REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Mouloud Mammeri de Tizi-Ouzou
Faculté de Génie Electrique et d'Informatique
Département d'Electronique

Mémoire de fin d'étude

En vue de l'obtention du diplôme d'ingénieur d'état en électronique
Option : contrôle

Thème

Tatouage d'images médicales par la technique CDMA

Proposé par :
M^r^ : M. LAHDIR

Réalisé par:
M^r^ : Boualem AIT SADOUNE
M^r^ : Younes OUALLOUCHE

Promotion: 2008

Remerciements

Nous tenons à exprimer nos vifs remerciements à notre promoteur M^{r} LAHDIR M. qui a proposé et dirigé ce travail. Qu'il trouve ici l'expression de notre profonde reconnaissance pour son soutien, son aide, ses conseils et sa patience tout au long de ce travail.

Nous remercions également les membres du jury pour l'honneur qu'ils nous font en acceptant de juger et d'évaluer notre travail.

Bien évidement, nous remercions nos familles respectives ainsi que nos amis.

Enfin, nous remercions tous ceux qui ont participé de prés ou de loin à notre formation tout au long de notre cursus universitaire.

Chapitre II : Le tatouage dans le domaine médicale

Chapitre III : Méthode adoptée

Introduction générale

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.

Le travail que nous présentons, a pour objectif de proposer une nouvelle méthode de tatouage des images numériques fondées sur la technique de multi-couche (CDMA -Code Division Multiple Access-) qui est une technique de multiplexage par code utilisé. Nous étudierons l'apport et les limites de cette méthode, ainsi les mesures objectives et subjectives de la qualité des images tatouées permettront d'évaluer les résultats.

Dans le premier chapitre, nous exposons les principes et propriétés générales des processus de tatouages et les différentes attaques qu'ils peuvent subir, ainsi que les différentes méthodes de tatouages d'images numériques. Les différentes images ainsi que l'importance du tatouage dans l'imagerie médicale est présentée dans le deuxième chapitre. Le troisième chapitre sera consacré à la présentation détaillée de notre méthode de tatouage. Les résultats des différents tests effectués en appliquant notre méthode sur images tests sont représentés dans le quatrième chapitre. Le dernier chapitre sera consacre à la description de notre logiciel. Nous terminons notre méthode par une conclusion générale et des perspectives.

I.1 Introduction

Depuis quelques années, l'utilisation des supports numériques a explosé. Ceux-ci offrent plusieurs avantages sur le support analogique: la qualité des données, que ce soit du texte, du son ou de l'image est supérieure, l'édition de ces données est facile, la copie est rapide et sans perte d'information, enfin la transmission en est aisée grâce aux nouveaux réseaux d'information. Cette facilité de la copie à l'identique est loin d'être sans dérive. Elle a notamment entraîné un boom du phénomène de piraterie sur la propriété intellectuelle, catalysé par l'expansion du système d'échange de données qu'est Internet et par le large accès à des supports de stockage. La lutte contre cette fraude s'organise autour de nouvelles techniques, entre autres celle du tatouage des données numériques (watermarking).

Le watermarking est une discipline récente qui trouve son origine dans le manque de techniques fiables de protections de donnée numérique. En effet, associé à d'autres techniques, cet axe de recherche a pour but de résoudre des problèmes aussi variés que la protection du copyright et des droits d'auteurs, la réglementation des copies, la prévention de la redistribution non autorisée, le suivi de documents et l'intégrité du contenu d'une donnée.

I.2 Définitions

I.2.1 Cryptographie

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité). Elle consiste à modifier le message primaire et rendre l'information que l'on désire transmettre complètement illisible pour toute personne ne possédant pas la donnée nécessaire à son décodage.

I.2.2 Stéganographie

C'est une technique qui a pour but de dissimuler un message secondaire dans un message primaire. Le message primaire reste lisible de tous. Son apparition remonte à l'antiquité, Parmi les astuces historiques, on note les encres invisibles, qui furent la méthode la plus utilisée au cours des siècles.

Ce procédé ressemble aux encres sympathiques, qui fut la plus utilisée des méthodes de stéganographie . On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait ou de certains produits chimiques. Il est invisible à l'œil, mais une simple

flamme, ou un bain dans un réactif chimique, révèle le message. L'exemple de la figure II.1 a été réalisé à l'aide du lait.

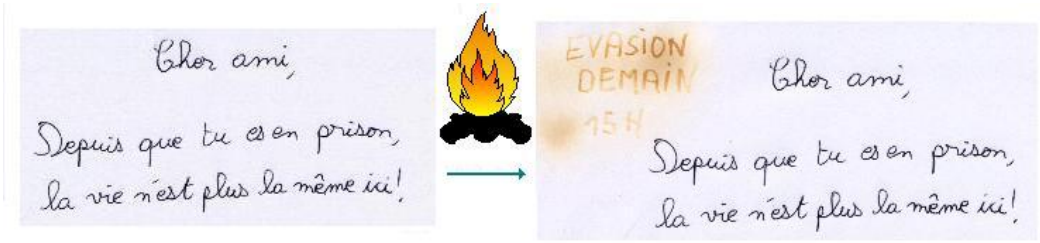


Figure I.1 procédé de la stéganographie ancienne

I.2.3 Tatouage d'images numériques

Le tatouage d'image numérique est une technique qui a été envisagé pour la première fois au cours des années 70, il a réellement trouvé ses applications lors de l'explosion de l'utilisation du support numérique, dans les années 90.

Le tatouage d'images numériques, plus connu sous le nom de «digital watermarking », est une technique encore jeune, qui consiste à dissimuler au sein même de l'information visuelle (une image numérique), une information cachée identifiant son propriétaire, ou son contenu. L'information ainsi ajoutée ne doit pas être perçue par l'œil humain. Ce qui permet de répondre à des problèmes de droit d'auteur ou d'intégrité.

I.3 Quelques applications du tatouage

I.3.1 Tatouage pour la protection de copyright

La première application envisagée pour le tatouage de documents a été la protection des droits d'auteurs. Son objectif est d'introduire une marque invisible, contenant un code copyright dans une image original. L'image marquée ou tatouée peut être distribuée en portant toujours la marque de son propriétaire. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, cette image peut subir diverses transformations licites ou illicites, ces transformations ont pour but de détruire la marque sans dégrader la qualité de l'image.

Le marquage étant protégé par un code secret ou une clé, seules les personnes autorisées peuvent savoir si l'image a été marquée ou lire la marque, d'où l'application des algorithmes de tatouage en utilisant une clé privé appartenant au propriétaire de l'image.

I.3.2 Le tatouage et l'authentification

L'information insérée au sein de l'image peut permettre de certifier qu'elle n'a pas été modifiée. On entre ici dans une problématique de contrôle d'intégrité des documents. Dans ce cas précis, la signature ajoutée est dite fragile à l'inverse des autres applications de tatouage, la marque est conçue de manière à se détériorer dès que le document est modifié.

I.4 Principe du tatouage

Le schéma de tatouage d'images se décompose en deux opérations distinctes illustrées par la figure I.2 :

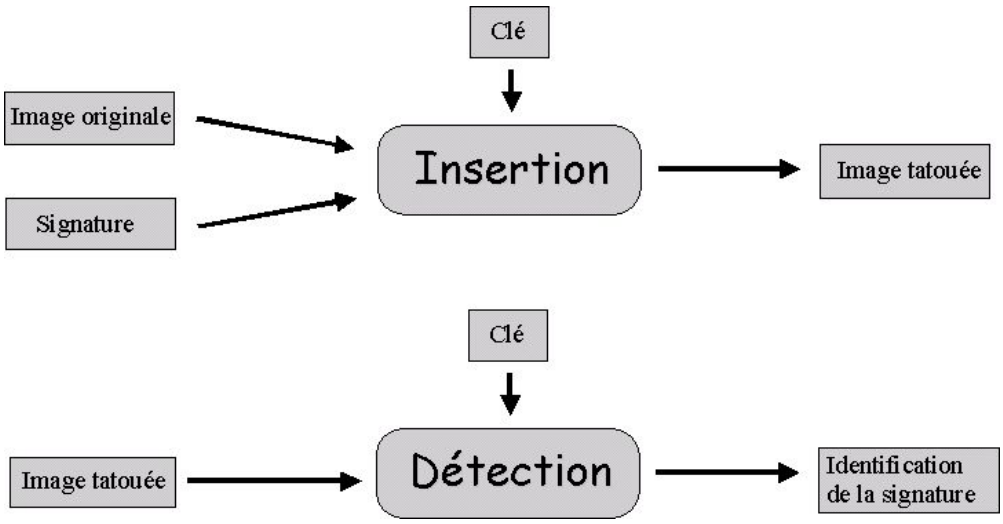


Figure I.2 Insertion et détection pour le tatouage d'images

I.4.1 La phase d'insertion

Elle consiste à introduire une marque dans l'image en vue d'identifier son propriétaire (le nom de l'auteur ou de l'entreprise par exemple). Cette insertion peut se faire dans le domaine spatial ou dans le domaine transformée (transformée de Fourier, en cosinus discrète, en ondelettes …).

I.4.2 La phase de détection

Elle permet de retrouver la marque ou la signature insérée. Cette étape est la plus souvent effectuée en aveugle, c'est à dire sans utiliser l'image originale (utiliser l'image originale donnerait un schéma plus lourd et pourrait poser des problèmes de sécurité). Entre l'insertion et la détection, l'image marquée peut subir des modifications licites ou illicites sous forme d'attaques qui visent a détérioré la marque.

I.5 Les caractéristiques générales du marquage

Pour être performant et efficace, le tatouage doit vérifier les trois critères suivants :

I.5.1 Le ratio ou capacité

C'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.

I.5.2 L'invisibilité

En pratique, l'intérêt d'un watermark efficace réside dans son invisibilité pour l'œil humain, et cela en évitant de rajouter le tatouage dans les zones uniformes de l'image. Il faut plutôt le mettre dans les zones fortement texturées et les contours, de telle sorte que la différence entre l'image tatouée et l'image originale soit la plus minime possible. Car le marquage ne doit pas empêcher la compréhension et ne doit pas dégrader la capacité diagnostique de ses images. Ainsi cachée, la marque est plus difficilement détruite par piratage.

I.5.3 Robustesse

Le tatouage doit être résistant aux attaques et manipulation de l'image. En effet, beaucoup d'attaques et de manipulations permettent de modifier l'image, de telle sorte qu'on ne puisse plus y déceler la marque du propriétaire. Donc l'algorithme doit être robuste pour tolérer certain changement de l'image tel que la compression, les rotations ou ajout de bruit.

Mais dans certain cas (contrôle d'intégrité), il est plus intéressant de favoriser la fragilité à la robustesse, car un tatouage avec un algorithme fragile permet par la suite de savoir si l'information marquée est toujours présente ou non.

I.6 Les différentes formes de marquage

I.6.1 Le marquage fragile

Dans le cas d'un marquage fragile ou faible, l'imperceptibilité doit être très grande et la robustesse très faible. Ainsi la marque ne supportera aucun traitement, ce qui nous permet de certifier ou non l'intégrité de l'image.

I.6.2 le marquage robuste

Il s'agit de la forme la plus utilisée en tatouage numérique, elle est en général imperceptible. Dans ce type de marque, on détermine le marquage visible comme un logo mais avec une robustesse à rude épreuve.

I.6.3 Marquage symétrique (privé)

Même principe que dans la cryptographie, le marquage symétrique signifie que l'on utilise la même clé pour insérer et détecter le tatouage, illustré sur la figure I.3.

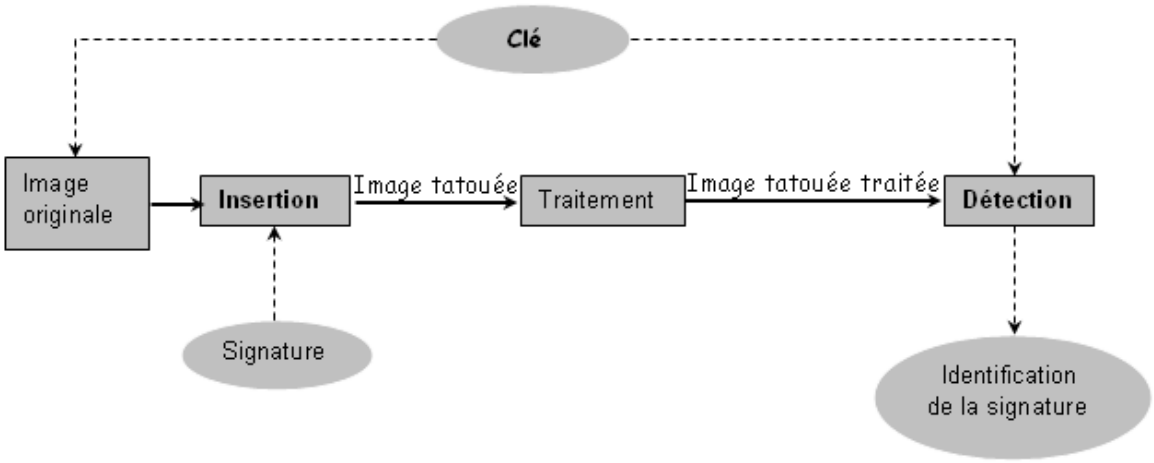


Figure I.3 Marquage symétrique

I.6.4 Marquage asymétrique

Dans ce type de marquage, la clé d'insertion et celle de détection sont différentes (voir la Figure I.4). L'intérêt est que n'importe qui peut lire la signature, sans pour autant pouvoir l'enlever ou la modifier.

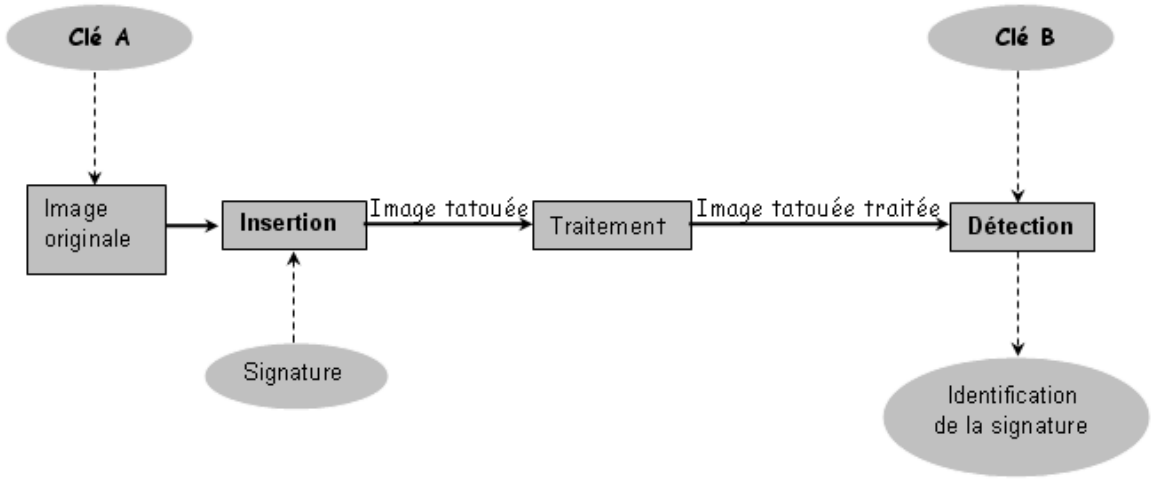


Figure I.4 Marquage asymétrique

I.7 Modèle général de marquage

I.7.1 Principe [1]

Nous verrons par la suite que, s'il existe de très nombreuses méthodes de marquage, toutes se basent sur le même principe général. La figure I.5 ci-dessous illustre ce principe (le médium peut être une image, un son, une vidéo,...):

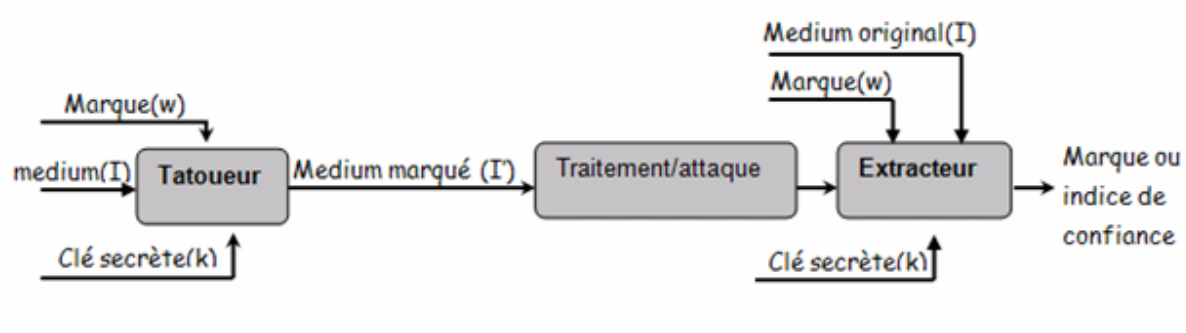


Figure I.5 Principe général d'un système de tatouage

Un système de marquage est constitué de deux entités: le tatoueur et l'extracteur. Le tatoueur a pour objectif d'insérer une marque (w) dans un médium (I) original. Cette insertion peut se faire suivant une clé secrète (k) qui sera alors nécessaire à l'extracteur.

