République Tunisienne
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique
et de la Technologie

Université de Sfax
École Nationale d'Ingénieurs de Sfax

Cycle de Formation Doctorale
dans la Discipline Génie électrique

Doctorat en Electronique

Thèse de *DOCTORAT*
N° d'ordre: 2009– 144

THESE

Présentée à

L'École Nationale d'Ingénieurs de Sfax

En vue de l'obtention du

DOCTORAT

Dans la discipline Génie Electrique
Doctorat en électronique
Par

Imen FOURATI KALLEL

(Mastère Electronique)

Assistante à l'institut supérieur d'électronique
et des communications de Sfax

Elaboration d'une nouvelle approche de tatouage réversible pour la vérification d'intégrité des images médicales.

Soutenu le 11 Décembre 2009, devant le jury composé de :

M.	**Mohamed MASMOUDI**	*Président*
M.	**Mohamed Salim BOUHLEL**	*Encadreur*
M.	**Jean Christophe LAPAYRE**	*Encadreur*
Mme.	**Dorra SALLEMI MASMOUDI**	*Rapporteur*
M.	**Franck MARZANI**	*Rapporteur*
M.	**Abdenaceur KACHOURI**	*Examinateur*

A mes parents bien aimés, à mon cher mari et mon agréable fils qui ont compris et accepté mon absence durant ces quatre ans. Cette thèse est pour vous.

Remerciements

En premier lieu, je tiens à remercier mes deux directeurs de thèse sans qui ce travail n'aurait jamais pu aboutir.

Professeur **Mohamed Salim Bouhlel,** directeur de l'institut supérieure de l'électronique et de communication de Sfax et directeur de l'unité de recherche sciences et technologies de l'image et des télécommunications pour sa disponibilité illimitée durant toute la période de réalisation de ce travail. Ses directives et ses qualités humaines, ses nombreuses remarques ont montré une très vaste connaissance des sujets abordés et m'ont donné les conduits et les améliorations de mon travail.
Je lui suis considérablement reconnaissante et je manque d'expressions de remerciement digne de tout ce qu'il m'a donné durant ces années de recherche.

Et Mr **Jean Christophe LAPAYARE** professeur Directeur du Département Enseignement Informatique de l'UFR Sciences et Technique de Besançon et directeur du Laboratoire d'Informatique de l'Université de Franche-Comté qui m'a donné de son temps, de sa patience et de son savoir faire. Je vous remercie vivement Monsieur pour tous les conseils et toute l'aide que vous n'avez pas manqué à me prodiguer durant cet encadrement.

Ensuite je voudrais remercier les membres de jury d'avoir accepté d'évaluer mon travail. Je commence par remercier le président de mon jury Monsieur **Mohamed MASMOUDI** professeur à l'Ecole Nationale d'Ingénieur de Sfax, pour le grand honneur qu'il m'a fait en acceptant de présider le jury de cette thèse.

Je remercie également Monsieur **Abdenaceur KACHOURI** Maître de conférences à l'école d'ingénieurs de Gabes pour l'intérêt qu'il a porté à mon travail en acceptant d'examiner avec sa rigueur scientifique ma thèse.

Je remercie en particulier Madame **Dorra SALLAMI MASMOUDI** Maître de conférences à l'école d'ingénieurs de Sfax et Monsieur **Frank MARZANI** professeur à l'université de Bourgogne d'avoir accepté de rapporter ma thèse, et de l'intérêt qu'ils y ont porté. J'ai conscience de la lourde charge de travail que cela a représenté.

Mes remerciements vont aussi aux membres de l'Equipe sciences et Technologies de l'Image et des Télécommunications (SETIT) pour l'exceptionnelle ambiance de travail qu'ils ont tous contribué à en bâtir. Ils étaient l'exemple des membres d'une seule famille solidaire et affective. Je ne peux donc que remercier Mr **Mohamed ELLOUZE**, **Wiem**, **Wafa**, **Manel**, **Souhir**, **Ali**, **Habiba**, **Nizar**, **Olfa**, **Sami**, **Hédi** et **walid**.

Je remercie mes amis **Houda**, **Souhir**, **Emna**, **Noura**, **Sana**, **Mariem, Ikram** pour ses sincères amitiés et pour me soutenir dans les moments difficiles.

Ma reconnaissance va également à Dr. **Mounir MAHDI** radiologue, Dr **Chaouki DABBECHE**, médecin radiologue exerçant au service de radiologie du CHU Habib Bourguiba de Sfax et Dr **Sonia BOUDAYA**, Maître de conférences agrégée au service de dermatologie, CHU Hédi Chaker de Sfax; pour l'aide précieuse, pour l'intérêt constant qu'ils ont porté à mon travail, ainsi que pour la confiance et le soutient dont ils m'ont gratifié tout au long de la validation clinique de mes travaux de thèse.

Je tiens à exprimer ma reconnaissance également à la famille de l'institut supérieure de l'électronique et de communication de Sfax, ISECS

Je ne peux terminer sans mentionner mes proches remerciements à mes parents, à toute la famille **FOURATI**, **KALLEL**, et **KCHAOU** pour leur confiance et leur soutient sans faille au cours de toutes ces années, et pour m'avoir supporté pendant ces longues études.

et merci enfin à tous ceux que je n'aurais pas dû oublier…

Que ces mots vous apportent le minimum de gratitude dont vous méritez

Imen

Sommaire

Liste des figures

Liste des tableaux

Introduction Générale

L'évolution des technologies et des connaissances, le développement des réseaux de communication et des supports numériques a encouragé l'utilisation des réseaux informatiques pour la transmission des informations médicales (dossiers des patients contenant des images et données textuelles ….). Beaucoup d'organisations, publiques et privées, ont remplacé leurs dossiers, dispersés et tenus manuellement, par des systèmes informatiques leur offrant un meilleur accès aux données : on parle par exemple du DMP (Dossier Médical du Personnel). Ces nouvelles pratiques posent le problème de la sécurité des données.

Compte tenu de l'aspects médico-légal et confidentialité (secret professionnel), la sécurité accordée aux dossiers électroniques des patients doit au moins égaler, si ce n'est dépasser, celle appliquée aux dossiers papiers habituels. Ces données et en particulier les images médicales doivent être protégées de toute falsification.

Concernant les images elles-même, l'une des solutions les plus adaptées est l'utilisation du tatouage (en particulier le tatouage fragile) : l'idée consiste à insérer une signature au sein même de l'image. Cette signature doit être imperceptible pour ne pas dénaturer ces images (pour ne pas conduire à un diagnostic erroné) et doit disparaître (d'où le terme de fragile) en cas de manipulation visant à modifier le contenu du document (accès illégal à l'image).

Nous avons étudié les méthodes classiques de tatouage qui sont des méthodes irréversibles et qui présentent l'inconvénient de la distorsion permanente de l'image originale : ce qui nous a conduits à étudier le cas particulier du tatouage réversible.

Comme tout type de tatouage fragile, le tatouage réversible est utilisé pour assurer l'intégrité de l'image, mais il a l'avantage de permettre de retrouver l'image originale. Cette réversibilité est importante pour tous les secteurs d'imagerie sensible, surtout pour le secteur médical. En effet, après avoir la certitude de garantie d'intégrité de l'image (grâce au tatouage), le médecin reconstitue l'image originale (non tatouée : intacte sans aucune dégradation) et l'utilise dans son diagnostic évitant tout risque de modification (lors de l'insertion de la signature), puisque la moindre mutation dans l'image médicale peut conduire à un diagnostic faux.

Ce rapport est constitué de trois sections, elles-mêmes sous-divisées en sections puis en chapitres.

La première section traite l'état de l'art du tatouage. Le premier chapitre de cette section présente un état de l'art de l'aspect général du tatouage des images. Il expose le besoin de sécurité des images médicales, les nécessités qui ont poussé à définir le tatouage réversible et les contraintes auxquelles il est soumis.
Le deuxième chapitre est intitulé tatouage réversible. Dans ce chapitre nous focaliserons notre intérêt sur la présentation du tatouage réversible en termes de caractéristiques, domaines d'insertion et modèle d'extraction pour passer par la suite à énumérer les travaux de la littérature qui ont trait dans ce domaine.

La deuxième section est intitulée "notre apport". Elle résume les travaux originaux qui ont été effectués au cours de notre travail et les valeurs ajoutées. Cette section est divisée en deux chapitres, chacun de ces chapitres traite une nouvelle approche que nous avons développée ou bien une amélioration que nous avons faite.
Dans le premier chapitre nous commençons par exposer notre approche de tatouage réversible. Nous présenterons par la suite l'amélioration proposée et les résultats obtenus. Enfin, nous terminons par une comparaison et une évaluation de notre nouvelle méthode par rapport à cinq autres techniques de tatouage réversible pour mettre en relief l'intérêt de notre approche.
Dans le deuxième chapitre, nous présentons une nouvelle approche de tatouage réversible afin de contourner le problème de dépassement ; l'approche développée est basée sur les caractéristiques des images médicales.

La troisième section présente la validation de notre travail dans le cadre du projet Européen DECOPREME. Elle s'étale sur trois chapitres. Un premier chapitre qui décrit le projet DECOPREME : ses axes principaux et la structuration de notre travail dans le cadre de ce projet qui consiste à vérifier l'intégrité des images lors de leur transfert.
Un deuxième chapitre qui nous permet d'exposer les validations et les mesures de performances pour les images en niveaux de gris et enfin un troisième chapitre qui donne les résultats obtenus dans le cas des images en couleur.

En fin de document, nous concluons sur l'ensemble de ces travaux et nous donnons les nouvelles directions de recherche que nous souhaitons explorer.

Nous pouvons remarquer que les résultats de ces travaux ont été publiés pour une grande part. La liste des publications personnelles est donnée juste avant la bibliographie placée en fin du document.

Section 1 :

Etat de l'art du tatouage

Chapitre I

Aspect général du tatouage

Introduction

L'utilisation en médecine de l'image en tant qu'outil diagnostic contribue à un changement sans pareil des pratiques médicales.
En effet, l'image numérique a permis de passer de la médecine clinique à l'ère de l'imagerie médicale. Ces notions offrent le partage d'un certain nombre d'éléments diagnostiques avec des confrères, le patient,… voire même des observateurs extérieurs comme cela se pratique en télémédecine.

Nous commencerons ce chapitre en définissant le domaine de la télémédecine concerné par nos travaux. Puis nous montrerons la nécessité de sécurité dans ce domaine. La notion d'intégrité sera introduite, et ainsi nous montrerons comment le tatouage peut être une réponse à la problématique.

1. La télémédecine

La télémedecine permet l'utilisation de technologies de télécommunications avancées dans le but de faire des diagnostics à distance : permettre un co-diagnostic entre spécialistes ou encore diagnostiquer à distance un patient. Dans le même cadre, il est possible de conduire des recherches, de transférer les données d'un patient ou encore d'améliorer le traitement et la gestion de la maladie du patient se trouvant sur un autre site.
Dans ce cadre, il est intéressant de proposer des banques de données (images médicales par exemple). Ce système temps réel devra permettre la traçabilité et l'historisation des interventions des acteurs de la télémédecine (praticiens hospitaliers), des conseils théoriques et avis empiriques émis.

Nécessité de la vérification d'intégrité dans la télémédecine

Actuellement, de nombreuses plateformes de télémédecine voient le jour : elles permettent en particulier une manipulation plus sûre et plus pratique, une transmission plus rapide, un stockage plus économique et une indexation plus efficace.

Mais le développement de telles plateformes n'est pas sans dérive : elles favorisent la large expansion de la falsification et du piratage. L'intégrité est donc devenue une exigence en télémédecine : l'expérience montre qu'en l'absence de contrôle sévère d'intégrité, environ un message sur 10000 peut être erroné.

Si l'information fournie par le système est erronée, le médecin peut prendre des décisions causant du tort au patient, ou pire, le tuant. Si l'information n'est pas fiable, dans le sens où on ne peut pas garantir son intégrité, la démarche de diagnostic se basant sur cette information ne peut pas non plus être fiable. De plus, dans le cadre médico-légal, un professionnel de la santé ne pourra pas utiliser les dossiers informatisés pour justifier ses actions.
Il est donc prudent de s'interroger sur les méthodes qui peuvent garantir l'intégrité des dossiers et empêcher les attaques qui pourraient compromettre l'authentification de ces donnés.

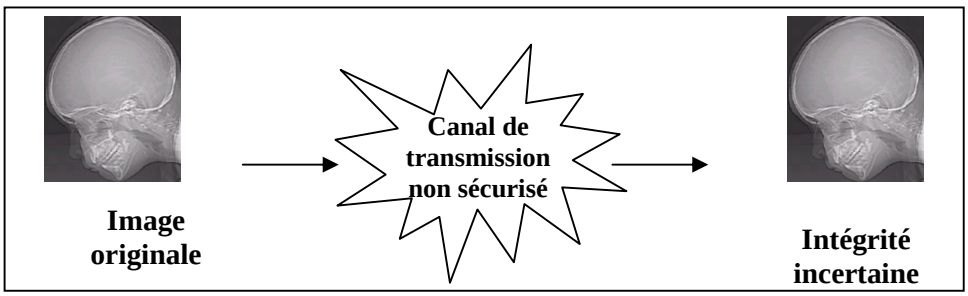


Figure 1. *Transmission d'image non sécurisée*

D'après G.Coatrieux et al.[COA00] les règles de sécurité reposent sur 3 principes fondamentaux : confidentialité, authentification et intégrité :
Confidentialité : action de conserver le caractère privé et secret d'un élément pour toutes les personnes non autorisées,
Authentification : permet de prouver l'authenticité par la confirmation de l'identité d'une entité,

Intégrité : garantie selon laquelle les données ne sont pas modifiées (par des utilisateurs non autorisés) lors du stockage ou du transfert.

2. Services de sécurité

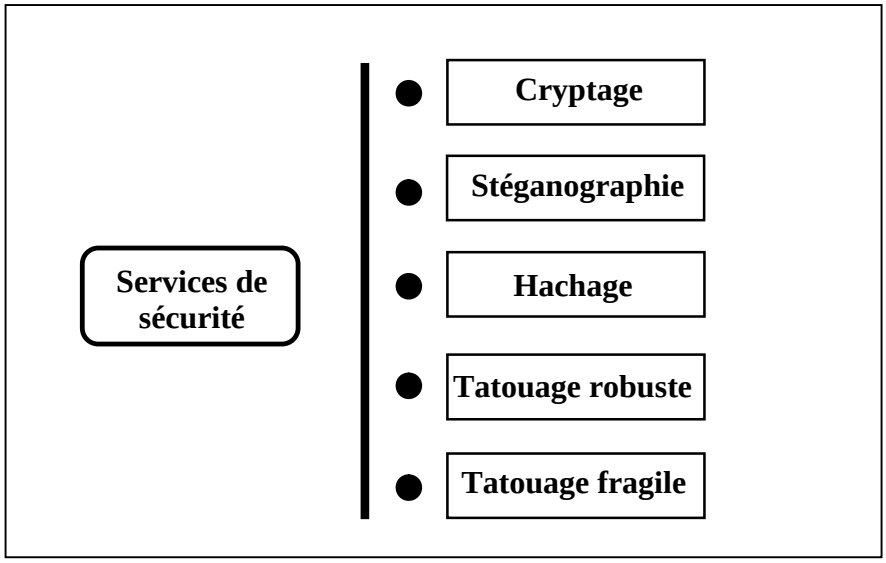


Figure 2. *Services de sécurité*

Cryptographie, stéganographie, hachage et tatouage sont les garants actuels de l'authentification, de l'intégrité et de la confidentialité des données médicales.

2.1. La stéganographie

La stéganographie [MIT99] [FEN05] est l'art de cacher un message primaire au sein d'un autre message secondaire (texte, image, son...).

Il faut que le message secondaire reste visuellement inchangé et que le message inséré soit parfaitement invisible mais accessible par toute personne qui possède une information secrète (clé) permettant son extraction.

2.2 Le cryptage

Le cryptage consiste à transformer un texte normal en un texte inintelligible appelé texte chiffré [CHC01] [ABD03] [BOR04]. Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le décryptage.

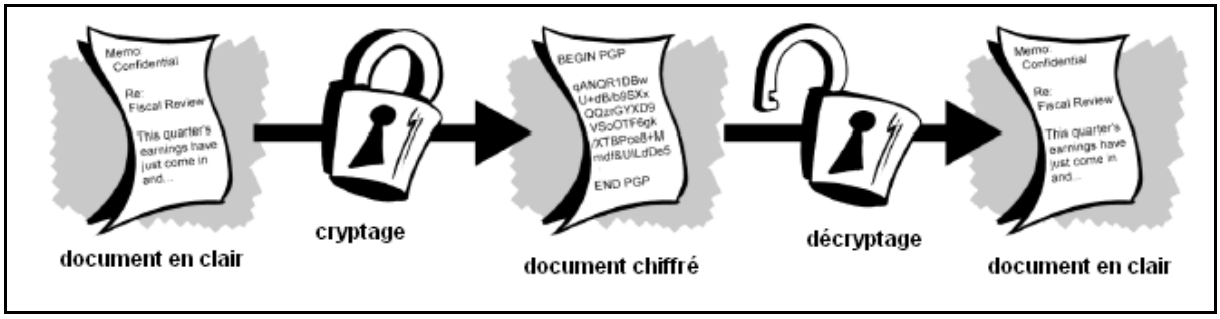


Figure 3. *Cryptage et décryptage*

On distingue deux catégories d'algorithme de cryptage (à clé unique et à clé publique) :
Les algorithmes de cryptage à clé unique ou symétrique nécessitent le partage d'un secret (la clé) [LV01] entre l'émetteur et le destinataire qui sert à la fois pour chiffrer et déchiffrer un message. Il existe plusieurs algorithmes symétriques dont le DES, le triple DES, le IDEA…
Les algorithmes de cryptage à clé publique ou asymétrique évitent le partage d'un code entre deux interlocuteurs, chaque utilisateur dispose de deux clés : une publique et une privée. Les messages chiffrés avec l'une des clés de la paire peuvent seulement être déchiffrés par l'autre clé de la paire. Il existe plusieurs algorithmes asymétriques [BOUH 02] dont le RSA, le PGP…

2.3. Le hachage

Une fonction de hachage est une fonction mathématique qui, à partir d'un message (d'une donnée), génère une autre chaîne (généralement plus courte) [AND93] [PRE93]. On distingue dans la littérature de notions :
Celle de fonction de hachage à sens unique (« one way function ») [MER90] :
C'est une fonction f(M) facile à calculer mais telle qu'il est extrêmement difficile de déduire M de f(M) : c'est à dire qu'il est presque impossible de retrouver le texte original en possédant celui haché (dit autrement, la fonction n'est pas bijective).
Celle de fonction de hachage à sens unique avec clé :
C'est une fonction f(M) facile à calculer telle qu'il est extrêmement difficile de déduire M sauf si l'on connaît une clé secrète K.

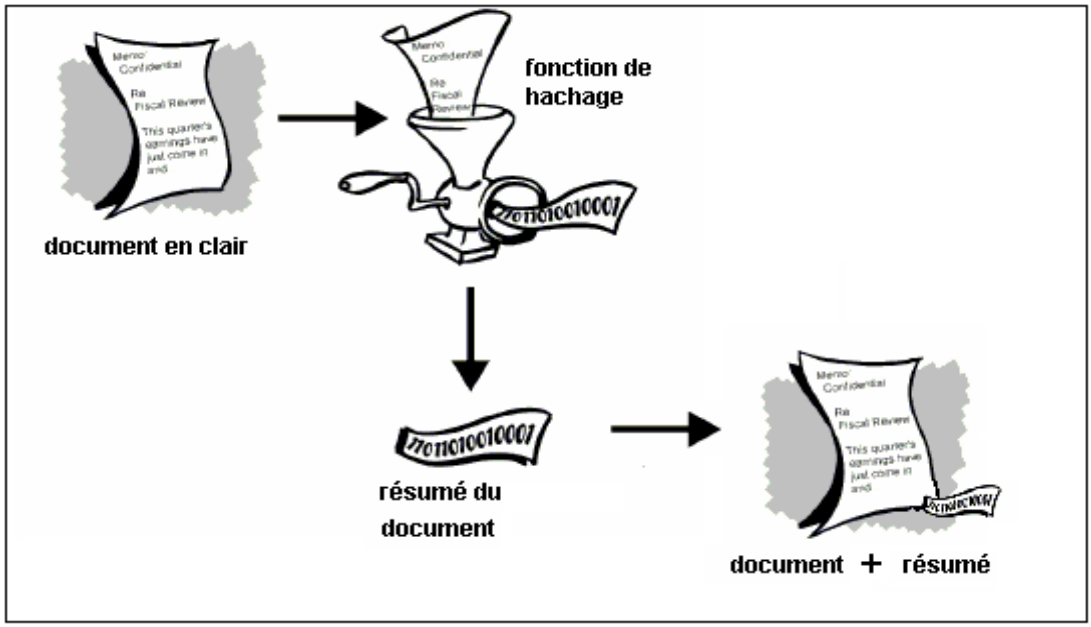


Figure 4. *Hachage d'un document*

L'ensemble haché résumé du document et document est transmis. Il est impossible de récupérer le résumé d'un document pour la joindre à un autre document ou d'altérer le document original. La moindre modification apportée entraîne l'échec du processus de vérification.

2.4. Le tatouage

Le tatouage numérique est l'art de cacher une signature dans un document [BEN96] [HSU99] [NIK99]. Cette marque invisible ou non aura des caractéristiques propres à chaque domaine d'utilisation (robustesse, réversibilité, capacité ...).

En effet, les méthodes de tatouage doivent tenir compte d'une part de l'application visée et des contraintes de sécurité et d'autre part de la nature des données à traiter.

2.4.1. Différents types de tatouage

Le tatouage robuste : l'application envisagée pour le tatouage robuste [RAM05] d'images a été la protection des droits d'auteurs [RUA96][HER99] associés au document numérique. La signature dissimulée dans le médium est le garant de l'identité de son ayant droit. Ce tatouage doit d'être imperceptible, robuste et sûr.

Le tatouage fragile : L'information insérée au sein de l'image permet de vérifier si l'image a été modifiée par une tierce personne [KUN99]. C'est ce que l'on appelle le contrôle

d'intégrité. Dans ce cas, la signature ajoutée doit être fragile [FOU06a] : dans le sens où si le document est modifié la signature doit disparaître. Ce type de contrôle d'intégrité trouve ses champs d'application dans la détection des faux papiers (carte d'identité, passeport, permis,…) mais également dans le cadre médical.

Le tatouage semi fragile : C'est un tatouage fragile par rapport aux différentes attaques mais qui permet de tolérer des attaques bien définies telles que la compression avec un facteur de qualité bien déterminé (de 100% jusqu'à 70%) [ES04] [BOU05][FOUR06c] [FOU08].

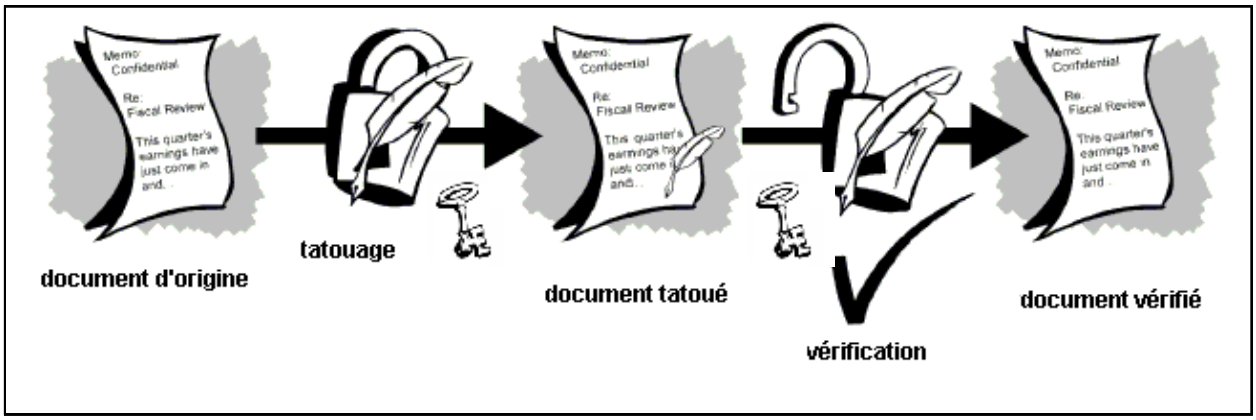


Figure 5. *Insertion et détection du tatouage*

2.4.2. Domaines d'insertions

La diversité des différents schémas de tatouage est liée au choix du domaine d'insertion de la signature. Chaque espace de représentation de l'image apporte diverses possibilités en termes de performance [BOU03].

Le domaine spatial :

C'est le schéma primaire de tatouage [BRU95]. Il se base sur la manipulation directe de la luminance des pixels. Les opérations d'insertion et de détection de la signature sont peu coûteuses en temps de calcul.

Le domaine fréquentiel :

La représentation fréquentielle de l'image est obtenue suite à une transformation TFD (Transformée de Fourier Discrète) ou TCD (Transformée en Cosinus Discrète). Grâce à l'évolution des algorithmes de transformations rapides, le calcul de la transformée d'une image est moins coûteux. Cela a encouragé l'utilisation de ce domaine.

Le choix des coefficients à tatouer représente donc la problématique principale de ce type de schéma. Les meilleurs schémas optent généralement pour une insertion dans les hautes fréquences de l'image afin d'assurer à la fois une bonne imperceptibilité et sensibilité.

Le domaine de multirésolution :

Les informations représentées dans le domaine multirésolution sont bien localisées en fréquences et en temps [XIA 97] [BOU 97].

Les caractéristiques de ce domaine de transformation motivent l'utilisation de la technique de tatouage dans le domaine des ondelettes.

Il est souvent préférable que l'insertion se fait dans les trois sous bandes de détail afin de préserver une meilleure imperceptibilité de la signature.

2.4.3. Les modèles de détection

Le modèle aveugle : l'extracteur n'a pas connaissance ni du document original, ni de la marque. La détection de la signature exige la connaissance de la clé secrète pour extraire la signature. Dans cette catégorie de marquage nous pouvons distinguer les travaux publiés dans [YLLS00].

Le modèle semi-aveugle : ce modèle nécessite la possession de la marque à tester, sans avoir de connaissance du document original [EL06].

Le modèle non aveugle : la détection de la signature dans ce type de modèle nécessite la possession du document original. Ceci facilite l'extraction de la marque [GET06].

Remarque : Les méthodes de vérification de l'intégrité des documents ne font pas recours aux documents originaux ce qui explique l'utilisation fréquente du modèle aveugle.

Dans ce qui suit nous présentons un tableau récapitulant l'application habituelle de chaque service de sécurité.

Tableau 1. *Les services de sécurité*

Service	Cryptage	Hachage simple	Hachage avec clé	Tatouage robuste	Tatouage fragile	Tatouage semi fragile
Confidentialité	✓					
Intégrité		✓	✓		✓	✓
Authentification			✓	✓	✓	✓

Nous avons exposé les concepts et techniques de sécurité de données. Nous avons pu remarquer que les approches existantes pour la sécurisation d'images sont nombreuses et variées, et que chacune possède ses avantages.

