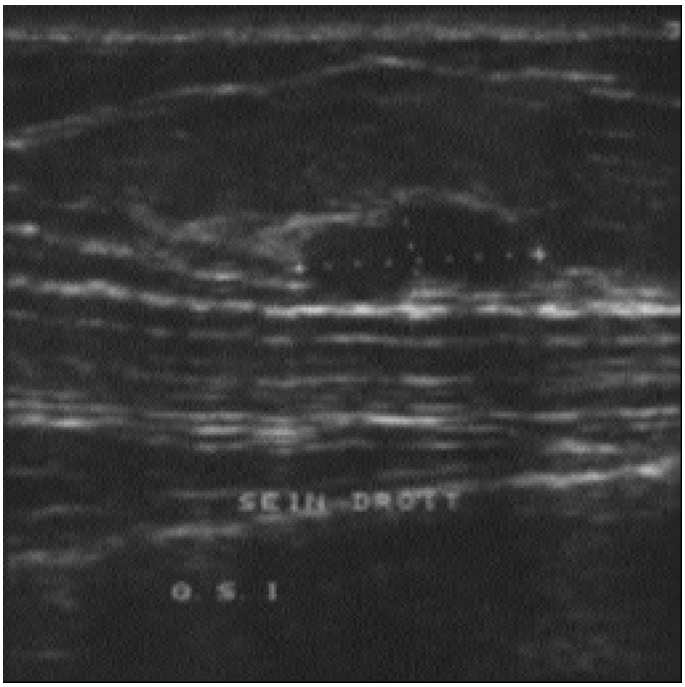
Après l'application de la transformée en ondelettes discrète en appliquant le filtre de Haar (voir section 3.2.2.c), nous insérons la marque au niveau des détails horizontaux, verticaux et diagonaux. Dans ce cas, la surface de la SBPA 2D est réduite du quart par rapport au domaine spatial ce qui entraîne un problème de détection du message inséré. La figure 4.13 représente une image IRM tatouée avec un message de 64 bits, en utilisant 8 couches et un coefficient de visibilité de 0.3. A la détection 30 bits seulement sont détectés.

Figure 4.13 Exemple d'image IRM tatouée
dans le domaine DWT

Pour améliorer la détection des bits insérés, on doit d'une part augmenter le coefficient de visibilité et d'autre part, augmenter le nombre de couches utilisées (c'est-à-dire la surface de la SBPA 2D), ceci entraîne malheureusement une dégradation importante de l'image médicale (voir figure 4.14).

L'utilisation de la méthode multicouche dans le domaine DWT pour des images médicales est donc à éviter.

(a)



(b)

Figure 4.14 Dégradation d'une image échographique tatouée
(wPSNR = 40,59dB)
(a) Image originale
(b) Image tatouée

4.5 Conclusion

Dans ce chapitre nous avons étudié l'application de la méthode multicouche pour l'image médicale dans le but de vérifier son authenticité.

Cette méthode, basée sur la technique CDMA vise à augmenter le nombre de bits insérés dans l'image sans pour autant la dégrader.

L'application de cette technique dans le domaine spatial donne de bons résultats pour l'insertion de 64 bits sur les plans qualité de l'image tatouée et robustesse du tatouage à la compression JPEG. Cependant, les résultats obtenus dans le domaine DWT ne sont pas satisfaisants vu la dégradation apportée à l'image tatouée.

A partir des trois types d'échantillons des images étudiées, il semblerait que cette méthode s'adapte mieux à l'image radiographique, notamment lorsqu'on augmente le nombre de bits à insérer, ceci peut être du à sa texture qui permet de mieux dissimuler la marque.

L'un des inconvénients de cette méthode est que l'utilisateur doit manipuler plusieurs données: Clés, nombre de couches, nombre de bits, etc., ceci devient contraignant lorsqu'il s'agit de gérer un nombre important d'images.

Chapitre 5
Intégrité et Confidentialité des données

5.1 Introduction

Dans ce chapitre nous présentons une méthode de tatouage fragile qui a pour objectif la vérification de l'intégrité de l'image médicale et la préservation de la confidentialité des données du patient. Cette méthode est basée sur l'utilisation des bits les moins significatifs de l'image (LSB) associée à la cryptographie et plus particulièrement au calcul de l'empreinte de l'image et le chiffrement.

Nous expliquons dans un premier temps l'une des premières méthodes de tatouage, elle consiste à dissimuler les données dans les LSBs de l'image. Cette partie nous permettra d'évaluer l'intérêt et les limites de l'utilisation des LSBs. Nous présentons ensuite l'apport de la cryptographie dans ce domaine en se basant sur la méthode de référence expliquée dans la section 2.7.2. Nous apporterons à cette méthode quelques modifications qui nous permettrons d'améliorer la qualité de l'image médicale tatouée pour une application de télémédecine et améliorer également l'aspect "sécurité".

Les tests sont appliqués sur des images médicales de type radiographique, échographique et IRM.

5.2 Méthode basée sur l'utilisation des LSBs

5.2.1 Description

Cette méthode consiste à remplacer les Nb bits les moins significatifs de l'image originale par les Nb bits les plus significatifs de l'image à dissimuler.

Ce tatouage fragile permet de détecter les éventuelles manipulations que peut subir l'image médicale. Il est donc très simple d'enlever la marque en mettant, par exemple, à 0 tous les bits de poids faibles ou en appliquant un filtre ou une compression.

.

5.2.2 Etapes d'insertion / détection du tatouage

La figure 5.1 illustre les étapes d'insertion de cette méthode pour les trois bits les moins significatifs du pixel (Nb=3) [27].

1/ Lecture de la valeur de la luminosité du pixel (x, y) de l'image originale

2/ Mettre à 0 les Nb bits les moins significatifs de cette valeur

3/ Lecture de la valeur de la luminance du pixel (x, y) correspondant à l'image à dissimuler

4/ Faire un décalage à droite de cette valeur de 8 -Nb bits

5/ Faire la somme des deux valeurs résultante.