Le médium, une fois marqué, peut subir diverses attaques, volontaires ou non, qui risquent de supprimer la marque ou de la rendre illisible.

L'extracteur a alors pour but (à partir du médium marqué et éventuellement de la clé et/ou de la marque et/ou du support original non marqué) d'extraire soit la marque elle-même, soit un indice de présence caractérisant la probabilité de présence de la marque dans le médium.

I.7.2 Caractérisation des modèles de marquage

Les systèmes de marquage peuvent être distingués grâce à différents paramètres, le premier et le plus caractéristique étant le domaine d'insertion/détection qui peut être par exemple : le domaine spatial, ou bien le domaine transformé.

La réversibilité ou l'irréversibilité des algorithmes est aussi une caractéristique importante. En effet, certaines méthodes offrent la possibilité, sous le contrôle d'une clé, de retirer la marque du support après qu'elle ait été lue.

De plus il existe plusieurs schémas de détection:

- **Schéma privé**

Le support original (image hôte) est nécessaire pour la détection, le détecteur peut être de type I ou type II;

Le détecteur est dit de Type I si :

(K, I, I') ⟶ W' *Extraction de la marque*

Le détecteur est dit de Type II si :

(W, K, I, I') ⟶ 0, 1 *la présence de la marque (1 ; la marque est détectée, 0 ; sinon)*

Ce schéma apporte beaucoup de robustesse grâce à la présence de l'image originale à la détection, ce qui facilite la création du schéma général de marquage.

- **Schéma semi-privé**

Ce type de schéma donne seulement une réponse sur la présence de la marque, sans utiliser l'image originale :

(W, K, I') ⟶ 0, 1

- **Schéma aveugle**

La détection aveugle extrait la marque insérée sans avoir à utiliser ni l'image originale, ni la marque W, seule la clef K est nécessaire pour ce type de schéma:

(K, I') ⟶ W

Enfin, le type des données marquées est bien sûr fondamental et peut être soit une image fixe (cas le plus répondu auquel nous nous limiterons), soit une vidéo, ou bien un son.

I.8 Evaluation des processus de tatouage

I.8.1 Qualité de l'image

Conformément aux cahiers des charges d'un processus de tatouage, il faut d'une part que l'image tatouée soit de la même qualité que l'image originale. D'autre part les attaques auxquelles le tatouage doit être robuste, doivent conserver la qualité de l'image.

I.8.2 Compromis invisibilité-robustesse

La force de tatouage est un coefficient α qui apparaît dans la plus part des algorithmes de tatouages, tel que : $I^{*}=I+\alpha W$. Ce qui implique que ce coefficient α intervient directement dans les performances de robustesse du schéma. Plus le marquage est fort, plus il est visible et plus il est robuste à certaines attaques.

I.9 Les Attaques

Les attaques sont toutes ces transformations licites ou illicites, ayant une influence directe sur l'image et sa marque. Pour être robuste, l'algorithme de tatouage doit permettre de pouvoir retrouver la marque du propriétaire dans l'image tatouée dans tous les cas, même si celle-ci a subi ces attaques malveillantes de la part de pirates. On distingue plusieurs cas d'attaques qui ont toutes comme objectif d'empêcher la bonne détection de la marque [2] :

I.9.1 Les attaques non-intentionnelles

Les images sont toujours le sujet de manipulation ayant pour objectif de faciliter leur exploitation. Alors, le tatouage doit résister à ces manipulations. Dans les exemples qui suivent, nous décrivons les principales attaques sur les images qui sont susceptible d'altérer la détection de la marque :

a. Le filtrage : Les images contenants des bruits ont toujours besoin d'être filtrées afin d'améliorer leur qualité et de minimiser l'effet de bruit. Le bruit peut provenir de sources diverses : de la conversion numérique analogique (impression), de la conversion analogique

numérique (scannage), ou encore de systèmes de transmission d'images,…De ce fait, cette attaque peut aussi être considérée comme une attaque malveillante.

b. La compression : Les algorithmes de compression sont particulièrement dangereux pour le processus de tatouage puisque leur objectif est l'opposé de celui du tatouage. En effet, la compression vise à ne garder de l'image que les composantes essentiels à sa compréhension ce qui engendre d'enlever le message inséré dans cette image.

c. Les transformations géométriques : Les transformations géométriques sont des modifications géométriques dans l'espace apporté sur l'image. On va étudier l'influence de ces transformations sur le tatouage des images. On peut distingué :

- **L'agrandissement de la taille de l'image :** L'agrandissement de l'image nous fait perdre le repérage des pixels tatoués dans l'image. Par conséquent, il est difficile d'extraire le message inséré par le processus de tatouage.
- **La réduction de l'image :** La réduction de l'image nous fait perdre aussi le repère des pixels tatoués. Par conséquent, il est difficile de localiser les pixels tatoués dans l'espace puisque la position de l'image transformée est différente de celle de l'image originale. D'où la nécessité de trouver des schémas de tatouage dans le domaine spatial qui soit robuste contre ce type de transformation.
- **La rotation :** Cette rotation imperceptible à l'œil nue engendrera la désynchronisation totale de l'image surtout lors du tatouage dans les transformées (fréquentiels et multi-résolutions).
- **Le cropping :** Faire le cropping d'une image consiste à en extraire une partie de l'image non désiré ou de la pertinence de détail d'une photo. Pour être résistant à ce type d'attaque, le tatouage doit être présent sur toute l'image. D'où la nécessité d'un tatouage dans le domaine spatial de l'image.

I.9.2 Les attaques intentionnelles (illicites)

Plusieurs outils commerciaux visent à détruire ou invalider le marquage d'une image, ces programmes sont appelés « crackers ». Ils ont pour but de détruire ce message et/ou de le désynchroniser. Ce type d'attaque devient nuisible lorsque le traitement arrive a retirer le message sans dégrader l'image. Dans ce cas, l'image risque de rester exploitable sans la

présence du message inséré. Nous nous contenterons de citer que les attaques les plus connues et les perturbations qu'elles font subir à l'image hôte, entre autre ;

a. Le debruitage : consiste à retrancher l'estimée de la marque causé par des opération de rehaussement et de lissage de l'image.

b. jettering : En traitement d'images, il s'explique par la suppression ou la duplication des lignes ou colonnes de l'image. Cette attaque dégrade peu l'image et déplace le message inséré, ce qui provoque pour la plupart des schémas une désynchronisation lors de la détection.

c. L'attaque par mosaïque : Elle consiste à diviser l'image tatouée en une mosaïque de plusieurs petites images. Les morceaux de l'image tatouée provoquent principalement une perte de synchronisation. Il suffit de la découper en plusieurs carrés de mosaïques.

d. Le logiciel stirmark [3] **:** Combine les différentes opérations géométriques principalement des destorsions, rotation et des translations qui permettent de désynchroniser le message insérer afin qu'il ne soit plus détectable.

e. Le logiciel unzign [4] **:** il permet d'effectuer des modifications invisibles sur les pixels de l'image (déplacement, suppression et/ou duplication de lignes et colonnes).

I.10 Les principales méthodes de tatouage d'images

Le but dans tout algorithme de tatouage d'images numériques est de pouvoir insérer une marque (ou signature) qui soit liée au propriétaire. Le plus souvent on choisit le nom du propriétaire ou celui de l'entreprise qui souhaite utiliser la méthode. Ce nom appelé label est ensuite codé en un message composé de 0 et de 1. La tendance actuelle est d'utiliser un message d'au moins 64 bits.

On peut classé les différentes méthodes de tatouage d'images selon :

I.10.1 Le domaine d'insertion :

I.10.1.1 Insertion dans le domaine spatial

Les méthodes spatiales consistent à insérer la marque directement dans l'image. Elles ont l'avantage d'être facilement implantables et les opérations d'insertions et de détections de la signature sont alors très rapides on temps de calcul mais sont pour le moment peu robustes aux attaques géométriques.

I.10.1.2 Insertion dans le domaine fréquentiel

Les méthodes fréquentielles sont des méthodes plus récentes dont le principe est d'insérer la marque non pas directement dans l'image mais dans le domaine transformée [7] : DCT, TFD, Ondelletes, fractales. Pour retrouver l'image marquée, on effectue la transformée inverse. Ces méthodes résistent mieux aux attaques géométriques.

I.10.1.3 Insertion dans le domaine multi résolution

Le domaine multi résolution est un espace du tatouage très intéressant car il est utilisé dans de récent standard de compression JPEG2000 ou encor MPEG4. Il se caractérise par la décomposition de l'image en sous bandes permettant d'isoler des composantes basse fréquences, celle-ci constituent un espace d'insertion pour la signature moins sensible aux modification sur l'image.

D'autre part, le contenu spatial de l'image reste conservé après une transformation multi résolution, ce même contenu peut alors servir à la localisation de la marque après une transformation géométrique.

I.10.2 L'état d'insertion de la marque :

I.10.2.1 Les méthodes additives :

Les processus de tatouage additifs sont les plus nombreux, ils consistent à ajouter la signature à des composants de l'image correspondant à un bruit.

Dans de telles circonstances, la difficulté consiste à mettre en forme le signal de telle sorte qu'il puisse être détecté malgré la présence de l'image originale.

a. Méthode du patchwork [6]

Cette méthode part d'une approche statistique de l'image. Elle se base sur le fait suivant: si l'on prend un grand nombre de fois deux points au hasard et qu'on soustrait leur luminance l'une à l'autre ($S=a-b$) la probabilité pour que S soit nul est très importante. La méthode du patchwork modifie artificiellement S pour une image donnée. Il est possible d'apporter à cette méthode certaines variantes comme modifier la forme des patchs ou même utiliser simplement des pixels seuls.

Cependant, elle possède plusieurs inconvénients, en plus de son manque de robustesse. D'une part elle ne permet d'insérer qu'une faible quantité de données. D'autre part le tatouage est facilement décryptable par une personne possédant plusieurs images utilisant la même clé.

b. Insertion dans le domaine transformée en cosinus discrète

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. La figure I.6 décrit un exemple de schéma d'insertion dans le domaine fréquentiel qui est la DCT.

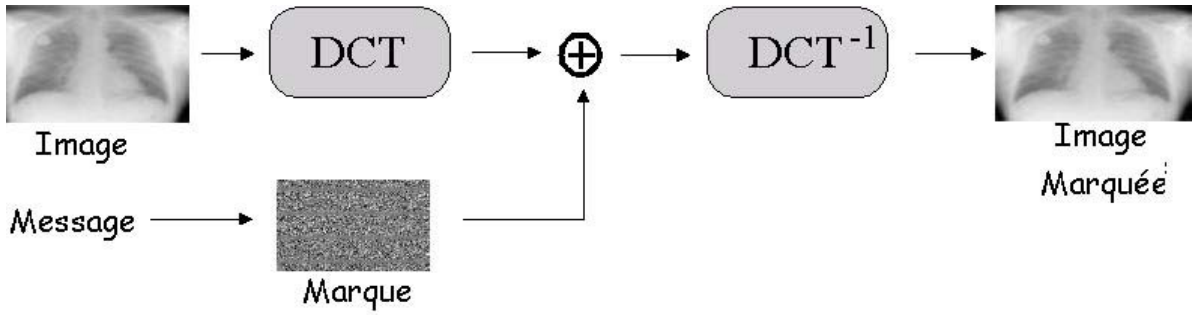


Figure I.6 Insertion d'une marque dans le domaine DCT

c. 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 [8].

I.10.2.2 Les méthodes substitutives :

Actuellement un grand intérêt est porté aux tatouage substitutifs qui représentent les méthodes pour lesquelles la marque n'est pas ajouter mais substituer et formée par modification de certaines composantes de l'image, ces composantes sont choisie de la même façon que pour les tatouages additifs, à l'aide d'une clé secrète K, la signature est ensuite adaptée à l'image originale par un masque psychovisuel par exemple.

a. Utilisation des bits de poids faible (LSB)

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. Si cette méthode obtient de bons résultats pour ce qui est de l'invisibilité, par contre, elle a l'inconvénient de facilité d'effacer la marque insérer [5]. Ce type de marquage n'est donc absolument pas robuste.

b. Utilisation de la transformée 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 [9]. 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.

I.11 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.

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.

II.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 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.

II.2 Imagerie médicale

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 pour l'établissement d'un diagnostic ou pour le traitement de pathologies mais également dans le cadre de travaux de recherche scientifique étudiant la physiologie des êtres vivants.

L'importance que revêt l'imagerie médicale tient d'abord au fait qu'une image est un concentré d'informations bien plus efficaces qu'un texte ou qu'une explication verbale. Elle est certainement l'un des domaines de la médecine qui a le plus progressé ces vingt dernières années. Ces récentes découvertes permettent non seulement un meilleur diagnostic mais offrent aussi de nouveaux espoirs de traitement pour de nombreuses maladies. Cancer, épilepsie…

II.3 Les différents types d'imagerie médicale

Suivant les techniques utilisées, les examens d'imagerie médicale permettent d'obtenir des informations sur l'anatomie des organes (leur taille, leur volume, leur localisation, la

forme d'une éventuelle lésion, etc.) ou sur leur fonctionnement (leur physiologie, leur métabolisme, etc.). Dans le premier cas on parle d'imagerie structurelle et dans le second d'imagerie fonctionnelle.

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

II.3.1 Imagerie par résonance magnétique (IRM) [15]

Définition

Le nom complet de l'IRM est image à résonance magnétique nucléaire (ou IRMN), on omet souvent son caractère nucléaire. Cette omission est surtout là pour ne pas effrayer les patients qui associent souvent, et à tort, le mot nucléaire avec les rayonnements ionisants.
L'IRM est une technique de diagnostique médical puissante qui fournit des images tridimensionnelles et en coupe de grande précision anatomique. L'IRM est une technique radiologique récente, non invasive et sans effets secondaires connus, basée sur le phénomène physique de résonance magnétique nucléaire. Il s'agit simplement d'observer la résonance magnétique nucléaire (RMN) des protons de l'eau contenue dans l'organisme, c'est à dire la réponse des noyaux soumis à un champ magnétique extérieur et à une excitation électromagnétique.

Principe

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 standard, 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 figure II.1 représente une image IRM d'un cerveau humain.

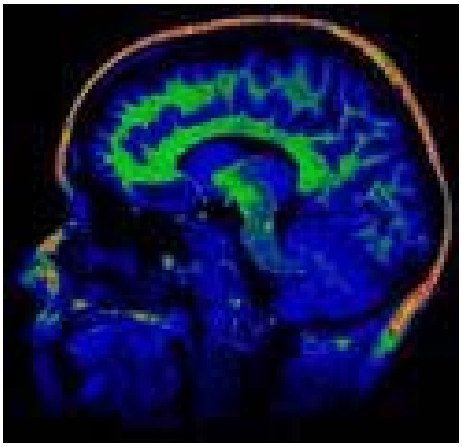


Figure II.1 Image IRM du cerveau humain

II.3.2 La Radiographie [16]

La radiographie par rayons X résulte des travaux de Roentgen en 1895. Même, si la technologie d'imagerie a évolué, le principe est resté le même. Il réside en une transmission de rayons X, qui 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 forte 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, comme illustré sur la figure II.2.

Le terme radiographie peut désigner l'ensemble des techniques permettant de réaliser des clichés à l'aide de rayons X des structures internes d'un patient ou d'un composant mécanique (la radiographie en général) et le cliché obtenu est une radiographie.

Généralement, la radiographie est utilisée pour le système osseux car il s'agit du système le plus visible sur une radiographie du corps. Permet donc d'effectuer des radiographies afin, par exemple, de déceler une fracture ou des tissus endommagés par une maladie (par exemple, radiographies pulmonaires).

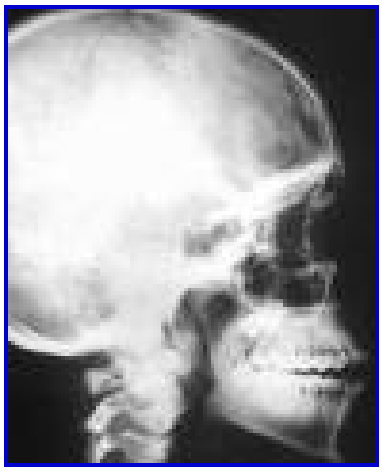


Figure II.2 Radiographies du crâne humain

II.3.3 Scanner ou tomodensitométrie (TDM) [17]

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, tel représenté sur la figure II.3. 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.

Figure II.3 Scanner cérébral

II.3.4 Ultrasonographie ou échographie [18]

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 des 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.)

En vérité, l'échographie est une étude des ombres, car les images ne sont pas des photographies en noir - blanc ou en couleurs de l'organe étudié ; elles ne sont que les ombres de cet organe et l'échographie (Figure II.4). À plusieurs reprises pendant l'examen, le radiologue ou sonagraphe gèlera l'image sur l'écran pour sauvegarder une image fixe dans le dossier du patient.

Figure II.4 Échographie d'un fœtus

II.3.5 La scintigraphie [19]

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, comme représenté sur la figure II.5.