Le choix d'une méthode appropriée est fortement lié aux objectifs recherchés : intégrité, authentification [TRI02] [KAL06] ou simplement transmettre un message.

3. Les principes de sécurité

Les principes les plus classiques en sécurité sont le principe de Kerckoffs et le théorème de C.E. Shannon.

3.1. Principe de Kerckhoffs

Un chiffrement est une fonction F(:) qui encrypte un message clair m en un message chiffré c = F (m). Cette fonction est bien sûr inversible. Si un attaquant connaît c, il doit être très difficile de retrouver m (chiffrement partiellement cassé) ou F(:) (Chiffrement totalement cassé).

En fait, le chiffrement appartient à une classe de fonctions paramétrées par une clé secrète k appartenant à l'espace K des clés possibles. Dans ce cadre A. Kerckhoffs rédige en 1883, un article présentant quelques principes élémentaires [AUG83]. Nous ne retenons aujourd'hui que le principe suivant : « toute méthode de chiffrement doit être supposée connue de l'adversaire ; par conséquent, la sécurité du système ne repose que sur la connaissance de la clé. »

Une attaque toujours possible est de tester les ki clés possibles : il est possible virtuellement de décrypter c, il faut juste parcourir l'ensemble K. La question n'est pas de savoir si l'attaquant trouvera la clé mais quand il la trouvera.

3.2. Théorème de Shannon

Dans l'article [SHA49], C.E. Shannon introduit la notion de chiffrement parfait. m et c étant des éléments des ensembles de messages possibles et de leur chiffrement correspondant, on nomme Prob(m) la probabilité a priori que m soit transmis. Ces probabilités sont connues de l'attaquant. Puis, celui-ci intercepte un message chiffré c, il en déduit les probabilités a posteriori Prob(m\c).

Un système de chiffrement est qualifié de parfait si :

$$\forall(m,c) \quad \text{Prob (m\c)} = \text{Prob (m)} \qquad \text{(Eq } \mathbf{1}\text{)}$$

Cela signifie qu'un chiffrement parfait ne délivre aucune information supplémentaire quant au message clair envoyé. L'interception du message chiffré c ne décroît en rien l'ignorance de l'attaquant qui se réduit aux probabilités a priori.

4. Protection de l'intégrité des images

4.1 Notion d'intégrité

La définition de la notion d'intégrité repose sur une décision binaire qui garantit que les données reçues sont rigoureusement identiques à celles émises. Cette définition est applicable à tout type de documents numériques.

Le problème de l'intégrité des images se pose généralement en termes de contenu sémantique : c'est à dire la détection des modifications du document pouvant engendrer une gêne dans sa visualisation et/ou une erreur dans son interprétation (modification, disparition d'un visage, …). Mais dans des cas particuliers, par exemple l'imagerie médicale [COA01], des manipulations anodines, comme une simple compression, un filtrage ; une égalisation d'histogramme, … peuvent causer la disparition de certains signes visibles d'une pathologie faussant alors le diagnostic du médecin.

Les premières méthodes proposées pour assurer l'intégrité des images sont basées sur l'utilisation d'un tatouage fragile [WOL96] [FRI98] [YEU97]. Le principe de ces approches est d'insérer une marque ou un logo dans l'image d'origine de telle manière que les moindres modifications apportées à l'image se répercutent également sur la marque insérée [VAR05]. Pour vérifier l'intégrité d'une image, il suffit alors de vérifier localement la présence de cette marque [REY02] [MIN 97].

L'insertion de la signature se fait par modification du signal initial, par exemple, par modification des bits de poids faibles LSB [WON 99] ou encore des coefficients d'ondelettes hautes fréquences [FOUR06d].

Ces techniques de tatouages ont garanti l'intégrité des données et empêché les attaques qui pourraient compromettre l'authentification de ces donnés.

4.2. Les contraintes du tatouage : Les attaques

Le document hôte dans lequel les informations sont cachées peut subir de nombreuses transformations. Il est important de noter que ces transformations ne sont pas nécessairement des attaques dont l'exécutant vise à falsifier l'image et à l'utiliser illégalement. Elles peuvent être des transformations visant à adapter l'image à l'usage personnel.

4.2.1. Falsification

La falsification est définie correspondant à toute substitution, ajout ou suppression de valeurs des composantes d'une image visant une modification du contenu de l'image.

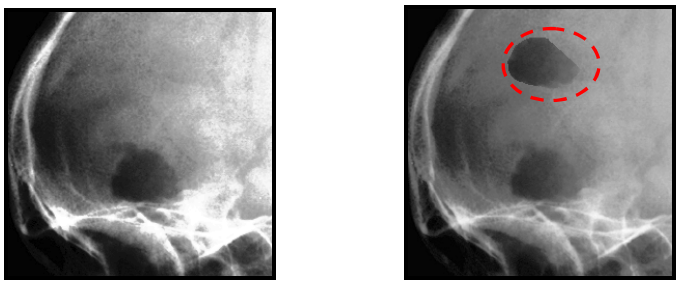


Figure 6. *Image falsifiée*

4.2.2 L'ajout de bruit

Nous allons étudier deux types de bruits : le bruit gaussien et le bruit multiplicatif.

A. Bruit gaussien

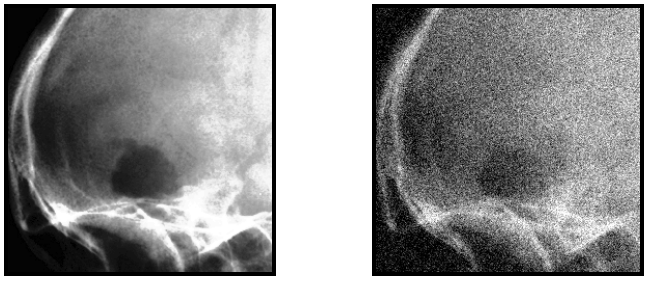


Figure 7. *Image attaquée par ajout de bruit gaussien*

Le gaussien possède une densité de probabilité définie par une loi normale :

$$f_X(x,t_k) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{1}{2}\frac{(x-m)^2}{\sigma^2}\right) \qquad \text{(Eq 2)}$$

m étant la moyenne et σ l'écart type

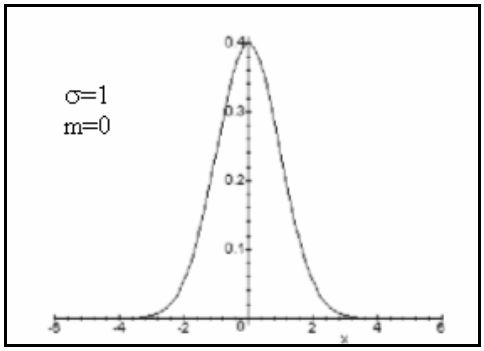


Figure 8. *Distribution du bruit gaussien*

B. Bruit speckle

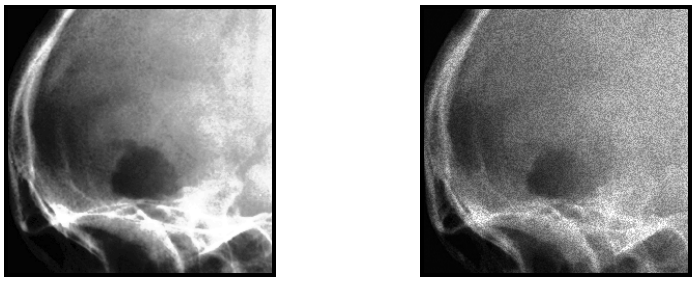


Figure 9. *Image attaquée par ajout de bruit speckle*

Etant donné une image initiale I. Si l'on suppose J l'image finale obtenue par application du bruit multiplicatif sur l'image originale, on a alors : J = I + n*I,

où n est un bruit aléatoire uniformément distribué.

4.2.3. Filtrage

Le filtrage a pour but la réduction voire l'annulation du bruit qui s'introduit dans l'image lors de son acquisition.

Dans les cas présentés ici, le filtrage consiste à balayer l'image par une fenêtre d'analyse de taille finie.

A. Filtre moyen

La procédure de filtrage consiste à remplacer la valeur d'un pixel par la somme des valeurs des pixels qui l'entourent, affectée de certains coefficients (poids).

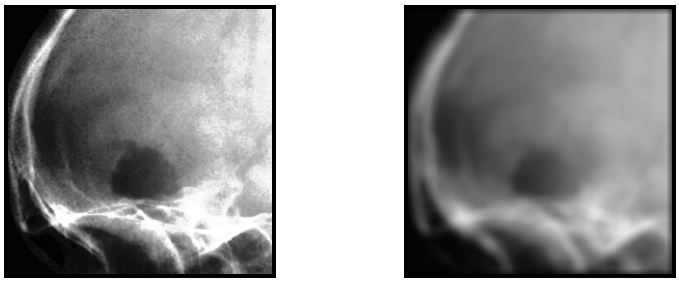


Figure 10. *Image attaquée par filtre moyen*

B. Filtre médian

C'est un filtre non linéaire dont le principe est le suivant :

Nous classons les pixels voisins du pixel courant (compris dans la fenêtre) par valeurs croissantes.

Puis nous prenons la valeur médiane des pixels classés et on l'affecte au pixel courant.

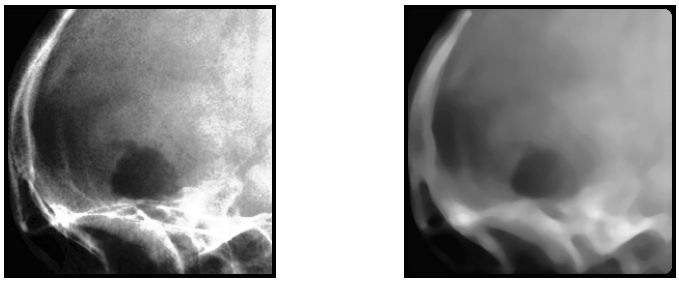


Figure 11. *Image attaquée par filtre médian*

C. Filtre gaussien

C'est un filtre linéaire qui tient son nom des valeurs de ses coefficients qui sont ceux d'une courbe de Gauss à deux dimensions.

Un filtrage gaussien consiste en la convolution d'une image avec une gaussienne $G(x, y, \sigma)$:

$$I_f = I_i \otimes G \qquad \text{(Eq 3)}$$

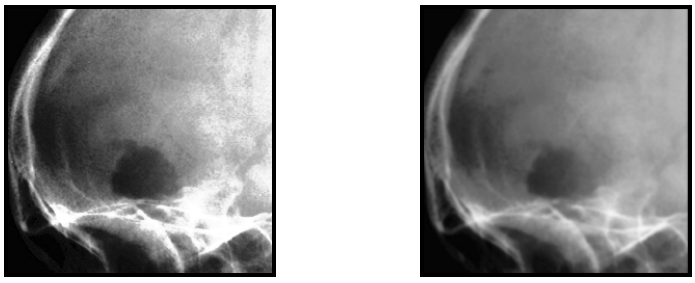


Figure 12. *Image attaquée par filtre gaussien*

D. Filtre unsharp

Ce filtre est appelé aussi filtre de rehaussement de contraste. Le rehaussement des images s'effectue en accentuant les composantes hautes fréquences de l'image. Il augmente le contraste de l'image. C'est pourquoi nous l'appelons rehaussement de contraste. Les détails de l'image deviennent alors plus prononcés.

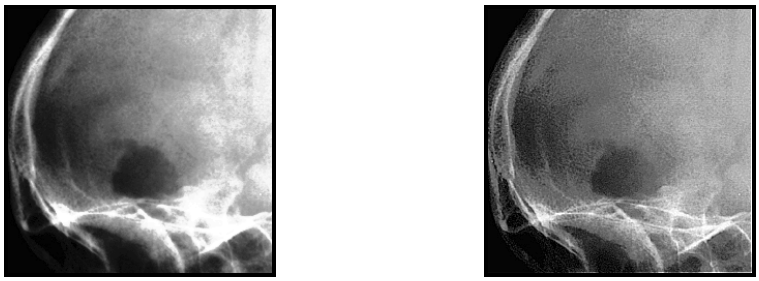


Figure 13. *Image attaquée par filtre unsharp*

4.2.4. Egalisation d'histogramme

Elle consiste à transformer les intensités de l'image à l'aide d'une fonction telle que leur distribution résultante moyenne soit uniforme. Dans le cas d'intensités discrètes l'histogramme résultant n'est pas plat, mais le plus homogène possible. Ainsi la transformation a pour effet de dilater ou de compresser localement l'histogramme (de séparer les valeurs d'intensité) pour obtenir une distribution des valeurs qui soit aussi régulière que possible.

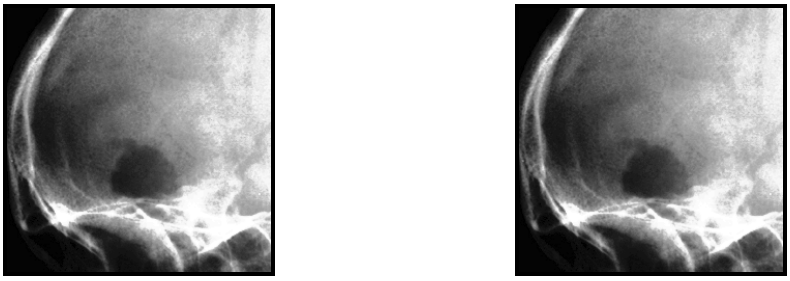


Figure 14. *Image attaquée par égalisation d'histogramme*

4.2.5. Compression

Les nécessités de stockage et /ou de transmission des images numériques nous poussent souvent à utiliser des outils de compression pour réduire la taille des fichiers images. Le format JPEG est le standard classique le plus utilisé pour la compression des images.

L'idée principale de la compression est d'éliminer les hautes fréquences (les détails) de l'image.

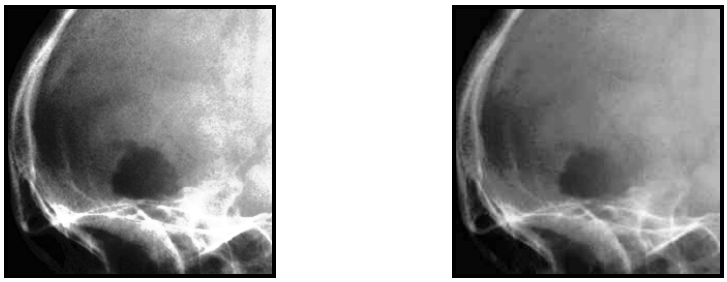


Figure 15. *Image attaquée par compression*

4.2.6. Rotation

Suite à une déviation de l'image d'un certain angle. Les intensités des pixels ne peuvent jamais retourner leurs valeurs initiales.

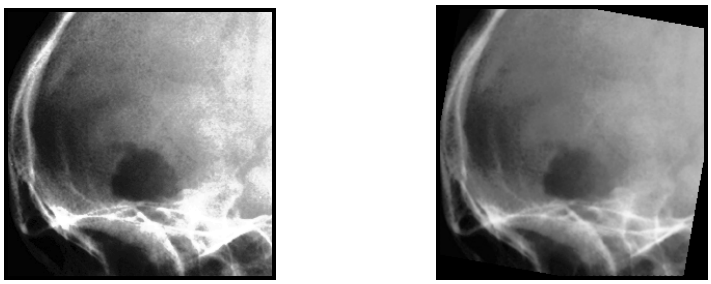


Figure 16. *Image attaquée par rotation*

Conclusion

Dans ce chapitre, nous avons tout d'abord présenté le secteur d'applications visé, la télémédecine et en particulier le télédiagnostic. Ensuite nous avons décrit plusieurs services de sécurité pour la sécurisation d'informations en évoquant tout d'abord les notions formelles de sécurité et leurs accusations. Nous avons ensuite mis en évidence le tatouage fragile et nous avons enfin prouvé la nécessité de la réversibilité.

Ainsi, ce premier chapitre nous a permis de bien définir la problématique de cette Thèse. L'image médicale porte des informations essentielles et nécessaires au diagnostic du patient et à l'évaluation de son état de santé. En découle la nécessité de protéger l'information médicale contenue dans l'image et de ne pas l'altérer. En effet, l'insertion de la signature peut modifier les intensités de quelques pixels ce qui peut éventuellement engendrer la disparition de certains signes visibles d'une pathologie faussant alors le diagnostic du médecin.

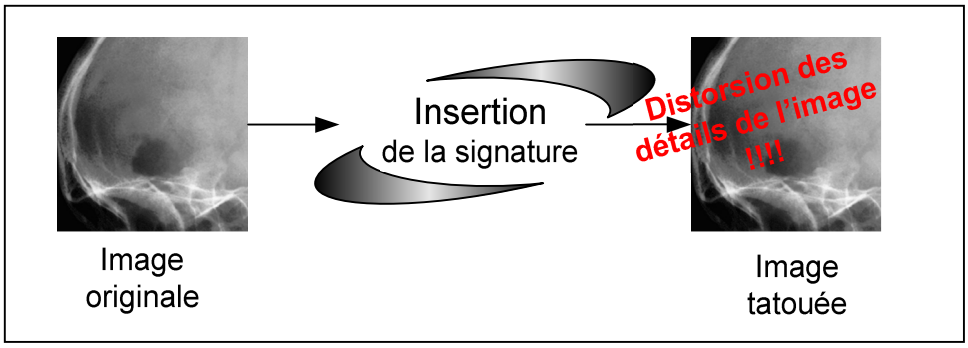


Figure 17. *Problématique des techniques de tatouage non réversible*

Actuellement, plusieurs efforts se concrétisent pour dépasser ce problème, la solution la plus adaptée pour retrouver l'image originale à partir de l'image tatouée après le passage de cette dernière par le processus d'authentification est le tatouage réversible [FRI04] [KAM05] [FOU07].

Comme tout type de tatouage fragile [KUN 99], le tatouage réversible [FOU06b] [ALA04] est utilisé pour assurer l'intégrité de l'image, mais il a l'avantage de retrouver l'image originale. Cette réversibilité est nécessaire dans tous les secteurs d'imagerie sensible, surtout pour le secteur médical [ZAI04].

En effet, après avoir garanti l'intégrité de l'image, le médecin reconstitue l'image originale (non tatouée : intacte sans aucune dégradation) et l'utilise dans son diagnostic évitant tous les risques de modification (lors de l'insertion de la signature).

Chapitre II

Tatouage réversible

Introduction

Le tatouage réversible consiste à insérer d'une manière invisible et réversible une signature au sein de l'image originale, la signature ajoutée doit être fragile dans le sens où si l'image est modifiée elle doit devenir inexploitable.

Après extraction et vérification de la validité de la signature, ce type de tatouage est capable de restituer un duplicata exact de l'image originale.

1. Caractéristiques du tatouage réversible

Trois paramètres caractérisent ce type de tatouage :

- **L'imperceptibilité** : l'imperceptibilité de la signature n'est pas une nécessité au bon tatouage [CRA 98]. En effet, il faut spécifier tout d'abord l'application visée pour pouvoir préciser si l'imperceptibilité de la signature insérée est nécessaire ou pas.

  Pour les images médicales la signature doit être imperceptible pour ne pas dénaturer les radiographies (pour ne pas conduire à un diagnostic erroné, en masquant une zone ou une ombre par exemple).

- **La fragilité** : l'image tatouée va subir des transformations de nature très diverses ; que ce soit les traitements dus à l'usage de l'image ou encore les attaques qui visent sa falsification. La signature doit disparaître à la moindre manipulation et sa présence garantit que rien n'est modifié.
- **La réversibilité :** après extraction et vérification de la validité de la signature les méthodes de tatouage réversible sont capables de restituer un duplicata exact de l'image originale**.**
- **la cohérence avec le principe de Kerchhoffs** : L'algorithme de tatouage doit être cohérent avec le principe de Kerchhoffs [AUG83] qui considère que toute méthode de chiffrement doit être supposée connue de l'adversaire.

- **la détection aveugle :** l'extracteur n'a pas connaissance de l'image originale.
- **la capacité d'insertion :** la quantité d'information qu'on peut insérer doit être assez importante.

2. Principe du tatouage réversible

Le schéma de tatouage réversible d'images se décompose en deux phases distinctes. Dans ce qui suit nous présenterons les caractéristiques de chacune de ces phases.

2.1. La phase d'insertion

Cette étape est fondamentale dans le schéma de tatouage, elle consiste à introduire de manière invisible une information dans une image. Cette information doit disparaître à la moindre manipulation.

Soit I notre image, W la signature à insérer qui dépend généralement d'une clef secrète et I_w l'image tatouée obtenue.

T(I) étant l'espace d'insertion qui peut être le domaine spatial ou bien le résultat d'une transformation réversible de l'image dans le domaine fréquentiel comme la transformée en cosinus discrète (TCD), la transformée de Fourier discrète (TFD) ou encore une transformation dans le domaine multirésolution comme la transformée par ondelettes.

D'une manière générale la fonction d'insertion se présente sous la forme suivante :

$$\mathbf{I_w = F\,(T(I),\, W(b_0,\, b_1,\, b_k,\, b_n))} \qquad \mathbf{(Eq\ 4)}$$

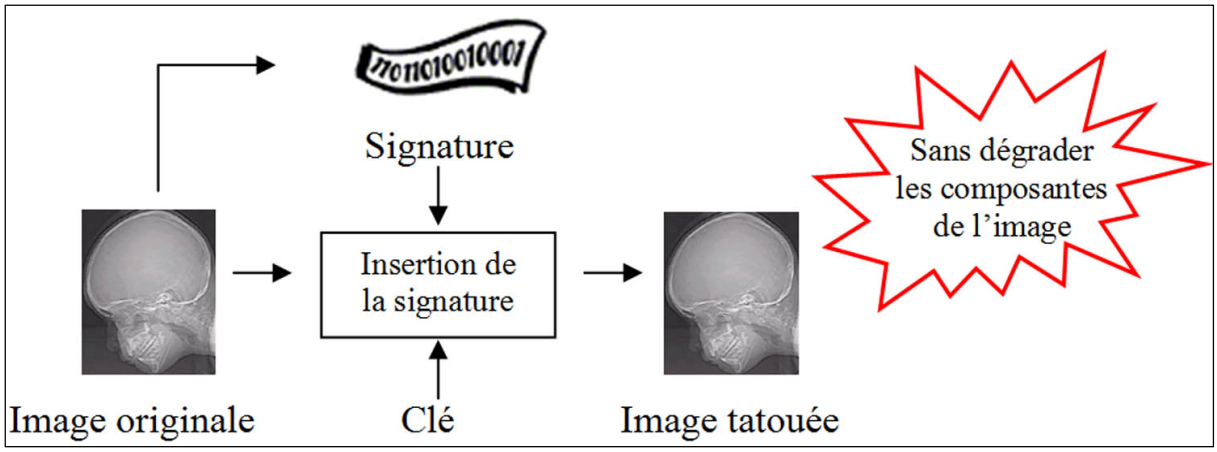


Figure 18. *Schéma d'insertion de la signature*

Le modèle général d'insertion de la signature

Le modèle général d'insertion de la signature (cf figure 18) peut se décomposer en plusieurs étapes :

- on transforme l'image dans le domaine d'insertion désiré,
- on précise les composantes de l'image originale dans lesquels on insère la signature. (nous entendons par composantes les pixels de l'image ou bien le résultat d'une transformation fréquentielle (TCD, TFD) ou multirésolution (ondelettes)).
- on applique à l'image une fonction de hachage permettant de prendre des informations sur l'image elle-même,
- la signature (qui peut être le résumé de l'image seulement ou bien l'association de ce dernier avec une autre donnée) est ajoutée sur les composantes sélectionnées de l'image.
- l'image marquée est reconstruite avec les composantes sélectionnées et modifiées.

2.2. La phase de détection

Cette phase se fait suivant deux 2 étapes complémentaires :

- La première vise à retrouver la signature insérée dans l'image originale. Elle consiste à inverser le processus de marquage.
- La seconde étape est la continuité de la première. Elle permet de comparer la signature extraite à celle insérée afin de savoir si l'image tatouée présente des altérations ou des transformations.

La phase de détection de la signature (cf figure 19) est capitale. C'est le résultat de cette étape qui peut déterminer l'intégrité de l'image.

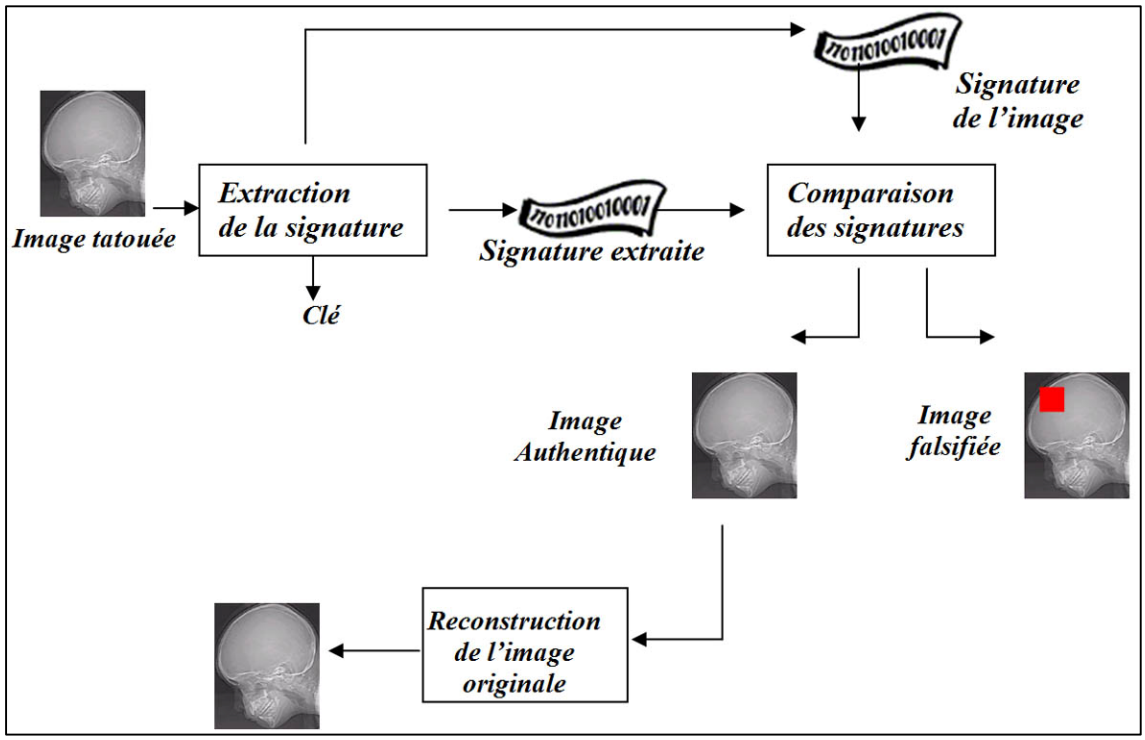


Figure 19. *Schéma de détection de la signature*

Le modèle général de détection de la signature

La détection de la signature peut généralement se décomposer en cinq étapes :

- transformer l'image dans le domaine d'insertion utilisé dans de tatouage,
- extraire les composantes marquées,
- prélever les éléments de la signature en inversant la fonction d'insertion,
- appliquer à l'image la fonction de hachage utilisée pendant la phase d'insertion,
- Comparer la signature extraite avec le résultat de la fonction de hachage, en vérifiant ainsi que les informations de l'image n'ont pas été modifiées,
- Si l'image est falsifiée elle sera rejetée, sinon cette image sera intégrée et l'on passe à la phase de reconstitution de l'image originale.