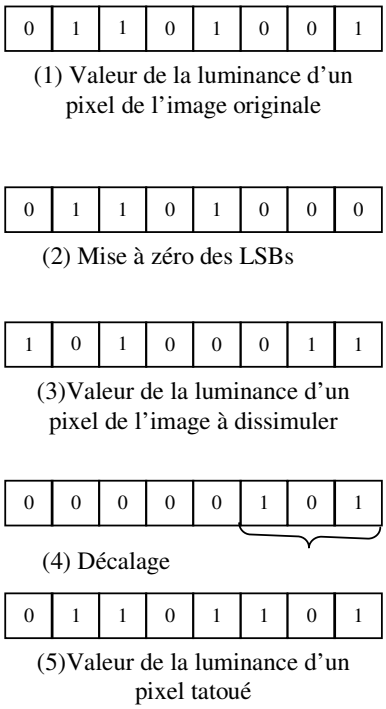


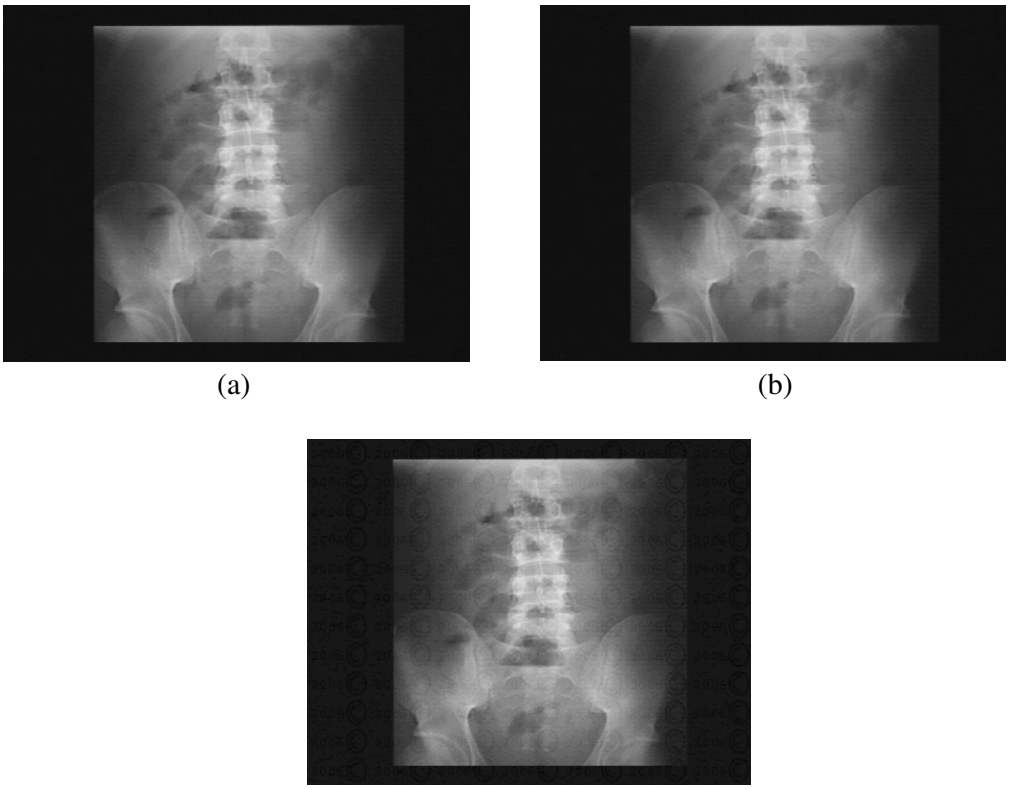
Figure 5.1 Exemple d'algorithme basé sur les LSBs, Nb = 3

Nous devinons que l'étape de détection est duale à l'insertion. En effet, il suffit d'effectuer sur l'image tatouée un décalage à gauche des (8-NB) bits pour récupérer la marque.

5.2.3 Résultats et interprétations

L'algorithme a été testé sur plusieurs images. Nous présentons ci-dessous les résultats obtenus pour une image radiographique de format BMP et de taille 376 x 288. La marque utilisée est une image BMP de la même taille.

a) Détection de la marque



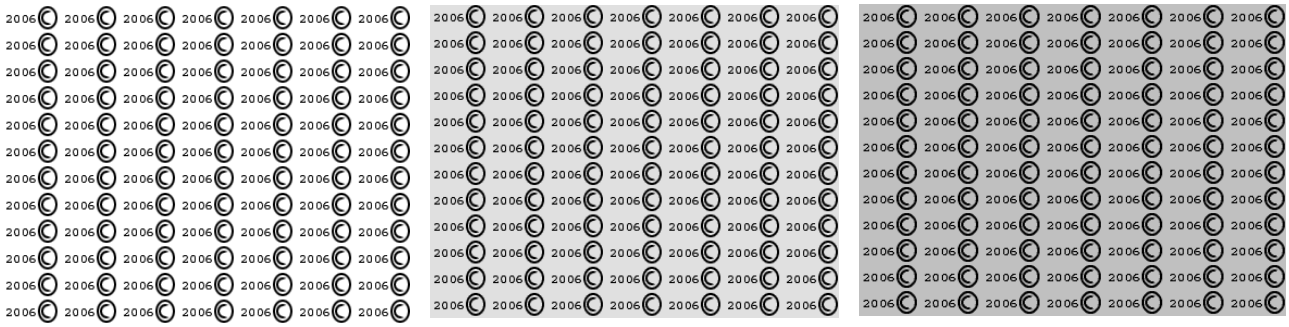
(a) (b)

(c)

Figure 5.2 Image tatouée en utilisant les LSBs
(a) Image originale
(b) Image tatouée (Nb = 1)
(c) Image tatouée (Nb = 3)

La figure 5.2 représente une image radiographique originale et deux cas de tatouage (Nb=1 et Nb=3). La figure 5.3 représente l'image à dissimuler et deux cas de son extraction.

Nous remarquons que plus Nb est grand, plus la qualité de l'image extraite est meilleure et plus l'image dissimulée est visible sur l'image marquée. Il faut donc faire un compromis entre la visibilité de la marque et la qualité de l'image extraite en choisissant la bonne valeur de Nb. Il est également possible de garder Nb=1 et choisir une image « marque » qui contiendrait l'information dans les Nb bits les plus significatifs (MSBs) des pixels.



(a) (b) (c)

Figure 5.3 Extraction de la marque en utilisant les LSBs
(a) Image à dissimuler (marque)
(b) Extraction de la marque avec Nb = 3
(c) Extraction de la marque avec Nb = 1