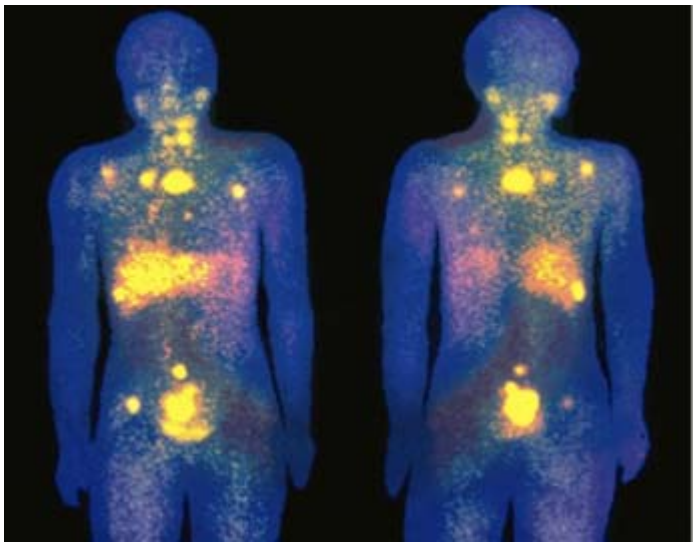


Figure II.5 La scintigraphie du corps humain

II.4 Définition de la télémédecine [10]

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).

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.

II.5 La sécurité des données médicales

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.

La sécurité des données médicale se fait pour des raisons de :

II.5.1 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.).

II.5.2 Authentification

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).

II.5.3 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.

II.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 standard, 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.

II.7 Le rôle du tatouage au sein des applications de Télémédecine

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 [11] :

II.7.1 Contrôle de la diffusion des images sur Internet

L'utilisation des réseaux publics pour transmettre ou donner accès à des images n'est pas sans poser problème. Ces images sont alors susceptibles d'être piratées et diffusées grâce à ces mêmes réseaux. L'utilisation des méthodes de tatouage d'image est alors assimilable à celle qui en est faite pour la protection du droit de propriété intellectuelle. Les propriétaires des images cherchent alors à contrôler la diffusion des images.

Ce contrôle se fait grâce à l'insertion d'une marque, la plus robuste possible, dans l'image. L'extracteur (un robot scrutant Internet) a accès aux marques insérées et les teste sur toutes les images qu'il rencontre. Les outils commerciaux répondant à cette demande sont nombreux, même si la robustesse des marques insérées est souvent mise en question.

II.7.2 Amélioration de la confidentialité

Les informations nécessaires à l'utilisation des images médicales sont présentes dans l'en-tête même de l'image. Ainsi le nom du patient, son âge, ses coordonnées mais aussi des informations concernant le médecin peuvent être lues par toute personne ayant accès à l'image. Cette facilité de lecture n'est pas sans poser un problème de confidentialité, question critique dans le domaine médical.

Le tatouage d'images permettrait alors de supprimer les informations confidentielles de l'en-tête pour les insérer directement dans l'image elle-même. Ces informations ne seraient plus alors directement accessibles mais leur obtention nécessiterait l'utilisation du logiciel d'extraction. Il serait de même possible, grâce à l'utilisation de clés, d'améliorer le contrôle de l'accès à ces informations.

II.7.3 Insertion de données intéressantes pour éviter la perte d'information

Malgré la taille de l'en-tête DICOM, toutes les informations intéressantes pour les médecins n'y ont pas leur place. Il pourrait donc être utile d'insérer ces données dans l'image. Cette solution permettrait de rester conforme à la norme DICOM car elle ne nécessiterait pas à l'ajout de nouveaux champs dans l'en-tête.

La facilité de l'accès aux informations de l'en-tête et de leur modification fait qu'elles peuvent être facilement perdues ou modifiées. Insérer les informations critiques, comme par exemple des identifiants du patient et de l'hôpital, peut être une réponse à ce type de problème. En effet, ceci permettrait, en cas de perte ou de doute quant à l'authenticité des informations de l'en-tête, de retrouver l'information originale.

II.8 Exemple de tatouage utilisé dans le domaine de l’imagerie médicale

Le tatouage multiple [12]

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. 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 II.6 présente un schéma d’insertion général de cette méthode de tatouage.

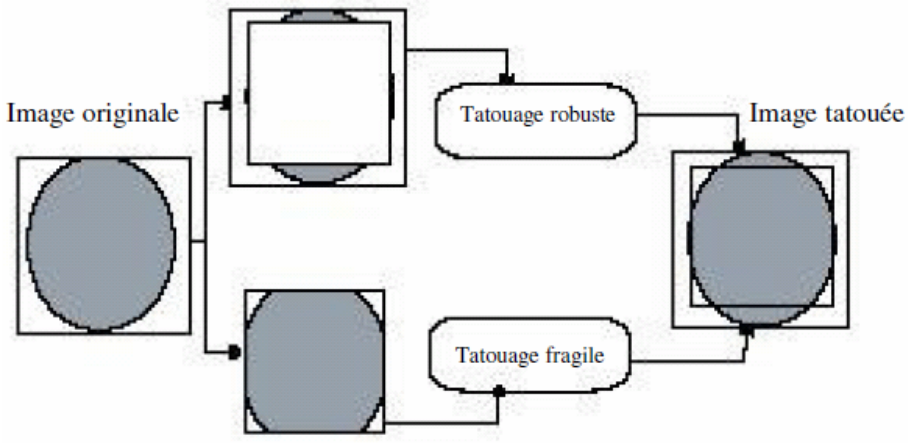


Figure II.6 schéma d'insertion d'un tatouage multiple

Pour la marque d'annotation, elle est arrangée sous forme d'un cadre qui s'adapte à la bordure de l'image (voir figure II.7), on l'insère ensuite d'une manière avec la transformée en ondelettes appliquée sur la bordure de l'image originale.

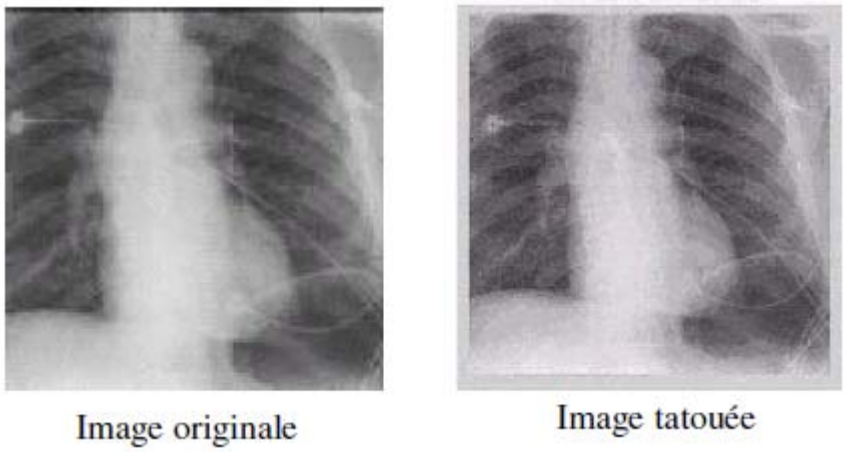


Figure II.7 Exemple d'image tatouée avec un tatouage multiple

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 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.

II.9 Conclusion

Malgré le fort développement qu'a connu l'imagerie médicale, son utilisation, en particulier, sa transmission en dehors et même au sein de l'hôpital à travers des réseaux publics et privés reste vulnérable face aux failles de sécurité liées aux différentes attaques, comme des erreurs de transmission et des compressions à perte, ce qui porte atteinte a la confidentialité des données médicales, l'authentification et l'intégrité des ces images.

Pour remédier au problème 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.

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.

III.1 Introduction

Notre projet a été consacré au tatouage d'imagerie médicale sous le format "BitMap Picture" que nous utilisons à travers l'extension "bmp", qui signifie en français "Cartographie binaire de l'image ", et plus spécifiquement dans le domaine spatial.

Il a été décidé de ne s'intéresser qu'à des images codées en 256 niveaux de gris. Ce choix est judicieux à plusieurs égards :

La plupart des images médicales sont codées en 256 niveaux de gris qui sont la base de travail de la plupart des algorithmes de traitement d'images.

Il est préférable d'obtenir des résultats sous certaines contraintes et de rendre ensuite l'algorithme générique que d'essayer d'obtenir directement un algorithme générique sans jamais y parvenir.

Pour passer d'images codées en niveaux de gris à des images couleurs une première approche consiste à appliquer l'algorithme à la luminance des images couleurs.

III.2 Innovation

L'innovation principale de la méthode multicouche consiste à utiliser une technique très connue en communication numérique « la technique CDMA » et à l'appliquer au domaine du traitement d'images.

En communication et plus particulièrement en communication sans fil, la technique CDMA (Code Digital Multi Access) permet de pouvoir mélanger plusieurs signaux à l'émission, le but étant de pouvoir transmettre plusieurs communications en même temps et non pas l'une après l'autre.

Appliquée au tatouage d'images cette méthode peut nous permettre d'insérer une quantité d'information plus importante dans l'image sans pour autant dégrader sa capacité diagnostique.

III.3 Principe de la méthode

La méthode proposée suit un schéma classique d'insertion dans le domaine spatial, la détection s'effectue en utilisant des méthodes de corrélation. Dans ce qui suit on décrit cette méthode.

III.3.1 Méthode de référence

La première étape consiste à générer une Séquence Binaire Pseudo Aléatoire (SBPA) à l'aide d'une clé secrète, uniquement connue du propriétaire. Cette séquence est composée uniquement de +1 et de –1 et elle est de moyenne nulle.

Cette séquence à une dimension est ensuite transformée en une séquence à deux dimensions qui formera la marque (on la nommera SBPA 2D).

La détection se fait le plus souvent par corrélation : en effet 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. Donc pour détecter la signature, il suffit de calculer l'intercorrélation de la marque avec l'image marquée.

Cette méthode très simple et efficace nous permet donc de pouvoir insérer un seul bit dans l'image. On dira que le bit 1 a été inséré dans l'image si le résultat de la corrélation est positif (+SBPA), dans le cas contraire c à d si le bit inséré est un 0, le résultat de la corrélation serait négatif (-SBPA). La section suivante montre une première approche qui permet de pouvoir insérer plusieurs bits en utilisant la même démarche.

III.3.2 Découpage en blocs

Pour pouvoir insérer plusieurs bits, l'idée est de découper l'image en blocs et de répéter la méthode précédente sur chaque bloc de l'image. Par exemple pour insérer un message de 8 bits dans une image 64*64, on suivra la démarche suivante :

- On découpe l'image en 8 blocs de taille 16*32.
- On génère une SBPA 2D avec une clé secrète de taille 16*32, qu'on appellera S.
- On remplit chaque bloc i par +S (si le bit i du message est égal à 1) ou par –S (si le bit i du message est égal à 0).
- La marque ainsi formée est ajoutée à l'image.

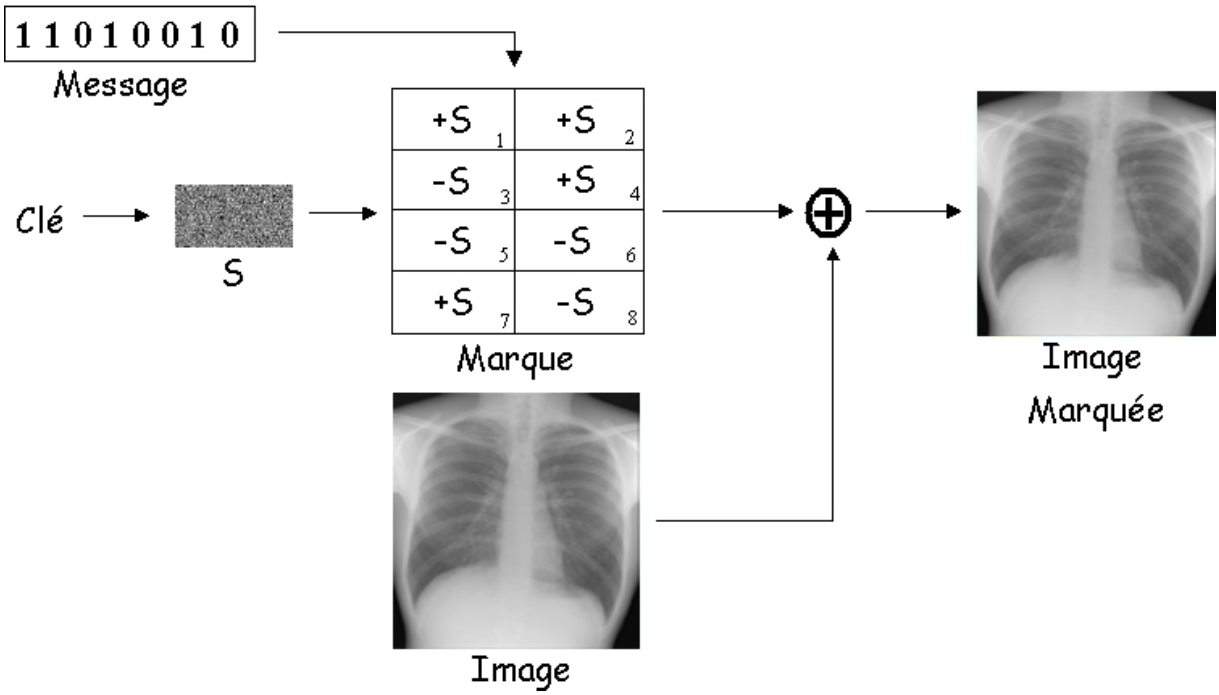


Figure III.1 Insertion pour un découpage en blocs

Pour détecter le message sur l'image marquée, on effectue la corrélation de S avec chaque bloc de 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.

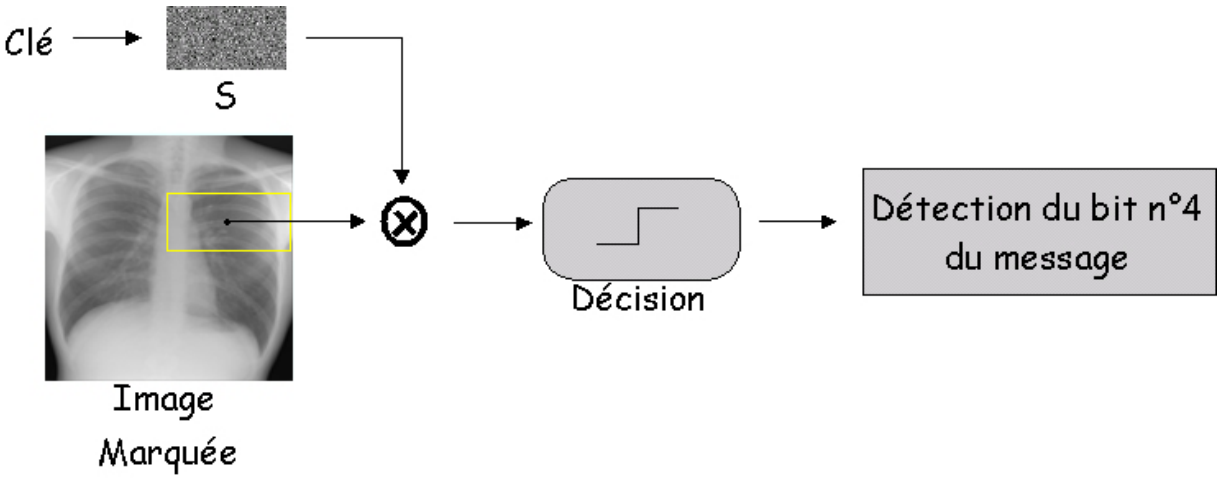


Figure III.2 Détection pour un découpage en blocs

Exemple de détection d'un bit

Soient $B_1(m,n)$ le bloc n°1 de l'image et $S(m,n)$ la SBPA 2D générée, avec $0 \leq m \leq 15$ et $0 \leq n \leq 31$. Pour insérer un bit égal à 1 dans B_1, on forme le bloc marqué B_{w1} de tel sorte que :

$$B_{w1}(m,n) = B_1(m,n) + S(m,n) \quad \text{(III.1)}$$

Chacun des blocs de l'image est marqué de la même manière pour former la totalité de l'image marquée. Ensuite la détection du bit du bloc n°1 sera effectuée en calculant :

$$Corr(B_{w1}, S) = Corr_0(B_1, S) + Corr_0(S, S) \quad \text{(III.2)}$$

$$Corr(B_{w1}, S) = \sum_{m=0}^{16}\sum_{n=0}^{32} B_1(m,n) \times \pm 1 + \sum_{m=0}^{16}\sum_{n=0}^{32} 1 \times 1 = \varepsilon + 512 = 512 \quad \text{(III.3)}$$

Avec $\varepsilon << 512$

Le résultat est positif, donc le bit détecté est 1. Si on avait inséré le bit 0, on aurait eu:

$$Corr(B_{w1}, S) = Corr_0(B_1, S) - Corr_0(S, S) \quad \text{(III.4)}$$

Dans ce qui suit on va présenter l'apport majeur de la technique multicouche qui consiste à combiner la technique CDMA éprouvée en communications à la méthode décrite ci-dessus.