3. Etat de l'art sur le tatouage réversible

Les premières méthodes de tatouage dites « réversibles » ou « d'insertion de données sans perte » ont été présentées par Jm. Barton en 1997 [BAR97]. Ces méthodes ont été optimisées par Fridrich[FRI01], puis Celik[CEL02]. L'utilisation de la compression de données est un élément clé de ces méthodes et aussi des méthodes développées par Fridrich [FRI02], Tian

[TIA03] et Celik[CEL03]. En effet la compression permet de libérer un espace libre supplémentaire dans l'image à marquer.

3.1. Approches basées sur la compression

En 1997 Barton[BAR97] a proposé une première technique de tatouage réversible qui consiste d'une part à compresser (sans perte) les bits consacrés à l'insertion pour garder les données originales de l'image et d'autre part à libérer de l'espace supplémentaire dans l'image pour insérer la signature[LEE03].

L'utilisation de la compression est un élément clé pour plusieurs méthodes de tatouage réversible.

Ce processus de compression est adopté par la suite par Fridrich[FRI01] en 2002. Cette méthode consiste à calculer le *haché* de l'image (de longueur 128 bits) à l'aide de l'algorithme MD5[RIV92], puis à chercher le plan de bit le plus adéquat pour lui appliquer l'algorithme de compression JBIG[SAY96] et ensuite à insérer le *haché* et les donnés compressées dans ce plan de bit.

Dans le même cadre Celik[CEL02] a proposé une technique qui commence par calculer le *haché* de longueur de 128 bits (à l'aide de l'algorithme MD5). Puis un algorithme de compression CALIC est appliqué au plan de bit de niveau le plus bas, ensuite il s'agit de vérifier si l'espace libre créé par cette compression suffit pour insérer les 128 bits du *haché* ou sinon il faut passer au plan de bit suivant (tout en tenant compte de la qualité de l'image tatouée).

L'avantage majeur de ces techniques de tatouage réversible est la simplicité d'implémentation.

Dans ce qui suit nous allons détailler la technique de tatouage réversible la plus connue.

3.1.1. Schéma d'insertion

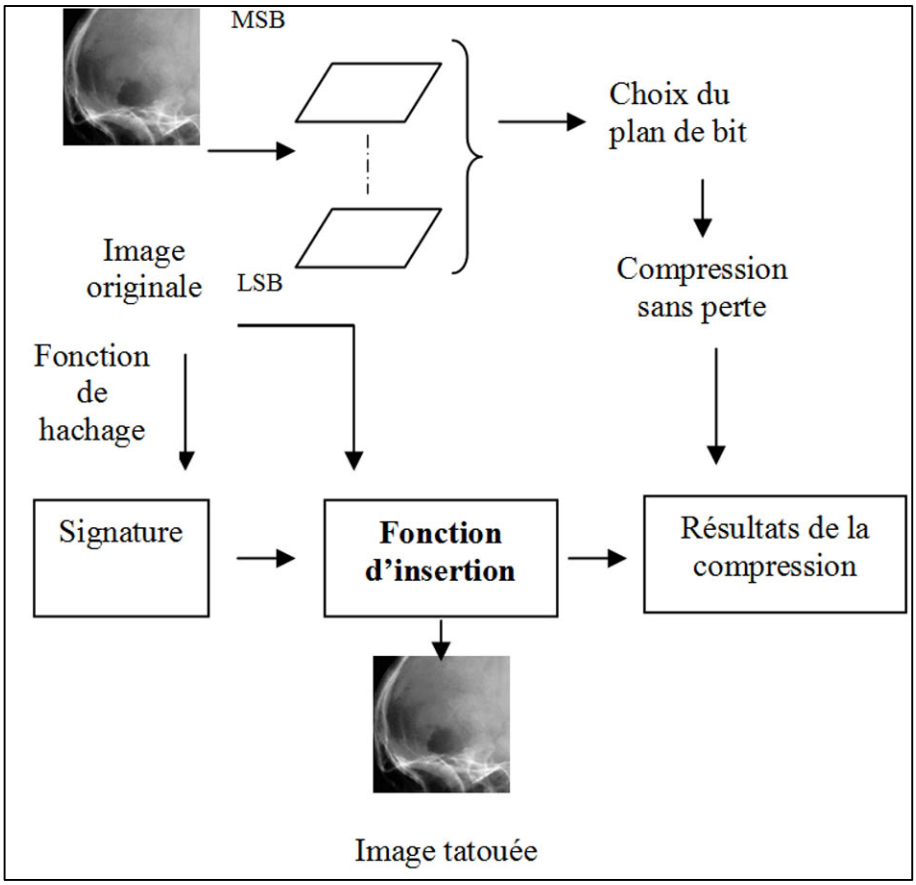


Figure 20. *Schéma d'insertion*

Pour le schéma d'insertion illustré dans la figure 20, il s'agit d'appliquer un algorithme de compression sans perte sur le plan de bits choisi pour l'insertion de la signature.

Cet algorithme de compression est utilisé pour garder les données originales (sans perte) d'une part et d'autre part pour libérer de l'espace pour l'insertion de la signature.

Ensuite le résultat de la compression et la signature sont insérés dans le plan de bits choisi pour aboutir à l'image tatouée.

3.1.2. Choix bu plan de bit

Le plan de bits est choisi tout en assurant le bon compromis entre la qualité de l'image tatouée d'un coté et la sensibilité et la capacité d'insertion.

En effet, le huitième plan de bits (les MSB) présente les composantes de l'image perceptuellement significatives (basses fréquences). Cependant la modification des basses fréquences engendre un impact visuel assez important .Pour ceci, il est intéressant de choisir

les plans de bits de niveaux le plus bas que possible afin d'assurer une dégradation minimale de la qualité d'image.

Ce choix est aussi favorable pour assurer une meilleure sensibilité par rapport aux différentes attaques que peut subir l'image lors de sa transmission. En effet, la plupart des attaques altèrent les hautes fréquences : on peut citer par exemple la compression qui soustrait quelques détails (les hautes fréquences) de l'image et le filtrage qui efface les détails fins et étale les contours. Pour cela il est intéressant d'insérer la signature dans les hautes fréquences qui correspondent au plan de bits de bas niveau (LSB) pour qu'elle soit sensible aux attaques que peut subir l'image tatouée.

Mais en contre partie, les plans de bits de bas niveau présentent moins de redondance que les plans de bits de haut niveau. Autrement dit, pour les plans de bits de bas niveau le résultat de la compression sera de taille plus importante, donc un espace libre (capacité d'insertion) moins important.

Cependant, il faut bien choisir un plan de bits assurant le bon compromis (cf figure 21) entre la capacité d'insertion d'un coté et la qualité d'image tatouée et la sensibilité d'autre côté.

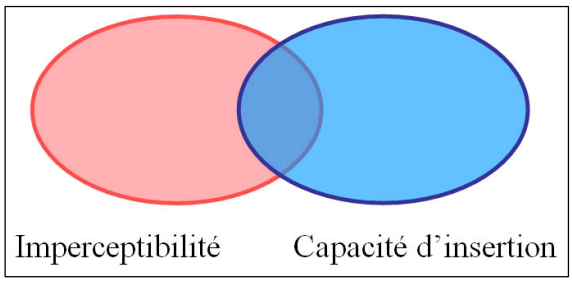


Figure 21. *Compromis entre la qualité de l'image tatouée et la capacité d'insertion*

3.2. Approche Région ou Bloc

En 2003 Celik présente [CEL03] une nouvelle méthode de tatouage réversible, nommée LAW (Localized Lossless Authentication Watermark). Cette méthode utilise des blocs de pixels de l'image dans lesquels sera inséré le message.

Une opération de quantification est tout d'abord effectuée :

$$Q_L(x) = L * \left[\frac{x}{L} \right] \qquad \textbf{(Eq 5)}$$

$[x]$: représente la fonction du plus grand entier inférieur ou égal à x.

Exemple :

Pour un bloc de l'image originale de taille 4x4

O :

20	37	7	22
35	12	32	13
22	12	18	23
12	23	12	26

Pour L=5

Q :

20	35	5	20
35	10	30	10
20	10	15	20
10	20	10	25

Un résidu r est ensuite créé (équation 5)

$$r = x - Q_L(x) \qquad \textbf{(Eq 6)}$$

r :

0	2	2	2
0	2	2	3
2	2	3	3
2	3	2	1

Pour optimiser la taille du flux des données r, l'algorithme de compression CALIC est utilisé. La compression est un élément majeur pour améliorer la capacité d'embarquement de la méthode.

La signature binaire est convertie en base L puis elle sera ajoutée avec le résidu aux coefficients de l'image quantifiée suivant l'équation suivante :

$$x_w = Q_L(x) + w \qquad \textbf{(Eq 7)}$$

x_w est le signal marqué. w représente la marque constituée de symboles w_i dit L-aire symboles, c'est-à-dire $w_i \in \{0,1,...,L-1\}$

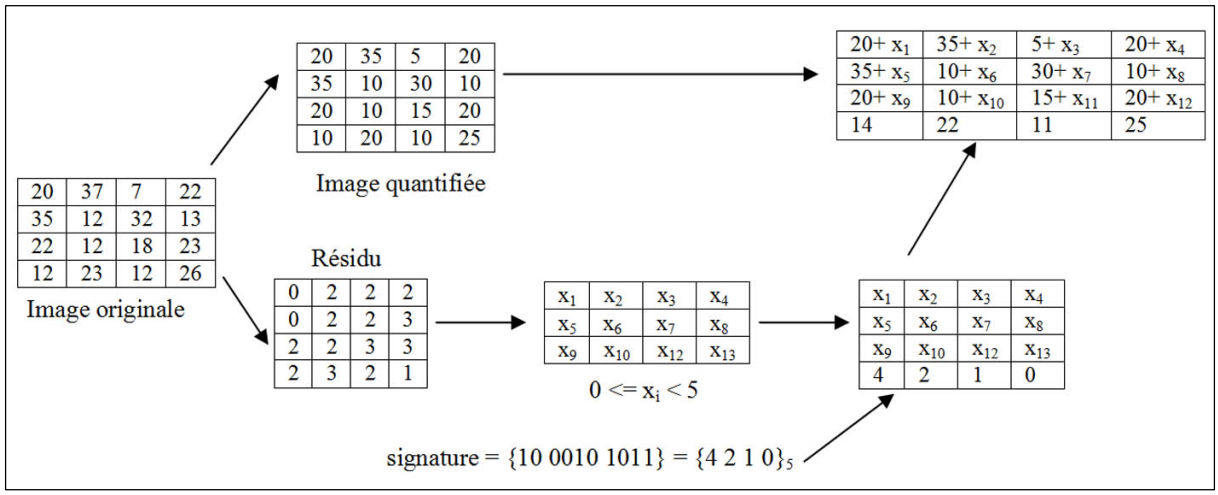


Figure 22. *Exemple du schéma d'insertion de la méthode de Celik*

Lors du détatouage, les valeurs de r seront récupérées et le signal original pourra être recalculé (cf figure 22).

3.3. Approche Regroupement

Les algorithmes développés par Tian [TIA03] et Fridrich [FRI02] regroupent les pixels par groupes suivant un voisinage choisi pour en étudier les variations suivant une fonction de discrimination. Les nouvelles valeurs obtenues par cette fonction seront classées en groupes puis tatouées ou non suivant les groupes.

3.3.1. La méthode de Fridrich(RS)

En 2002 Fridrich propose une méthode de tatouage réversible [FRI02a], [FRI02b] :

- Les pixels de l'image sont assemblés en groupes de pixels (blocs),
- deux fonctions commutatives f(x1;x2;…) et F(X) sont définies :
  - la fonction f dite de discrimination cherche à mesurer la régularité des groupes de pixels. Cette fonction peut être, par exemple, la fonction "variation"

$$f(x_1, x_2, ...x_n) = \sum_{i=1}^{n-1} \left| x_{i+1} - x_i \right|$$

  - La fonction F de permutation telle que F(F(x)) = x . Cette fonction peut-être par exemple la fonction qui à 1 associe 0 et à 1 associe 0, à 3 associe 2 et à 2 associe 3, ...
- Pour chaque groupe de pixels est attribuée une catégorie R, S ou U suivant le schéma suivant :

- R (‟Regular″) si f(F(G)) > f(G)
- S (‟Singular″) si f(F(G)) < f(G)
- U (‟Unusable″) si f(F(G)) = f(G)

- La carte binaire de localisation contenant les positions de R et S est compressée et rajoutée aux données à insérées.
- Le code 0 est attribué au groupe R, le code 1 au groupe S. Pour faire changer l'état un groupe de pixels, il suffit de lui appliquer la fonction F.
- Lors de la reconstruction, il suffira d'appliquer à nouveau la fonction de permutation, suivant la carte de localisation, sur un pixel pour obtenir la valeur initiale du pixel.

Par exemple

Soit le groupe de pixel G suivant :

A	B
C	D

La fonction de discrimination est calculée sur ce groupe :

f1 = f(A;B;C;D)

La fonction de permutation est calculée pour chaque pixel :

A' = F(A) B' = F(B) C' = F(C) D'= F(D)

La fonction de discrimination est calculée sur le nouveau groupe :

f2 = f(A';B';C';D')

- Si f1 = f2 le groupe est dit « unusable » et donc non retenu.
- Si f1 > f2 le groupe est dit « singular » et équivaut à la valeur 1.
- Si f1 < f2 le groupe est dit « regular » et équivaut à la valeur 0.

Si le groupe ne correspond pas à la valeur désirée pour le marquage, les valeurs (A, B, C, D) du groupe de pixels sont substituées par les valeurs du groupe permuté (A', B', C', D').

Lors de la reconstruction suivant la carte insérée, il suffira d'appliquer à nouveau la fonction de permutation sur (A', B', C', D') pour obtenir (A, B, C, D).

3.3.2. La méthode de Tian

Une transformation par ondelettes de Haar [DAU 90],[SAI96] est appliquée à l'image originale.

L'ondelette de Haar est la plus ancienne et la plus simple (cf figure 23). Les fonctions Ψ(t) et Φ(t) sont décrites par les expressions :

$$\left.\begin{array}{lll} \Psi(t) = 1 & \text{si} & 0 \le t \le 0.5 \\ = -1 & \text{si} & 0.5 < t \le 1 \\ = 0 & \text{ailleurs} & \end{array}\right\} \quad \textbf{(Eq 8)}$$

$$\left.\begin{array}{lll} \Phi(t) = 1 & \text{si} & 0 \le t \le 1 \\ = 0 & \text{ailleurs} & \end{array}\right\} \quad \textbf{(Eq 9)}$$

Elle est principalement caractérisée par sa réversibilité [ADA 00] et sa symétrie.

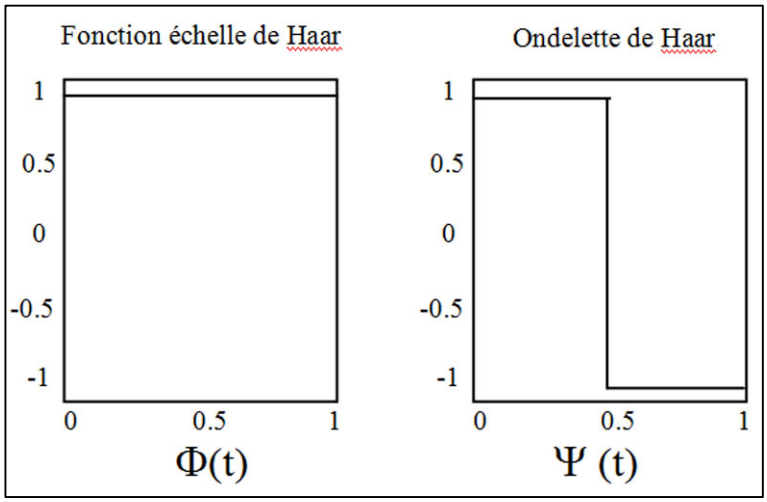


Figure 23. *Ondelettes de Haar*

Dans [TIA02] Tian insère les bits de la signature dans les coefficients de détail de l'image transformée aptes à être marqués.

$$\left.\begin{array}{l} 0 \le P_{1tatoué} \le 255 \\ 0 \le P_{2tatoué} \le 255 \end{array}\right\} \quad \textbf{(Eq 10)}$$

Ces conditions vont ainsi définir 2 groupes disjoints de coefficients selon des critères indiquant s'ils sont aptes à être marqués.

La carte de localisation $\mathcal{L}$ est une carte binaire qui précise les coefficients qui peuvent être marqués.

Elle permet ainsi à l'émetteur et au récepteur de l'algorithme de tatouage de partager les mêmes informations sur les positions des coefficients porteurs de la signature**.**

Cette carte de localisation est ensuite compressée en utilisant la compression sans perte JBIG2.

La marque à insérer est obtenue en concaténant la carte de localisation compressée $\mathcal{L}$ et un résumé de l'image à tatouer. Ce résumé est le résultat d'une fonction de hachage de l'image originale (SHA-256 ou MD5). La modification d'un seul bit de l'image originale modifie la valeur du résumé. Cette fonction permet de réaliser le contrôle d'intégrité de l'image.

Plusieurs techniques de tatouage réversible ont été conçues. Les techniques étudiées précédemment sont les plus réputées, et les plus efficaces.

Ces techniques répondent à notre objectif: tatouer l'image avec une faible dégradation de l'image tatouée tout en assurant une sensibilité assez importante par rapport aux différentes attaques que peut subir l'image.

Dans [VLE03], [YAN04], [CHA05], et [NI03] les auteurs présentent d'autres techniques de tatouage réversible robuste qui ne répondent pas à notre objectif : tatouer l'image avec une faible dégradation de l'image tatouée, assurer la vérification d'intégrité suite à sa transmission et restituer l'image originale afin de servir de support visuel au diagnostic.

4. Discussion

4.1. Limitation

Le tatouage réversible est une discipline récente : plusieurs techniques ont été étudiées et validées, mais aucune d'entre elles n'est parfaitement efficace.

L'inconvénient des méthodes de tatouage réversible qui utilisent la compression comme processus principal pour l'insertion de la signature [CEL03] [FRI01] [BAR97] est que la capacité d'insertion dépend des caractéristiques de l'image (de l'espace libre créé par la compression).

Pour les attaques qui consistent à ajouter, changer ou même éliminer des parties de l'image ; une aptitude de localisation de l'anomalie est importante pour le schéma de tatouage fragile. Néanmoins la méthode de Tian est incapable de localiser la falsification que peut subir l'image.

Dans le cas d'une image très texturée la capacité d'insertion pour la méthode de Tian sera très petite et on risque de tomber dans le cas de transmettre une image non signée ; une autre fois on se trouve dans le cas ou la capacité d'insertion dépend de la nature de l'image

En plus de la signature, Tian a inséré dans l'image originale la carte de localisation binaire qui sert à préciser les pixels dont la différence est apte d'être tatouée ; ce qui engendre une dégradation importante dans l'image surtout pour les images qui ont une grande capacité d'insertion (toute différence entre deux pixels voisins peut être tatouée).

4.2. Compromis réversibilité/précision (localisation)

Il n'existe pas aujourd'hui de méthode de tatouage réversible qui soit à la fois totalement réversible, imperceptible et qui puisse insérer une grande quantité d'information [TIA03]. Logiquement, plus la taille des informations est importante et plus la dégradation apportée à l'image sera visible (cf figure 24). De plus, si le processus de tatouage modifie perceptuellement l'image, il sera plus difficile de retrouver l'image originale et la méthode ne sera plus réversible.

La problématique du choix d'une méthode de tatouage réversible se dégage donc : *il s'agit de faire un compromis entre la taille de la signature, l'imperceptibilité et la réversibilité*.

Ce choix n'est pas à priori évident et dépend beaucoup du type de support que l'on désire marquer. Ainsi, pour les images médicales, la réversibilité sera le facteur déterminant. Il faudra cependant que la taille de la signature ne soit pas trop réduite pour qu'elle puisse contenir les informations nécessaires pour la détection et la localisation des différentes attaques que peut subir l'image lors de sa transmission.

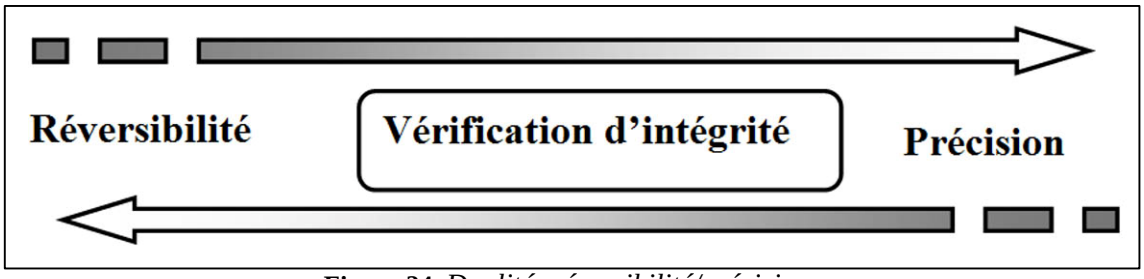


Figure 24. *Dualité: réversibilité/précision*

En effet, plus on insère d'information, plus la réversibilité risque d'être égarée, plus l'image sera dégradée, et plus notre système sera sensible et précis.

Conclusion

Dans ce chapitre nous avons présenté le tatouage réversible ses caractéristiques et son principe général .Nous avons par la suite énuméré l'état de l'art des travaux qui ont été

effectués dans ce contexte ainsi que les limitations que présentent ces techniques déjà étudiées et validées.

En se basant sur les différentes techniques existantes rencontrées ; on a étudié le compromis entre la taille de la signature, l'imperceptibilité et la réversibilité. On a conclu que plus on insère d'information, plus la réversibilité risque d'être égarée, plus l'image sera dégradée, et plus notre système sera sensible et précis.

Section 2

Notre contribution

Chapitre III

Méthode proposée

Introduction

Dans ce chapitre nous commençons par expliquer notre choix pour le domaine de travail, la signature à insérer ainsi que les pixels à tatouer ; pour passer par la suite à décrire les différentes phases de notre technique de tatouage réversible [FOU07].

L'approche développée tient compte des différentes difficultés rencontrées par les schémas existants. Dans ce contexte, nous avons fixé pour objectif la restitution d'un duplicata exact de l'image originale suite à la vérification d'intégrité de l'image transmise tout en assurant une localisation des zones modifiées en cas de falsification.

1. Préambule

La technique proposée consiste à découper l'image que l'on souhaite protéger en blocs de taille 8_x8 pixels et d'insérer dans chacun d'eux, une marque. Afin de vérifier l'intégrité de l'image, on teste la présence de la marque dans les différents blocs.

1.1. Choix du domaine de travail

Dans nos travaux il est intéressant d'utiliser le domaine spatial qui est caractérisé par la redondance spatiale ; lorsque des informations sont similaires ou se répètent dans des zones contiguës de l'image.

En effet, le domaine spatial se base sur la manipulation directe de la luminance des pixels et comme aucun traitement initial n'est requis il possède l'énorme avantage que les opérations d'insertion et de détection de la signature sont peu coûteuses en temps de calcul (ce qui permet le travail en temps réel).

1.2. Choix de la signature

L'idée de base est d'insérer le résultat d'une fonction de hachage dans l'image ; cette dernière doit être sensible à toute modification afin de détecter toute attaque appliquée à l'image tatouée.

Pour assurer une sensibilité par rapport aux différentes modifications que peut subir l'image tatouée ; la fonction de hachage doit résumer les informations de l'image.

La signature insérée est constituée de deux séries binaires : chaque série est le résultat d'une fonction de hachage, elle présente 1024 bits.

Comme il est illustré dans la figure 25, on applique sur chaque ligne (32 blocs de taille 8x8) une première fonction de hachage H_l ; le haché obtenu est présenté sur 32 bits. Chaque bit sera inséré dans un bloc.

La même procédure est appliquée pour chaque colonne (32 blocs de taille 8x8) ; Le haché obtenu à partir de la deuxième fonction de hachage H_c est présenté sur 32 bits. Chaque bit est inséré dans un bloc :

$$H = \frac{1}{\alpha}\sum_{i=1}^{32} M_i \qquad \textbf{(Eq 11)}$$

Avec

$$M_i = \frac{1}{\beta}\sum_{i=1}^{n-n_1}\sum_{j=1}^{n-n_1} P(i,j) \qquad \textbf{(Eq 12)}$$

tel que n : nombre de pixels dans un bloc.

n_1 : nombre de pixels utilisés pour établir le haché.

Donc on aura dans chaque bloc 2 bits b_l et b_c.

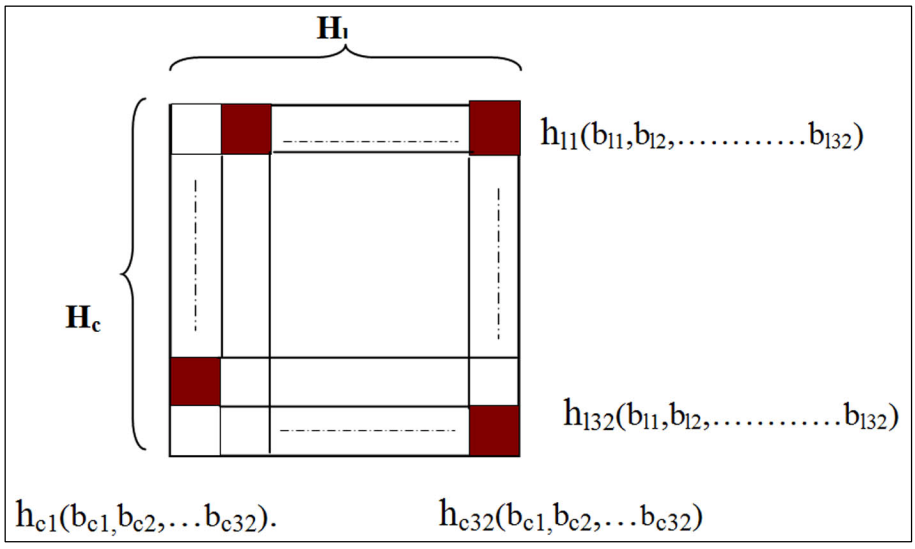


Figure 25. *Principe de la fonction de hachage*

Lors de la détection on extrait pour chaque ligne les 32 bits b_l et on détermine la première signature extraite S_{ln} qui sera comparée avec le haché h_l recalculé. De même, pour chaque colonne on extrait les 32 bits b_c et on détermine la deuxième signature extraite S_{cn} qui sera comparée avec le haché h_c recalculé.

Si $h_{ln} \neq S_{ln}$ et $h_{cn} \neq S_{cn}$ le $n^{ième}$ bloc est falsifié et il apparaît avec une nuance de cyan localisant la modification qu'a subie l'image ; sinon le bloc est intact et il apparaît similaire au bloc de l'image originale.

1.3. Choix des pixels à tatouer

On précise les pixels à tatouer pour chaque bloc à l'aide d'une clé d'insertion K. Cette clé permet aussi bien d'inscrire la marque que de la lire ou de l'enlever. C'est pourquoi elle doit rester secrète.