b) Mesure de la qualité de l'image

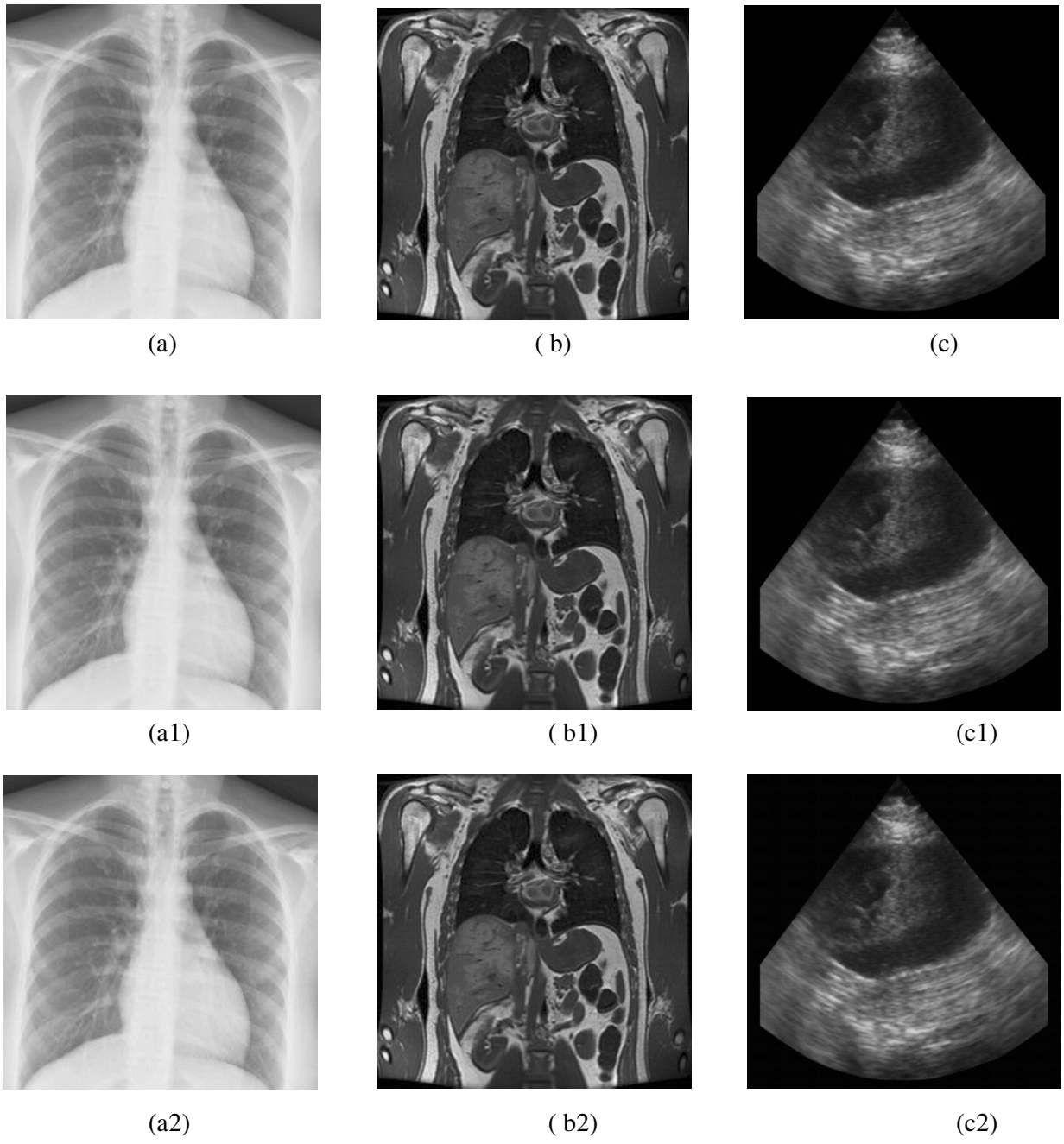
Les tests de mesure de la qualité de l'image ont été effectués sur trois images de taille 512 x 512, format BMP (voir figure 5.4).

Les résultats du calcul du wPSNR sont représentés dans le tableau 5.1.

		Image Radiographique	Image IRM	Image Echographique
wPSNR (dB)	**Nb= 1**	**58,55**	**62,31**	**51,13**
	Nb= 2	**50,31**	**53,86**	**41,72**

Tableau 5.1 Calcul du wPSNR pour trois types d'images marquées

L'avantage principal de l'utilisation des LSBs dans le tatouage des images est d'une part la quantité d'information relativement importante qu'on peut insérer dans l'image et la qualité de l'image marquée par rapport à l'image originale pour la valeur de Nb=1.



(a) (b) (c)

(a1) (b1) (c1)

(a2) (b2) (c2)

Figure 5.4 Exemple d'images tatouées
en utilisant la méthode des LSBs
(a), (b), (c) sont les images originales de type radiographique,
IRM et échographique respectivement.
(a1), (b1), (c1) sont les images tatouées avec Nb =1
(a2), (b2), (c2) sont les images tatouées avec Nb =2

c) Détection de la marque après manipulation de l'image tatouée :

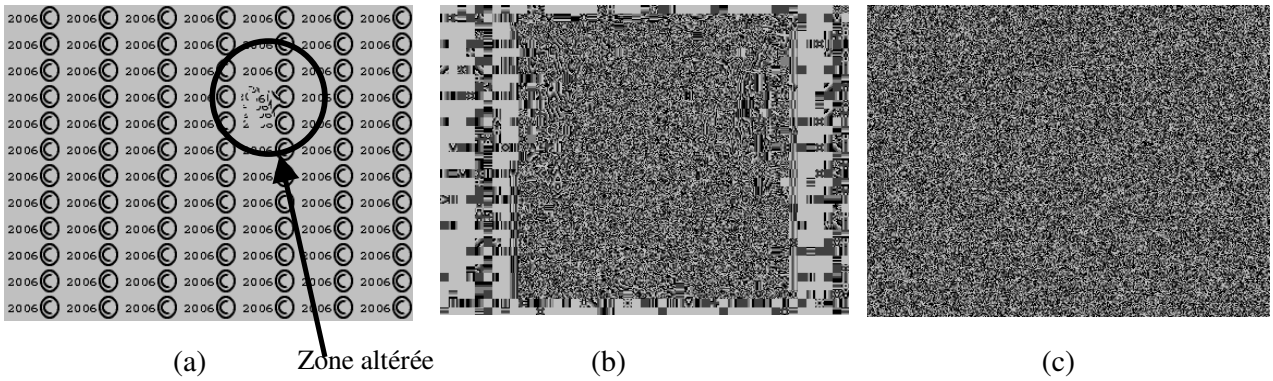


Figure 5.5 Extraction de la marque après trois types d'attaques
(a) Attaque copier/coller
(b) Attaque par ajout de bruit
(c) Attaque JPEG

La figure 5.4 nous montre qu'à la moindre manipulation de l'image, la marque est altérée. Il est donc nécessaire que la marque soit présente dans tous les LSBs de l'image originale.

d) Aspect ″Sécurité ″

La méthode de tatouage basée sur l'utilisation des LSBs, telle qu'elle est présentée, ne peut assurer la sécurité de l'image médicale ou des données insérées. En effet, il peut être possible à un pirate d'accéder aux images partagées sur le réseau, et de récupérer les LSBs de l'image marquée, la modifier, ensuite remettre les valeurs des LSBs à leur emplacement. Dans ce cas, la confidentialité des données de la source n'est plus vérifiée, de plus, l'image apparaîtrait non manipulée pour l'utilisateur qui vérifie son intégrité.

5.3 Méthode basée sur les LSBs et la cryptographie

L'utilisation des LSBs est intéressante si elle est associée à d'autres méthodes qui assureraient la sécurité des données insérées. Dans ce qui suit nous présentons une méthode basée sur l'utilisation des LSBs et la cryptographie. Nous choisissons Nb=1 pour minimiser la dégradation de l'image tatouée.

5.3.1 Description

La méthode de référence, proposée dans [20] est décrite dans la section 2.7.2.

La qualité de l'image tatouée peut être améliorée en prenant en considération les points suivants :

- Pour une application de télémédecine, nous visons à augmenter la qualité de l'image marquée lors de son affichage sur le réseau, dans ce cas l'insertion des "LSBs compressés" dans l'image pour une récupération ultérieure de l'intégrité de l'image s'avérerait inutile. Il serait préférable de garder les LSBs intacts.

- L'empreinte de l'image étant représentée sur 32 caractères (en hexadécimal) et les données du patient (Nom, prénom, age et sexe) sont sur environ 34 caractères, et en codant chaque caractère sur 8 bits nous devront ainsi insérer ''au fond'' de l'image environ 528 bits, ce nombre de bits est négligeable par rapport au nombre de pixels de l'image notamment si les recommandations relatives aux dimensions des images pour les systèmes de télémédecine (section 2.5) sont respectées.