III.3.3 La technique CDMA en tatouage d'images

La méthode présentée ci-dessus nous permet d'insérer plusieurs bits dans l'image ; cependant plus le nombre de bit sera élevé et plus la SBPA 2D aura des dimensions faibles. Par exemple, si on veut insérer 64 bits dans une image 512*512, la SBPA 2D sera de taille 64*64. La détection de chaque bit se fera donc autour de 4096 (= 64*64). Après un filtrage malveillant ou une compression JPEG, ce seuil de détection chutera très vite et il deviendra donc très difficile de pouvoir 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.

L'idée est donc d'appliquer cette méthode au tatouage d'images pour pouvoir insérer un nombre de bits plus conséquent dans l'image. Pour ce faire on va ajouter plusieurs marques pour former la marque définitive. Donc pour ajouter les 64 bits dans l'image 512*512 on ne formera pas 64 blocs 64*64 mais 2 couches de 32 blocs 128*64 que l'on superposera, ou encore 4 couches de 16 blocs 128*128. La section suivante va nous permettre d'expliciter plus amplement cette démarche.

III.4 Description de la technique multicouche

III.4.1 Principe

Cette méthode consiste à superposer plusieurs couches pour pouvoir augmenter la taille de la SBPA 2D de départ et donc d'améliorer la détection de chaque bit du message.

Pour chaque couche on affectera une SBPA 2D différente (et donc une clé différente) : en effet si deux couches avaient la même SBPA 2D initiale, il arriverait que sur certains blocs on ajoute la SBPA 2D avec la première couche puis on la retranche avec la seconde; finalement la marque ne serait pas présente pour ce bloc et la détection serait donc fausse dès le départ. Cette méthode a l'avantage de ne pas trop détériorer l'image : en effet sur un schéma à 8 couches, on ajoutera sur chaque bloc de l'image des coefficients égaux à +8, +6, +4, +2, 0, -2, -4, -6, -8, avec une probabilité plus importante pour le coefficient 0 et une probabilité qui décroît d'autant plus que le coefficient est élevée.

Dans notre application, on s'est limité à un nombre maximal de 8 couches ; au delà de 8 couches il y aurait en effet un risque de trop détériorer l'image. Si on prend 12 couches par exemple, il est possible sur un bloc d'ajouter à l'image des valeurs égales à +12 ou –12 .La figure III.3 décrit la méthode pour un schéma à 1, 2, 4 ou 8 couches pour une image 512*512 et pour l'insertion d'un message de 64 bits.

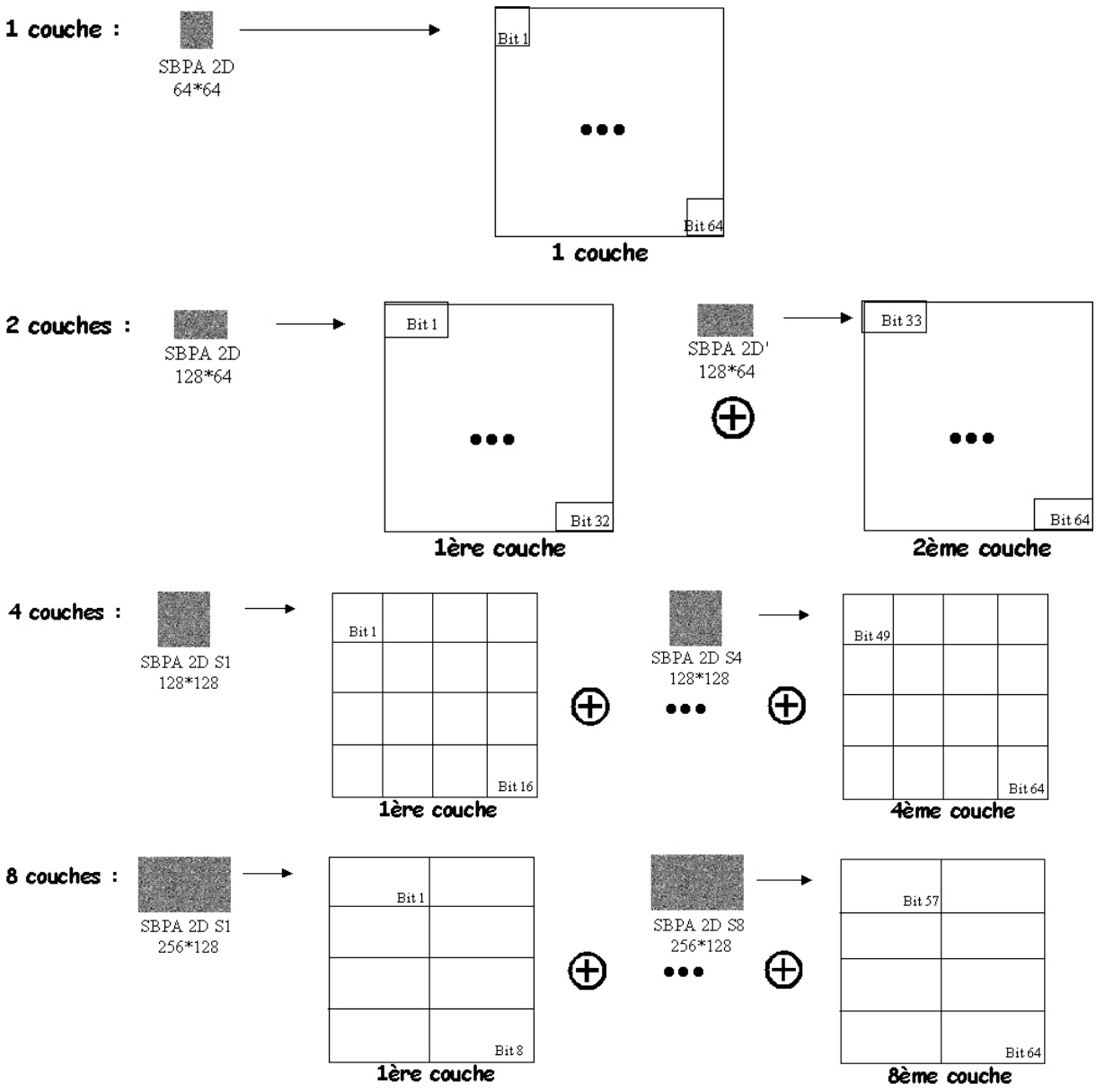


Figure III.1 Construction de la marque dans un schéma multicouche

III.4.2 Intérêts et inconvénients de la technique multicouche

La technique multicouche permet d'améliorer la détection de chaque bit : en effet, plus il y a de couches et plus les dimensions de chaque SBPA 2D augmentent et donc plus le seuil de détection (valeur moyenne de l'intercorrélation Marque/Image Marquée) pour chaque bit augmente. Le tableau ci-dessous donne les seuils de détection pour une image 512*512 :

	1 couche	2 couches	4 couches	8 couches
Nombre de blocs par couche	64	32	16	8
Taille de chaque SBPA 2D	64*64	128*64	128*128	256*128
Seuil de détection	4096	8192	16 384	32768

Tableau III.1 seuil de détection fonction du nombre de couches

Plus le seuil de détection est grand et plus l'algorithme est robuste aux attaques malveillantes dues au traitement d'images. En outre à chaque couche correspond une SBPA 2D qui elle-même dépend d'une clé secrète; le nombre de clés secrètes à posséder est donc égal au nombre de couches utilisées. Ainsi plus on utilisera de couches, plus on utilisera de clés secrètes et plus la SBPA sera de grande taille donc plus l'algorithme sera robuste à des attaques cryptographiques.

L'inconvénient de cette méthode concerne l'aspect visuel, puisque l'on n'ajoute pas seulement des +1 ou –1, mais on peut ajouter, dans le cas du modèle à 8 couches, jusqu'à des +8 ou –8 ; ce qui peut dégrader sérieusement et porter atteinte à la capacité diagnostique de l'image. Cependant il faut noter que la probabilité d'avoir des +8 ou des –8 est très faible par rapport à celle d'avoir des 0 ou des +/- 2 par exemple. Le tableau ci-dessous résume les différentes probabilités dans le cas d'un schéma à 8 couches :

Coefficient ajouté	+/-8	+/-6	+/-4	+/-2	0
Probabilité	1/256	8/256	28/256	56/256	70/256

Tableau III.2 les différentes probabilités d'un schéma à 8 couches

De ce tableau on peut constater que les coefficients les plus fréquents sur une marque dans un schéma à 8 couches sont les coefficients –2, 0 et +2, c'est à dire ceux qui ont l'avantage de ne pas trop marquer l'image.

Cependant il peut arriver que parfois des coefficients égaux à +/-6 ou +/-8 soient présents. Ceci nous pousse donc à avoir une stratégie spécifique sur la marque pour éviter que ces coefficients nuisent à l'invisibilité de la marque. C'est l'objet de la section III.6.

III.5 Génération de la SBPA

La SBPA est un signal pseudo aléatoire car elle est caractérisée par une «longueur de séquence» à l'intérieur de laquelle les variations de la largeur des impulsions varient aléatoirement. Elle est générée à l'aide de registres à décalage (réalisés en matériel ou logiciel) bouclés. La longueur maximale d'une séquence est 2^N où N est le nombre de cellules (étages) du registre à décalage. La figure III.4 présente la génération d'une SBPA de longueur $8 = 2^3$ obtenue à l'aide d'un registre à décalage ayant 3 cellules.

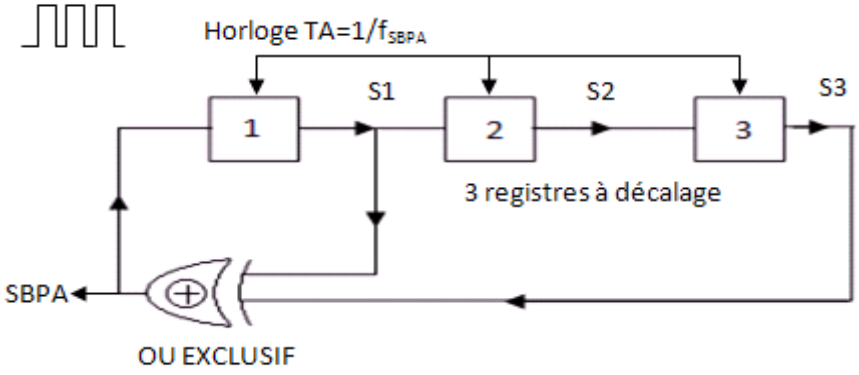


Figure III.4 Génération d'une SBPA de longueure 8

Pour cet exemple on aura le chronogramme suivant :

T_A	S1	S2	S3	SBPA
0	1	1	1	0
$1T_A$	0	1	1	1
$2T_A$	1	0	1	0
$3T_A$	0	1	0	0
$4T_A$	0	0	1	1
$5T_A$	1	0	0	1
$6T_A$	1	1	0	1
$7T_A$	1	1	1	0
$8T_A$	0	1	1	

Tableau III.3 chronogramme de la SBPA de l'exemple précédant

Comme la SBPA ne contient que des 1 et -1, on a fait en sorte dans notre application que le 0 redevient un -1 et le 1 reste tel quel. Et bien sûr l'exemple nous montre que la séquence est bel et bien de moyenne nulle.

Pour bien choisir le montage qui nous donne la bonne SBPA, on défini le polynôme f(x) qui caractérise les déffirents montages possibles :

$$F(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \qquad \text{(III.5)}$$

avec $a_j = 1$ si l'étage j est relié au OU EXCLUSIF ;

$a_j = 0$ Sinon ; et aussi $a_0 = 1$ comme condition initiale;

n (nombre d'étages) qui est fonction de la longueur da la séquence ($l=2^n$) étant fixé, le montage qu'il faut choisir est celui qui correspond au polynôme octal irréductible donné par le tableau suivant:

Nombre de bascules (n)	Longueur de la SBPA ($l=2^n$)	Polynôme irréductible	Ecriture octale de ce polynôme
2	4	$1+x+x^2$	7
3	8	$1+x+x^3$	13
4	16	$1+x+x^4$	23
5	32		45
6	64	$1+x+x^6$	103
7	128		211
8	256		435
9	512	$1+x^4+x^9$	1021
10	1024	$1+x^3+x^{10}$	2011
11	2048	$1+x^2+x^{11}$	4005
12	4096	$1+x+x^4+x^6+x^{12}$	10123
13	8192	$1+x+x^3+x^4+x^{13}$	20033
14	16383	$1+x+x^6+x^{10}+x^{14}$	42103
15	32767	$1+x+x^{15}$	100003

Tableau III.4 polynômes irréductibles sous forme octale (base8)

Une fois que la SBPA qui est composée uniquement de +1 et de –1 et est de moyenne nulle (c'est à dire autant de –1 que de +1) a été générée, on va la modulée avec le message à insérer puis ensuite la transformé en un signal à deux dimensions : pour cela on remplit ligne par ligne ce signal 2D. Pour un bloc 12*12, il faudra donc une séquence S de 144 échantillons. Cette marque est ensuite ajoutée directement au bloc de l'image qu'on veut marquer.

Pour avoir une marque très peu visible, l'idée est de cacher l'information dans les zones texturées et les contours de l'image, là où elle sera la moins visible. Dans ce contexte, nous avons utilisé un masque psychovisuel.

III.6 masque psychovisuel

Le masque psychovisuel utilisé découle du calcul de la variance locale. Pour chaque pixel de l'image, on calcule la variance du bloc de taille arbitraire 3*3 centré sur le pixel :

-	-	-
-	*	-
-	-	-

Sa formule mathématique est :

$$VarB_i(x,y) = \frac{1}{9} * \sum_{u=x-1}^{x+1} \sum_{v=y-1}^{y+1} \left(B_i^2(u,v) - \left(\frac{1}{9} * \sum_{u=x-1}^{x+1} \sum_{v=y-1}^{y+1} B_i(u,v) \right)^2 \right) \quad \text{(III.6)}$$

Cette 'image-variance' est ensuite recadrée entre deux coefficients min et max que l'on peut régler avant d'utiliser l'algorithme, pour être ensuite directement multiplié à la SBPA 2D. Avec ces deux coefficients on peut ainsi décider de plus ou moins marquer l'image: plus max est grand et plus la marque sera visible mais plus elle sera facilement détectable (pour les parties les plus texturées). Plus min sera faible et moins l'image sera dégradée mais plus difficilement elle sera détectable (pour les parties les moins texturées). Notre masque sera défini comme suit :

$$Masque_{HVSF} = \min + \frac{\max + \min}{\max(Var_B)} * \left(Var_B - \min(Var_b)\right) \quad \text{(III.7)}$$

Après avoir construit le masque, il suffit de le multiplier à la SBPA 2D pour former la marque à insérer. La dernière étape consiste à la multiplier par le facteur *coeff* pour régler la puissance de la signature. Ce dernier produit nous donne la marque définitive que l'on pourra directement insérer dans l'image. La figure III.5 donne un exemple de marque modulée par un masque psychovisuel.