Dans ce contexte et afin d'assurer plus de sécurité nous avons choisi de déterminer une clé (Figure 26) suivant laquelle on fixe les pixels à tatouer pour chaque bloc de l'image originale.

Figure 26. *Clé d'insertion*

Chaque bloc sera tatoué seul, en effet pour chaque bloc on va choisir à l'aide de la clé K deux paires de pixels voisins.

On peut choisir trois directions pour définir le regroupement des pixels voisins deux à deux : vertical, horizontal et diagonales (Figure 27).

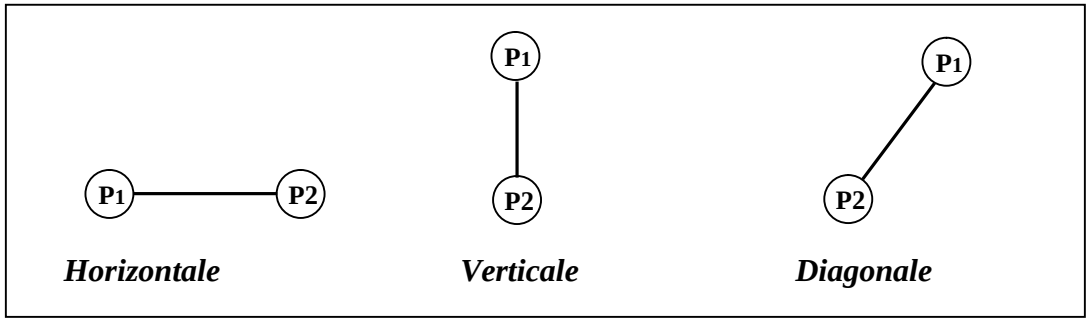


Figure 27. *Regroupements possibles*

Comme tout schéma de tatouage fragile le choix des pixels à tatouer doit tenir compte de la condition que les pixels tatoués (zone d'insertion) sont différents des pixels auxquels on a appliqué la fonction de hachage pour résumer les informations de l'image (voir figure 28).

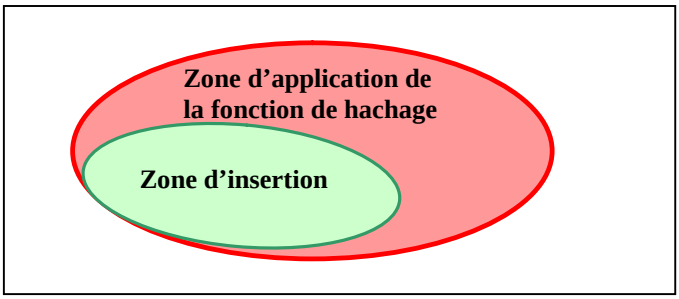


Figure 28. *Principe d'insertion des schémas de tatouage fragile*

1.4. Choix de la taille du bloc de vérification d'intégrité

Plus la taille du bloc est petite plus la localisation de l'anomalie est précise, et pour cela nous avons choisi de travailler avec un bloc de taille 8x8 garantissant une localisation satisfaisante.

2. Méthode proposée

Comme tout schéma de tatouage, l'approche proposée est composée de deux étapes : l'insertion et la détection. Dans ce qui suit, nous détaillons les algorithmes d'insertion et de détection.

2.1. Schéma d'insertion

Cette étape est fondamentale dans le schéma de tatouage, elle consiste à introduire de manière invisible et réversible une information dans une image. Cette information doit disparaître à la moindre manipulation.

Soit I notre image, W la signature à insérer qui dépend généralement d'une clé secrète et I_w l'image tatouée obtenue.

T(I) étant l'espace d'insertion, pour notre approche nous avons choisi le domaine spatial. D'une manière générale la fonction d'insertion se présente sous la forme suivante :

$$I_w = F\,(T\,(I),\, W\,(b_0, b_1, \ldots\ldots, b_n)) \qquad \textbf{(Eq 13)}$$

On précise les composantes de l'image originale dans lesquelles on insère la signature. On applique à l'image une fonction de hachage permettant de prendre des informations sur l'image même :

$$H(I) = W(b_0, b_1, \ldots, b_n) \quad \textbf{(Eq 14)}$$

La signature est insérée dans les composantes sélectionnées de l'image d'une façon réversible.

L'image marquée est enfin reconstruite avec les composantes sélectionnées et modifiées.

Principe de l'insertion

On applique la transformation Walsh Hadamard sans perte WHT (réversible, à exacte reconstruction) introduite dans [JPC97] définie comme suit:

Soit deux entiers x_0 et x_1 ; la WHT de dimension 2x2 est déterminée par:

$$\begin{pmatrix} Z_0 \\ Z_1 \end{pmatrix} = \left[\begin{pmatrix} 1/2 & 1/2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \right] \quad \textbf{(Eq 15)}$$

Soit $P_i$et P'_i deux valeurs d'intensités de pixels telles que $0 \le P_i, P_i^{'} \le 255$

Soit $b_i \in \{0,1\}$

$$\mathbf{F:} \begin{cases} Moy_i = \left\lfloor \dfrac{P_i + P_i^{'}}{2} \right\rfloor & 1 \le i \le n \\ Diff_i = P_i - P_i' \end{cases} \quad \textbf{(Eq 16)}$$

Par suite la différence $Diff_i$ est représentée sous sa forme binaire :

$$Diff_i = d_{i,0} d_{i,1} \ldots\ldots\ldots d_{i,n} \quad \textbf{(Eq 17)}$$

Le bit b_i de la signature est inséré dans la représentation binaire de la différence $Diff_i$.

$$Diff_i^{'} = d_{i,0} d_{i,1} \ldots\ldots\ldots d_{i,n} b_i \quad \textbf{(Eq 18)}$$

Finalement on calcule les nouvelles valeurs des intensités de pixels :

$$P_{1i} = Moy_i + \left\lfloor \frac{Diff_i^{'} + 1}{2} \right\rfloor \quad \textbf{(Eq 19)}$$

$$P_{1i}^{'} = P_{1i} - Diff_i^{'} \quad \textbf{(Eq 20)}$$

2.2. Schéma de détection

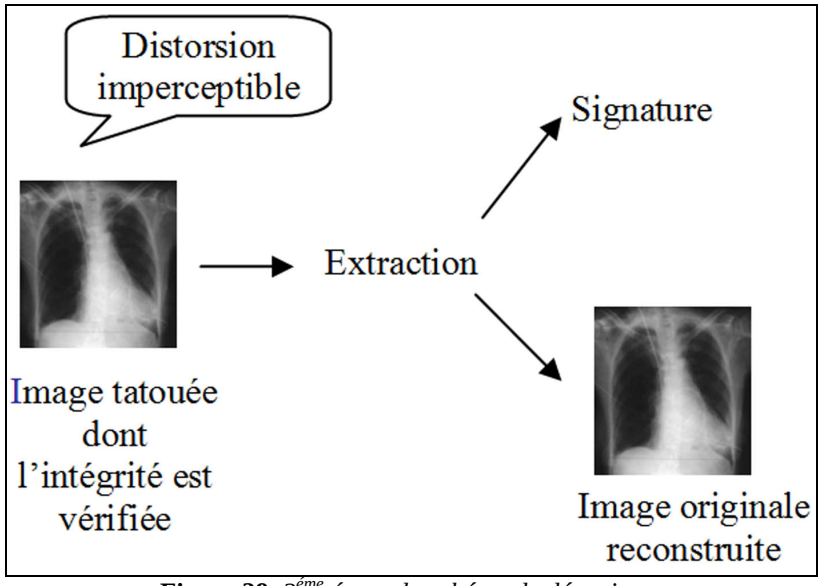


Figure 29. *2éme étape du schéma de détection*

Cette phase se fait suivant deux étapes complémentaires ; la première vise à retrouver la signature insérée dans l'image originale. Elle consiste à inverser le processus de marquage.

La seconde étape est la continuité de la première. Elle permet de comparer la signature extraite (résumé de l'image originale présent dans la marque) à celle insérée (résumé de l'image restaurée) afin de savoir si l'image tatouée présente des altérations ou des transformations. Si les deux signatures coïncident, alors l'image n'a pas été dégradée**.**

Si l'image est falsifiée elle sera rejetée, sa valeur comme base de diagnostic est perdue, sinon cette image est intègre et on passe à la reconstitution de l'image originale qui sera utilisée lors des diagnostics sans aucune peur que l'insertion de la signature n'ait détruit des détails significatifs de l'image médicale (voir figure 29).

L'image restaurée est construite à partir de l'image tatouée en enlevant la marque présente dans les bits de poids faible des valeurs de $Diff_1^{'}$ marquées puis en restaurant les valeurs $Diff_1$ originales et enfin les amplitudes des pixels.

Principe de détection

A partir des deux valeurs P'_{1i} et P_{1i} le récepteur (le détecteur) peut extraire le bit b_i inséré ainsi que les valeurs de P'_i et P_i la paire originale.

$$Moy_{1i} = \left\lfloor \frac{P_{1i} + P_{1i}^{'}}{2} \right\rfloor \qquad \textbf{(Eq 21)}$$

$$Diff_{1i}^{'} = P_{1i} - P_{1i}' \quad \textbf{(Eq 22)}$$

$$Diff_{1i}^{'} = d_{1i,0}d_{1i,1}.....d_{1i,n}b_i \xrightarrow{b_i} \quad \textbf{(Eq 23)}$$

Suite à l'extraction de la signature, on s'assure de l'intégrité de l'image tatouée transmise pour passer par la suite à reconstruire les valeurs des pixels originaux afin de retrouver l'image originale.

$$Diff_{1i} = d_{1i,0}d_{1i,1}.....d_{1i,n} \quad \textbf{(Eq 24)}$$

$$P_i = Moy_{1i} + \left\lfloor \frac{Diff_{1i}+1}{2} \right\rfloor \quad \textbf{(Eq 25)}$$

$$P_i^{'} = P_i - Diff_{1i} \quad \textbf{(Eq 26)}$$

Les valeurs d'intensités des pixels rétablis sont équivalentes aux valeurs d'intensités des pixels originaux. (Voir la démonstration en détail mise en annexe) ce qui prouve la réversibilité de cette méthode.

Dans ce qui suit on présente un exemple de l'insertion et de l'extraction de la signature insérée ainsi que la reconstruction des valeurs des pixels originaux.

2.3. Exemple

Soit P = 198, P' = 170 deux pixels de l'image originale et b = 0 un bit de la signature à insérer.

- **Insertion**

$Moy = \left\lfloor \frac{P+P^{'}}{2} \right\rfloor = \left\lfloor \frac{198+170}{2} \right\rfloor = 184$

$Diff = P - P^{'} = 198 - 170 = 28 = 11100$

$Diff^{'} = 11100$ b $= 111000 = 56$

$P_1 = Moy + \left\lfloor \frac{Diff^{'}+1}{2} \right\rfloor = 184 + \left\lfloor \frac{56+1}{2} \right\rfloor = 212$

$P_1^{'} = P_1 - Diff^{'} = 212 - 56 = 156$

- **Détection**

$$Moy_1 = \left[\frac{P_1 + P_1^{'}}{2} \right] = \left[\frac{212 + 156}{2} \right] = 184$$

$$Diff_1^{'} = P - P^{'} = 212 - 156 = 56 = 111000$$

- **Reconstruction de valeurs originales**

$$Diff_1 = 11100 = 28$$

$$P = Moy_1 + \left[\frac{Diff_1 + 1}{2} \right] = 184 + 14 = 198$$

$$P^{'} = P - Diff_1 = 198 - 28 = 170$$

3. Validation de l'approche développée

Matériel utilisé

L'exécution des différents programmes était effectuée sur un PC Pentium IV® de fréquence 1.5 GHz, de mémoire vive RAM de 256 Mo.

Langage de programmation

L'implémentation logicielle des différents algorithmes présentés dans ce mémoire était développée sous MATLAB 7.0.

On applique cette technique à 30 différentes images médicales de taille 256x256 pixels et de résolution 8 bits/pixel afin d'évaluer la qualité de l'image tatouée, de vérifier la sensibilité de l'approche par rapport aux différentes attaques, la précision de la localisation des zones modifiées et surtout l'aptitude de l'approche à reconstruire l'image originale à partir de l'image tatouée (réversibilité).

3.1. Fragilité par rapport aux attaques

Parmi les problèmes principaux dans le domaine de tatouage, il y a l'absence de références connues pour les tests d'efficacité. Néanmoins, afin de tester l'efficacité de notre approche, nous avons essayé de simuler un ensemble d'attaques possibles que l'image peut subir fréquemment et de vérifier la présence de la signature après chaque opération.

Nous avons choisi de faire subir à l'image tatouée un ensemble d'attaques et de vérifier l'aptitude de notre méthode à localiser l'anomalie introduite dans l'image.

3.*1.1. Image tatouée non attaquée*

Image tatouée non attaquée	
	
Image originale	***Image de vérification d'intégrité***

Figure 30. *Image tatouée non attaquée*

L'image tatouée non attaquée dont l'intégrité est vérifiée apparaît sans aucune partie colorée (Figure 30) ce qui montre et garantit à l'utilisateur que la marque insérée n'a subi aucune modification et par conséquence l'image est intègre.

3.*1.2. Fragilité par rapport à la compression*

La première transformation d'image sur laquelle nous envisageons de tester l'efficacité de notre méthode est la compression JPEG. C'est une transformation largement utilisée puisqu'elle est une norme de compression exploitée pour l'archivage et le stockage des images (par exemple dans le domaine médical les images extraites du DICOM sont au format JPEG). Il est donc nécessaire de vérifier que cette méthode assure une bonne détection des modifications pour les images ayant subi une compression JPEG de 50%.

Compression JPEG 50%	
	
Image tatouée compressée	***Image de vérification d'intégrité***

Figure 31. *Fragilité par rapport à la compression*

Puisque cette norme de compression est avec perte elle soustrait quelques détails de l'image (les hautes fréquences). Et comme la compression altère la totalité de l'image, l'image de vérification d'intégrité apparaît entièrement colorée (voir la figure 31).

3.1.3. Fragilité par rapport au filtrage

Face à la diversité des filtres utilisés dans le domaine de l'imagerie numérique, nous avons jugé qu'il serait impératif de tester la sensibilité de cette méthode par rapport aux filtres les plus utilisés : filtre moyen, filtre médian, filtre gaussien, filtre unsharp.

A. Filtre moyen

La première famille de filtres testés est celle des filtres moyenneurs.

Nous avons testé la méthode étudiée avec des images filtrées par des filtres moyenneurs de taille 3x3.

Filtre moyen 3x3	
	
Image tatouée filtrée	***Image de vérification d'intégrité***

Figure 32. *Fragilité par rapport au filtre moyen*

Les résultats obtenus dans la figure 32 montrent d'une part la sensibilité de cette méthode pour ce type d'attaques et d'autre part le résultat de ce type de filtre qui altère complètement l'image.

B. Filtre médian

La deuxième famille de filtres est celle des filtres médians.

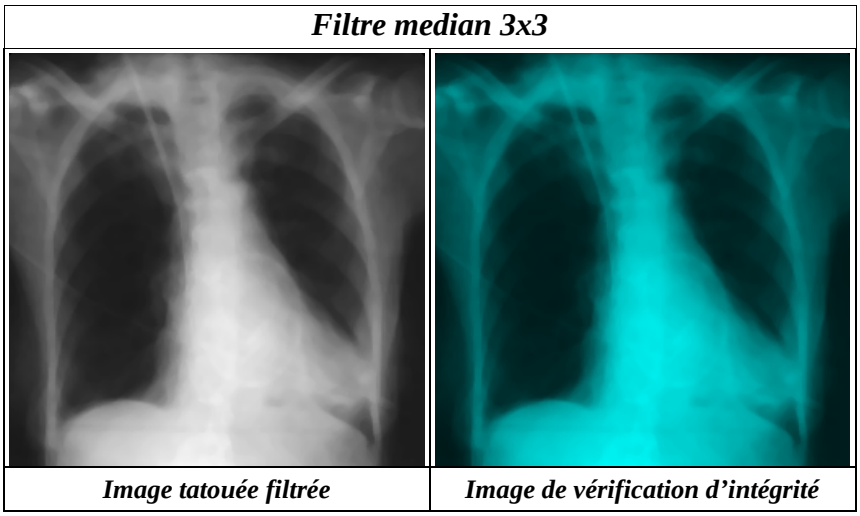


Figure 33. *Fragilité par rapport au filtre médian*

Ce type de filtrage appliqué à l'image est détecté et localisé sur l'image entière comme le précédent (cf figure 33).

C.Filtre Gaussien

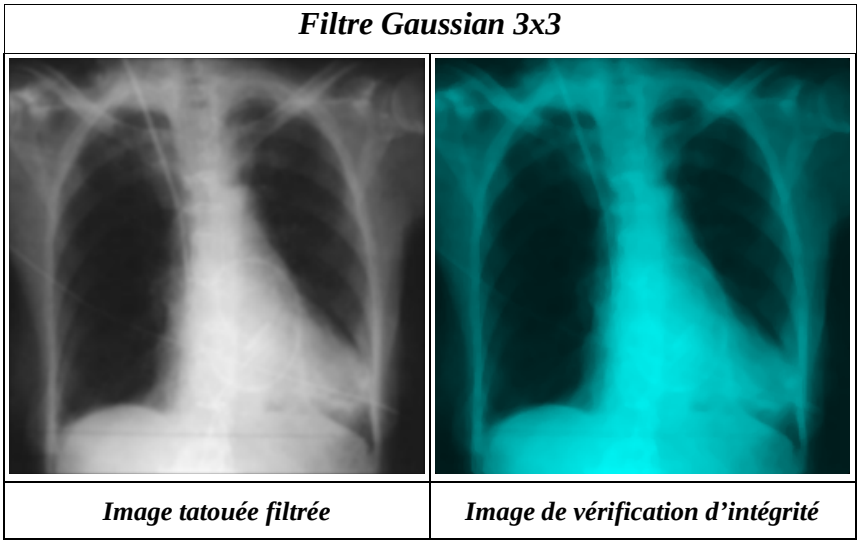


Figure 34. *Fragilité par rapport au filtre gaussien*

Une fois encore le filtrage appliqué à l'image est détecté et localisé sur l'image entière (Figure 34).

D. Filtre unsharp

Le dernier type de filtres utilisé pour évaluer notre approche est le filtre de rehaussement de contraste (le filtre unsharp) avec **α=0.4** (paramètre du filtre). Ce type de filtres met en évidence l'importance des composantes hautes fréquences de l'image.

Filtre unsharp α=0.4	
	
Image tatouée filtrée	***Image de vérification d'intégrité***

Figure 35. *Fragilité par rapport au filtre unsharp*

Une fois encore l'attaque altère la signature déjà insérée, et on remarque à partir de la figure 35 résultante que l'image de vérification d'intégrité est entièrement colorée avertissant l'utilisateur de la mutation de l'image.

3.1.4. Fragilité par rapport à l'égalisation d'histogramme

L'égalisation d'histogramme a pour effet de dilater ou compresser localement l'histogramme (séparer les valeurs d'intensité) pour obtenir une distribution des valeurs qui soit aussi régulière que possible.

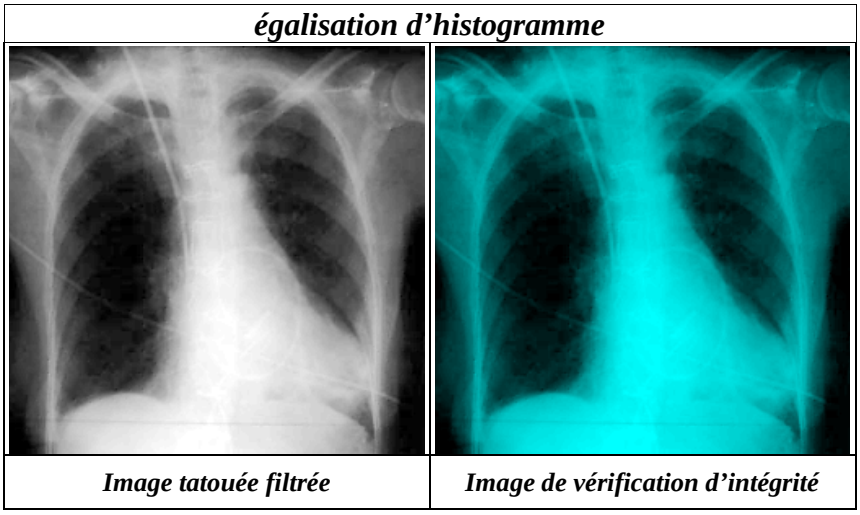


Figure 36. *Fragilité par rapport à l'égalisation d'histogramme*

Le résultat obtenu dans la figure 36 montre bien que l'attaque est détectée et le résultat montre l'altération de l'image complète.

3.1.5. Fragilité par rapport à la rotation

Une simple rotation de l'image même de 1 degré peut engendrer une désynchronisation.

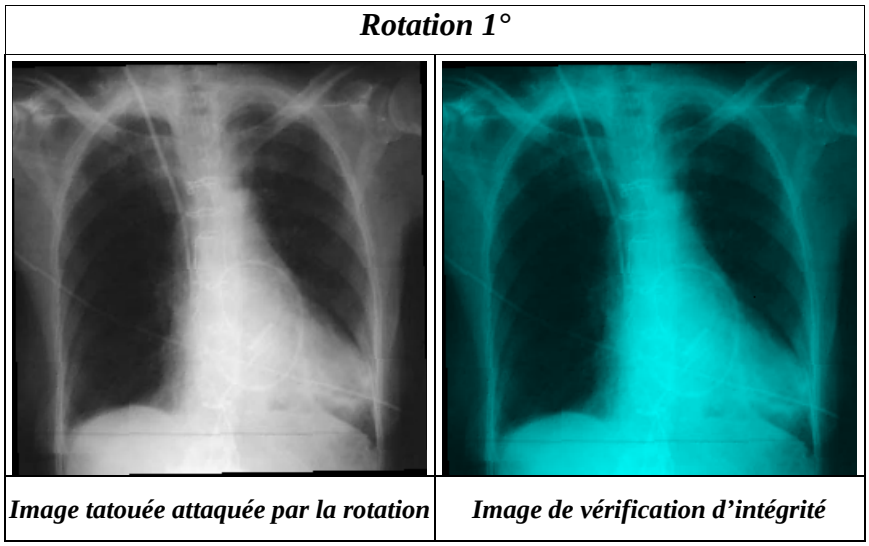


Figure 37. *Fragilité par rapport à la rotation*

La rotation est détectée même pour un angle minime (voir figure 37), le résultat montre l'altération de l'image complète.

3.1.6. Fragilité par rapport à l'ajout de bruit

Le premier bruit simulé est le bruit gaussien de moyenne nulle et de variance 0.02.

A. Bruit gaussien

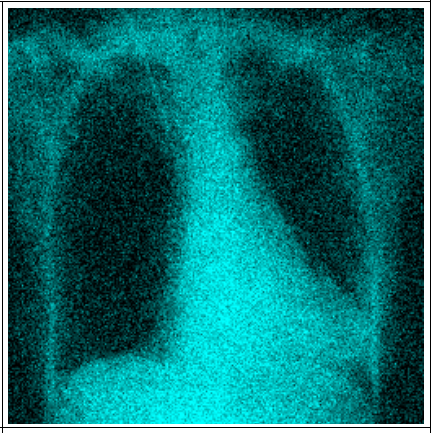
Bruit gaussien 0.02	
	
Image tatouée bruitée	***Image de vérification d'intégrité***

Figure 38. *Fragilité par rapport à l'ajout de bruit gaussien*

Les résultats obtenus dans la figure 38 montrent l'aptitude de cette méthode à détecter le bruit gaussien ajouté à l'image.

B. Bruit Speckle

Bruit Speckle 0.02	

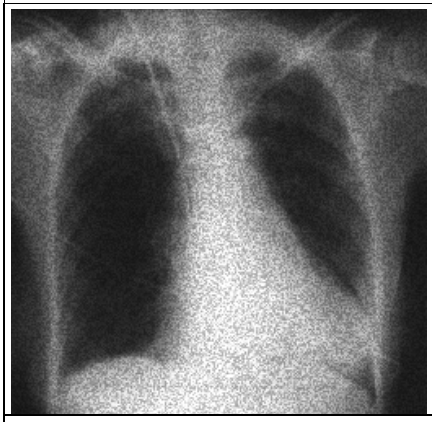
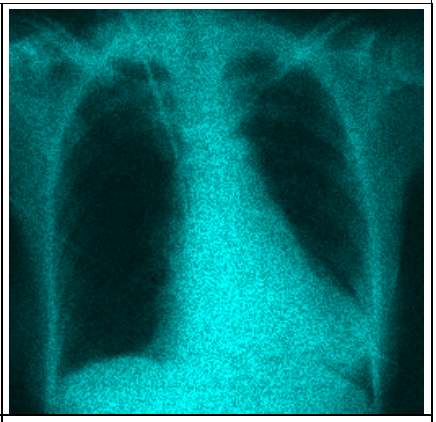

	

Image tatouée bruitée	***Image de vérification d'intégrité***

Figure 39. *Fragilité par rapport à l'ajout de bruit speckle*

Notre approche a également détecté un faible bruit speckle (voir figure 39).

3.1.7. Fragilité par rapport à l'absence de la signature

Le cas d'absence de signature a été aussi évalué. En effet, nous avons essayé de chercher les résultats lorsqu'aucune signature n'est insérée.

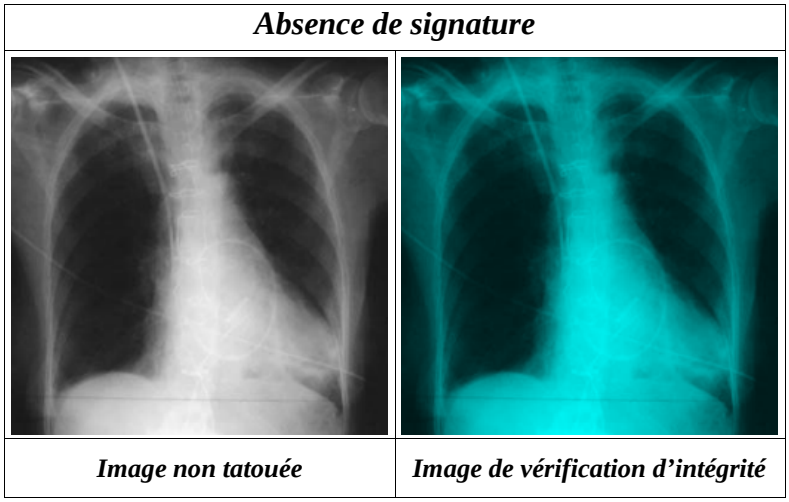


Figure 40. *Fragilité par rapport à l'absence de signature*

Cette image sans tatouage apparaît lors de sa vérification complètement avec une nuance de Cyan (voir figure 40) pour que le récepteur n'ait aucun risque lors de son utilisation.