L'algorithme d'insertion devient :

- Calculer l'empreinte des MSBs de l'image en utilisant l'algorithme MD5 (en prenant en considération 7 bits sur 8 pour chaque pixel dans le calcul de l'empreinte).
- Concaténer l'empreinte de l'image avec les données du patient et crypter le résultat avec le chiffrement de Vigenère.
- Faire une conversion ASCII/ binaire du résultat codé, et calculer sa longueur N (nombre de bits).

Le calcul de N permet de mettre à « 0 » les LSBs qui serviront à dissimuler l'information et le reste des LSBs de l'image restent intacts.

Afin d'identifier la fin de la chaîne de caractères à décoder lors de la détection on rajoute lors de l'insertion, à la fin des données du patient, un caractère rarement utilisé tel que le « @ ».

La figure 5.6 illustre le schéma d'insertion de cette méthode.

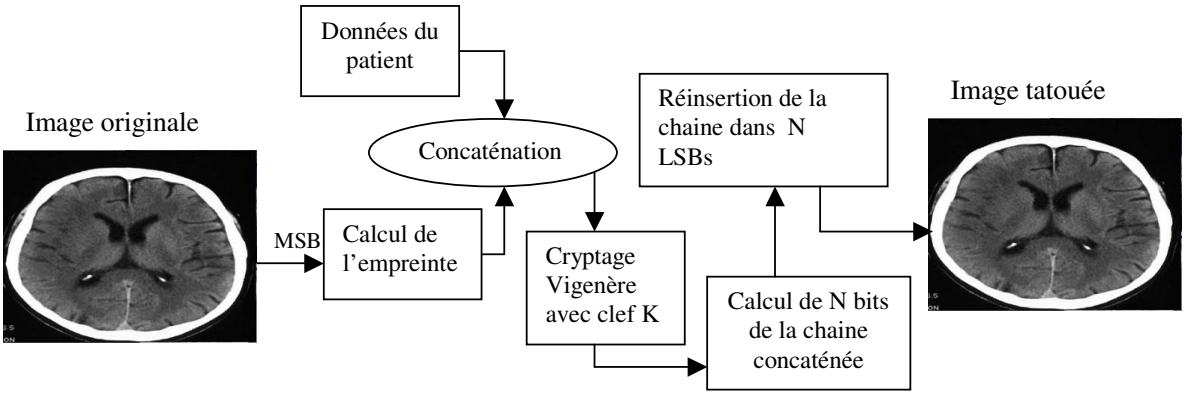


Figure 5.6 Schéma d'insertion de la méthode basée sur les LSBs et la cryptographie

L'étape de détection consiste à extraire les données du patient ainsi que l'empreinte qui permettra de vérifier l'intégrité de l'image. L'algorithme de détection suivra alors les opérations inverses à l'insertion :

- Extraire les données des LSBs
- Faire une conversion binaire/ASCII jusqu'à arriver au caractère « @ » qui représente la fin des données insérées.
- Faire un décodage de Vigenère en utilisant la clef de l'insertion K.
- Séparer l'empreinte (de taille connue) des données du patient.
- Vérifier l'intégrité de l'image en calculant son l'empreinte et en la comparant avec l'empreinte extraite de l'image.

Le schéma de détection est illustré dans la figure5.7.

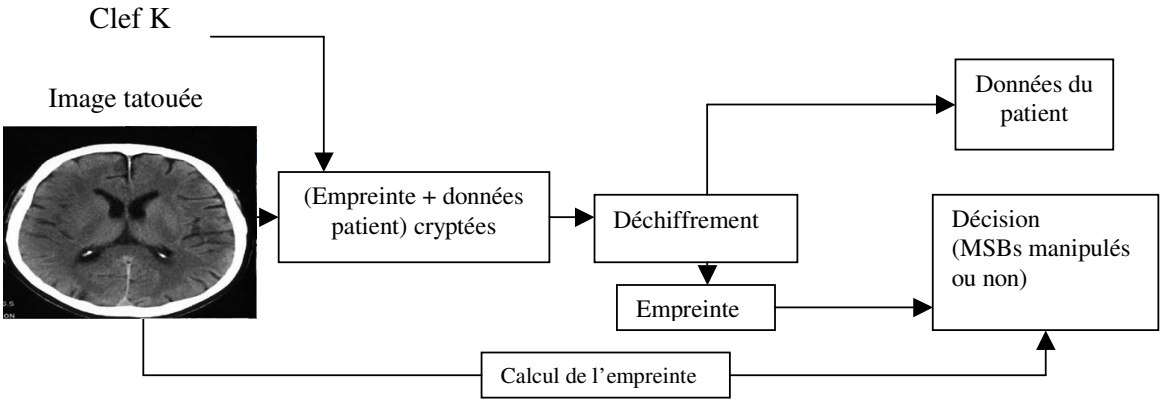


Figure 5.7 Schéma de détection de la méthode basée sur les LSBs et la cryptographie

5.3.2 Résultats et interprétations

Nous avons effectué des tests sur trois types d'échantillons d'images médicales (IRM, radiographie, échographie) codées sur 256 niveaux de gris, format BMP et de taille 512 x 512.

a) Format des données insérées dans l'image

Le tableau 5.2 représente le format des données insérées dans l'image.

Vérification de l'intégrité	Nombre de caractères
Empreinte	32

Données du patient	Nombre de caractères
Nom	15
Prénom	15
Age	3
Sexe	1

Tableau 5.2 Le format des données insérées dans l'image

Le nombre de bits maximal qu'on veut insérer dans l'image est : (32+34) x 8 = 528 bits

b) Insertion et détection des données

- Pour insérer les données du patient, l'utilisateur doit remplir les champs de saisie suivants :

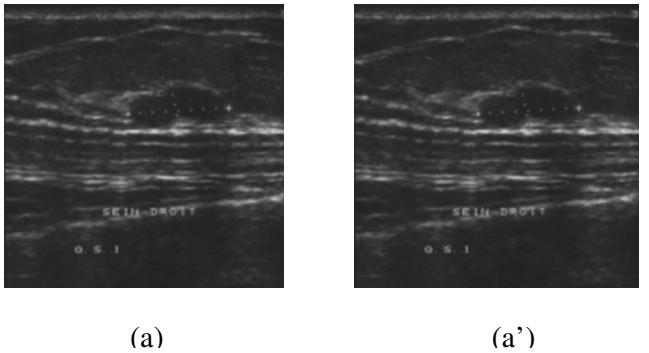
- Données du patient : nom, prénom, âge et sexe ;
- La clé secrète K (nécessaire pour le codage de Vigenère).