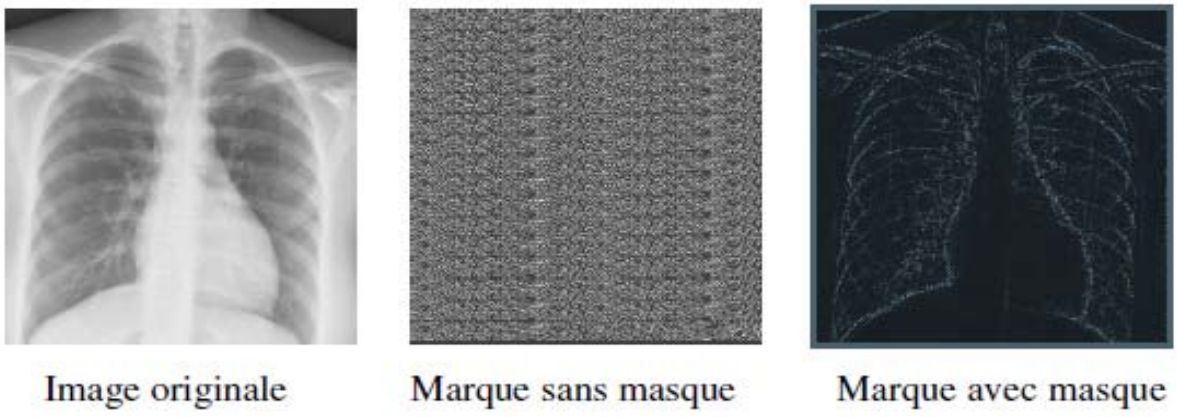


Figure III.5 Utilisation d'un masque psychovisuel

III.7 Insertion

Après avoir résumé les différentes étapes de création de la marque, nous pouvons maintenant résumer le schéma définitif d'insertion de la marque :

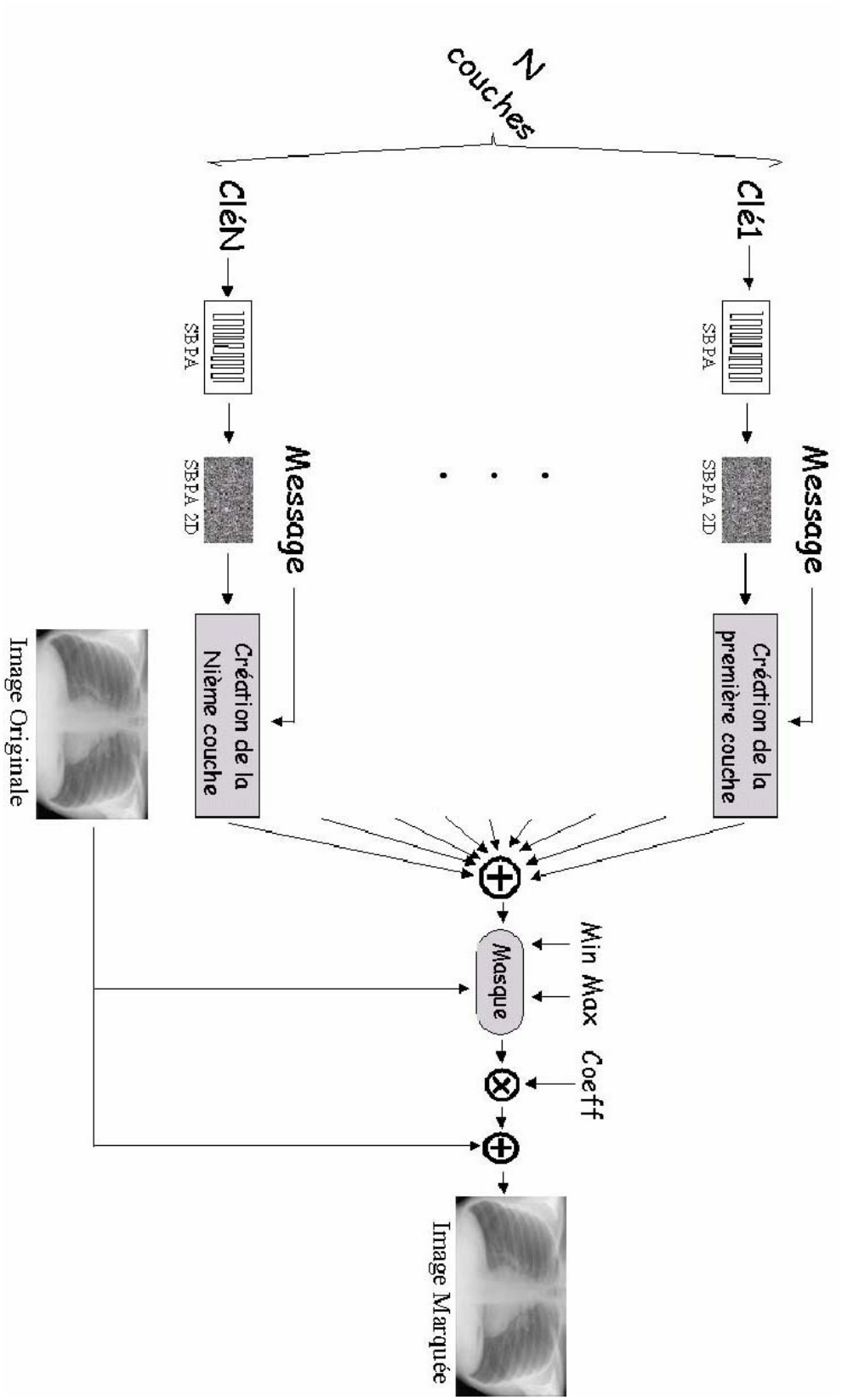


Figure III.6 Schéma d'insertion

Sans utilisation de masque psychovisuel, on peut donc résumer la phase d'insertion par la formule suivante :

$$B^w = B + M * S \tag{III.8}$$

Avec le coefficient de visibilité α et ⊗ (qui représente une multiplication pixel à pixel), on peut définir finalement la phase d'insertion comme suit :

$$B^w = B + \alpha * (M * S) \otimes Masque_{HVSF} \tag{III.9}$$

Mathématiquement, on peut donc définir la phase d'insertion complète par la formule (III.10) qui suit :

$$B^w(x,y) = B(x,y) + \alpha\left(\sum_{j=0}^{k-1} m_{j,i} * S(x,y)\right)\left(\min + \frac{\max - \min}{256} * \left[\frac{1}{9}\sum_{u=x-1}^{x+1}\sum_{v=y-1}^{y+1}\left(B^2(u,v) - \left(\frac{1}{9}\sum_{u=x-1}^{x+1}\sum_{v=y-1}^{y+1} B(u,y)\right)^2\right)\right]\right)$$

III.8 Détection

Pour améliorer la détection des différents bits du message, l'image marquée a d'abord été filtrée pour prédire la marque. Nous allons remédier a cela on utilisant le filtrage de Wiener.

Prédiction de Wiener : La formule de Wiener provient d'une méthode d'estimation par les moindres carrés ; on considère que l'on travaille avec des réalisations d'un processus aléatoire stationnaire et ergodique. On va chercher à retrouver notre marque W à partir de l'image marquée I_W. La formule de Wiener est la suivante :

$$W_{est} = \frac{Var(W)}{Var(W) + Var(I_w)} * \left(I_w - Moy(I_w)\right) \tag{III.11}$$

Les variances et les moyennes sont calculées localement, c'est à dire sur un bloc 5*5 autour de chaque pixel.

Pour chaque bit du message insérer, la détection suit le même schéma que celui de la figure III.2. En y ajoutant la prédiction de Wiener on obtient donc le schéma définitif de détection qui représenté sur la figure suivante :

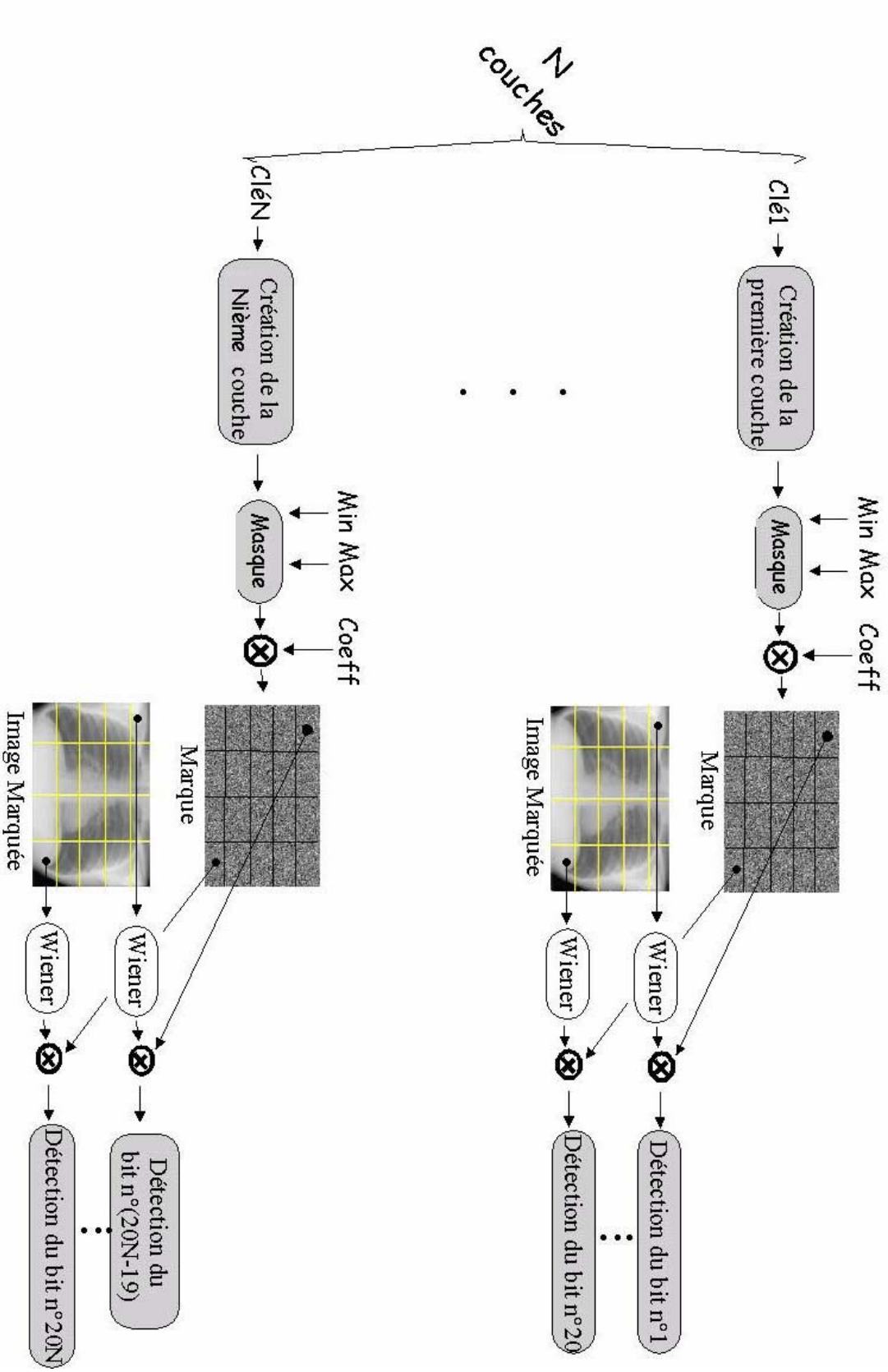


Figure III.7 Schéma de détection

III.9 Conclusion

Dans ce chapitre, on a étudié l'application de notre méthode de tatouage qui est basée sur la technique de multicouche (CDMA) pour l'image médicale en générant la séquence binaire pseudo aléatoire (SBPA) combiné par des formules mathématiques nécessaire pour l'insertion et la détection du message, avec l'illustration de tout par des schémas explicite.

Cette méthode vise à augmenter le nombre de bits insérer dans l'image sans pour autant la dégrader. L'un des inconvénients de cette méthode est que l'utilisateur doit manipuler plusieurs données : Clés, nombre de couche, nombre d'étage (nombre de bits de la clé), etc., ceci devient contraignant lorsqu'il s'agit de gérer un nombre important d'images.

On évaluera notre méthode dans le chapitre suivant grâce aux testes et résultats pour conclure après sur sa robustesse et son invisibilité.

IV.1 Introduction

Nous allons dans ce chapitre évaluer notre méthode de tatouage par une série de tests sur une image de radiographie médicale du thorax humain qui est représentée sur la figure IV.1, les résultats obtenus seront représentés sous forme de tableaux et de graphes commentés, tout en discutant ses avantages et ses inconvénient (limites).

Pour cela, plusieurs paramètres entrant dans notre étude seront pris en compte afin de servir de critères d'évaluation de la méthode.

Ces paramètres sont :

- Nombres de bits erronés du message.
- Invisibilité de la marque ou taux de dégradation de l'image.
- PSNR et wPSNR qui mesurent la qualité de l'image traitée par rapport à l'image originale.

Notons que ces paramètres évoluent selon :

- Le nombre de couches pour le tatouage ainsi que leurs seuils de détection.
- La valeur du coefficient de tatouage α.
- La présence ou pas du masque psychovisuel lors de l'insertion, ainsi que ses paramètres min et max.
- La présence ou pas du filtre de Wiener lors de la détection.

Figure IV.1 Radiographie thoracique de face

IV.2 Détection

Tout algorithme de tatouage d'images doit pouvoir détecter la marque insérée dans l'image, et il doit aussi pouvoir la différencier des autres marques. Cette distinction doit être la plus évidente possible, dans le but d'éviter toute confusion.

On a donc testé notre méthode sur une large fourchette de jeux de clés, avec des schémas à 1, 2, 4 et 8 couches, sur une image 256*256 dans laquelle on a insérée un message de 64 bits. Pour comparer les 4 schémas, on a calculé le seuil moyen de détection pour les 64 bits. Aucune attaque n'a été portée sur l'image ni de masque psychovisuel utilisé. Le tableau IV.1 représente le seuil moyen de détection pour les déférents schémas :

Nombre de couches	1 couche	2 couches	4 couches	8 couches
Seuil de détection	1020	2040	4080	8160

Tableau IV.1 seuil moyen de détection

Ces résultats sont obtenus sans marquer considérablement l'image comme on peut le voir sur la figure IV.2 :

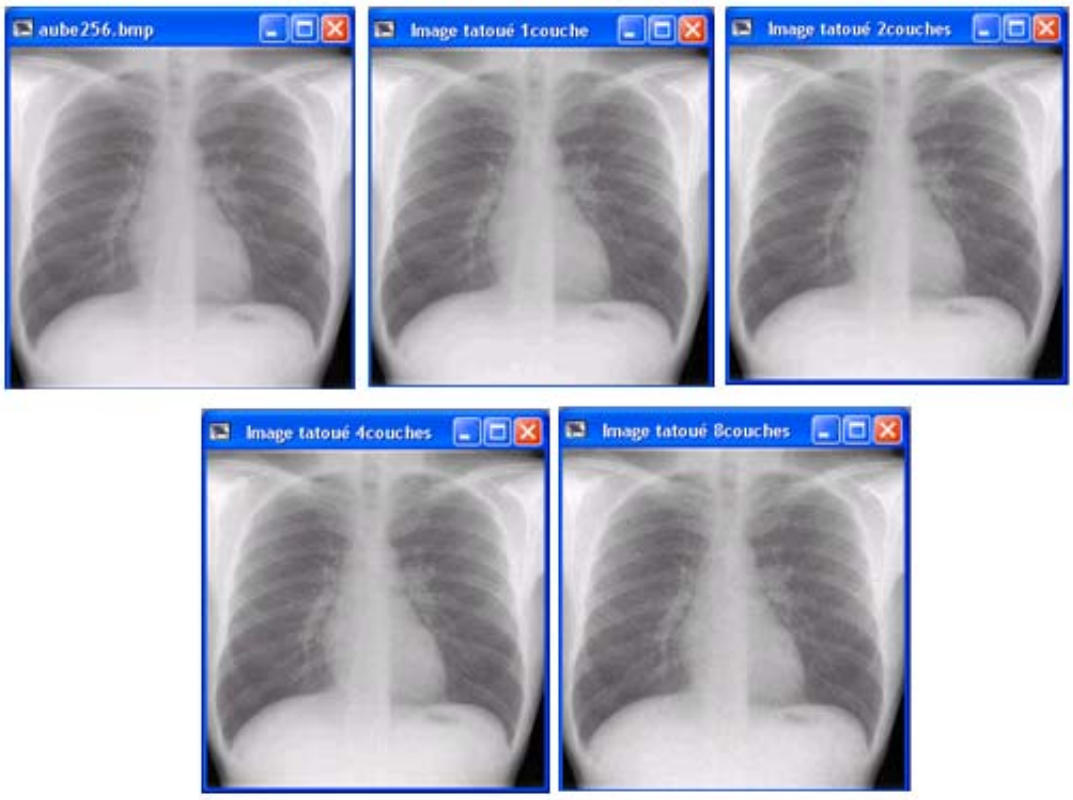


Figure IV .2 Influence de la marque sur l'image

Puisque la détection ne pose aucun problème sans attaque, il faut maintenant confronter l'algorithme à des attaques. On a décidé de le valider face aux attaques de traitement d'images et aux attaques géométriques, pour cela on a testé la détection de la marque tout d'abord après une compression JPEG pour fixer les paramètres de notre algorithme, ensuite on a validé notre schéma face à d'autres attaques de traitement d'images (filtrage, image négative …), puis au finale on le teste par rapport aux attaques géométriques.

IV.2 Robustesse

Pour bien préserver les données d'un passion ou d'un médecin, l'algorithme de tatouage doit en premier lieu faire face aux différentes attaques (section I.9) qu'il peut subir. Nous allons commencer nos tests par la compression JPEG afin de fixer les paramètres de notre algorithme.

IV.2.1 Compression JPEG [13]

Cette méthode a été adoptée comme norme internationale depuis 1992. Le JPEG est libre de tous droits, donc gratuit, ce qui lui a permis d'être largement diffusé sur Internet, car il permet aussi bien de traiter les images en couleur qu'en niveaux de gris. Il a de nombreuses utilisations aussi bien en imagerie médicale que satellitaire.

Cette norme a été mise au point à la fin des années 1980 par un groupe d'experts nommés par des organismes nationaux de normalisation et des industriels : le Joint Photographic Expert Group (JPEG). Le JPEG est un format de compression des images numériques non entropique, c'est à dire qui ne conserve pas la qualité de l'image initiale. Le principe est simple : il s'agit de créer une dégradation de l'image indiscernable à l'œil ou suffisamment faible pour qu'on ne la remarque pas, de façon à offrir un taux de compression beaucoup plus intéressant que les autres méthodes, donc à permettre de réduire considérablement l'espace occupé par le fichier sur le disque ou la vitesse de son transfert sur un réseau.