3.1.8. Fragilité par rapport à la falsification

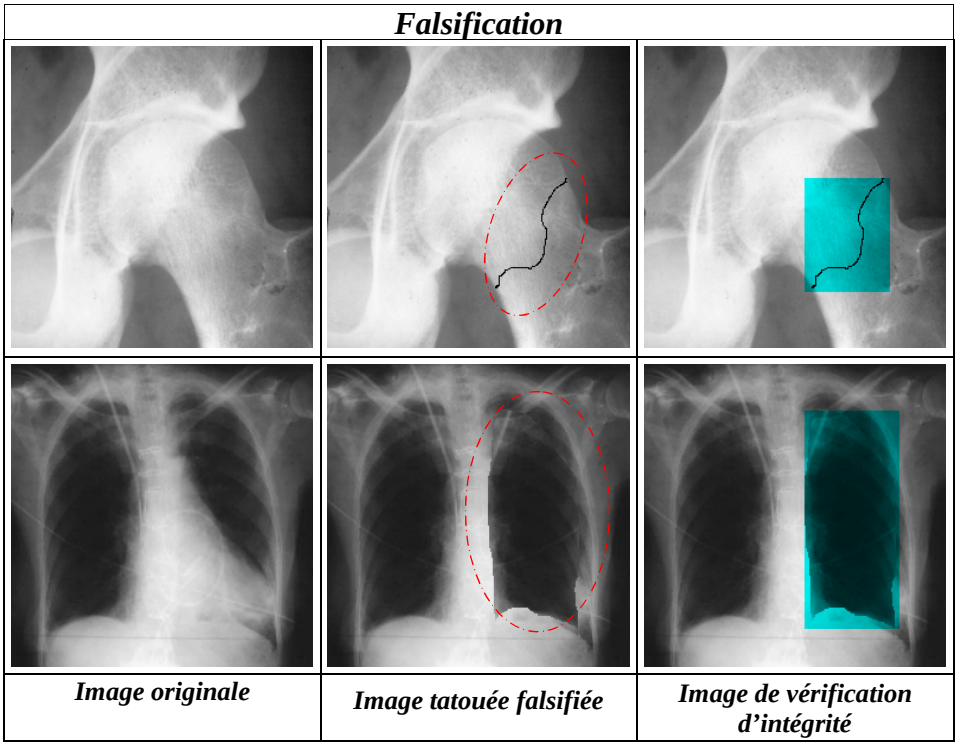


Figure 41. *Fragilité par rapport à la falsification*

Comme nous le montrons sur la figure 41, en cas de falsification, la partie ajoutée se présente bien sur l'image de vérification d'intégrité comme étant une zone colorée en cyan localisant la falsification avec une précision remarquable.

Les résultats obtenus dans la figure 41 prouvent l'efficacité de notre nouvelle approche et son aptitude à détecter et localiser les différentes attaques que peut subir l'image tatouée.

Après avoir présenté les résultats de la vérification de la signature extraite, il est utile de présenter les résultats de ce schéma de manière quantitative. Nous allons pour ceci, présenter le nombre des blocs affectés détectés qui peut nous renseigner sur la sensibilité de la méthode pour chaque type d'attaque.

- **Efficacité de détection**

L'efficacité de détection est définie comme étant :

$$E = \frac{N_{ad}}{N_a} * 100 \qquad \textbf{(Eq 27)}$$

N_{ad} **:** Nombre de blocs affectés détectes.

N_a **:** Nombre de blocs affectés.

On remarque d'après les résultats obtenus que l'on a une efficacité de 100% à la taille du bloc prés (8x8) pour toutes les attaques utilisées.

3.2. Qualité de l'image tatouée

La qualité de l'image joue un rôle majeur pour une meilleure utilisation de l'image médicale**.**

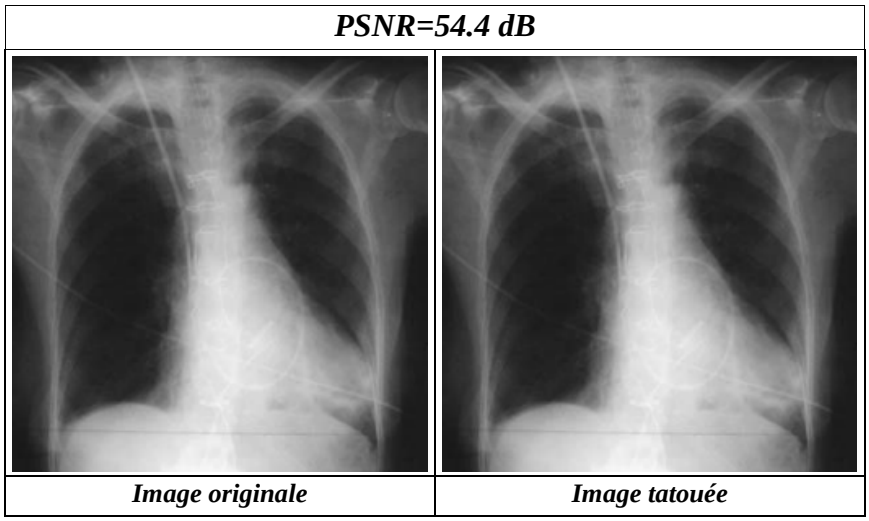


Figure 42. *Image originale et Image tatouée*

Pour les images médicales la signature doit être imperceptible : comme nous l'illustrons dans la figure 42, l'image tatouée devra être globalement similaire à l'image originale pour ne pas dénaturer les radiographies (pour ne pas conduire à un diagnostic erroné).

Dans les techniques de tatouage, la mesure de la perturbation apportée sur l'image lors de l'insertion du message est très importante. La démarche la plus courante est alors d'utiliser une

métrique d'erreur quadratique moyenne (EQM) pour calculer le PSNR - (Peak Signal to Noise Ratio).

- **Le MSE: Medium Square Error**

Le MSE représente l'erreur quadratique moyenne entre l'image étudiée et l'originale afin de permettre d'évaluer l'influence de la variation sur l'image. Il est définit comme suit :

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(I_{ij} - I_{ij}^{*}\right)^2}{nm} \qquad \textbf{(Eq 28)}$$

I et I^* sont respectivement l'image originale et l'image tatouée de taille m_xn avec I_{ij} et I_{ij}^* leurs composantes.

- **Le PSNR : Peak Signal to Noise Ratio**

Le PSNR est une fonction du MSE. Il permet de déterminer la variation qu'a subie l'image, ou en d'autres termes la dégradation de la qualité d'image originale en dB provoquée par l'insertion de la marque, par la compression de l'image ou par tout type d'attaque.

Le PSNR est défini comme suit :

$$PSNR = 10 \log_{10} (255^2/MSE) \qquad \textbf{(Eq 29)}$$

Indépendamment de la technique utilisée, avoir un bon PSNR est une condition importante particulièrement pour des images médicales, où la qualité de l'image joue un rôle majeur pour une meilleure utilisation de l'image**.**

Nous présentons dans ce qui suit les résultats en termes de qualité visuelle PSNR pour les images tests après avoir subi l'opération de tatouage selon l'approche proposée.

Les résultats obtenus dans la figure 43 illustrent l'efficacité de cette approche du point de vue imperceptibilité de la marque.

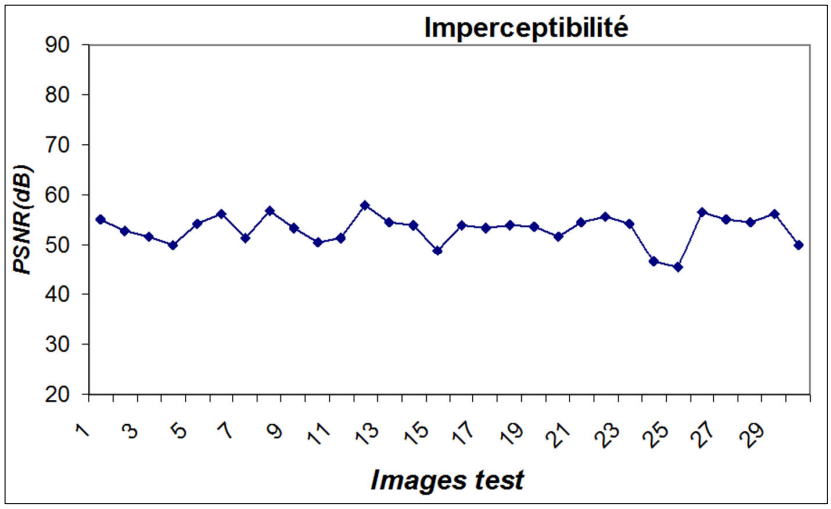


Figure 43. *Les valeurs du PSNR pour les 30 images tatouées*

L'image tatouée devra être globalement similaire à l'image originale pour ne pas dénaturer les images radiographiques.

Il ne faut pas oublier que ces méthodes étant réversibles, la qualité de l'image tatouée est peut-être uniquement intéressante pour une prévisualisation et que le corps médical ne consultera dans un but de diagnostic que l'image originale.

3.3. Détection des fausses alarmes

Les images naturelles présentent une redondance de valeurs de pixels importantes ; par conséquence la différence entre les valeurs de deux pixels voisins est très petite tandis que pour les images qui présentent beaucoup de contours et les images très texturées la valeur de la différence entre la paire de pixels est très importante, d'où le risque que les valeurs de pixels restituées soient hors de l'intervalle [0,255] (voir figure 44) ce qui pose le problème de dépassement.

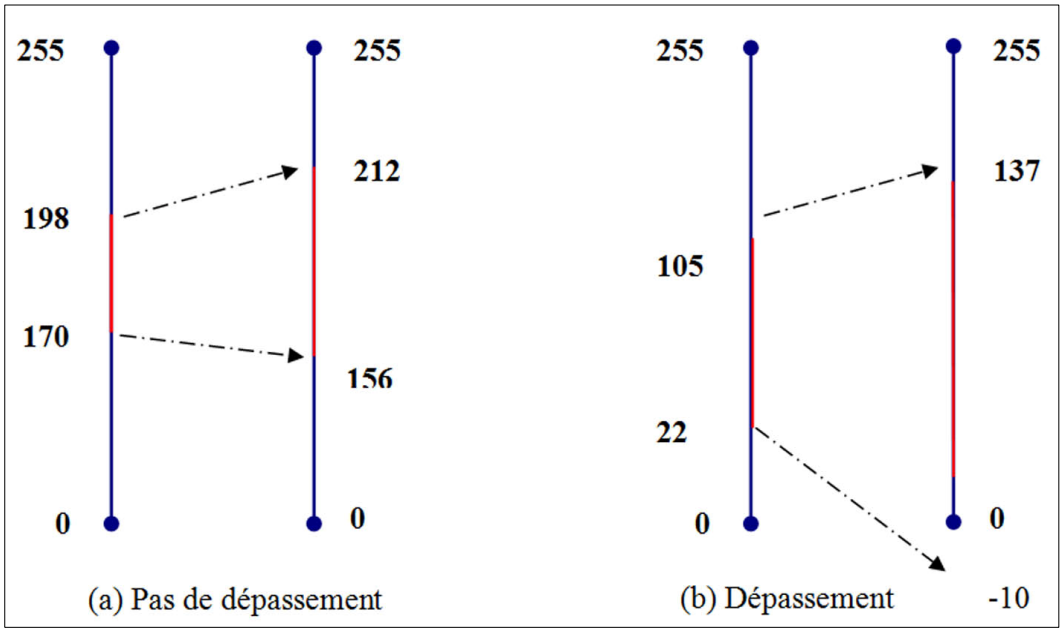


Figure 44. *Problème de dépassement*

Pour les images médicales les contours (francs) sont souvent absents (flous) pour cela le problème de dépassement (‟underflow″ ou ‟overflow″) ne se pose pas fréquemment pour ce type d'image mais parfois il peut exister ce qui engendre la détection de fausses alarmes lors de la phase d'extraction comme nous l'illustrons dans la figure 45.

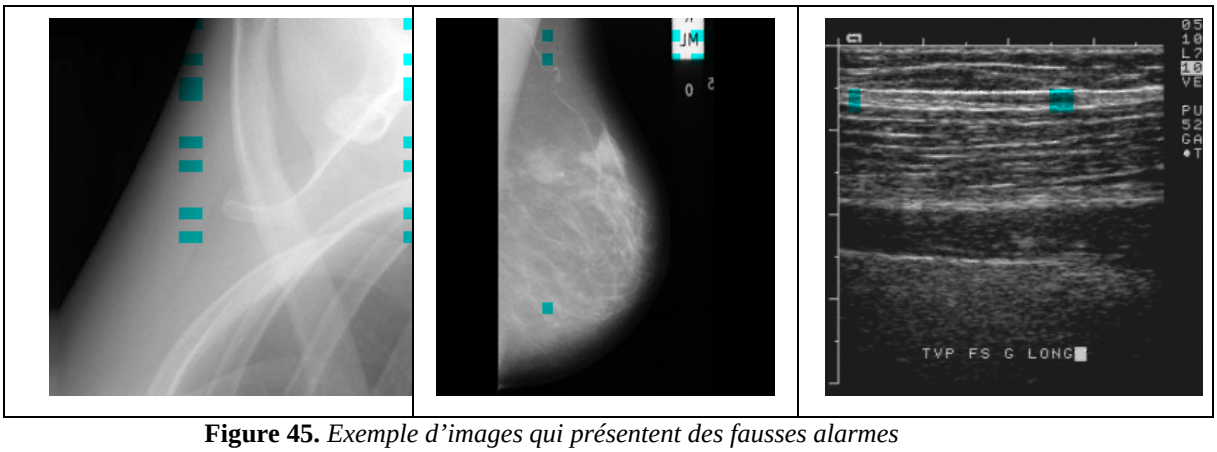


Figure 45. *Exemple d'images qui présentent des fausses alarmes*

Après avoir présenté les résultats de détection de fausses alarmes, nous avons jugé utile de présenter les résultats de ce schéma de manière quantitative. Nous allons pour ceci, présenter le taux de fausses alarmes comme suit :

- **Taux de fausses alarmes**

$$RFA = \frac{Nout}{N} * 100 \qquad \textbf{(Eq 30)}$$

N_{out} : Nombre de blocs affectés hors de la zone falsifiée

N : Nombre de blocs dans l'image

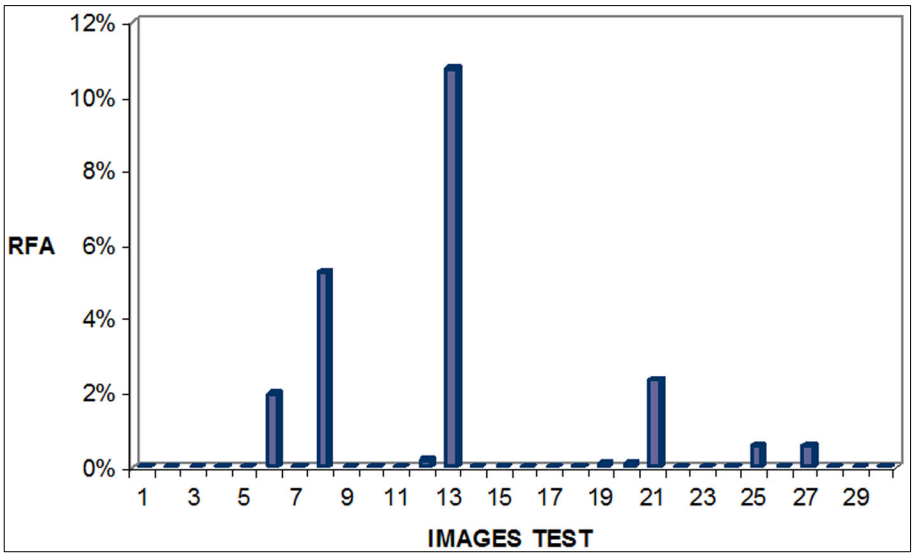


Figure 46. *Les valeurs du RFA pour les 30 images tatouées*

L'histogramme ci-dessus (Figure 46) prouve que le taux de fausses alarmes est pratiquement nul pour la plupart des images tests.

Tous ces résultats mettent en relief l'intérêt de cette approche.

4. Problème de dépassement ("underflow"/"overflow")

Pour les images médicales le flou est un défaut que l'on s'efforce de réduire. Le flou est en fait inévitable et les phénomènes qui le produisent sont nombreux [RAD07].

A titre d'exemple nous pouvons citer :

- Le flou géométrique : Ce flou est lié à la disposition géométrique des éléments concourant à la formation de l'image : taille du foyer, agrandissement, et surtout décalage par rapport au rayon directeur.

De ce fait on peut distinguer trois zones de l'image :

- *L'ombre* : aucun rayon provenant directement du foyer ne touche le film,
- *La lumière* : tout point du récepteur est en vue directe de la totalité du foyer ; l'éclairement est maximum,
- *Le prénombre* : cette zone intermédiaire ne reçoit qu'une partie du rayonnement du foyer ; le passage de l'ombre à la lumière se fait progressivement et la limite entre ces deux zones est indistincte, floue.

- Flou de mouvement : Le malade respire, le cœur bat, les organes digestifs bougent, l'immobilité musculaire ne peut être maîtrisée longtemps.

  C'est le flou le plus préoccupant. L'élément anatomique mobile se déplace à une vitesse parfois importante (vitesse instantanée atteignant 100 à 200 mm/seconde). La longueur parcourue est fonction du temps d'exposition ou temps de pose.

  Sans oublier les mouvements causés par les déficiences mécaniques (vieillissement du matériel, vibrations ...).

Ce flou qui caractérise les images médicales explique l'absence remarquable des contours et des francs bien définis pour ce type d'image. Pour cela le problème de dépassement se pose plus fréquemment pour les images non médicales.

L'absence des contours bien définis explique l'absence des variations brusque pour les intensités des pixels voisins ce qui engendre des petites valeurs de la différence *diff* entre les pixels voisins (porteuse de la signature).

Les différences *diff* et $diff' = 2 \times diff + b$ sont proportionnelles ; de ce fait, plus la différence *diff* est petite plus les valeurs des pixels tatoués sont proches des pixels originaux.

Par conséquences, on aura d'une part moins de problème de dépassement et d'autre part on aura une meilleure qualité de l'image tatouée.

Pour plus de détails nous présentons l'exemple suivant :

Soit P et P' deux pixels voisins et b un bit de la signature à insérer.

On prend le cas idéal ou P = P' et b = 0 ;

$$Moy = \left[\frac{P + P'}{2} \right] = P = P'$$

$$Diff = P - P' = 0$$

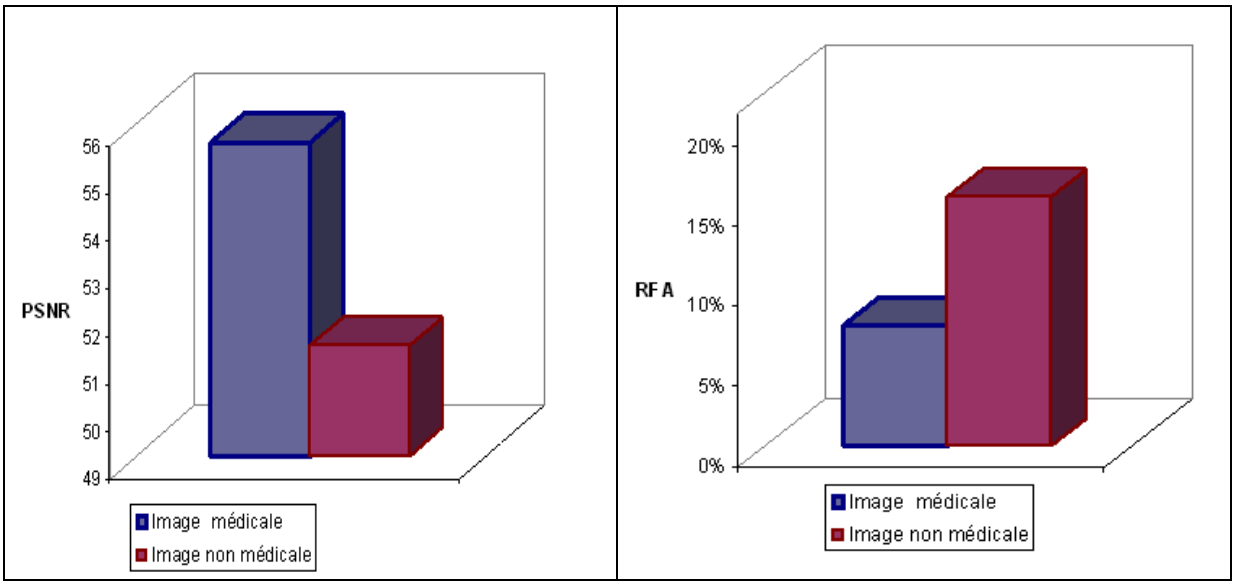
$$Diff^{'} = 2 * Diff + b = 0$$

$$P_1 = Moy + \left[\frac{Diff^{'} + 1}{2} \right] = P$$

$$P_1^{'} = P_1 - Diff^{'} = P'$$

Afin d'éclairer ce concept on applique notre approche à 30 images médicales différentes et à 30 images non médicales différentes de taille 256x256 pixels et de résolution 8 bits/pixel.

Par la suite, on compare les résultats obtenus du point de vue qualité de l'image tatouée et fausses alarmes détectées (problème de dépassement).



(a)Qualité d'image tatouée | ***(b) Taux des fausses alarmes***

Figure 47. *Les valeurs moyennes du PSNR et du RFA pour 30 images médicales et 30 images non médicales.*

La figure 47(a) montre que la qualité de l'image tatouée pour les images médicales est supérieure à celle des images non médicales.

La figure 47(b) montre que le taux de fausses alarmes obtenues pour les images médicales est remarquablement inférieur à celui obtenu pour les images non médicales.

Ainsi, on a obtenu pour les images médicales une qualité d'image tatouée meilleure et un taux de fausses alarmes infime (inférieure à 0.2%).

5. Optimisation de l'approche proposée

Nous allons présentons dans ce qui suit les améliorations que nous avons proposées afin de minimiser le taux des fausses alarmes.

Amadasum [AMA89] a mis en évidence des critères fondés sur l'étude des niveaux de gris d'une image qui sont utilisés par les radiologues lors de l'interprétation. Chacun de ces

critères permet plus ou moins caractériser la répartition des niveaux de gris d'une image médicale.

Les images médicales sont caractérisées par une texture grossière qui possède des primitives larges. Il existe alors peu de variations entre l'intensité d'un pixel et celle de ses pixels voisins. De ce fait le principe de l'algorithme amélioré se base sur la différence d'amplitude entre un pixel et sa valeur prédite grâce à son voisinage. En effet, en vertu de la corrélation spatiale d'une image, il est possible de prédire la valeur de l'amplitude du point courant par la seule connaissance de son voisinage.

5.1. Notion de connexité

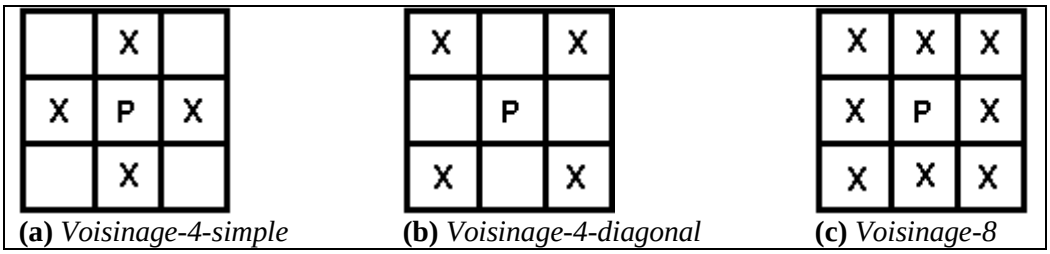
Deux pixels dans l'image sont "connexes" s'il existe au moins une suite de pixels qui les joint, et tel que deux pixels consécutifs de la suite satisfont à la condition de "connexité immédiate". La connexité immédiate entre deux pixels traduit le fait que ces pixels partagent des caractéristiques communes et qu'ils sont "voisins". Elle est conditionnée par la définition du "voisinage" d'un pixel. On distingue classiquement trois types de connexités : le voisinage-4-simple, voisinage-4-diagonal, et voisinage-8 [CHA00].

La distance métrique utilisée est la distance Euclidienne définie entre deux pixels $p(i_p,j_p)$ et $q(i_q,j_q)$ par :

$$d_E(p,q) = [(i_p - i_q)^2 + (j_p - j_q)^2]^{1/2} \qquad \textbf{(Eq 31)}$$

- Le voisinage-4 est défini par: $v4(p) = \{q \in I, d(p,q) \leq 1\}$
  - Connexité simple : Le "voisinage-4-simple" d'un pixel est défini comme l'ensemble des pixels qui l'entourent et qui ne se trouvent pas sur une des deux diagonales passant par ce pixel. Ce voisinage est représenté sur la figure 48(a). Le point p possède 4 voisins adjacents non diagonaux situés à une distance d = 1.
  - Connexité diagonale : Le "voisinage-4 diagonal" est défini à partir de la connexité diagonale entre les pixels. Ce voisinage est représenté sur la figure 48(b). Le point p possède 4 voisins adjacents diagonaux situés à une distance d = $\sqrt{2}$.
- Le voisinage-8 est défini par : $v8(p) = \{q \in I, d(p,q) \leq \sqrt{2}\}$

Le voisinage-8 connexe d'un pixel est défini comme l'union des deux types de voisinage-4. Il est défini comme l'ensemble de tous les pixels qui l'entourent (situés à une distance $d \leq \sqrt{2}$). Ce voisinage est représenté sur la figure48(c) .



(a) *Voisinage-4-simple* **(b)** *Voisinage-4-diagonal* **(c)** *Voisinage-8*

Figure 48*. Les différents types de voisinage.*

5.2. Principe d'insertion

Soit P_i la valeur d'intensité du pixel et $\hat{P}_i$ tel que $0 \leq P_i,\ \hat{P}_i \leq 255$

Soit $b_i \in \{0,1\}$

Soit $\hat{P}_i$ la valeur prédite du pixel.

$$Diff_i = P_i - \hat{P}_i \qquad \textbf{(Eq 32)}$$

Ensuite la différence $Diff_i$ est représentée sous sa forme binaire.

$$Diff_i = d_{i,0}d_{i,1}.....d_{i,n} \qquad \textbf{(Eq 33)}$$

Le bit b_i de la signature est inséré dans la représentation binaire de la différence $Diff_i$.

$$Diff_i^{'} = d_{i,0}d_{i,1}.....d_{i,n}b_i \qquad \textbf{(Eq 34)}$$

Finalement on calcule la nouvelle valeur d'intensité de pixel :

$$P_{1i} = \hat{P}_i + Diff_1^{'} \qquad \textbf{(Eq 35)}$$

5.3. Principe de détection

A partir de la valeur du P_{1i} le récepteur (le détecteur) peut extraire le bit b_i inséré ainsi que la valeur de P_i la valeur originale.

$\hat{P}_{1i}$ est la valeur prédite du pixel.

$$Diff_{1i} = P_{1i} - \hat{P}_i \qquad \textbf{(Eq 36)}$$

$$Diff_{1i}^{'} = d_{1i,0}d_{1i,1}.....d_{1i,n}b_i \longrightarrow b_i \qquad \textbf{(Eq 37)}$$

Suite à l'extraction de la signature, on s'assure de l'intégrité de l'image tatouée transmise pour passer ensuite à la reconstruction de la valeur du pixel original afin de retrouver l'image originale.

$$Diff_{1i} = d_{1i,0}d_{1i,1}.....d_{1i,n} \quad \textbf{(Eq 38)}$$

$$P_{1i}^{'} = \hat{P}_i + Diff_{1i} \quad \textbf{(Eq 39)}$$

Nous avons testé différents modèles de prédiction afin de trouver la technique optimale dans notre cas (pour notre objectif). En effet nous appliquons le modèle linéaire, linéaire avec pondération et le modèle non linéaire.