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

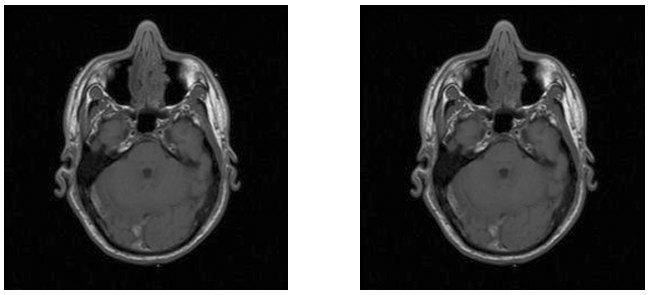
- L'image tatouée ;
- La clé K.

La figure 5.7 représente trois images tatouées par cette méthode.

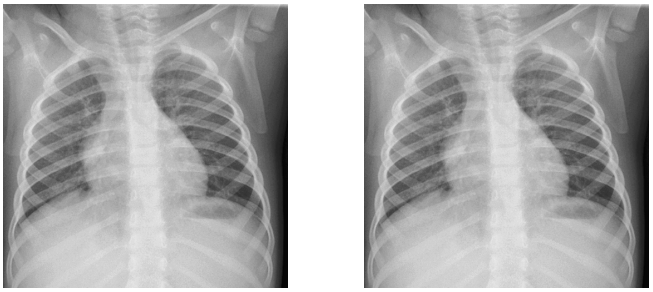
La détection des données du patient et l'empreinte se fait avec succès pour les images médicales tatouées n'ayant subi aucune attaque.



(a) (a’)



(b) (b’)



(c) (c’)

Figure 5.8 Exemple d’images tatouées par la méthode basée sur les LSBs et la cryptographie.
(a), (b) et (c) sont des images échographiques, IRM et radiologiques respectivement
(a’), (b’) et (c’) sont les images tatouées

c) Vérification de l'intégrité de l'image tatouée

Pour les images médicales n'ayant subi aucune attaque, la vérification de l'intégrité se fait avec succès.

On fait subir à quelques images des attaques fréquentes dans le domaine médical telles que l'attaque du « copier/ coller » ou bien la compression JPEG de 10 % (section 1.5.2.a), on vérifie ensuite l'intégrité de l'image et l'extraction des données du patient.

La figure 5.8 représente trois images tatouées, avant et après l'attaque « copier/ coller » ou la compression JPEG.

Le tableau 5.3 présente une vérification de l'intégrité de ces images avant et après l'attaque, et ce, en calculant l'empreinte et en la comparant avec la valeur de l'empreinte extraite des LSBs.

On remarque que dans le cas des images attaquées, les valeurs de l'empreinte (calculée et extraite) sont différentes. Dans le cas d'une attaque JPEG ou d'une autre attaque qui affecterait les pixels contenant les informations "empreinte et données du patient", l'extraction de ces dernières ne se fait pas, car lors de la conversion binaire/ ASCII, certains octets ne trouvent pas leurs équivalents dans la table de conversion.

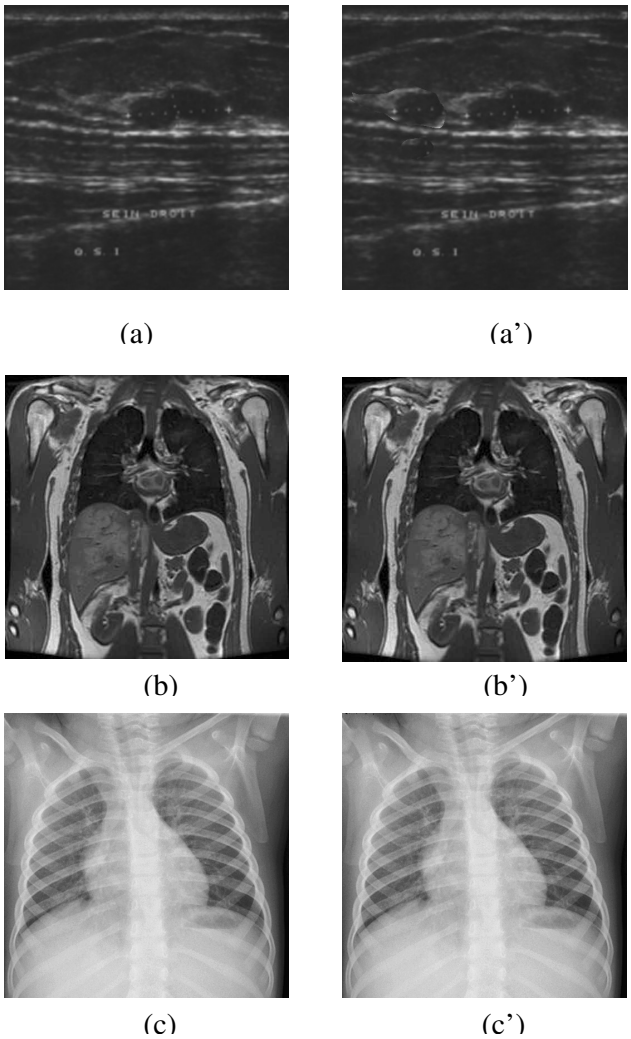


Figure 5.9 Images tatouées, avant et après une attaque
(a), (b) et (c) images tatouées
(a'), (b') images tatouées ayant subies l'attaque « copier coller »
(c') image tatouée ayant subie l'attaque JPEG

La valeur de l'empreinte extraite des LSBs	Image (a) : B36938DC92C5110D61AF995E8A5CFAB1 Image(a') : B36938DC92C5110D61AF995E8A5CFAB1
Calcul de l'empreinte	Image (a) : B36938DC92C5110D61AF995E8A5CFAB1 Image(a') : 454AD9E4541AA91C7DD52C616E56B99E

La valeur de l'empreinte extraite des LSBs	Image (b) : 03826EBD3048F9BCD66F74DCE3E08B8D Image(b') : Aucune empreinte n'est extraite
Calcul de l'empreinte	Image (b) : 03826EBD3048F9BCD66F74DCE3E08B8D Image(b') : C503E793385D85E8214410B369FBE729

La valeur de l'empreinte extraite des LSBs	Image (c) : 0A2FB76CCEBE8B7835815C106B328596 Image(c') : Aucune empreinte n'est extraite
Calcul de l'empreinte	Image (c) : 0A2FB76CCEBE8B7835815C106B328596 Image(c') : C503E793385D85E8214410B369FBE729

Tableau 5.3 Vérification de l'intégrité en comparant l'empreinte calculée avec l'empreinte extraite

d) La qualité de l'image tatouée

- **Mesures de la qualité des images tatouées**

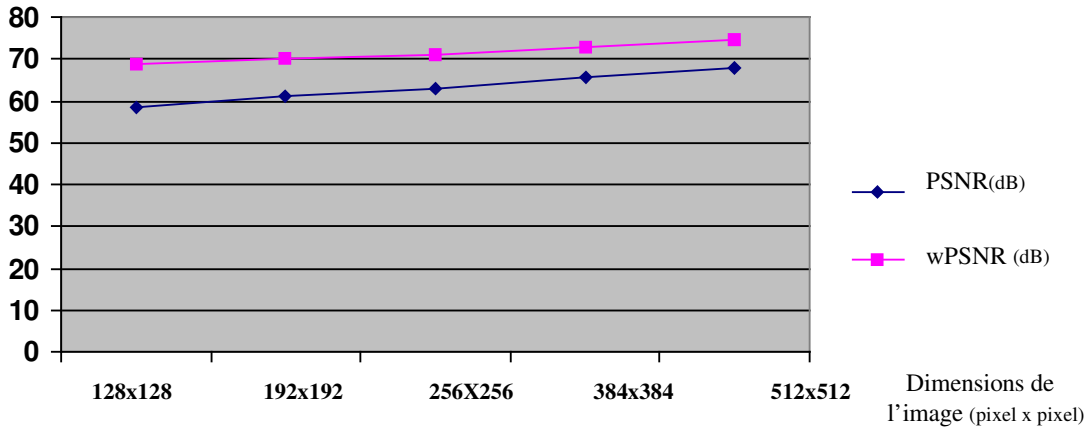
On calcule pour chaque échantillon d'images les wPSNR. Les résultats sont comme suit :