Voici le schéma de principe de la compression JPEG

Figure IV.3 principe de la compression JPEG

La phase de quantification réduit l'importance de tous les coefficients *DCT* en les divisant par un pas de quantification et en les remplaçants par leur quotient avec ce pas. La quantification est donc une simple division euclidienne des coefficients *DCT* par un certain diviseur (le pas), qui remplace les coefficients d'origines par le quotient de la division. C'est donc à cette étape que nous allons perdre une partie de l'information, car après quantification le reste de la division est perdu.

De ce fait, on commence nos tests pour la compression JPEG avec un pas de quantification inferieur ou égal à 4 afin de ne pas trop affecter la capacité diagnostique de notre image test. La figure IV.4 nous permit de voir l'influence du pas de quantification sur notre image test :

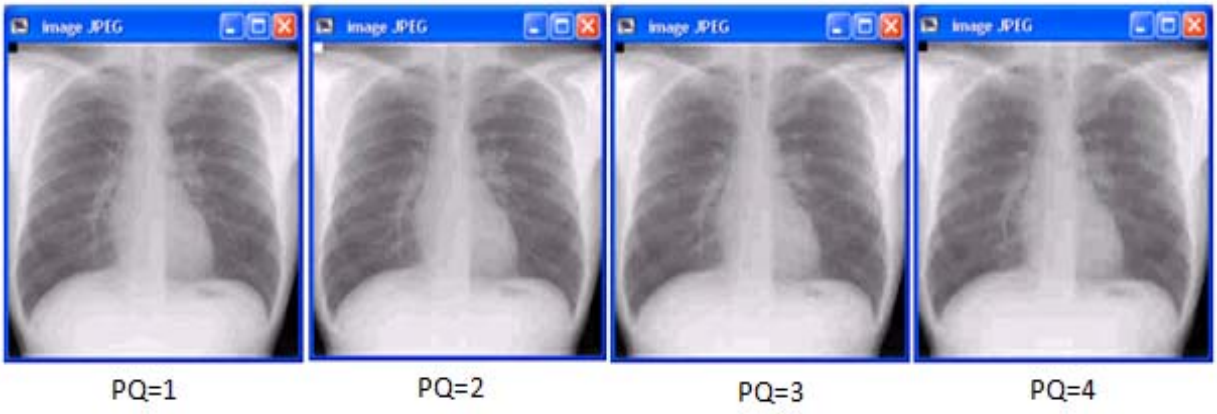


Figure IV.4 influence du pas de quantification

En faisant varier le *coefficient* **α** pour régler la puissance de la marque, on teste notre algorithme sur 50 jeux de clés différents et on aura nos résultats sur le graphique suivant:

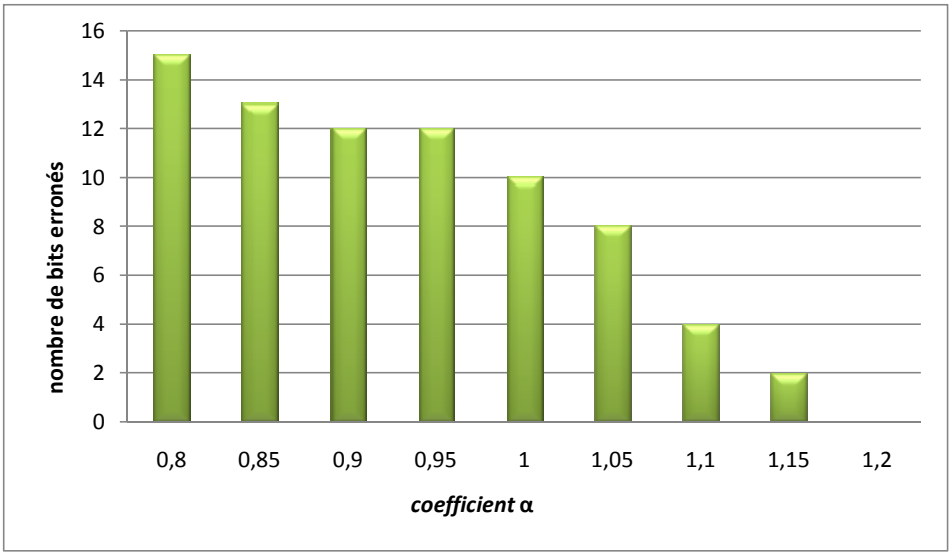


Figure IV .5 Influence du *coefficient* α sur la compression JPEG

A partir de la figure IV.5 ; fixer la valeur de 1,2 pour le *coefficient* **α** nous donnera de bons résultats, car cette valeur n'influe pas sur la capacité diagnostique de notre image test (voir section IV.4), et aussi elle rend notre algorithme bien plus efficace contre la compression JPEG.

Pour faciliter encore la détection on a appliqué à la marque un masque psychovisuel. Pour construire ce masque, il nous faut régler les deux coefficients min et max. on a donc fait varier le coefficient min sur l'image teste avec les paramètres max et *coefficient* **α** fixes. Ensuite on a fait varier le coefficient max avec les paramètres min et *coefficient* **α** fixes. On a obtenu les deux tableaux qui nous ont permis de fixer ces deux coefficients (max et min) pour notre algorithme.

min	0	0,5	1	1,1	1,2	1,3	1,4	1,5
Nombre de bits erronés	64	64	8	0	0	0	0	0

Tableau IV.2 nombre de bits erronées fonctions de min

max	0	0,5	1	2	3	4	5	6
Nombre de bits erronés	8	4	4	3	1	0	0	0

Tableau IV.3 nombre de bits erronées fonctions de max

Finalement min a été fixé à 1,2 et max à 5.

La figure IV.6 représente le tatouage de l'image test avec le masque psychovisuel pour les déférentes couches :

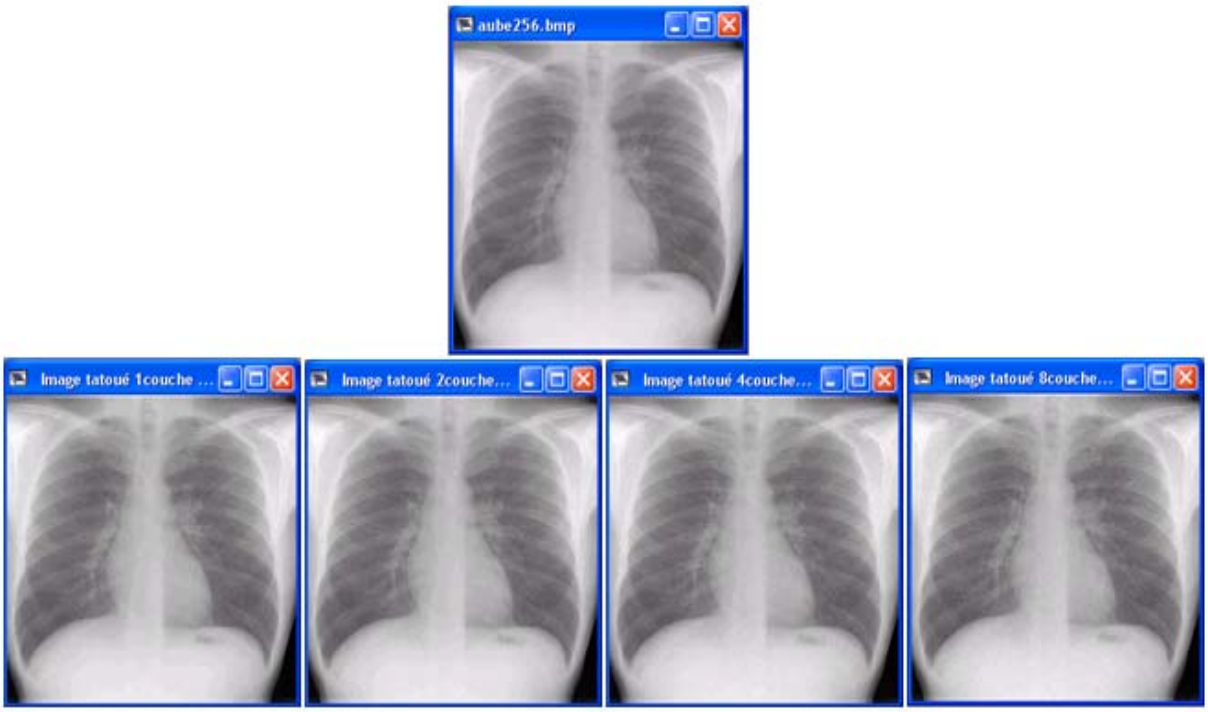


Figure IV.6 tatouage avec masque

Les paramètres de notre algorithme étant fixés pour faire face à la compression JPEG, nous allons à présent passer aux autres attaques de traitement d'images (filtrage, image négative …).

IV.2.2 Filtrage [14]

Pour améliorer la qualité visuelle de l'image, on doit éliminer les effets des bruits (parasites) en lui faisant subir un traitement appelé filtrage. Le filtrage consiste à modifier la distribution fréquentielle des composantes d'un signal selon des spécifications données. Le système linéaire utilisé est appelé filtre numérique. Parmi ces systèmes on trouve :

IV.2.2.1 Filtre passe bas (lissage)

Ce filtre n'affecte pas les composantes de basse fréquence dans les données d'une image, mais doit atténuer les composantes de haute fréquence. L'opération de lissage est souvent utilisée pour atténuer le bruit et les irrégularités de l'image. Elle peut être répétée

plusieurs fois, ce qui crée un effet de flou. En pratique, il faut choisir un compromis entre l'atténuation du bruit et la conservation des détails et contours significatifs surtout pour l'imagerie médicale.

IV.2.2.2 Filtre passe haut (accentuation)

Le renfoncement des contours et leur extraction s'obtiennent dans le domaine fréquentiel par l'application d'un filtre passe-haut. Le filtre digital passe-haut a les caractéristiques inverses du filtre passe-bas .Ce filtre n'affecte pas les composantes de haute fréquence d'un signal, mais doit atténuer les composantes de basse fréquence.

Notre logiciel nous permet de tester plusieurs sortes de filtrage : filtre passe bas, filtre passe haut, laplacien, sobel… on va les appliqués sur notre image teste et voir les résultats en suite.

La figure IV.7 montre les transformations apportées sur l'image tatouée pour les différents types de filtres :

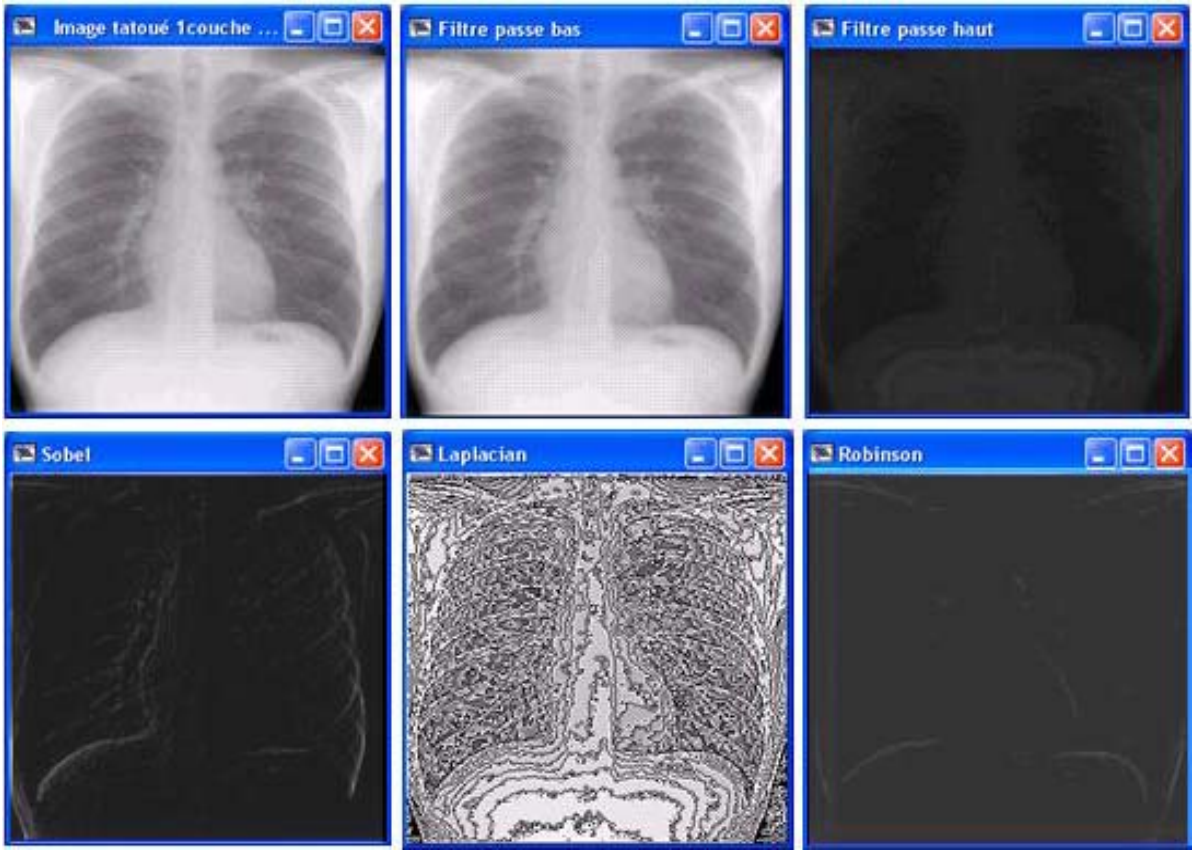


Figure IV.7 les différents filtrages appliqués sur l'image tatouée

On constate que la marque reste robuste face aux attaques apportées par ces différents filtres, même pour un schéma à une seule couche et aussi en faisant varier le *coefficient* **α**. En revanche juste quelques bits erronés pour le filtre passe bas, la figure qui suit nous le montre :

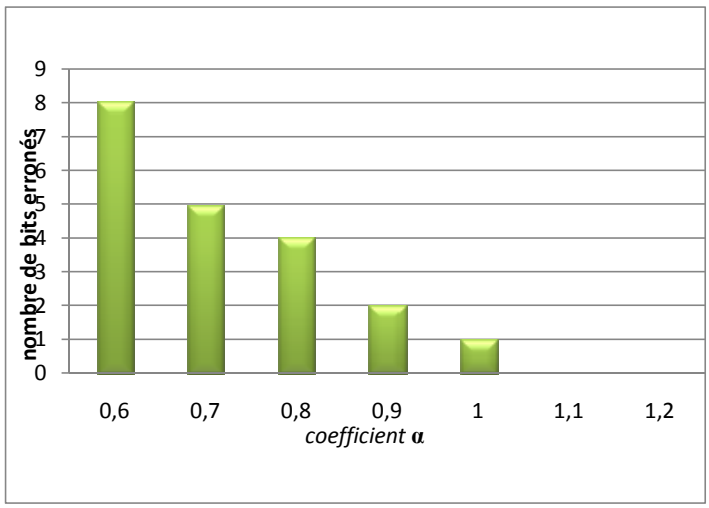


Figure IV.8 influence du filtre passe bas sur l'image tatouée

IV.3 Critère pour améliorer la détection

Pour améliorer la détection avant de calculer l'intercorrélation. La marque est estimée au sein de l'image grâce à un filtre de Wiener, on a donc testé la détection avec et sans un filtrage de Wiener sur l'image test avec un schéma à 1 couche en faisant varier les valeurs de *coefficient* **α**. Les résultats suivants montrent l'efficacité du filtre de Wiener :

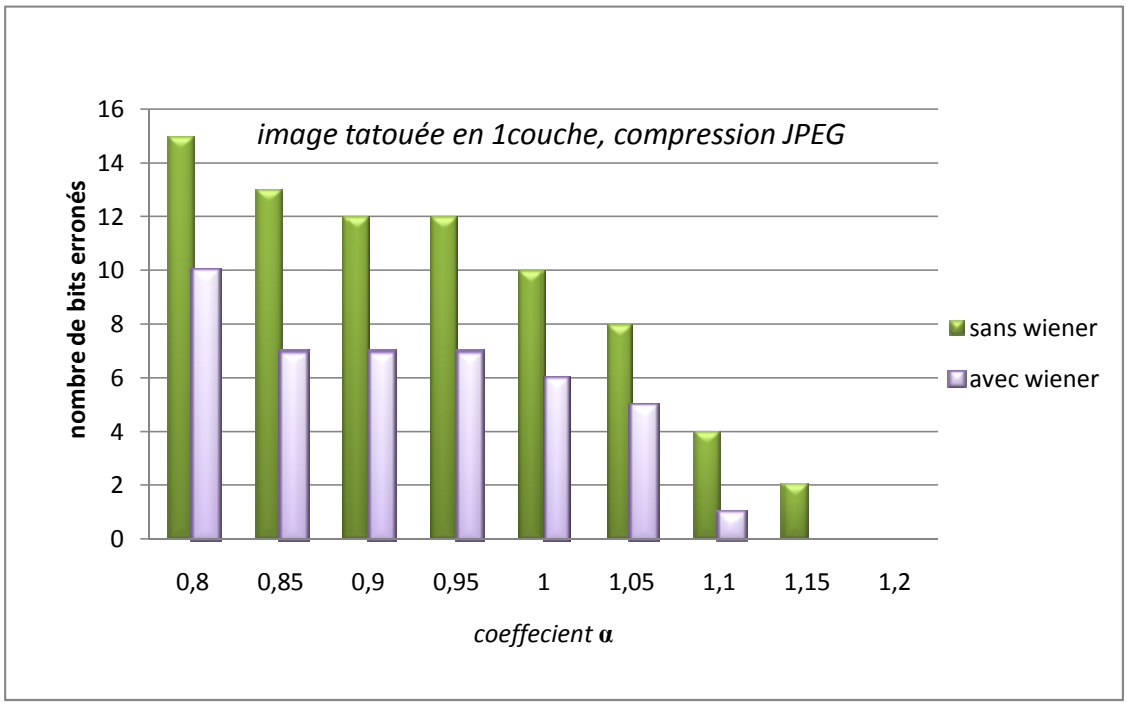


Figure IV.9 Apport du filtre Wiener sur la détection

IV.4 Invisibilité

L'efficacité d'un algorithme de tatouage d'images est jugée sur sa capacité à résister aux attaques mais aussi sur l'invisibilité de la marque ainsi que la capacité diagnostique. Cependant il est assez difficile de pouvoir quantifier numériquement la visibilité d'une marque. Pour remédier à ce problème, la première idée est de calculer le rapport signal sur bruit (PSNR) acronyme de **Peak Signal to Noise Ratio**:

Tout d'abord on calcule la somme des différences au carré de l'image marquée par rapport à l'image originale (pour une image 256*256) :

$$sum = \frac{1}{256*256} * \sum_{i,j=1}^{256} \left(I_w(i,j) - I(i,j)\right)^2 \qquad \text{(IV.1)}$$

Ensuite on calcule le PSNR (unité : le dB) :

$$PSNR = 10 * \log_{10}\left(\frac{d^2}{sum}\right) \quad \text{(IV.2)}$$

Où d est la dynamique au carré de l'image. Dans notre cas les composantes du pixel de l'image sont codées sur 8 bits, donc $d = 255$ et on aura :

$$PSNR = 10 * \log_{10}\left(\frac{255 * 255}{sum}\right) \quad \text{(IV.3)}$$

Le PSNR quantifie l'intensité de la marque. Cependant il ne s'adapte pas aux caractéristiques de l'image : la marque est en effet plus visible dans les zones peu texturées (à variance faible) et moins visible dans les zones plus texturés (à variance plus forte). Pour quantifier plus efficacement la visibilité de l'image, il faudrait donc un PSNR' qui serait plus pénalisant dans les zones planes que dans les zones texturées.