6. Les modèles de prédiction

6.1. Modèles linéaires

Ce modèle effectue une prédiction à base d'une combinaison linéaire des valeurs des pixels voisins.

La valeur prédite du pixel est définie comme étant :

$$\hat{P}_i = \frac{\sum\sum P_i}{8} \quad \textbf{(Eq 40)}$$

6.2. Modèles linéaires avec pondération

Création du masque

En définissant les poids à accorder à chaque pixel voisin, il se forme un masque propre au voisinage d'ordre 8. Ce masque (Figure 49) sera utilisé afin de calculer la valeur prédite du pixel central P.

1	2	1
2	**P**	2
1	2	1

Figure 49. *Masque de voisinage d'ordre 8*

La valeur prédite du pixel est définie comme étant :

$$\hat{P}_i = \frac{\sum\sum \alpha_i P_i}{\sum \alpha_i} \quad \textbf{(Eq 41)}$$

6.3. Modèles non linéaires

Le prédicteur médian MED, prédicteur non linéaire utilisé dans le standard de compression LOCO-I [WSS96] est défini comme suit :

$$\hat{P} = \begin{cases} \min(a, b) & \text{si } c \geq \max(a, b) \\ \max(a, b) & \text{si } c \leq \min(a, b) \\ a + b - c & \text{sinon} \end{cases} \qquad \textbf{(Eq 42)}$$

Ainsi, la valeur prédite correspond à la valeur médiane des sorties des prédicteurs a, b, a+b- c.

Nous testons ensuite l'efficacité des trois modèles de prédiction présentés ci-dessus. En effet on applique ces trois modèles pour les 30 images tests.

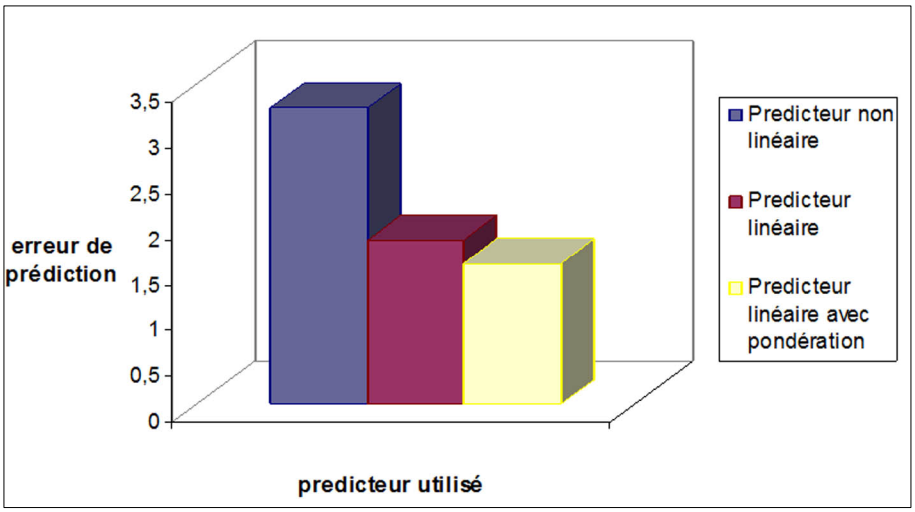


Figure 50. *Erreur de prédiction*

L'histogramme ci-dessus (Figure 50) prouve que le prédicteur linéaire avec pondération est le prédicteur qui a donné l'erreur de prédiction minimale (différence entre l'intensité du pixel et sa valeur prédite) donc ce modèle de prédiction est le modèle optimal pour notre objectif.
Nous avons donc choisi d'utiliser ce type de prédicteur pour le calcul de la valeur du pixel prédite utilisée dans notre algorithme.
L'étape suivante concerne l'évaluation de l'amélioration proposée et la mise en œuvre de son efficacité.

7. Comparaison

Notons qu'au niveau des performances, l'amélioration présentée a gardé l'efficacité de détection assurée par la méthode proposée dans (4.1)

7.1. Qualité de l'image tatouée

Nous présentons par la suite les variations du PSNR des différentes images tatouées.

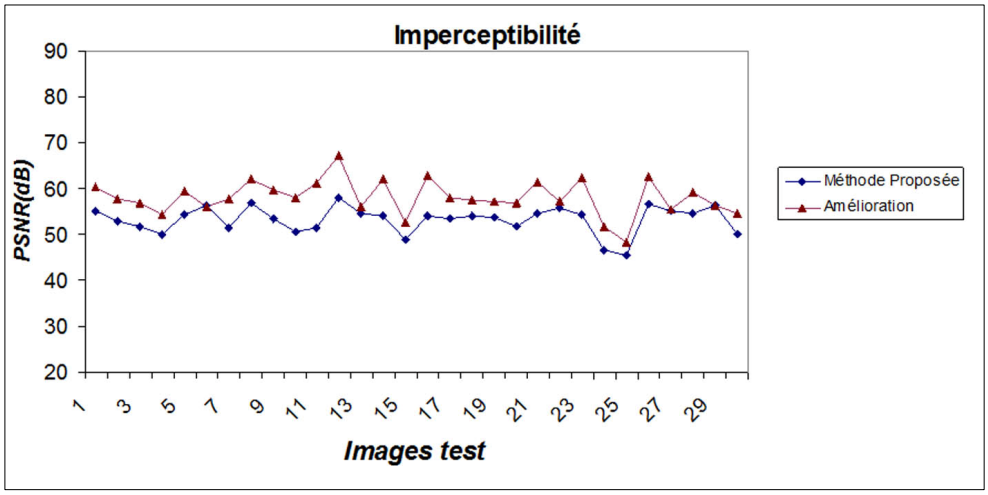


Figure 51. *Qualité visuelle des images tests pour les deux méthodes étudiées*

Avec la figure ci-dessus (figure51), il est possible d'évaluer les méthodes étudiées d'une manière plus précise. Les résultats trouvés montrent que la qualité visuelle de l'image obtenue par l'algorithme de la méthode proposée est améliorée en tenant compte d'un voisinage de pixel plus important.

Pour la méthode proposée, l'image tatouée présente deux valeurs de luminance de pixels modifiées pour chaque bloc ; ces deux valeurs de luminances de pixels sont calculées à partir de la nouvelle valeur de différence ***Diff'*** où on a inséré la signature.

Donc la variation qu'a subie l'image suite à cette opération de tatouage est plus importante que celle pour l'amélioration proposée qui modifie la valeur de la luminance d'un seul pixel par bloc (de taille 8x8).

7.3. Détection des fausses alarmes

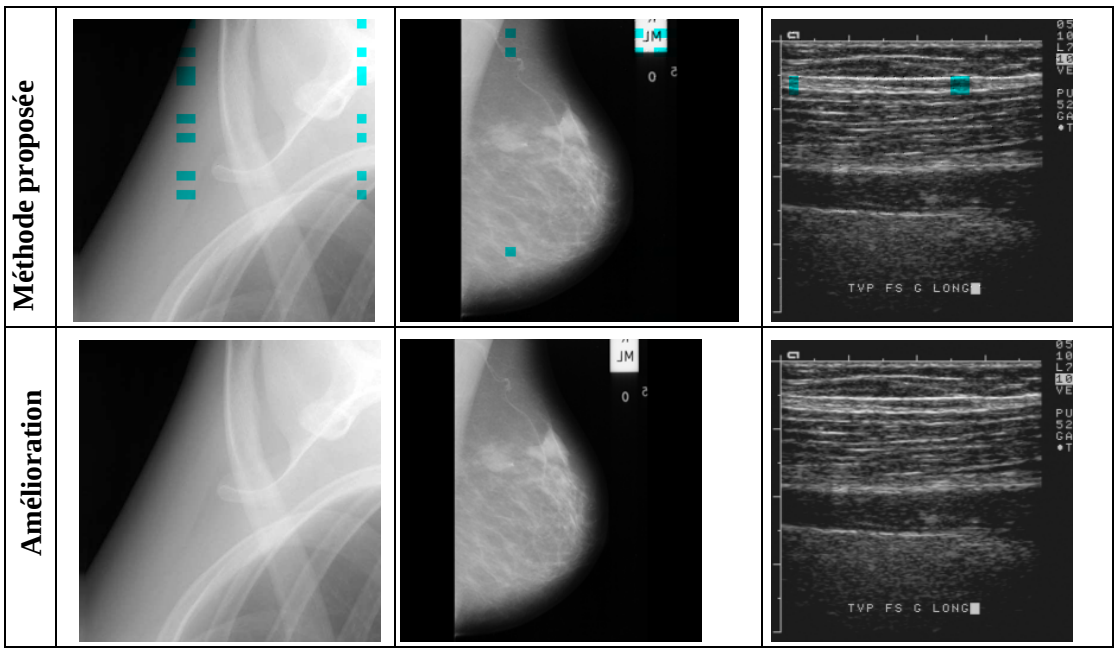


Figure 52. *Elimination des fausses alarmes*

La figure 52 illustre que l'amélioration proposée a assuré la minimisation des fausses alarmes qui se présentent pour certaines images tatouées non attaquées.

Après avoir présenté les résultats des fausses alarmes éliminées, nous présentons les résultats d'une manière quantitative. Nous allons pour ceci, présenter l'histogramme ci-dessous (Figure 53).

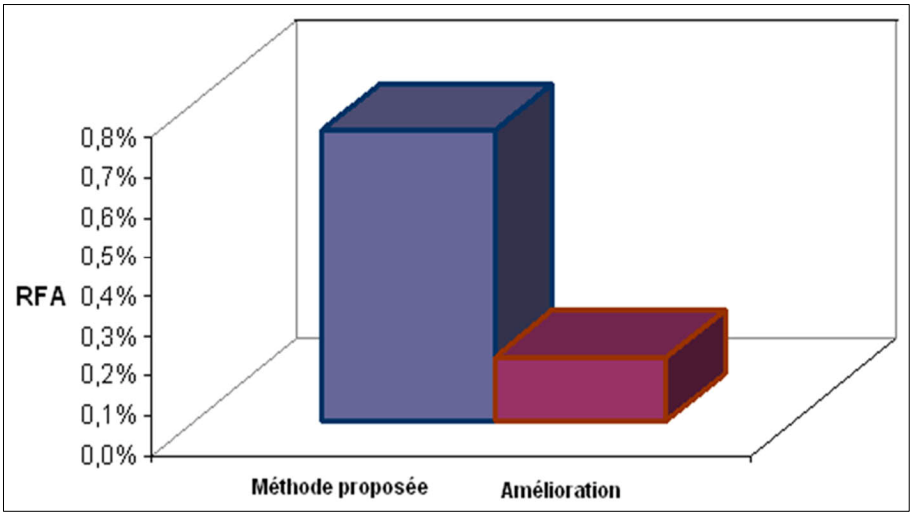


Figure 53. *Diminution du taux des fausses alarmes*

Le taux de fausses alarmes *RFA* obtenu par l'algorithme présenté peut-être amélioré en modifiant le calcul des valeurs de la différence *Diff* (Equation 36). En effet en tenant compte d'un voisinage de pixel plus important la valeur de la différence *Diff* diminue et donc le *RFA* diminue.

L'étude comparative que nous avons effectuée a conclu à l'efficacité de l'amélioration que nous avons proposée.

8. Evaluation de l'approche proposée

Dans cette partie, nous comparons notre méthode par rapport à 5 méthodes de tatouage réversible [CEL03] afin d'évaluer ses performances.

Pour évaluer l'efficacité d'une technique de tatouage réversible, il faut étudier les critères suivants :

- La localisation des zones altérées,
- La capacité d'insertion,
- La qualité de l'image tatouée.

8.1. Localisation des zones altérées

Une aptitude de localisation des zones modifiées est importante pour le schéma de tatouage réversible. Néanmoins, suite à notre étude bibliographique, nous nous sommes aperçus que notre approche et celle de Celik [CEL03] sont les seules méthodes capables de localiser les falsifications que peut subir l'image.

De ce fait nous commençons par comparer notre approche avec la méthode de Celik.

Tableau 2. *Moyenne des résultats pour notre approche et l'approche de Celik*

Méthode étudiée	**PSNR (dB)**	**Capacité d'insertion (b/p)**
Celik	52.09	0.0078
Notre approche	55.18	0.031

D'après les résultats présentés dans le tableau 2 on peut facilement constater que notre approche a assuré une meilleure qualité de l'image tatouée et elle a inséré plus d'informations

assurant ainsi une précision et une sensibilité pour la détection des différentes attaques que peut subir l'image lors de sa transmission.

Nous étudions le deuxième critère pour l'évaluation des techniques de tatouage réversible.

8.2. Capacité d'insertion

Pour comparer les méthodes étudiées, on a réglé les algorithmes afin de garantir le même PSNR.

- **PSNR ≈ 53 dB**

Dans le tableau ci-dessous nous présentons la capacité d'insertion pour les 6 méthodes étudiées.

Tableau 3. *Capacité d'insertion*

Méthode étudiée	Capacité d'insertion (b/p)
Tian	0.061
Chang	0.016
Fridirich (2)	0.025
Fridirich (1)	0.019
Celik	0.0078
Notre approche	0.031

L'ensemble de ces résultats est présenté par l'histogramme ci- dessous:

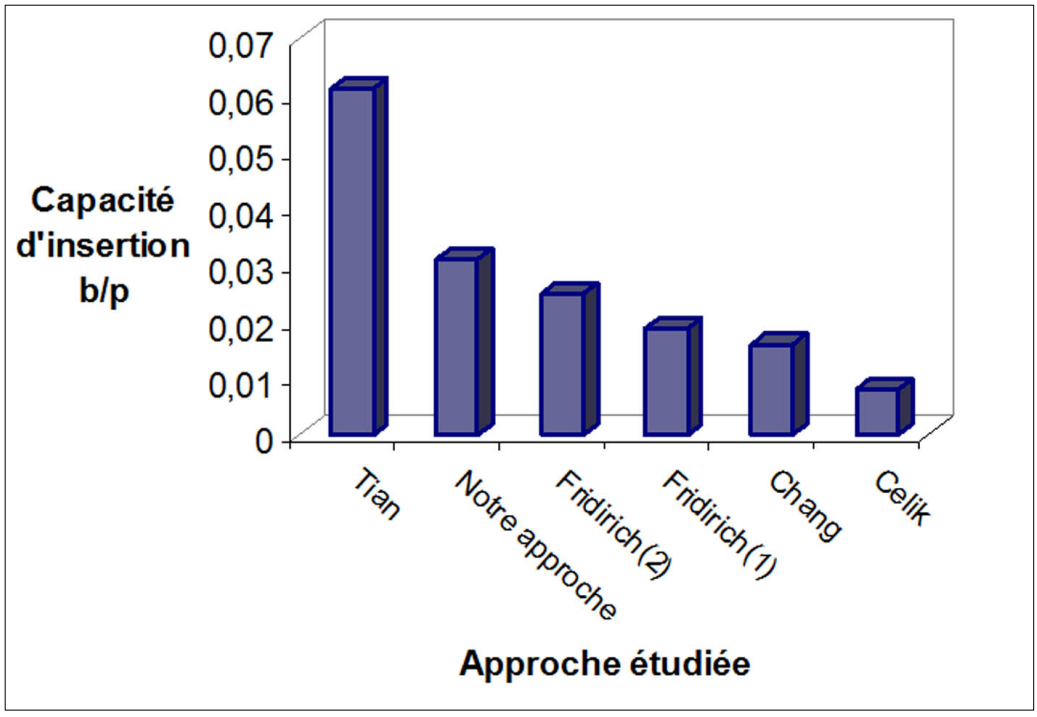


Figure 54. *Capacité d'insertion pour les différentes méthodes*

La figure 54 montre que notre approche a une capacité d'insertion importante par rapport aux différentes méthodes étudiées.
La méthode de Tian possède une capacité d'insertion plus importante que la capacité d'insertion de notre approche pour la moyenne des 60 images tests étudiées (30 images médicales et 30 images non médicales).

Mais il ne faut pas oublier que la capacité d'insertion de la méthode de Tian varie d'une image à une autre ; en conséquence la sensibilité de la méthode varie d'une image à une autre et dans le cas d'une image très motivée image (qui présente beaucoup de contours : passage brusque de couleur) la capacité d'insertion sera minime et on risque dans ce cas de transmettre une image non signée.
En effet, la probabilité d'avoir une grande différence entre deux pixels voisins augmente donc la probabilité d'avoir un dépassement augmente (pour la méthode de Tian : s'il y a un dépassement, on n'insère pas les bits de la signature).

8.3. Qualité de l'image tatouée

Pour comparer la qualité de l'image tatouée des méthodes étudiées on a réglé les algorithmes afin de garantir la même capacité d'insertion.
On effectue les mesures de la qualité de l'image tatouée par calcul de PSNR.

- **Capacité d'insertion ≈ 0.031 b/p**

Dans le tableau ci-dessous nous présentons le PSNR pour les 6 méthodes étudiées.

Tableau 4. *Les valeurs du PSNR pour les 6 méthodes étudiées*

Méthode étudiée	PSNR (dB)
Tian	54.24
Chang	56.03
Fridirich (2)	50.09
Fridirich (1)	53.12
Celik	50.17
Notre approche	55.18

L'ensemble de ces résultats est présenté par l'histogramme ci-dessous :

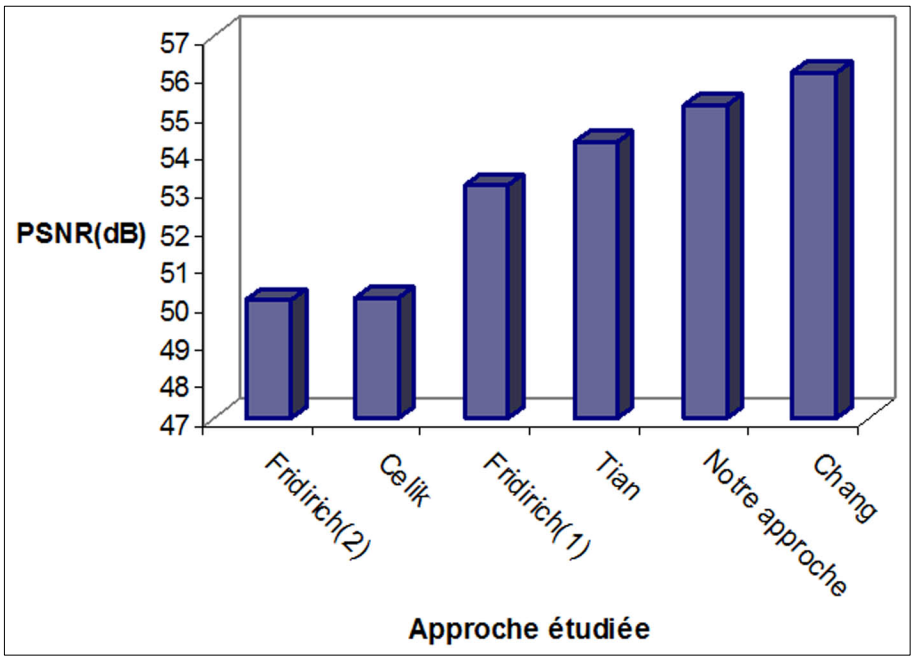


Figure 55. *Les valeurs de PSNR pour les différentes méthodes*

La figure 55 montre que toutes les valeurs de PSNR obtenues sont supérieures à 50dB ce qui garantit une bonne qualité de l'image tatouée pour toute les techniques étudiées.

Il ne faut pas oublier que ces méthodes étant réversibles, la qualité de l'image tatouée est peut-être uniquement intéressante pour sa prévisualisation. Pour un diagnostic, le médecin consultera l'image originale.

L'importance de notre méthode apparaît notamment en la comparant avec les cinq méthodes de tatouage réversible les plus récentes, connues et efficaces.

Pour comparer l'efficacité des différentes méthodes étudiées, il faut tenir compte des trois critères étudiés.

Il est remarquable que les cinq méthodes n'aient pas réussi à assurer une capacité d'insertion importante, fixe pour toutes les images tout en gardant la réversibilité de la méthode et la sensibilité par rapport aux différentes attaques.

Quand à notre méthode, elle a assuré une capacité d'insertion fixe, suffisante pour garantir une sensibilité remarquable aux différentes attaques que peut subir l'image et une localisation assez précise tout en gardant la réversibilité de la méthode.

Conclusion

Dans ce chapitre, nous avons présenté la méthode que nous proposons dans le domaine spatial. Ensuite nous avons essayé d'évaluer cette technique. Nos évaluations étaient menées sur trois volets : la sensibilité par rapport aux attaques, la qualité visuelle des images et la réversibilité.

Nous avons par la suite proposé une amélioration du schéma antérieurement présenté. Cette amélioration utilise la différence d'amplitude entre un pixel et sa valeur prédite grâce à son voisinage pour y insérer la signature. Les résultats présentés illustrent l'efficacité de l'amélioration que nous avons apportée.

Enfin, nous avons terminé par une comparaison et une évaluation de notre méthode optimisée et cinq autres techniques de tatouage réversible pour mettre en relief le développement de notre approche.

Chapitre IV

Méthode proposée pour répondre au problème de dépassement

Introduction

Dans ce chapitre nous présentons, en nous basant sur les caractéristiques des images médicales, une méthode de tatouage réversible qui permet de contourner le problème de dépassement.

La méthode de tatouage que nous proposons s'appuie sur l'approche présentée dans le chapitre précédent.

1. Préambule

Lors de l'insertion de la signature, la nouvelle valeur de l'intensité du pixel (le pixel tatoué) risque d'être très grande de telle manière qu'elle soit hors l'intervalle [0..255] (problème de dépassement) ce qui engendre des faux positifs lors de la vérification d'intégrité.

Afin de résoudre cette problématique nous avons opté pour l'ajout d'un bord virtuel à l'image par effet miroir. Les différentes valeurs de dépassement seront insérées dans les pixels du nouveau bord (voir figure 56).

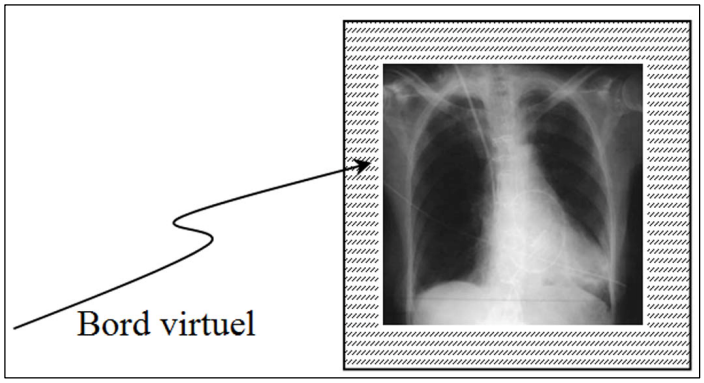


Figure 56. *Ajout du bord virtuel*

Lors de la réception, on effectue l'opération inverse. Il s'agit donc d'extraire les informations insérées dans le bord de l'image puis de supprimer ce bord afin de récupérer l'image originale Ce procédé augmente la taille de l'image tatouée ce qui pose des difficultés au niveau de la transmission de l'image.

En se basant sur les caractéristiques des images médicales [RAD07] on peut utiliser la bordure afin d'insérer les valeurs de dépassement.
En effet, les images médicales sont particulièrement caractérisées par :

- **Le centrage** : l'image utile doit se trouver au centre du cliché,
- **La netteté** : l'image doit être la plus nette possible, et présenter le minimum de flou.

Pour les images médicales, le flou est un défaut que l'on s'efforce de réduire. Le flou est en fait inévitable et les phénomènes qui le produisent sont nombreux. (cette caractéristique est déjà détaillée dans le chapitre précèdent).
Ainsi, l'image médicale utile doit se trouver au centre du cliché et les bords de l'image médicale sont peu importants : le flou qui les caractérise (cette partie de l'image ne reçoit pas directement les rayonnements).
Donc on peut conclure que les bords de l'image médicale ne présentent pas des informations importantes dans le cadre du diagnostic.

2. Méthode proposée

La méthode de tatouage réversible pour les images médicales que nous proposons s'appuie sur l'approche présentée dans le chapitre précédent.
Le principe général est le même et consiste à insérer un résumé de l'image (le résultat d'une fonction de hachage appliquée à l'image originale) dans les blocs 8x8 de l'image même d'une façon réversible.
La modification apportée à l'approche développée précédemment, pour qu'elle contourne le problème de dépassement, consiste essentiellement à utiliser les bords de l'image médicale pour insérer les valeurs de dépassement.

2.1. Schéma d'insertion

Le principe de l'insertion présenté dans la figure 57 est le suivant :

Soit P_i la valeur d'intensité du pixel et $\hat{P}_i$ la valeur prédite du pixel.

Soit $b_i \in \{0,1\}$

$$Diff_i = P_i - \hat{P}_i$$

Dans la suite la différence $Diff_i$ est représentée sous sa forme binaire.

$$Diff_i = d_{i,0}d_{i,1}.....d_{i,n}$$

Le bit b_i de la signature est inséré dans la représentation binaire de la différence $Diff_i$.

$$Diff_i^{'} = d_{i,0}d_{i,1}.....d_{i,n}b_i$$

Finalement on calcule la nouvelle valeur d'intensité de pixel:

$$P_{1i} = \hat{P}_i + Diff_1^{'}$$

Suivant la nouvelle valeur d'intensité de pixel (la valeur de l'intensité du pixel tatoué) on va attribuer à chaque pixel porteur de la signature deux valeurs permettant d'indiquer l'existence, le signe et la valeur du dépassement.

En effet :

Soit α : La valeur du dépassement,

β : Le signe de la valeur du dépassement,

- si $0 \le P_{1i} \le 255$ pas de dépassement, $\alpha = 0; \beta = 0$,
- si $P_{1i} \ge 255$, $\alpha = P_{1i} - 255; \beta = 0$,
- si $P_{1i} \le 0$, $\alpha = P_{1i} + 255; \beta = 1$,

Les valeurs de α et de β sont insérées dans les bords de l'image .Ces valeurs seront utilisées lors de l'extraction pour reconstruire l'image originale et assurer la réversibilité de cette technique de tatouage.

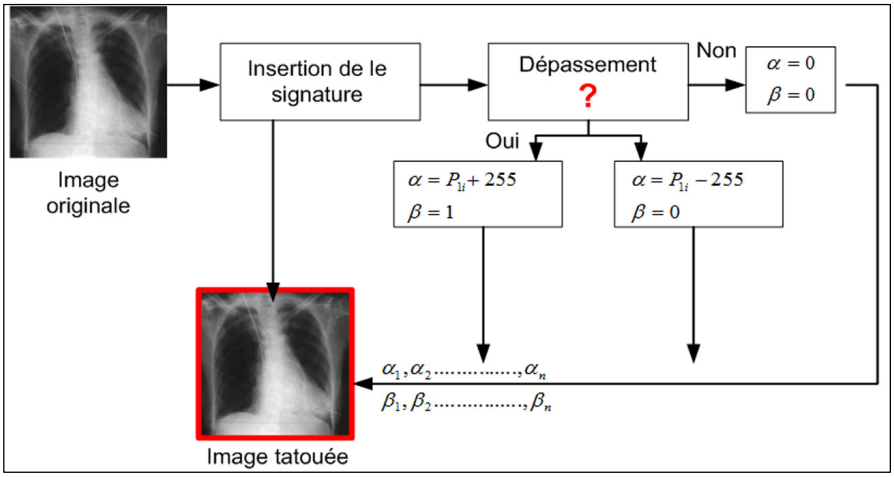


Figure 57. *Schéma d'insertion*

2.2. Schéma d'extraction

Le principe de l'extraction présenté dans la figure 58 est le suivant :

Soit P_{1i} le pixel de l'image tatouée porteur de la signature. Suivant les valeurs du dépassement et leur signe on va calculer la nouvelle valeur du pixel P_{2i}.