	WPSNR (dB)									
Image radiographique	78,23	72,22	74,43	79,18	72,22	76,66	74,38	72,18	74,14	71,50
Image échographique	73,30	73,95	74,07	73,72	78,03	74,99	76,33	72,78	75,39	73,61
Image IRM	74,99	75,86	76,00	75,68	75,35	77,76	73,30	75,37	71,43	67,28

Tableau 5.4 Calcul du wPSNR pour les trois types d'échantillons d'images médicales

Nous pouvons déduire à partir du tableau 5.4 et en comparant ces résultats avec ceux obtenus dans la section 4.4.1.d, que la marque est bien dissimulée. Les résultats sont donc bons pour les trois échantillons d'images médicales. Ceci a été confirmé par l'appréciation des spécialistes pour la qualité des images tatouées qui a été "Bonne" pour les trois échantillons (voir section 1.5.1.d). Les spécialistes consultés ont affirmé que le tatouage appliqué n'affecte en aucun cas le diagnostic pour ces trois échantillons.

- **Relation qualité de l'image/ dimensions**



Graphe 5.1 Relation qualité de l'image/dimensions

Le graphe 5.1 représente la relation entre la qualité de l'image (représentée par le PSNR et le wPSNR) et ses dimensions.

La qualité de l'image est proportionnelle à ses dimensions car le nombre de LSBs contenant le tatouage devient négligeable par rapport à tous les LSBs de l'image lorsque les dimensions sont grandes.

- **Comparaison avec la méthode de référence**

Bien que nous n'avons pas les même images utilisées dans la méthode de référence (section 2.7.2) pour pouvoir faire une comparaison objective entre les résultats, nous avons calculé le PSNR pour des image du même type et de mêmes dimensions. Elles sont représentées dans la figure 5.9.

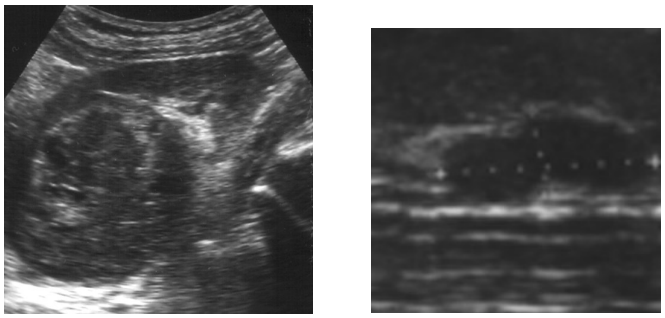


Figure 5.10 Images échographiques utilisées pour la comparaison avec la méthode de référence

Rappelons que dans la méthode de référence (section 2.7.2) le PSNR est de 39,72 dB pour une image de dimension 256 x 256 et 41, 33 dB pour une image de 512 x 512 dB.

	Dimensions	**PSNR (dB)**
Image 1	256 x 256	61,69
Image 2	512 x 512	68,44

Tableau 5.5 Calcul du PSNR pour deux images échographiques

Les résultats représentés dans le tableau 5.4 sont meilleurs que ceux obtenus dans la méthode de référence. Ceci est prévisible étant donné que le tatouage est placé dans un nombre réduit de LSBs, et la majorité des pixels de l'image reste intacte.

e) Amélioration de la sécurité de l'image

Bien que cette méthode améliore considérablement la qualité de l'image tatouée, elle pose cependant le problème suivant : Etant donné que le calcul de l'empreinte de l'image ne prend pas en compte les LSBs, la manipulation de ces derniers ne peut être détectée par l'utilisateur (médecin ou autre) lors d'une vérification de l'intégrité de l'image.

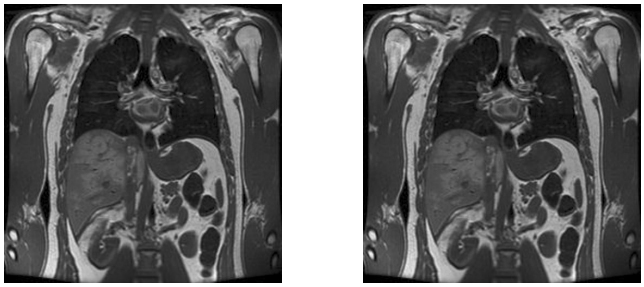
Les tests effectués sur les images médicales (voir section 5.2.3.b) montrent que la manipulation du bit le moins significatif n'est pas perceptible et n'affecte donc pas le diagnostic. Cependant, ceci ne peut pas être généralisé à toutes les images médicales, il serait donc plus prudent de détecter également la moindre manipulation non autorisée des LSBs dans une image médicale.

Nous pouvons remédier à ce problème en prenant en considération les valeurs des LSBs qui ne contiennent pas l'information « empreinte et donnée du patient » dans le calcul de l'empreinte.

Nous avons fait des tests sur plusieurs images médicales. L'attaque a été faite avec un programme qui modifie les valeurs des LSBs. Le contrôle d'intégrité montre que la moindre manipulation des LSBs de l'image est détectée. La figure 5.11 représente l'une des images testées le contrôle d'intégrité correspondant est indiqué dans le tableau 5.5.

La valeur de l'empreinte extraite des LSBs	Image (a) : 8C12ED177E82F3D99CD4B66BEE1B6DA7 Image(a') : 8C12ED177E82F3D99CD4B66BEE1B6DA7
Calcul de l'empreinte	Image (a) : 8C12ED177E82F3D99CD4B66BEE1B6DA7 Image(a') : A2D1D02D75353F405DFBA34882167529

Tableau 5.5 Contrôle de l'intégrité



(a) (b)

Figure 5.11 Amélioration de la sécurité de l'image tatouée
(a) Image tatouée
(b) Image tatouée/ Attaque des LSBs

5.4 Conclusion

Nous avons étudié dans ce chapitre une méthode de tatouage d'image médicale basée sur l'utilisation des LSBs et des outils de cryptographie à savoir le calcul de l'empreinte avec l'algorithme MD5 et le chiffrement de Vigenère. L'objectif de cette méthode était de vérifier l'intégrité de l'image médicale et de garder la confidentialité des données du patient. Les modifications apportées à cette méthode afin de l'adapter à une application de télémédecine ont donné des résultats satisfaisants quant à l'amélioration de la qualité de l'image ou de sa sécurité.