On a donc utilisé le wPSNR qui prend en compte la variance de l'image (Var : Image-Variance). Il est fort quand la variance est grande et plus faible quand la variance est petite :

$$sum' = \frac{1}{256 * 256} * \sum_{i,j=1}^{255}\left(\frac{I_w(i,j) - I(i,j)}{1 + Var(i,j)}\right)^2 \quad \text{(IV.4)}$$

$$wPSNR = 10 * \log_{10}\left(\frac{255 * 255}{sum'}\right) \quad \text{(IV.5)}$$

Pour tester l'efficacité du wPSNR, on l'a comparé avec le PSNR sur une image marquée sans masque psychovisuel, puis avec masque psychovisuel (donc avec une marque mieux adaptée à l'image). On constate sur le tableau IV.4 que le wPSNR a l'avantage de prendre en compte l'adaptabilité de la marque à l'image. Les tests ont été faits après insertion du message pour un schéma à 1 couche en faisant varier le *coefficient* **α**.

Coefficient **α**	0,6	0,7	0,8	0,9	1	1,1	1,2
PSNR Sans masque	56	55	53	52	51	50	48
PSNR avec masque	56	54	52	49	47	45	44
wPSNR Sans masque	70	68	67	65	63	62	60
wPSNR avec masque	83	80	77	76	74	73	70

Tableau IV.4 Evolution du PSNR et wPSNR sur l'image avec et sans masque

On constate donc que le wPSNR augmente quand on utilise un masque (ce qui est normal puisque la marque s'adapte à l'image) alors que le PSNR ne varie pas, voire diminue. Ceci démontre donc bien que le wPSNR prend en compte l'adaptabilité de la marque à l'image à la différence du PSNR. Pour quantifier la dégradation de l'image, on utilisera maintenant le wPSNR.

Sur la Figure IV.10 on a comparé à PSNR constant, la dégradation de l'image avec et sans masque. Le contraste a été rehaussé pour rendre la marque plus visible et donc pour pouvoir mieux comparer les performances du PSNR et du wPSNR.

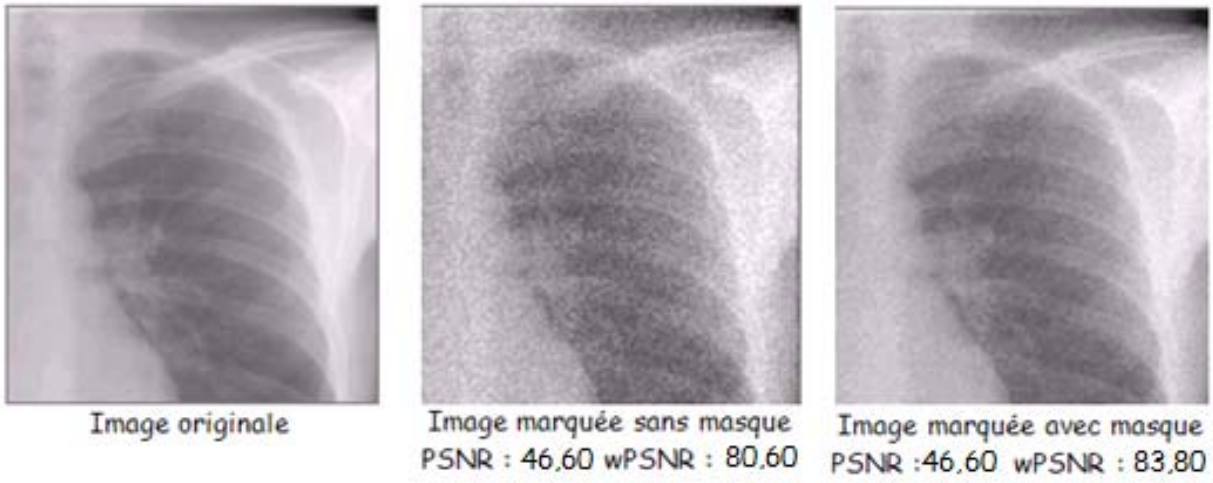


Figure IV.10 intérêt du wPSNR

La dégradation de l'image sans masque apparaît quand même plus importante, elle touche particulièrement les zones planes et donc affecte très sensiblement l'image. Cette dégradation est beaucoup moins importante quand on utilise un masque, en gardant le même PSNR et donc la même intensité de marque.

Avec le seul PSNR comme juge, on ne peut donc pas différencier les deux images marquées, alors que celle sans masque est beaucoup plus dégradée. Seul le wPSNR fait la différence entre les deux images marquées.

IV.5 Performance du schéma multicouche

Nous allons passer aux testes du multicouches face à la compression JPEG, sur 50 jeux de clés différentes et sans masque, on aura les résultats suivants :

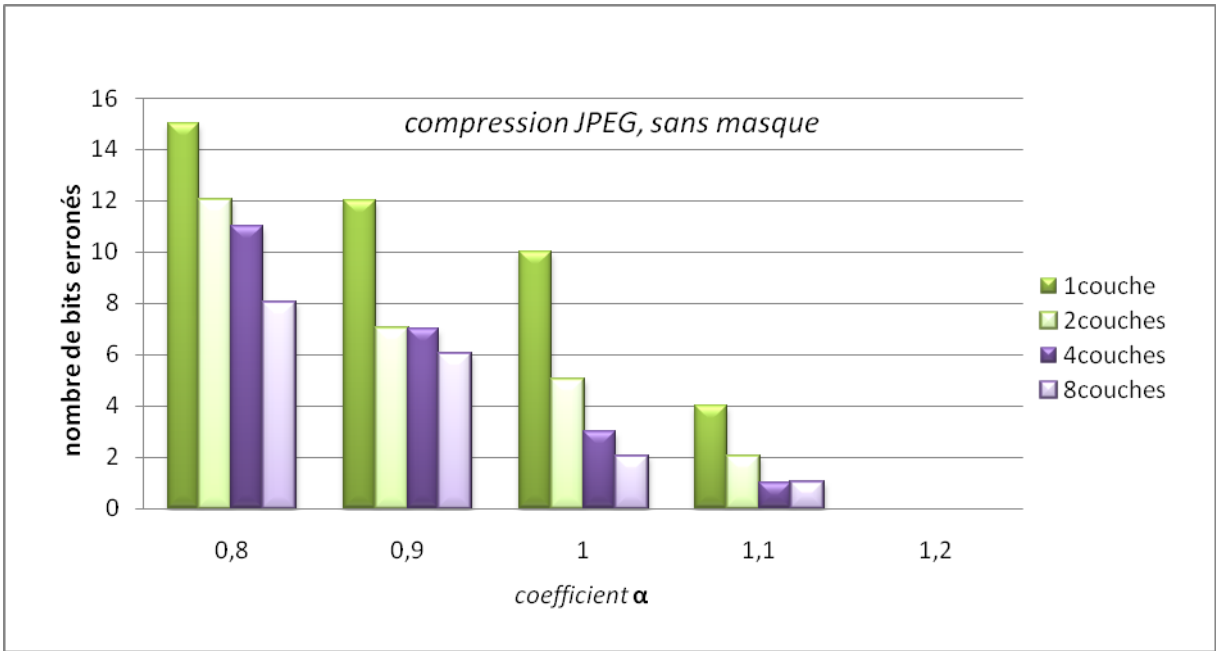


Figure IV.11 nombre de bits erronées fonctions du multicouche

On a aussi testé le schéma multicouche on calculant le $wPSNR_{moy}$ (en faisant varier *coefficient* **α**) qui permettait de n'obtenir aucun bit erroné (toujours après compression JPEG). Les résultats sont sur la figure IV.12 :

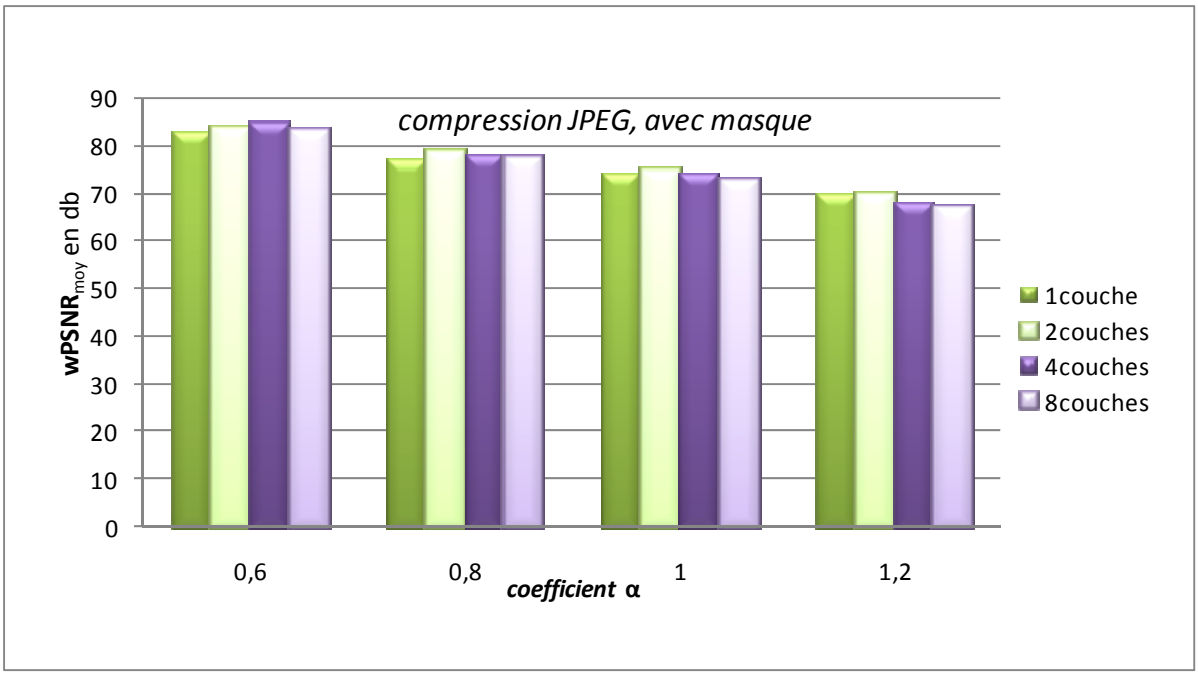


Figure IV.12 calcul du $wPSNR_{moy}$ pour le multicouche

Les résultats des graphiques précédents sont très explicitent et montrent tout l'intérêt de la technique multicouche. D'une part on voie que le nombre de bits erronés diminue en faisant augmenter le nombre de couches, ce qui rend la robustesse encore meilleure (le seuil de détection augmente). D'autre part on a eu un wPSNR presque identique c'est-à-dire que le multicouche préserve la qualité de l'image et ne porte pas d'influence sur la capacité diagnostique.

IV.6 Attaques géométriques

La méthode proposée est donc robuste face aux attaques de type traitement d'images. Ce résultat n'est pas suffisant puisque les attaques géométriques comme les translations et les rotations sont beaucoup plus néfastes. En effet toute désynchronisation spatiale rend la méthode inefficace puisque le principe de l'algorithme consiste en l'addition de la marque avec l'image pixel par pixel, donc l'image marquée est éventuellement attaquée avec la marque insérée. Ainsi il suffit par exemple de déplacer toute l'image d'un pixel dans l'une des quatre directions pour rendre la méthode inefficace.

Pour remédier à ce genre d'attaques, la solution la plus évidente est d'insérer la marque dans le domaine transformé et ensuite refaire les testes et voir les résultats.

IV.7 conclusion

Nous avons présenté dans ce chapitre les différents résultats obtenus après avoir tester la technique multicouche. Ces résultats montrent l'excellent comportement de notre algorithme face à la compression JPEG et aussi face au filtrage, cela en minimisant au maximum le nombre de bits erronés (robustesse) et en gardant la qualité de l'image marquée telle que l'originale (invisibilité), ce qui ne conduit pas à un diagnostique erroné.

Cependant, le principal défaut de notre algorithme réside dans son incapacité à faire face aux attaques géométriques, car ce type d'attaque fait décaler la marque en même temps que les pixels de l'image, le détecteur ne la retrouve pas à l'endroit attendu et conclut donc par sans absence.

V.1 Introduction

Dans ce chapitre, nous faisons un aperçu sur l'environnement de programmation Borland Delphi qui est doté d'une interface multi document (MDI) dont l'interface utilisateur encore vide est représentée sur la figure V.1. Ainsi que, nous présentons notre logiciel (tatouage d'images numériques par CDMA) et les différents menus utilisés pour les traitements appliqués sur les images numériques, illustré a chaque fois par des images.

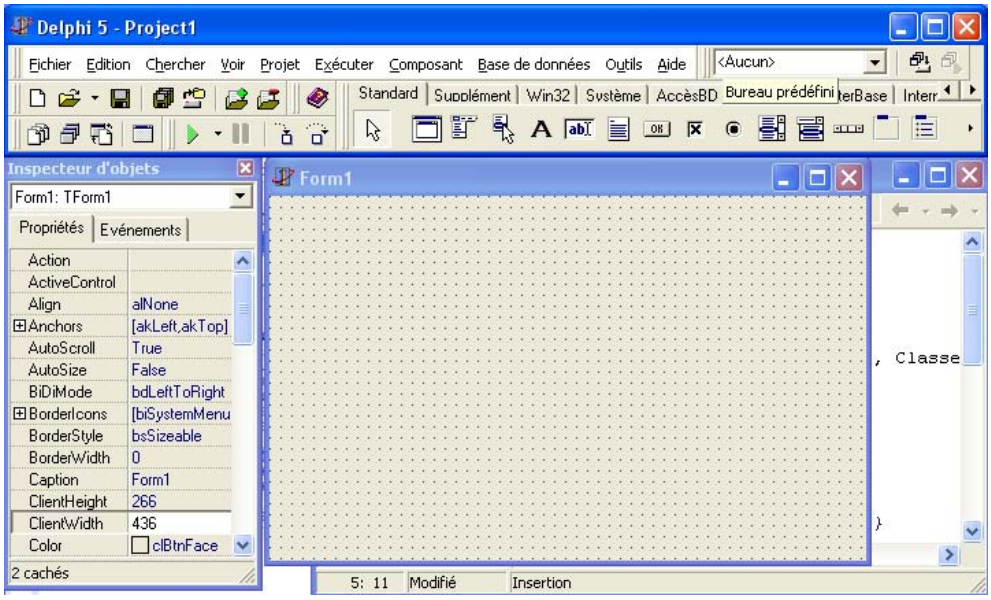


Figure V.1 La fiche de travail de Delphi encore vide

V.2 Présentation de Delphi et du logiciel de tatouage

Delphi est un logiciel de développement rapide (RAD, Rapid Application Development) conçu par Borland pour écrire des applications Windows disposant d'une interface graphique utilisateur (GUI, Graphic User Interface). Aussi, l'avantage de Delphi est de permettre de produire des applications à durée d'exécution très petite.