- si $\alpha = 0; \beta = 0$, $P_{2i} = P_{1i}$
- si $\beta = 0$, P_{2i} =255+ α
- si $\beta = 1$, $P_{2i} = \alpha$ -255

A partir de la valeur de P_{2i}, le récepteur (le détecteur) peut extraire le bit b_i inséré ainsi que la valeur de P_i la valeur du pixel original.

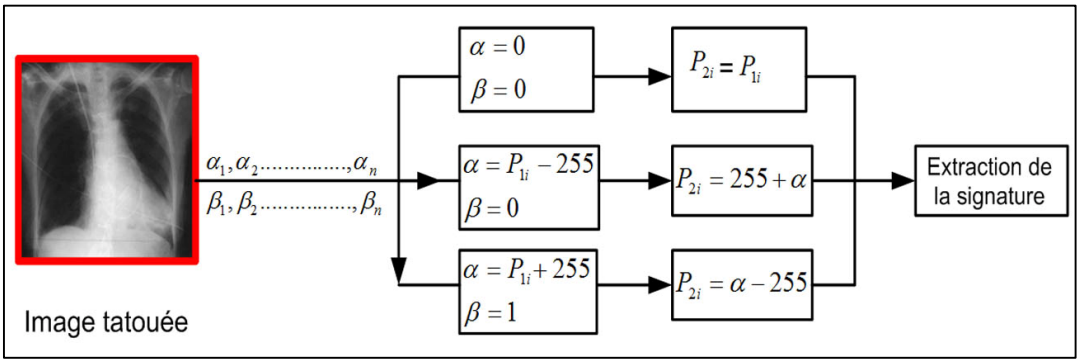


Figure 58. *Schéma d'extraction*

Le bord doit être le plus petit que possible pour ne pas dénaturer l'image tout en assurant une taille suffisante pour l'insertion des différentes valeurs du dépassement.

On a jugé suffisant de définir un bord de 8 pixels entourant la totalité de l'image. L'image utile serait de taille 240x240. On découpe cette image en 900 blocs de taille 8x8 pixels.

A titre de remarque, on peut utiliser l'espace libre pour l'insertion des données personnelles du patient (nom, âge, sexe….) dans l'image pour les éventuelles transmissions entre les praticiens.

3. Validation de la méthode proposée

Dans cette validation, nous étudions, dans une première étape, la qualité de l'image tatouée : le PSNR est la métrique utilisée pour évaluer la qualité de l'image tatouée.

Dans une deuxième étape, nous testons la sensibilité de notre approche et son aptitude à localiser les zones falsifiées.

Nous achevons notre validation par la vérification de la réversibilité de l'approche développée et son aptitude à rétablir l'image originale à partir de l'image tatouée.

3.1. Fragilité par rapport aux différentes attaques

Afin de prouver la sensibilité de notre approche et son aptitude à détecter et à localiser les modifications, nous avons simulé un ensemble d'attaques possible que l'image peut subir fréquemment et nous avons vérifié la présence de la signature après chaque attaque.

Nous présentons dans la figure 59 les résultats obtenus :

- par rapport à l'ajout de bruit, nous avons testé le bruit multiplicatif (speckle) de variance 0.02 et le bruit gaussien de moyenne nulle et de variance 0.02.

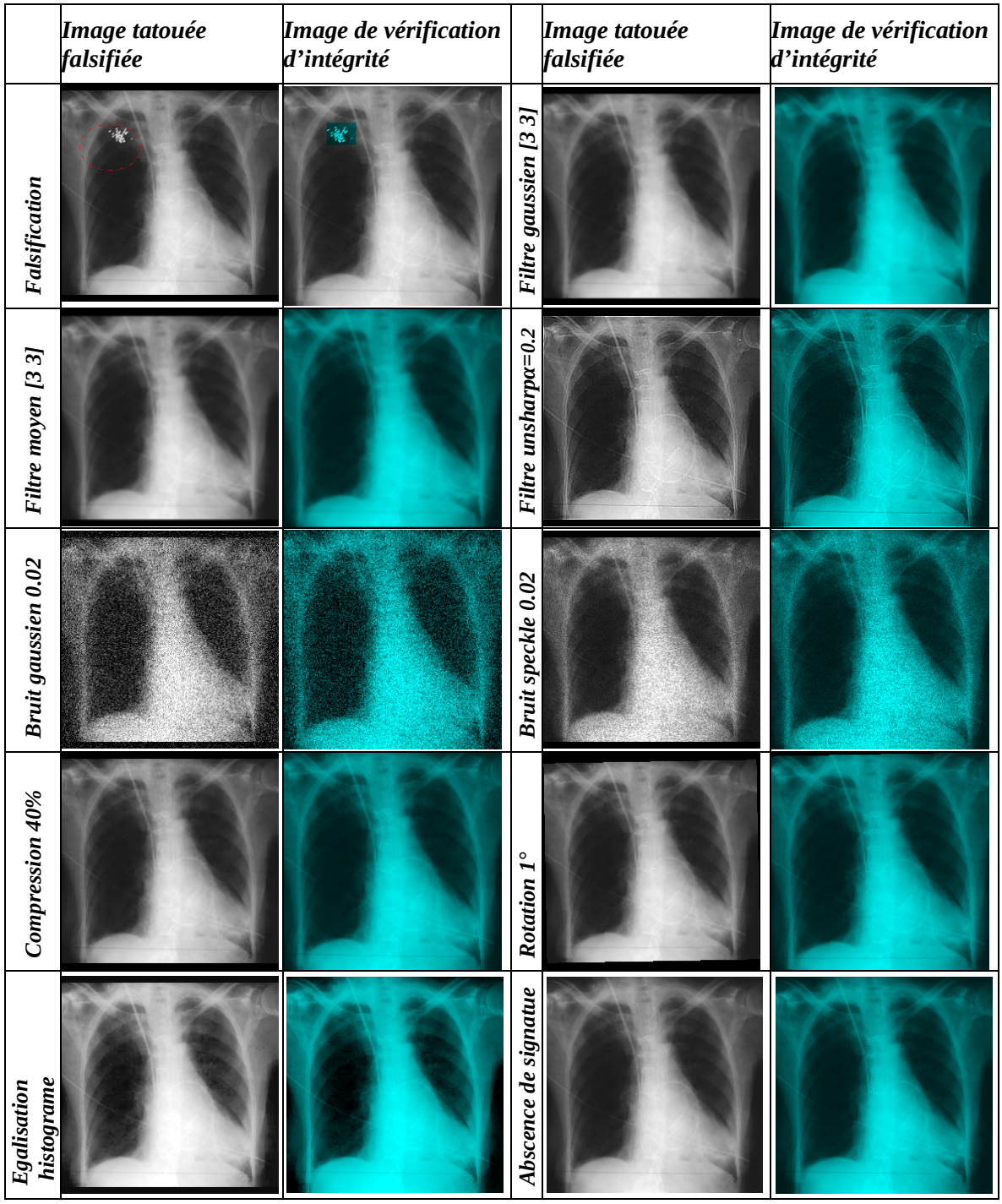


Figure 59. *Fragilité par rapport aux différentes attaques*

- par rapport à différents filtres : le filtre moyen, le filtre gaussien de taille 3x3 et le filtre unsharp de rehaussement de contraste avec $\alpha = 0.2$.
- et enfin par rapport à la compression JPEG pour un taux de compression 40%, à la rotation pour une petite déviation de 1° et à l'égalisation d'histogramme.

Les résultats obtenus prouvent l'efficacité de notre approche et son aptitude à détecter et localiser les différentes altérations que peut subir l'image tatouée.

Le bord noir apparu sur l'image tatouée peut attirer l'attention d'un pirate ou même d'un utilisateur ordinaire : ce qui donne l'idée de la suppression du bord et valide l'utilisation de l'image utile uniquement. Dans ce qui suit, nous étudions ce cas de falsification pour éviter tout risque et garantir l'intégrité de l'image médicale reçue.

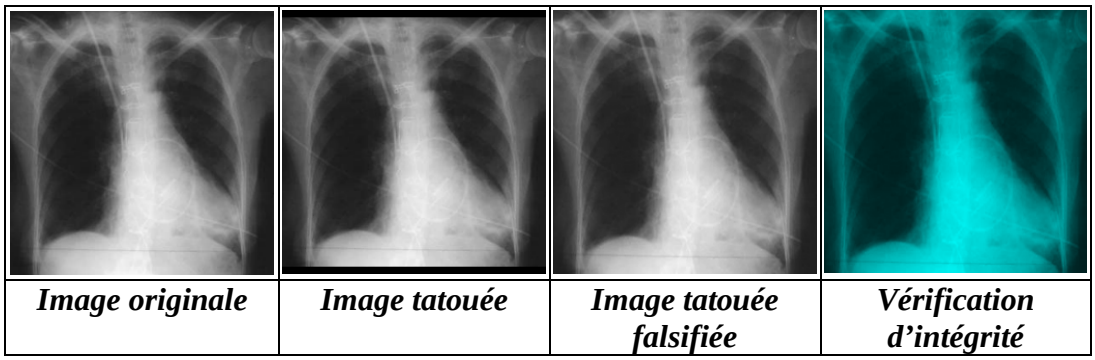


Image originale	***Image tatouée***	***Image tatouée falsifiée***	***Vérification d'intégrité***

Figure 60. *Résultat de la vérification d'intégrité suite à la suppression des bords de l'image*

La figure 60 montre qu'une image tatouée, dont le bord est supprimé, est considérée comme étant une image falsifiée lors de la vérification de son intégrité.

3.2. Qualité de l'image tatouée

L'image médicale porte des informations essentielles et nécessaires au médecin pour effectuer le diagnostic du patient et évaluer son état de santé ; d'où la nécessité de préserver l'information médicale contenue dans l'image et de ne surtout pas l'altérer.

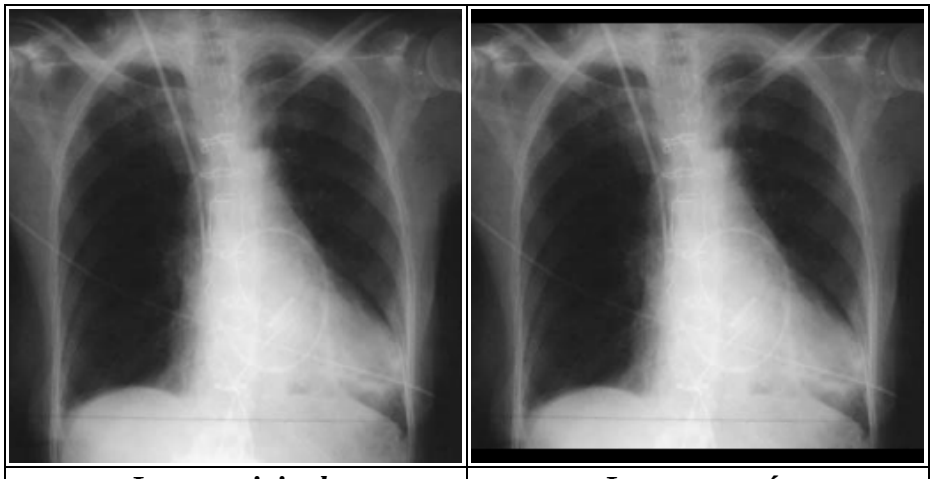


Image originale	***Image tatouée***

Figure 61. *Exemple d'une image tatouée*

La signature ne doit pas dénaturer l'image et ni modifier le contenu médical nécessaire pour faire le diagnostic (voir figure 61).

Dans notre cas l'image tatouée utile (c.à.d. qui sera utilisée lors d'une interprétation médicale) a gardé sa structure et ses caractéristiques. On peut remarquer d'après la figure que le bord inférieur et le bord supérieur porteurs des valeurs de dépassement ont changée, ce qui peut attirer l'attention d'un utilisateur ou surtout d'un pirate.

Mais comme on l'a déjà montré, la modification ou la suppression des bords est bien détectée lors de la phase de la vérification d'intégrité.

Nous présentons les valeurs moyennes du PSNR pour les 30 images médicales test.

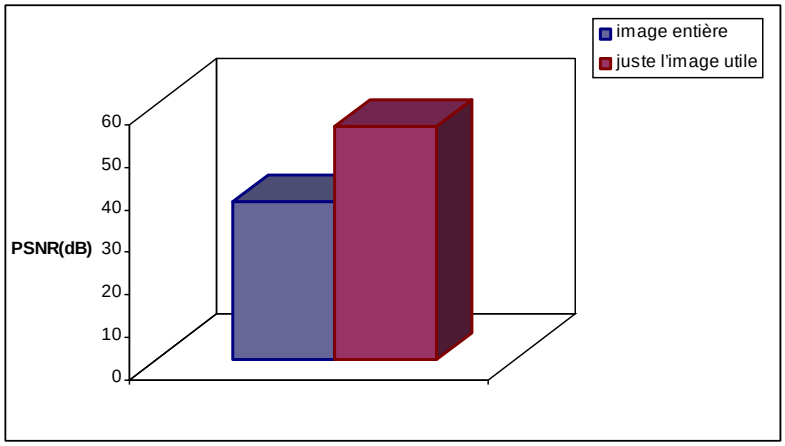


Figure 62. *Les valeurs moyennes du PSNR pour les 30 images tatouées*

En tenant compte de l'image tatouée entière (avec les bords modifiés) ; la valeur moyenne du PSNR pour 30 images médicales tatouées reste toujours supérieure à 41 dB (figure 62), ce qui permet à l'image d'être exploitable. Pour l'image utile, qui comporte l'information médicale, la qualité de l'image tatouée est ainsi validée.

La qualité de l'image tatouée est indispensable pour ce type d'image afin de préserver l'information médicale contenue dans l'image (essentielle pour la qualité du diagnostic).

3.3. Réversibilité

Après extraction et vérification de la validité de la marque, les méthodes réversibles sont capables de fournir un duplicata exact de l'image originale.

Le critère de réversibilité est bien entendu primordial pour des considérations d'ordre éthique : l'image est en partie à la source d'un diagnostic, le praticien doit avoir la garantie qu'il travaille sur un cliché source, intact.

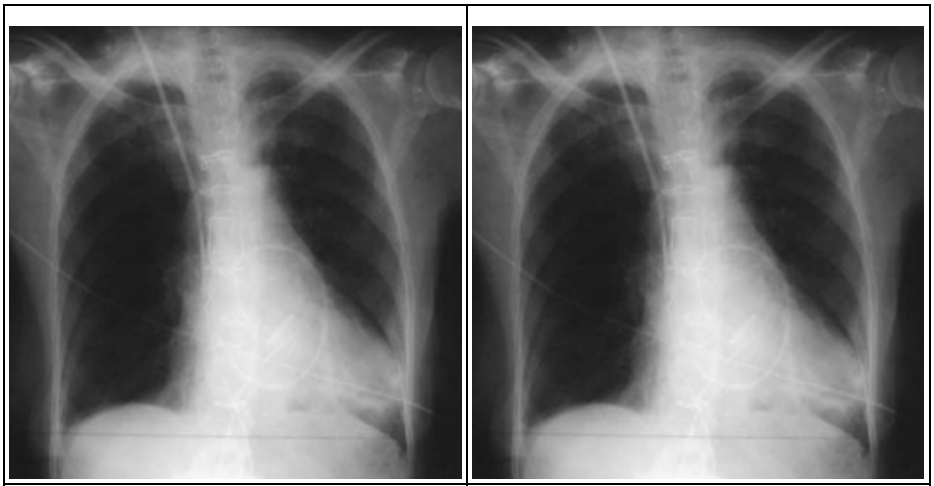


Image originale	*Image reconstruite*

Figure 63. *Image originale et image reconstruite*

Après la vérification d'intégrité de l'image reçue, le système permet au médecin qui reçoit les données transférées de reconstruire l'image originale à partir de l'image tatouée (voir figure 63).

Les interprétations médicales sont effectuées sur l'image reconstruite sans aucun risque de modification de quelques détails utiles de l'image médicale.

Conclusion

Suite au problème de dépassement rencontré dans les chapitres précédents, nous avons présenté dans ce chapitre une approche de tatouage réversible basée sur les caractéristiques des images médicales (images centrées) assurant une bonne qualité de l'image tatouée, la détection et la localisation des modifications que peut subir l'image tout en répondant au problème de dépassement.

Ainsi nous avons utilisé le centrage de l'image médicale pour utiliser les bords qui sont généralement flous (cette partie de l'image ne reçoit pas directement les rayonnements) pour insérer les différentes valeurs de dépassement obtenues sans affecter la globalité de l'image.

Nous avons validé l'approche développée en testant sa sensibilité et son aptitude à localiser les zones falsifiées. Cela nous a permis également de vérifier la réversibilité de la méthode présentée et son aptitude à rétablir l'image originale à partir de l'image originale.

Section 3 :

Validation de notre travail dans le cadre du projet DECOPREME

(DEpistage COllaboratif PREcoce des MElanomes)

Chapitre V

Description du Projet DECOPREME (DEpistage COllaboratif PREcoce des MElanomes)

DECOPREME est un projet européen crée entre le CHU de Besançon (France) et le CHU Vaudois de Lausanne (Suisse) afin de concevoir et de développer une plateforme favorisant le dépistage précoce des cancers cutanés, en particulier le mélanome.

Introduction

La fréquence des cancers cutanés, dont en particulier le mélanome, ne cesse d'augmenter depuis plusieurs décennies. On estime qu'une personne sur 50 sera confrontée à ce diagnostic en 2010. Alors qu'un dépistage précoce du mélanome malin suivi d'une exérèse chirurgicale permet une guérison, un diagnostic tardif signifie une morbidité et mortalité élevées [FRIE85]. C'est pourquoi les dermatologues ont développé depuis le début des années 90 une technique de microscopie cutanée de surface, la dermoscopie, qui permet une sémiologie spécifique pour interpréter les lésions cutanées pigmentées et améliorer sensiblement la détection des mélanomes à un stade précoce [SCH03] [HAL95] [SSS94].

Ce projet utilise les nouvelles technologies (Internet, téléphone portable, PDA, communications GSM, Bluetooth…) afin de réaliser une saisie numérique de l'image du mélanome puis son envoi à des experts qui feront un diagnostic rapide à l'attention du patient ou du médecin traitant. Cette technologie sera accessible au public par l'intermédiaire des pharmacies, des bus de dépistage et des consultations chez le médecin traitant ou à l'hôpital.

1. Description du projet

Ce projet se décompose en 4 axes principaux :

1. Le **système d'évaluation** des lésions pigmentées basé sur les technologies Internet qui nécessite la réalisation de trois portails distincts : le portail de soumission des images après acquisition, le portail du professionnel évaluant les images, et le portail du patient ou du médecin demandeur pour obtenir le résultat des évaluations.

    a. *Système d'acquisition* : Système d'acquisition: il doit être simple mais performant afin d'obtenir les images des lésions cutanées pigmentées dans des contextes permettant un dépistage de masse, par exemple dans des pharmacies, dans un bus de dépistage ou chez les médecins traitants. Le développement d'un système optique adapté est un des éléments de l'acquisition qui doit aussi permettre au moyen par exemple d'un petit ordinateur personnel (PDA) ou d'un téléphone l'identification du patient concerné et la réception rapide des images.

    b. *Serveur pour la réception, le stockage et l'analyse des images* : Cette partie du système permet de coordonner l'évaluation des images par les dermatologues experts en dermoscopie, d'appliquer divers pré-traitements et analyses d'images et de stocker les résultats de l'analyse.

    c. *Le système de mise à disposition des résultats aux divers intervenants du système*, c'est-à-dire aux médecins demandeurs et aux patients. Il s'agit de réaliser un site web dédié aux patients et leur permettant d'une part de suivre l'historique de leurs lésions cutanées pigmentées et d'autre part de recevoir des conseils de prévention personnalisés pour une lutte efficace contre les cancers cutanés.

2. **L'outil de collaboration pour le diagnostic à distance** des lésions dermatologiques qui offre une plateforme de télédermatologie grâce à laquelle les dermatologues peuvent participer à un consilium avec d'autres confrères généralistes ou des soignants. Dans ce cadre général, divers problèmes doivent être étudiés en vue de trouver une solution acceptable dans la pratique médicale. Il s'agit notamment des questions médico-légales, à savoir en particulier quels intervenants

du système ont accès aux images, quels diagnostics ou informations peut-on donner en retour à l'utilisateur qui soumet une image ou participe à la téléconférence.

3. Ensuite il est utile de prévoir l'**acquisition d'images macroscopiques** corps entier afin de faciliter l'identification de nouvelles lésions.
4. Et enfin, un système de **contrôle de qualité** sera élaboré et mis en place dès le départ pour s'assurer de la fiabilité des analyses d'images, des évaluations par les dermatologues experts et évaluation de la précocité du dépistage des mélanomes.

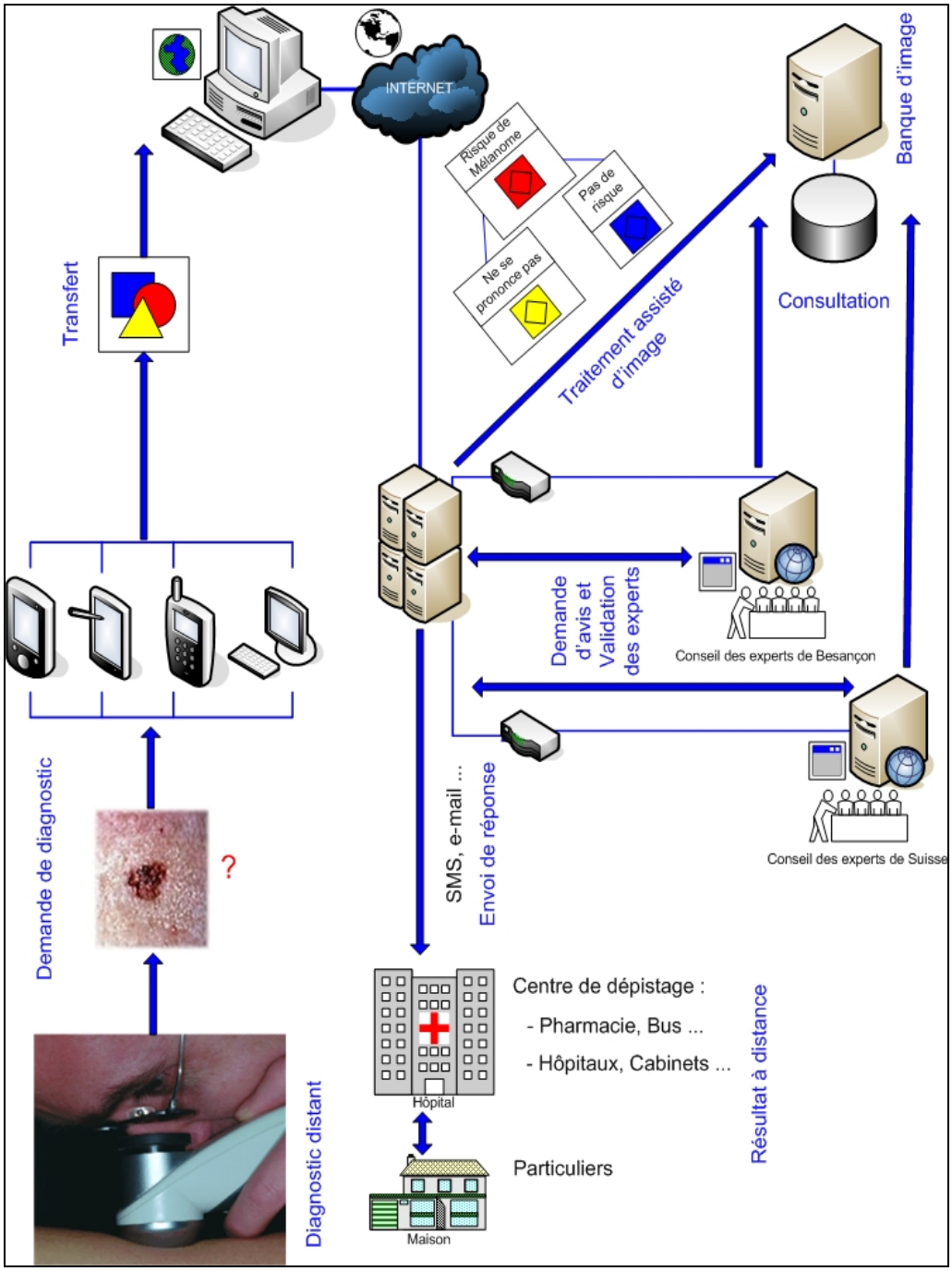


Figure 64. *Le projet DECOPREME*

La figure 64 présente le schéma de fonctionnement du projet DECOPREME :

- Le projet est de concevoir et développer une plate-forme pour faciliter le dépistage à distance du mélanome. Ce projet se limitera à cette spécificité de la dermatologie, mais son architecture pourra être étendue à d'autres domaines de cette spécialité.
- Cette plate-forme doit permettre l'acquisition d'image de la peau grâce à un équipement miniaturisé : ce qui permettra d'étendre le dépistage et d'en réduire les

coûts en évitant tout déplacement inutile. Pour cela, un dispositif d'acquisition doit être développé. La partie optique du dispositif, qui sera en contact avec la peau, est composée d'une lentille au grossissement fois 10 et d'un éclairage intégré : ce qui permettra de comparer objectivement (puisque l'éclairage et le grossissement seront constants) des images et d'avoir des résultats cohérents lorsque des algorithmes de détection automatiques seront appliqués sur ces images. Ce dispositif est également composé d'une partie logicielle qui permettra de saisir les informations pertinentes sur l'image (identification du patient, date, position géographique sur le corps…). Il pourra s'agir par exemple, d'un PDA muni d'une caméra sur laquelle vient se greffer un dispositif optique voir même d'un téléphone muni d'appareil photo numérique.