Conclusion

Conclusion

Le tatouage des images trouve une application dans le domaine de l'imagerie médicale et en particulier dans le domaine de la télémédecine. En effet, étant donné l'importance et l'essor que connaît la pratique de la médecine à distance, le tatouage peut être proposé pour contribuer à la sécurité des images médicales partagées sur le réseau Internet.

L'image médicale, vu ses spécificités, doit être manipulée avec beaucoup de précaution. Une dégradation de l'image, qui semblerait négligeable, n'est souvent pas acceptée dans ce domaine car elle pourrait conduire à un diagnostic erroné.

Dans ce mémoire nous nous sommes intéressées à deux méthodes de tatouage, que nous avons appliquées à des images médicales pour étudier leur adaptabilité à ce domaine en vérifiant l'authenticité et l'intégrité de l'image et en assurant la confidentialité des données du patient.

Nous avons d'abord étudié une méthode de tatouage robuste, proposée initialement pour le copyright. Notre objectif, était de vérifier l'authenticité d'une image et ce en insérant une signature. Cette première méthode, se base sur la technique de communication CDMA. La qualité de l'image médicale tatouée est améliorée par l'utilisation du masque psychovisuel. Nous avons vérifié la robustesse de la méthode pour une attaque de compression JPEG à un facteur de qualité supérieur à 50% pour l'image radiographique et supérieur à 60% pour les images échographiques et IRM.

Selon les mesures objectives et subjectives effectuées sur trois échantillons d'images médicales (images radiographiques, IRM et échographiques), nous avons obtenu de bons résultats pour l'insertion de 64 bits notamment pour l'image radiographique. L'inconvénient que présente cette méthode pour l'imagerie médicale est d'une part la limitation du nombre de bits à insérer, et d'autre part, la manipulation de plusieurs paramètres (clé, nombre de couches, nombre de bits à insérer) ce qui est contraignant surtout lorsqu'il s'agit de gérer un nombre important d'images médicales.

La deuxième méthode étudiée, concerne l'insertion d'un tatouage fragile dont les objectifs sont de vérifier l'intégrité de l'image médicale et de garder la confidentialité des données du patient. Cette méthode s'adapte parfaitement à l'imagerie médicale car elle tire profit de

l'utilisation des bits les moins significatifs (LSBs) de l'image et de la cryptographie. De plus, elle a été améliorée pour cette application pour donner de meilleurs résultats sur les niveaux qualité et sécurité de l'image. La fiabilité de cette méthode dépend toutefois de la robustesse des algorithmes de cryptographie utilisés.

Plusieurs perspectives peuvent être entrevues dans ce domaine. D'abord, une étude approfondie sur les caractéristiques des différents types d'images médicales contribuerait à améliorer ces méthodes pour pallier à leurs limites et optimiser les résultats.

Pour la première méthode, des améliorations doivent être apportées pour l'augmentation du nombre de bits à insérer sans dégrader l'image et identifier les paramètres optimaux pour chaque type d'image médicale.

Pour la deuxième méthode, il est important de mettre à jour les algorithmes de cryptographie par des algorithmes plus robustes pour assurer la sécurité de l'image.

Et enfin, Il serait intéressant d'étudier l'hybridation des deux méthodes présentées dans le but d'obtenir une seule méthode qui vérifie l'origine de l'image (l'authenticité), son intégrité et la confidentialité des données du patient ou du médecin.

Bibliographie

[1] P. BAS, Méthode de tatouage d'image fondé sur le contenu, Thèse de Doctorat, Institut National Polytechnique de Grenoble, 2000.

[2] B.VASSAUX, Technique multicouches pour le tatouage d'images et adaptation aux flux vidéo MPEG-2 et MPEG-4, Thèse de Doctorat, Institut National Polytechnique de Grenoble, 2003.

[3] J.L DUGELAY & S. ROCHE, Introduction au tatouage d'image, 5èmes journées d'études et d'échanges COmpression et REprésentation des Signaux Audiovisuels (CORESA), France, Juin 1999.

[4] A. MANOURY, Tatouage d'images numériques par paquets d'ondelettes , Thèse de Doctorat, Ecole Centrale de Nantes et Université de Nantes, 2001.

[5] A. Z. TIRKEL, G. A. RANKIN, R. M.V. SCHYNDEL, W. J. HO, N. R. A. MEE & C. F. OSBORNE, Electronic watermark, In Digital Image Computing, Technology and Applications (DICTA'93), pp. 666-673, Macquarie University, Sidney, 1993.

[6] W. BENDER, D. GRHL, N. MORNMOTO & A. LU, Techniques for data hiding, IBM Systems Journal 35, pp. 313-336, 1995.

[7] L.COX, J.KILLIAN & T.SHAMOON, Secure spread spectrum communication for multimedia, Technical report, NEC Research Institute, Princeton, NJ, USA, 1995.

[8] E. KOCH & J.ZHAO, Embedding robust labels into images for copyright protection, In Proceedings of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Techologies, Vienna, August 1995.

[9] V. LICKS, On digital image watermarking robust to geometric transformations, Master Thesis, University of New Mexico, July 2000.

[10] B.M. PLANITZ & A.J. MAEDER, Medical Image Watermarking: A Study on Image Degradation, Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC 2005), Brisbane, Australia, February 2005.

[11] J.L OLIVES, Optimisation globale d'un système imageur à l'aide de critère de qualité visuelle, Thèse de Doctorat, Ecole Nationale Supérieure de l'Aéronautique et de l'Espace, Toulouse, France, 1998.

[12] Recommandation CCIR 500-4, Méthode d'évaluation subjective de la qualité des images de télévision, Union Internationale des Télécommunications (ITU), 1990.

[13] C. DELGORGE, Proposition et évaluation de techniques de compression d'images ultrasonores dans le cadre d'une télé-échographie robotisée, Thèse de Doctorat, Université d'Orleans, 2005.

[14] F.A.P. PETICOLAS, M.G. KUHUN & R. J. ANDERSON, Attacks on copyright marking systems, Second workshop on Information Hiding, in Vol.1525 of Lecture Notes in Computer Science, Portland, Oregon, USA, pp.213-238, 14-17 April 1998.

[15] D. PLANTE, Tatouage d'image par quantification, Thèse de Doctorat, Université de La Rochelle, Juillet 2002.

[16] M. RAMKUMAR & A. AKANSU, Robust Protocols for Providing Ownership of images, In Proceedings of the The International Conference on Information Technology: Coding and Computing (ITCC'00), 2000.

[17] J.C. CHEVROLT, M. DENZ, BERTRAND MERMINOD, S. OSSWALD & M.ROULET, Télémedecine, Rapport, Académie Suisse des Sciences médicales, 2002.

[18] F. PETITCOLAS, R.J. ANDERSON & M.G. KUHN, Information Hiding - A Survey, In Proceedings of the IEEE, Vol 87, N°7, pp. 1062-1078 , Juillet 1999.

[19] C.S.WOO, J.DU & B. PHAM, Multiple watermark method for privacy control and tamper detection in medical images, In Proceedings APRS of Workshop on Digital Image Computing , pp. 59-64, Australia, 2005.