Ainsi, notre logiciel (tatouage d'images numériques par CDMA) grâce au langage de programmation Borland Delphi est doté d'une interface multi documents (MDI), et il reprend l'interface classique des logiciel développés sous Windows, dont est représenté sur la figure suivante :

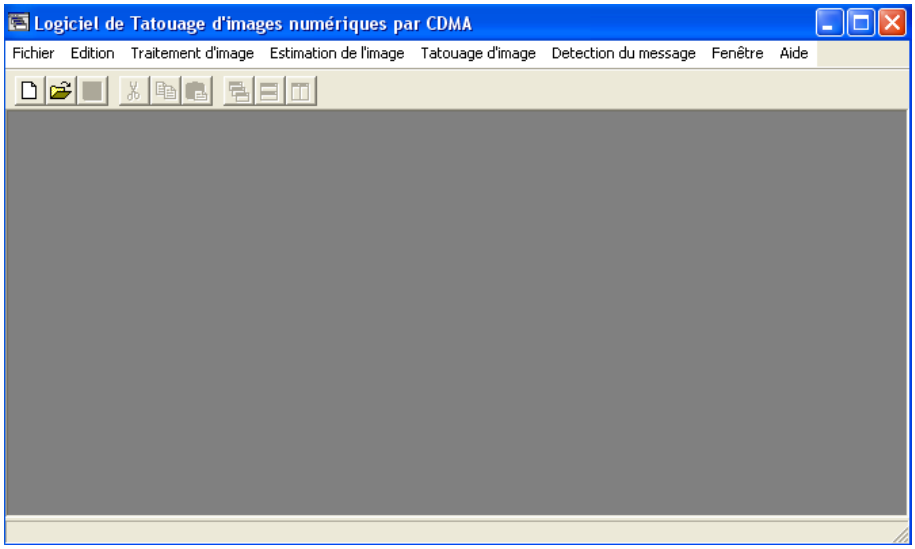


Figure V.2 Fenêtre principale du logiciel de tatouage d'images numérique par CDMA

V.3 Description des principaux menus

V.3.1 le menu Fichier

Nouveau : Permet d'ouvrir et de charger une nouvelle application.

Ouvrir : Permet d'ouvrir et de charger une image BMP a niveau de gris.

Fermer : Permet de fermer l'image active.

Enregistrer : Enregistre et sauvegarde l'image sous format bitmap.

Enregistrer sous : Permet d'enregistrer sous un nom de fichier.

Quitter : Permet de quitter l'environnement de l'application.

FigureV.3 Menu Fichier

V.3.2 Le menu Edition

Couper : Permet d'effacer l'image active.

Copier : permet de copier l'image active.

Coller : permet de coller l'image qui à été coupée ou copiée.

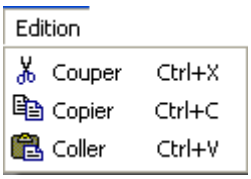


Figure V.4 Menu Edition

V.3.3 Le menu Traitement d'image

Image négative : Affiche le négative de l'image active.

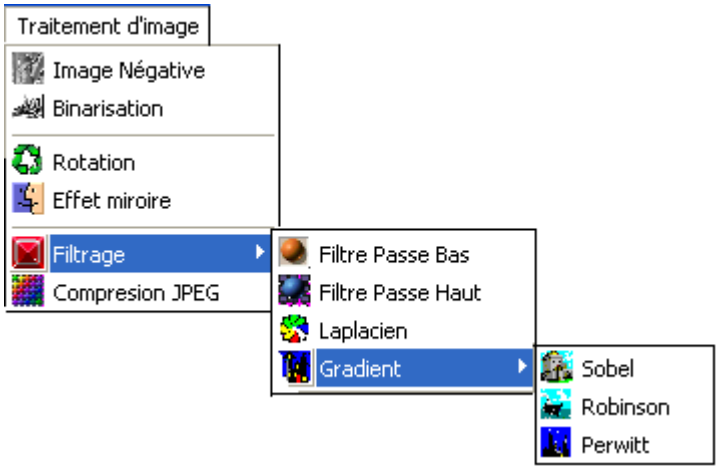
Binarisation : Affiche l'image binaire de l'image active.

Rotation : Permet d'effectuer des rotations de l'angle 90° à gauche, 90° à droite et 180°.

Effet miroir : Permet de donner l'image miroir.

Filtrage : Permet d'appliquer les filtres passe bas, passe haut et Laplacien. Ainsi que gradient de Sobel, Robinson et Perwitt.

JPEG : Affiche l'image compressée par JPEG de l'image active.



FigureV.5 Menu Traitement d'image

V.3.4 Le menu Estimation de l'image

PSNR : Calcul le PSNR en db entre l'image originale et l'image teste.

wPSNR : Calcul le wPSNR en db entre l'image référence et l'image teste.

Histogramme : Affiche l'histogramme de niveau de gris de l'image.

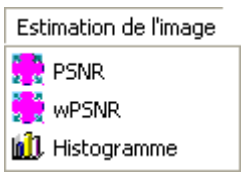
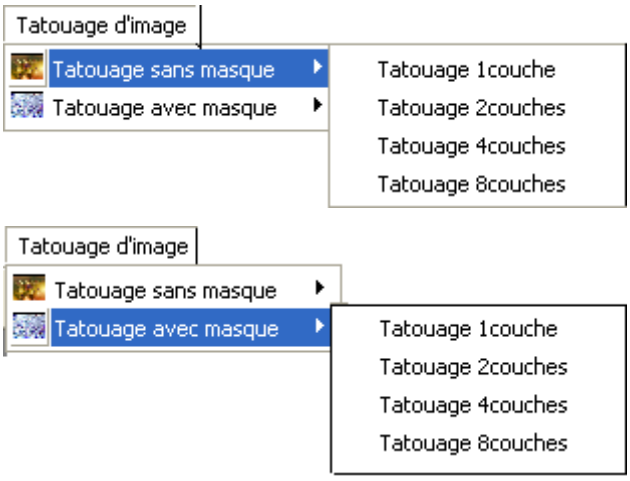


Figure V.6 Menu Estimation de l'image

V.3.5 Le menu Tatouage d'image

Tatouage sans masque : Permet de tatouer l'image active sans utiliser le masque en 1 ou 2 ou 4 ou 8 couches.

Tatouage avec masque : Permet de tatouer l'image active avec utilisation d'un masque en 1 ou2 ou 4 ou 8 couches.



FigureV.7 Menu Tatouage d'image

V.3.6 Le menu Détection du message

Détection sans masque

- **Sans Wiener :** Permet de détecter le message inséré sans utiliser ni le masque ni le filtre de wiener.
- **Avec Wiener :** Permet de détecter le message inséré sans utiliser le masque mais avec filtrage de Wiener.

Détection avec masque

- **Sans Wiener :** Permet de détecter le message inséré en utilisant le masque mais de filtre de wiener.
- **Avec Wiener :** Permet de détecter le message inséré en utilisant le masque ainsi que le filtre de Wiener.

Figure V.8 Menu Détection du message

V.3.7 Le menu Fenêtre

Cascade : Permet d'arranger les images ouvertes en cascades.

Mosaïque Horizontale : Permet d'arranger les images ouvertes en horizontale.

Mosaïque Vertical : Permet d'arranger les images ouvertes en vertical.

Tout réduire : Permet de réduire toutes les fenêtres ouvertes.

Tout réorganiser : Permet de réorganiser toutes les fenêtres ouvertes.

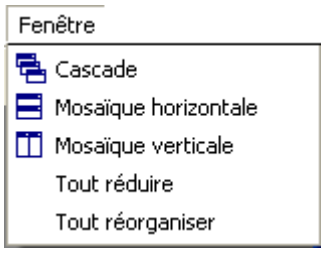


Figure V.9 Menu Fenêtre

V.3.8 Le menu Aide

A propos… : Permet d'avoir une aide sur un sujet déclarer.

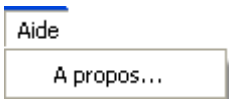


Figure V.10 Menu Aide

V.4 Boites de dialogue

V.4.1 Boite de dialogue « Binarisation » Permet de mettre un seuil de binarisation dans S.

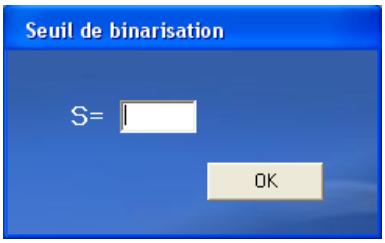


Figure V.11 Fenêtre de seuil de sélection

V.4.2 Boite de dialogue « Rotation » Permet de choisir entre la rotation 90° à gauche, 90° à droite ou rotation de 180°.

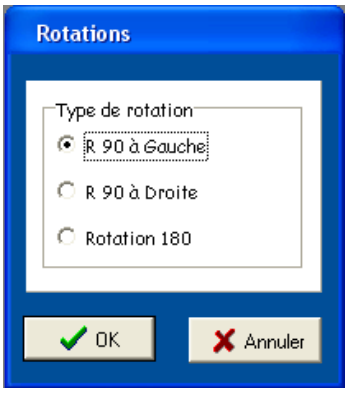


Figure V.12 Fenêtre de chois de rotation

V.4.3 Boite de dialogue « Paramètres de compression selon JPEG »

Permet de sélectionner les paramètres nécessaires au compression d'une image test.

Ces paramètres sont :

Hauteur du bloc.

Largeur du bloc.

Pas de quantification.

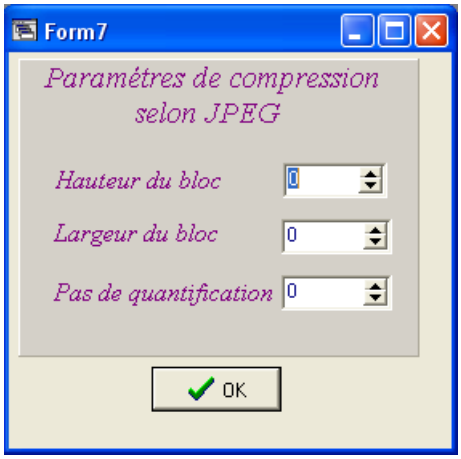


Figure V.13 Fenêtre des paramètres de compression selon JPEG

V.4.4 Boite de dialogue « Paramètres d'introduction de message » Permet d'introduire le message à insérer.

Figure V.14 Fenêtre d'introduction du message

V.4.5 Boite de dialogue « Paramètres d'introduction du nombres d'étages et la clé » Permet d'introduire :

Nombres d'étages : représentes le nombre de bascules selon la taille du bloc.

La clé : elle prend des valeurs binaires (0 ou1).

Cette opération se fait lors de l'insertion et détection du message.

Figure V.15 Fenêtre d'introduction de nombres d'étages et la clé

V.4.6 Boite de dialogue « Paramètres d'introduction de max, min et coef» Permet d'introduire le maximum, le minimum et le coefficient lors de tatouage et détection seulement avec masque psychovisuel.

Figure V.17 Fenêtre d'introduction de max, min et coef

Conclusion générale

Le tatouage des images numériques 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.

Après avoir présentes quelques méthodes de tatouages d'images numériques, nous nous sommes intéressés dans cette thèse à la méthode de multicouche (CDMA), que nous avons appliqué à des images médicales pour la protection de copyright et pour étudier leur adaptabilités à ce domaine en vérifiant l'authenticité et l'intégrité de l'image, ainsi que assurer la confidentialité des données du patient. La qualité de l'image médicale tatouée est améliorée par l'utilisation du masque psychovisuel. Cette méthode a l'inconvénient sur l'imagerie médicale d'être dépendante de plusieurs paramètres (clé, nombre de couches, nombre de bits à insérer) ce qui est contraignant surtout lorsqu'il s'agit de gérer un nombres important d'images médicales.

Enfin, on peut envisager d'adapter la méthode de tatouage par la technique de multi-couche à d'autres applications du copyright et à d'autres supports que les images fixes, tel que les vidéos ou le son.

Bibliographie

[1] : Application du tatouage d'images à l'imagerie médicale, DEA Signaux et Images en Biologie et en Médecine, Université d'Angers, Laboratoire d'Ingénierie des Systèmes Automatisés, UPRES-EA 2168

[2]: 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

[3]: KUHN M. & PETITCOLAS F. Stirmark. http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

[4]: UnZign. http://www.altern.org/watermark/

[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]: 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.].

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

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

[11]: Application du tatouage d'images à l'imagerie médicale, antoine, Université d'Angers Laboratoire d'Ingénierie des Systèmes Automatisés UPRES-EA 2168

[12]: 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.

[13]: http://www.chez.com/nico77/ LA COMPRESSION DES IMAGES NUMERIQUES

[14]: http://www.kaddour.com/chap1/chap1.htm/ les filtres numériques

[15] : http://fr.wikipedia.org/wiki/Imagerie_par_r%C3%A9sonance_magn%C3%A9tique

[16] : http://fr.wikipedia.org/wiki/Radiographie

[17] : http://fr.wikipedia.org/wiki/Scanneur

[18] : http://fr.wikipedia.org/wiki/%C3%89chographie

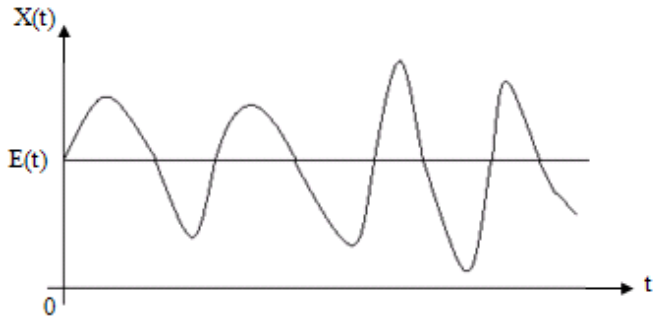
[19] : http://fr.wikipedia.org/wiki/Scintigraphie

I Outils mathématiques

I.1 Espérance mathématique (moyenne)

- **Dans le cas continu**

Soit un signal aléatoire X (t) :



- La moyenne de X(t) est donnée par :

$$E(x) = \int xf(x)dx$$

- **Dans le cas discret**

Pour une image (I) à titre d'exemple on a :

$$E(x) = \frac{1}{m*n} * \sum_{i,j=1}^{m*n} \left(I(i,j)\right)$$

Tel que (m*n) : taille de l'image ;

(i, j) : coordonnées d'un pixel de l'image ;

I.2 Variance

La variance permet de savoir si les amplitudes d'un signale aléatoire sont proches ou bien éloignés de la valeur moyenne de ce même signal.

Elle est donnée par la formule suivante :

$$Var(x) = E(x^2) - \left(E(x)\right)^2$$

D'où :

$$Var(I) = \frac{I}{m*n} * \left[\sum_{i,j=1}^{m*n} \left(I(i,j)\right)^2 - \left(\sum_{i,j=1}^{m*n} I(i,j) \right)^2 \right]$$

I.3 Ecart type

$$\sigma_x = \sqrt{Var(x)}$$

I.4 Outils d'évaluation

I.4.1 Corrélation

La notion de corrélation à pour objectif de savoir si deux signaux aléatoires ont une relation entre eux ou bien si ils sont indépendants. Donc c'est un moyen mathématique qui permet de comparer entre deux signaux.

I.4.2 Ecart quadratique moyen (sum)

$$sum = \frac{1}{m*n} * \sum_{i,j=1}^{mn} \left(I_w(i,j) - I(i,j)\right)^2$$

Sert à calculer l'erreur quadratique entre l'image traitée I_w , et l'image originale I.

I.4.3 Le rapport signal sur bruit (PSNR)

Le PSNR ***(Peak Signal Noise Ratio)*** dépend du sum. Il permet de déterminer l'imperceptibilité de l'image tatouée. En d'autre terme, il évalue la dégradation en dB de l'image originale provoquée par l'insertion du message et éventuellement par d'autres attaques.

Le PSNR est définit comme suit :

$$PSNR = 10 * \log_{10}\left(\frac{d^2}{sum}\right)$$

I.4.4 le wPSNR

Est le PSNR pondéré ***(Weighted Peak Signal Noise Ratio),*** qui prend en compte la variance de l'image (Var : Image-Variance). Il est fort quand la variance est grande et plus faible quand la variance est petite.

$$sum' = \frac{1}{256*256} * \sum_{i,j=1}^{255} \left(\frac{I_w(i,j) - I(i,j)}{1 + Var(i,j)} \right)^2$$

$$wPSNR = 10 * \log_{10} \left(\frac{255*255}{sum'} \right)$$

II Algèbre de Boole

II.1 Définition

C'est une algèbre binaire qui s'applique à des fonctions logiques dont les variables sont prises dans l'ensemble {0,1}.

II.2 Opérateur AND

Soit a, b Є {0,1}.

C = a.b

a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

II.3 Opérateur OR

C = a+b

a	b	c
0	0	0
0	1	1
1	0	1
1	1	1

II.4 Opérateur XOR

$C = a \otimes b$

a	b	c
0	0	0
0	1	1
1	0	1
1	1	0