[20] S.BOUCHERKHA & M. BENMOHAMED, A lossless watermarking based authentication system for medical image, In International Journal of Signal Processing, Vol.1, N°4, 2004.

[21] S. KROMMYDAS & A.N. SKODRAS, Digital watermarking of medical images using the Gabor transform, Technical report No. TR2001/10/01, Computer Technology Institute, Greece, October 2001.

[22] M. LOURDIANE, CDMA à séquence directe appliqué aux communications Optiques, Thèse de Doctorat, Ecole Nationale Supérieure des Télécommunications, Paris, France, 2005.

[23] M. MISITI, Y. MISITI, G. OPPENHEIM & J.M. POGGI, Les ondelettes et leurs applications, Edition Lavoisier, 2003.

[24] O. LE CADET, Méthodes d'ondelettes pour la segmentation d'images Applications à l'imagerie médicale et au tatouage d'images, Thèse de Doctorat, Institut National Polytechnique de Grenoble, Septembre 2004.

[25] D. STINSON, Cryptographie théorie et pratique, Edition Vuibert, Paris, 2003.

[26] H. DELFS & H. KNEBL, Introduction to cryptography, Edition Springer, 2002.

[27] A.Z. DJEDDI, Marquage des images fixes, Mémoire de Magister, Université Saad Dahleb, Faculté des sciences de l'ingénieur, Blida , Algérie, 2003.

ANNEXE

Les types d'images médicales

L'imagerie médicale est le procédé par lequel un médecin peut examiner l'intérieur du corps d'un patient sans l'opérer. L'imagerie médicale peut être utilisée à des fins cliniques, à la recherche d'un diagnostic ou pour le traitement d'un grand nombre de pathologies mais également pour la recherche dans le but d'étudier la physiologie des êtres vivants.

Les méthodes d'imagerie médicale sont nombreuses et utilisent plusieurs types de procédés physiques tels que :

- les rayons X
- les ultrasons
- l'émission de rayonnement par des particules radio-actives
- le magnétisme du noyau des atomes

Exemples des méthodes d'imagerie médicale :

La radiographie

La radiographie utilise les rayons X, ceux-ci permettent d'imprégner une plaque photographique et ont la faculté de traverser le corps. Plus la densité du corps sera importante, moins le rayon pourra passer au travers, c'est grâce à ce phénomène que l'image obtenue apparaîtra plus ou moins noire.

En effet, lors de la radiographie du corps humain, les rayons vont rencontrer soit des tissus, soit des muscles ou encore des os. Les rayons vont aisément passer à travers les tissus qui auront donc une apparence fort sombre. A l'inverse, lorsqu'ils rencontreront des os, ceux-ci vont être totalement arrêtés, il n'y aura donc aucune impression sur la plaque et celle-ci restera blanche.

Scanner ou tomodensitométrie (TDM)

Le Scanner appelé aussi tomodensitométrie est un examen qui utilise les rayons X.

Son principe consiste à réaliser des images en coupes fines du corps humain. Au lieu d'être fixe, le tube de rayons X va tourner autour du corps et grâce à un système informatique puissant, des images sont obtenues. Ensuite, elles sont imprimées sur un film pour être étudiées. Dans la

plupart des cas, un produit de contraste à base d'iode est utilisé pour améliorer leur qualité. Cet examen présente l'avantage de donner des informations très précises sur les organes étudiés.

Ultrasonographie ou échographie:

L'échographie est une technique d'exploration de l'intérieur du corps basée sur les ultra-sons. Une sonde envoie un faisceau d'ultrasons de fréquence appropriée (de 3,5 à 10 MHz pour le diagnostic) dans la zone du corps à explorer. Selon la nature des tissus, ces ondes sonores sont réfléchies avec plus ou moins de puissance. Le traitement de ces échos permet une visualisation des organes observés.

Lors du passage de ultrasons à travers les tissus, deux facteurs importants conditionnent la formation de l'image : l'atténuation et la réflexion. L'atténuation est causée par la perte d'énergie du système par suite de l'absorption, de la réflexion, de la réfraction et de la divergence du faisceau. Plus l'atténuation est forte et plus le signal de l'écho récupéré sera faible. C'est la réflexion des ondes ultrasonores en direction de la sonde émettrice-réceptrice qui produit l'image dont la texture ou « échostructure » traduit les différences d'indépendance acoustique des différents tissus examinés.

L'échographie permet l'analyse de nombreux organes superficiels (parotide, thyroïde, muscles et tendons, articulations, ganglions, vaisseaux , etc.) ou profonds (foie, vésicule, reins, rate, pancréas, ovaires, utérus, prostate, etc.)

Imagerie par résonance magnétique (IRM)

L'imagerie par résonance magnétique permet d'analyser à distance des organes tels que le cerveau, la colonne vertébrale, les articulations et les tissus mous de manière très précise. Cette technique permet de visualiser des détails invisibles sur les radiographies standards, l'échographie ou le scanner. Son principe consiste à réaliser des images du corps humain grâce aux nombreux atomes d'hydrogène qu'il contient. Placés dans un puissant champ magnétique, tous les atomes d'hydrogène s'orientent dans la même direction : ils sont alors excités par des ondes radio durant une très courte période (ils sont mis en résonance). A l'arrêt de cette stimulation, les atomes restituent l'énergie accumulée en produisant un signal qui est enregistré et traité sous forme d'image par un système informatique et la zone étudiée peut être restituée en deux ou trois dimensions.

La scintigraphie

Une scintigraphie est un examen de médecine nucléaire permettant de faire des images du corps humain par injection dans une veine d'un produit légèrement radioactif. Le produit peut mettre un certain temps à se fixer suivant l'organe à observer. L'appareil, appelé gamma caméra, capte les signaux émis par le produit, fixé de façon différentielle dans le corps.

Autoradiographie et fluorographie

La formation de l'image dans ces deux techniques se fait selon les mêmes principes que dans une photographie conventionnelle. Brièvement, de l'énergie est absorbée par des grains d'halogénure d'argent en suspension dans une émulsion de gélatine. La réduction de l'halogénure cause l'émission d'électrons qui seront trappés par des points sensibles à la surface ou à l'intérieur de l'émulsion. Les ions d'argent, chargés positivement, seront attirés par les points sensibles et se combineront pour donner de l'argent colloïdal métallique. Ce point sensible s'amplifiera et se stabilisera au fur et à mesure que d'autres atomes ionisés d'argent viendront s'agglomérer pour former un noyau réactionnel (de 4 à 6 sont nécessaires). Une image latente, invisible à l'oeil nu, se sera formée sur le film selon la position des sources énergétiques (lumière, rayonnement b).
L'image latente ainsi formée pourra être rendue visible par des procédures de développement et de fixation typique de la photographie. Le développeur sert à réduire l'halogénure d'argent en argent métallique autour du noyau réactionnel constituant l'image latente. Cela amplifie cette dernière des milliards de fois pour former une image visible. Après un rinçage à l'eau pour éliminer le développeur et éviter un sur-développement de l'image, on dissout l'halogénure d'argent résiduel avec le fixateur