- Une fois cette acquisition effectuée, les images et les informations pertinentes sur ces images devront être envoyées vers la plate-forme logicielle. Les images subiront un traitement informatique (pré-traitement assisté d'image) qui permettra d'obtenir des chiffres sur les caractéristiques des mélanomes (asymétrie, couleur…). Ces chiffres permettront d'une part de donner un avis sur le risque de mélanome, mais surtout d'avoir des chiffres qui seront utilisables facilement pour mesurer objectivement l'évolution d'un mélanome ou pour comparer différentes lésions. Cette phase permet d'enrichir les images saisies afin de les stocker dans une banque d'images qui facilitera le suivi des lésions ou une aide au diagnostic par comparaison.
- Après cette phase de traitement et de stockage, la plateforme permettra l'envoi des demandes d'avis médicaux sur la base de ces images et des informations vers des dermatologues distants. Ces derniers pourront, par le biais de la plateforme, retourner un avis vers le site émetteur, éventuellement par un professionnel de santé (généraliste, hôpital…).
- Nous envisageons également une plateforme totalement automatique, mais des problèmes de responsabilité apparaissent dans le cadre du mélanome. Cette fonctionnalité, serait néanmoins très intéressante dans des domaines moins critiques comme la cosmétologie. Dans le cas des dermatoses, les médecins ne souhaitent pas actuellement une automatisation, mais seulement une aide au diagnostic.

2. Nécessité de sécurisation sur la plateforme de télédiagnostic

L'avènement des nouvelles technologies de l'information et le déploiement des réseaux de télécommunications a notamment modifié en profondeur les pratiques médicales.

Les données des patients (texte, son, images, …) ont été numérisées (perte des versions papiers) se limitant ainsi au stockage des versions informatiques : ces dernières pouvant être facilement transférées entre deux praticiens éloignés et ce quasiment en temps réel. Les médecins peuvent formuler un diagnostic ou proposer un avis thérapeutique sans rencontrer directement le patient [GAR05]. De nombreux systèmes d'informations médicales sont opérationnels dans le monde [GUI03] et ont démontré leur utilité dans la prise en charge du malade.

Les informations médicales qui circulent dans les réseaux Internet ou Intranet de l'établissement sont accessibles depuis de nombreux ordinateurs. Il n'existe pas sur Internet de moyen de protéger efficacement les informations.

Les terminaux et les réseaux utilisés étant ouverts ils n'offrent donc aucune garanti d'intégrité des informations transmises. Rien ne garantit que l'information parvenue au récepteur soit conforme à l'information envoyée.

La sécurité des communications et des applications liées à la santé est devenue à la fois une nécessité et une évidence. En effet, le dossier informatique ne sera accepté par les professionnels de santé et par les patients, que si chacun est certain qu'il y a absence de danger. Par ailleurs, la sécurité des dossiers informatiques des patients doit au moins égaler, si ce n'est dépasser celle appliquée aux dossiers papiers habituels.

Pour toutes ces raisons, les techniques de tatouage dédiées à la vérification d'intégrité et la détection des falsifications [FOU06b] sont étudiées afin d'offrir à la plateforme DECOPREME la sécurité du transfert des données circulantes. Le tatouage consiste à insérer une signature dans l'image. Cette signature doit être imperceptible pour ne pas dénaturer ces images et doit disparaître après une manipulation visant à modifier le contenu du document.

Dans ce cadre la structuration de notre travail, qui consiste à vérifier l'intégrité des images médicales lors de leur transfert, repose sur la réalisation de plusieurs étapes successives :

- *1ére étape* : Vérification de l'intégrité de l'image transférée depuis les équipements d'acquisition d'image. En effet, avant de traiter l'image reçue il faut s'assurer que cette dernière est rigoureusement identique à celle émise et qu'elle n'a subit aucune modification lors de son transfert.
- *2éme étape* : Vérification de l'intégrité de l'image avant de l'archiver. L''image sera marquée avant d'être archivée ce qui permet de s'assurer de son intégrité avant une utilisation ultérieure.
- *3éme étape* : Vérification de l'intégrité de l'image transférée entre les praticiens sur l'anneau virtuel de communication (Figure 65). Pour que les échanges entre les praticiens fonctionnent il faut que le contenu du message (l'image) produit par l'émetteur soit préservé lorsque le message est interprété par le récepteur. Une condition indispensable est bien sûr que le message soit transmis au récepteur dans son intégrité.
- *4éme étape* : Vérification de l'intégrité de l'image suite à l'étude collaborative . Une fois que les intervenants ont terminé leur travail sur l'image, cette dernière sera marquée du diagnostic final. Il faut alors valider ce diagnostic commun en faisant circuler l'image tatouée du diagnostic sur l'ensemble de la plateforme. Une fois que l'image a parcouru l'ensemble des serveurs sur lesquels se trouve un praticien, si personne n'a effectué de modification (donc si tous acceptent le diagnostic) le tatouage est resté identique, l'image a gardé son intégrité. Cette conservation d'intégrité garantit que le diagnostic est assumé (validé) par chacun des intervenants. En cas de modification, les discussions peuvent continuer avant la conclusion finale qui sera resoumise à la validation.

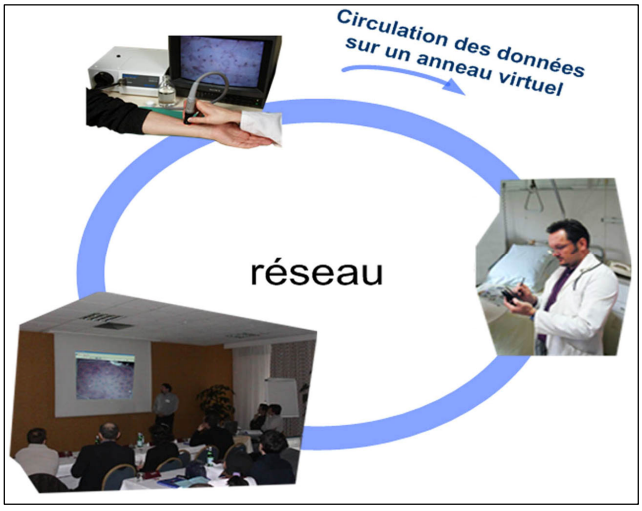


Figure 65. *Circulation des messages entre participant*

Conclusion

Dans ce chapitre nous avons présenté le contexte du projet Européen de télédiagnostic dans le cadre de la télédermatologie. Ce projet DECOPREME (DEpistage COllaboratif PREcoce des MElanomes) utilise les nouvelles technologies afin de réaliser :

- L'acquisition numérique de l'image d'un naevus,
- son envoi à des experts qui feront un diagnostic rapide à l'attention du patient ou du médecin traitant.

Dans ce contexte, apparaît la nécessité de garantir l'intégrité des données échangées (images de naevus) dans un tel contexte contraint (réseaux médical).

Pour assurer cette garantie nous proposons d'utiliser l'approche de tatouage réversible déjà présentée dans la section précédente. Cette approche est validée dans le chapitre suivant.

Chapitre VI

Validation de la méthode proposée dans le cadre du projet DECOPREME

Introduction

Dans cette partie nous validons la méthode proposée ; nous commençons en premier lieu par une validation technique permettant de vérifier l'efficacité de l'approche proposée : évaluation de la qualité de l'image tatouée, vérification de la sensibilité de l'approche par rapport aux différentes attaques, précision de la localisation des zones modifiée et surtout évaluation de l'aptitude de l'approche à reconstruire l'image originale à partir de l'image tatouée (réversibilité). Les images étudiées sont issues du domaine de la dermatologie et plus particulièrement de celui de la détection de nævus malins (mélanomes).

En deuxième lieu nous proposons une ébauche de validation clinique (médicale) afin de vérifier si l'information médicale contenue dans l'image a été préservée après l'opération de tatouage, et si elle est exploitable par médecins.

1. Validation technique

Afin de prouver l'efficacité de la méthode proposée, nous appliquons cette technique à 30 images différentes de taille 256x256 pixels et de résolution 8 bits/pixel afin de s'assurer des résultats obtenus.

1.1. Fragilité par rapport aux attaques

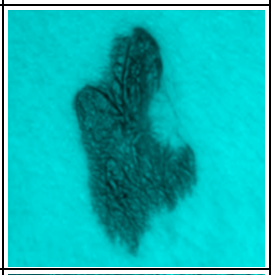
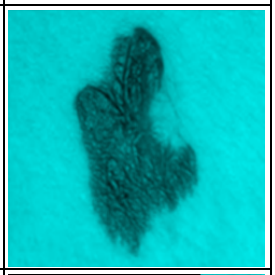
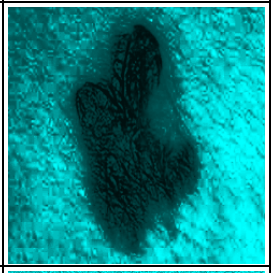
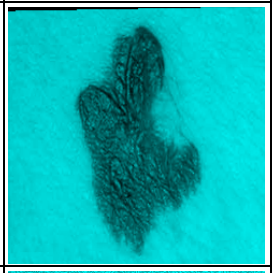
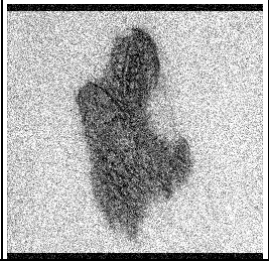
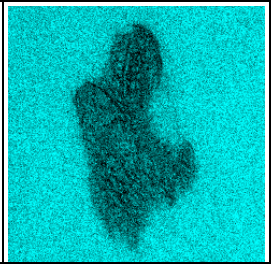
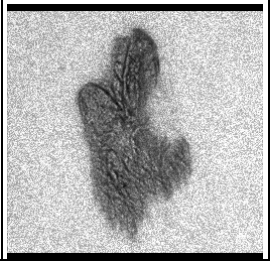
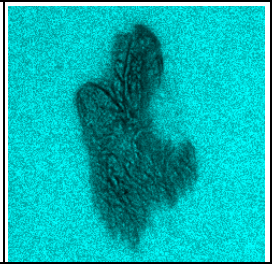
Nous avons choisi de faire subir à l'image tatouée un ensemble d'attaques pour vérifier l'aptitude de notre méthode à localiser l'anomalie introduite dans l'image.

1.1.1. Image tatouée non attaquée

Image tatouée non attaquée	
	
Image tatouée	***Image de vérification d'intégrité***

Figure 66. *Image tatouée non attaquée*

Suite à son passage par le processus de vérification d'intégrité, l'image tatouée apparaît sans aucune alarme (coloration des parties modifiées : cf figure 66) ce qui prouve l'intégrité de cette dernière.

	Image tatouée falsifiée	***Image de vérification d'intégrité***		***Image tatouée falsifiée***	***Image de vérification d'intégrité***
Filltre Gaussian [3 3]			***Filtre moyen [3 3]***		
égalisation d'histogramme			***Rotation 1°***		
Bruit gaussien 0.02			***Bruit Speckle 0.02***		

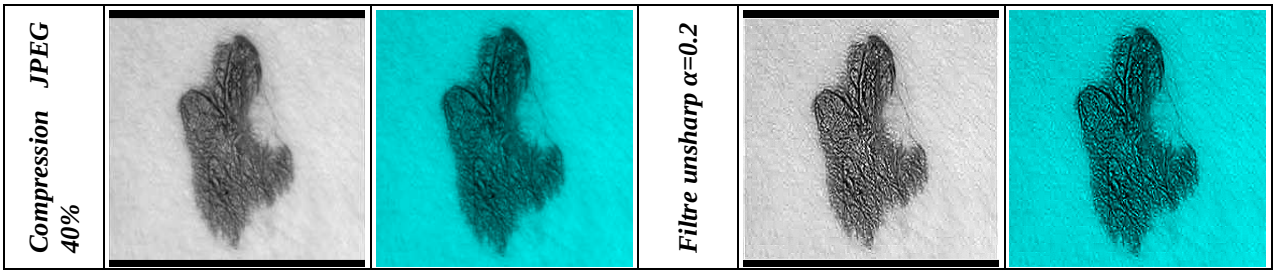


Figure 67. *Fragilité par rapport aux différentes attaques*

La figure 67 montre bien que toutes les attaques sont détectées et les zones falsifiées sont facilement localisées.

1.1.2. Fragilité par rapport à l'absence de la signature

Afin d'approfondir notre étude de l'efficacité de notre approche de tatouage, nous avons étudié le cas d'absence de signature. En effet, un système de tatouage efficace ne devrait pas accepter une image non signée (non sécurisée : cf figure 68).

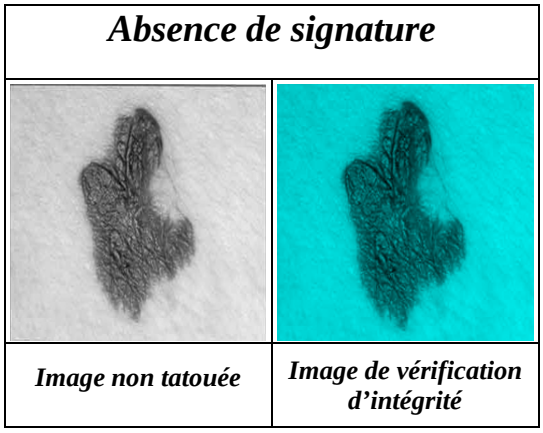


Figure 68. *Fragilité par rapport à l'absence de signature*

1.1.3. Fragilité par rapport à la falsification

L'attaque que peut subir l'image doit respecter deux contraintes pour falsifier l'image sans que cela soit décelable. Tout d'abord, la zone de modification doit être la plus petite possible : en effet, plus la taille augmente, plus le risque de voir la modification grandit. De plus, la modification doit se fondre dans l'image donc elle ne doit pas être trop forte pour rester quasi-invisible.

Nous avons choisi de faire subir à l'image tatouée une falsification (nous avons ajouté une partie sur l'image tatouée) et nous avons vérifié l'aptitude de notre méthode à localiser l'anomalie introduite dans l'image.

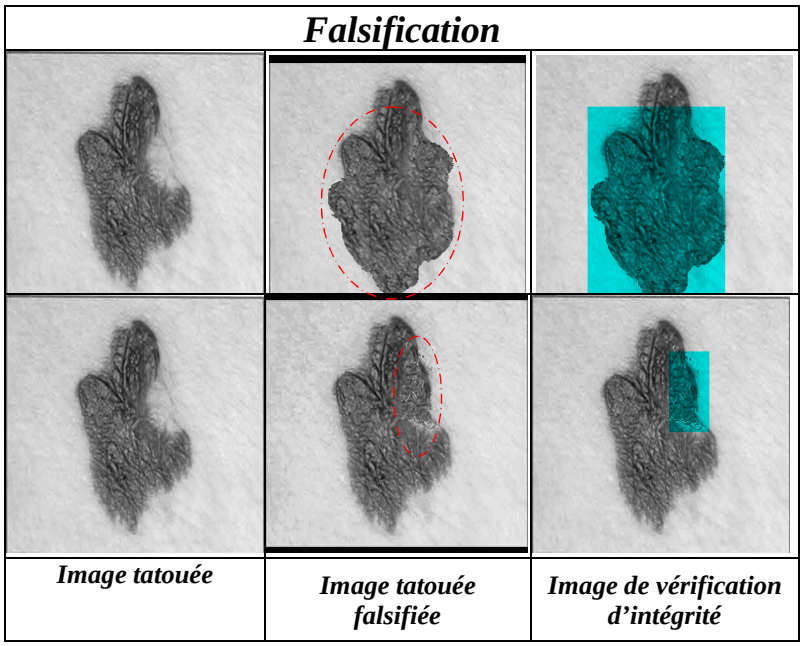


Figure 69. *Fragilité par rapport à la falsification*

La partie ajoutée se présente bien sur l'image de vérification d'intégrité comme étant une zone colorée en cyan localisant la falsification avec une précision remarquable.

La figure 69 montre l'aptitude de notre approche à détecter et localiser les falsifications apportées à l'image tatouée.

1.2. Qualité de l'image tatouée

Nous devons tatouer l'image avec une faible dégradation de l'image tatouée. L'image tatouée devra être globalement similaire à l'image originale (voir figure 70).

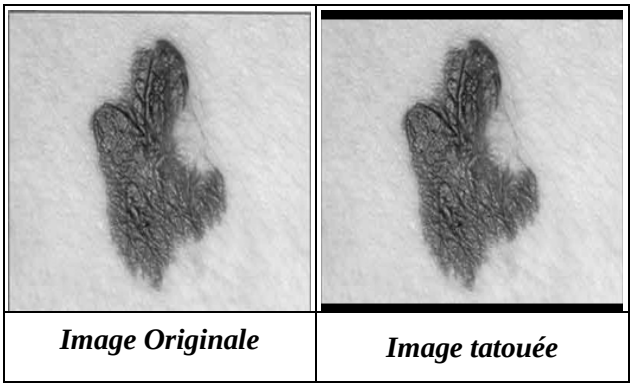


Figure 70. *Image originale et Image tatouée*

Nous mesurons la dégradation de l'image tatouée. Pour ceci, nous avons effectué des mesures de la qualité de l'image tatouée par calcul du PSNR (métrique courante de validation de qualité d'image).

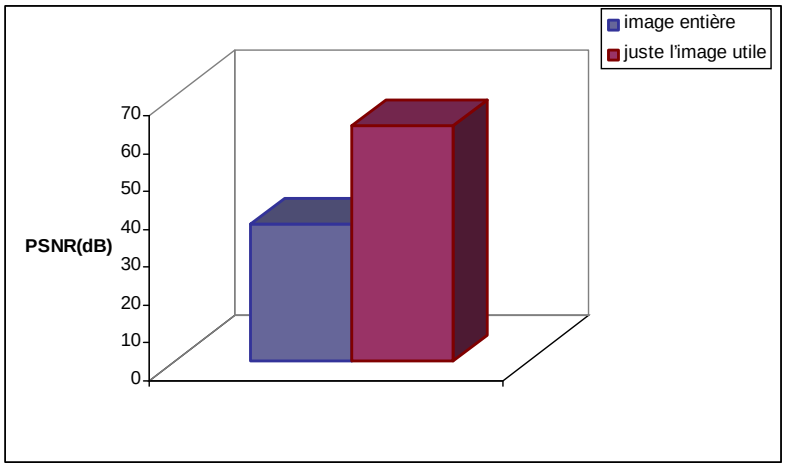


Figure 71. *Les valeurs moyennes du PSNR pour les 30 images tatouées*

D'après les résultats trouvés dans la figure 71, nous pouvons conclure que si l'on tient compte de l'image tatouée entière (avec les bords modifiés) la valeur moyenne du PSNR pour 30 images de mélanome tatouées reste toujours supérieure à 40 dB : valeur qui montre que l'image est exploitable.

Pour l'image utile comportant l'information médicale, la qualité de l'image tatouée est très satisfaisante.

1.3. Réversibilité

La réversibilité de notre approche de tatouage réversible doit également être validée.

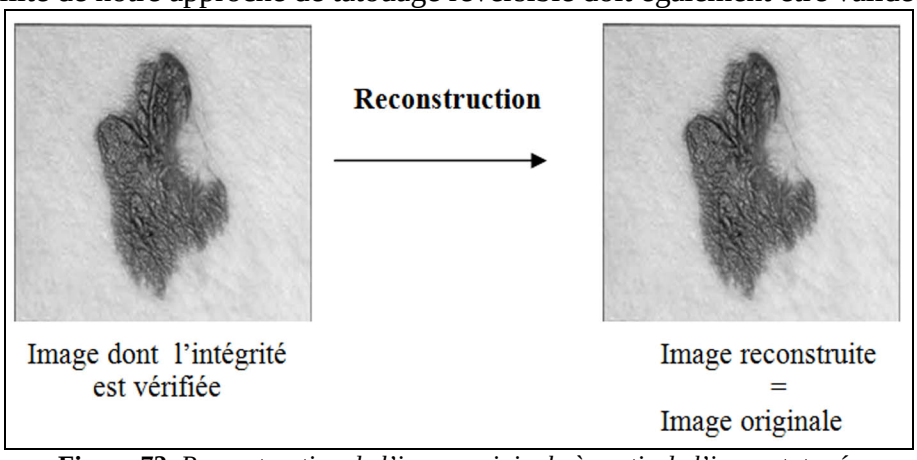


Figure 72. *Reconstruction de l'image originale à partir de l'image tatouée*

Après avoir garanti l'intégrité de l'image, le médecin reconstitue l'image originale (non tatouée : intacte sans aucune dégradation ; voir la figure 72). Puis il l'utilise dans son diagnostic évitant tout risque de modification (lors de l'insertion de la signature) : la moindre mutation dans l'image médicale pouvant conduire à des décisions médicales erronées pouvant

nuire au patient.

2. Validation clinique

Cette validation se base sur les avis des médecins spécialistes en imagerie médicale (dermatoscopie) et au type particulier de pathologie (mélanome) traité. Leur avis est nécessaire pour affirmer que l'opération de tatouage a préservé le contenu médical et n'a pas modifié l'interprétation de l'image (diagnostic).

Notre approche de tatouage est réversible, comme son nom l'indique, elle est capable de restituer l'image originale à partir de l'image tatouée après la vérification d'intégrité de cette dernière.

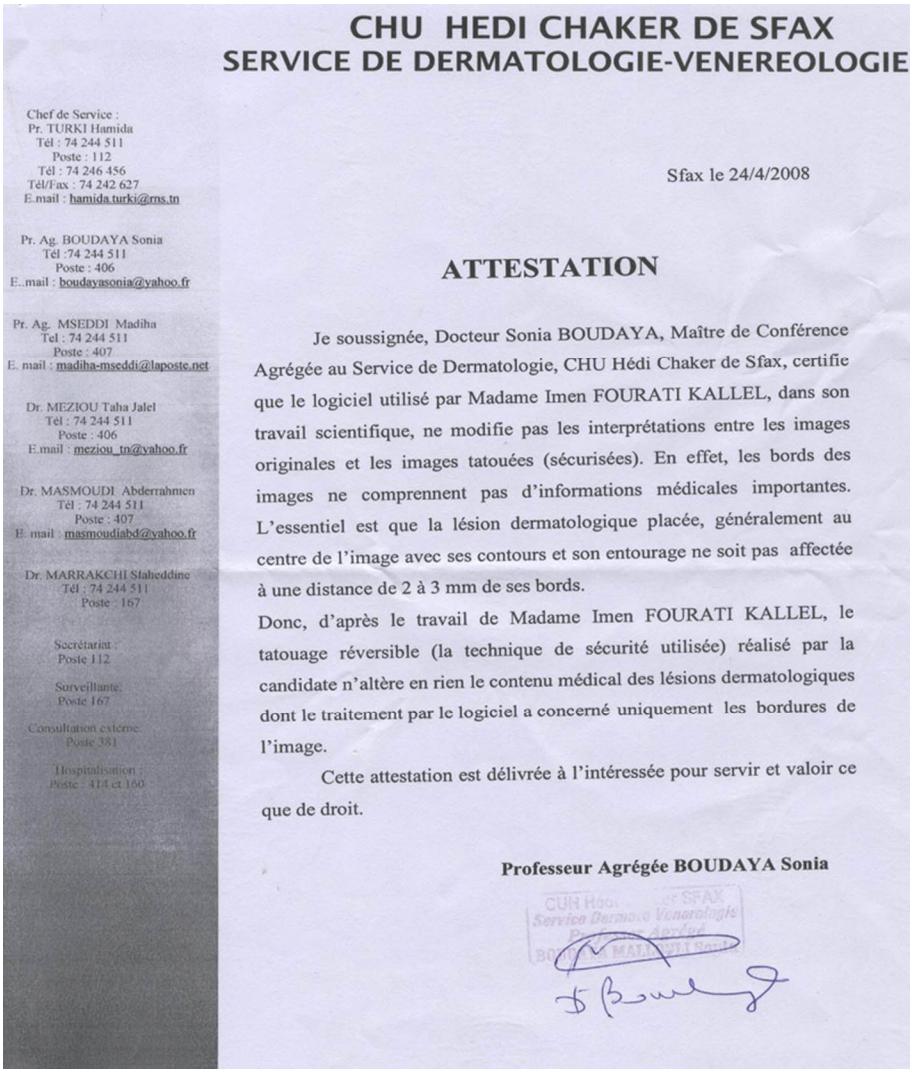
Donc le médecin va s'assurer en premier lieu de l'intégrité de l'image reçue, en deuxième lieu il élabore son diagnostic et rédige ses interprétations sur l'image originale reconstruite.
Ce procédé écarte tous risques de modification même pour les détails minimes qui peuvent être utiles pour identifier les signes d'une pathologie.

Mais il ne faut pas oublier que l'image tatouée peut être utilisée par une personne qui ne sait pas qu'elle est signée (étudiant, praticien, expert…) sans avoir accès à la reconstruction de l'image originale. Donc cette image doit garder l'intégralité de son contenu médical.

La validation clinique réalisée consiste essentiellement en deux volets :

- Le premier volet concerne la préservation du contenu médical pour l'image utile. En effet, l'image médicale comporte des petits détails nécessaires pour l'interprétation de l'image que seul un médecin peut vérifier et ainsi que la persistance après insertion de la signature.
- Dans le même contexte le deuxième volet touche la préservation de l'information médicale suite à l'utilisation du bord du cliché.

Cette validation clinique est effectuée par Dr. Mounir MAHDI radiologue, Dr Chaouki DABBECHE, médecin radiologue exerçant au service de radiologie du CHU Habib Bourguiba de Sfax et Dr Sonia BOUDAYA, Maître de conférence agrégée au service de dermatologie, CHU Hédi Chaker de Sfax.
Dans ce qui suit (cf Figure 73), nous présentons le rapport de Dr. Mounir MAHDI, Dr Chaouki DABBECHE et Dr. Sonia BOUDAYA.



CHU HEDI CHAKER DE SFAX
SERVICE DE DERMATOLOGIE-VENEREOLOGIE

Chef de Service :
Pr. TURKI Hamida
Tél : 74 244 511
Poste : 112
Tél : 74 246 456
Tél/Fax : 74 242 627
E.mail : hamida.turki@rns.tn

Pr. Ag. BOUDAYA Sonia
Tél :74 244 511
Poste : 406
E..mail : boudayasonia@yahoo.fr

Pr. Ag. MSEDDI Madiha
Tel : 74 244 511
Poste : 407
E. mail : madiha-mseddi@laposte.net

Dr. MEZIOU Taha Jalel
Tél : 74 244 511
Poste : 406
E.mail : meziou_tn@yahoo.fr

Dr. MASMOUDI Abderrahmen
Tél : 74 244 511
Poste : 407
E. mail : masmoudiabd@yahoo.fr

Dr. MARRAKCHI Slaheddine
Tél : 74 244 511
Poste : 167

Secrétariat :
Poste 112

Surveillante:
Poste 167

Consultation externe
Poste 381

Hospitalisation :
Poste : 414 et 160

Sfax le 24/4/2008

ATTESTATION

Je soussignée, Docteur Sonia BOUDAYA, Maître de Conférence Agrégée au Service de Dermatologie, CHU Hédi Chaker de Sfax, certifie que le logiciel utilisé par Madame Imen FOURATI KALLEL, dans son travail scientifique, ne modifie pas les interprétations entre les images originales et les images tatouées (sécurisées). En effet, les bords des images ne comprennent pas d'informations médicales importantes. L'essentiel est que la lésion dermatologique placée, généralement au centre de l'image avec ses contours et son entourage ne soit pas affectée à une distance de 2 à 3 mm de ses bords.

Donc, d'après le travail de Madame Imen FOURATI KALLEL, le tatouage réversible (la technique de sécurité utilisée) réalisé par la candidate n'altère en rien le contenu médical des lésions dermatologiques dont le traitement par le logiciel a concerné uniquement les bordures de l'image.

Cette attestation est délivrée à l'intéressée pour servir et valoir ce que de droit.

Professeur Agrégée BOUDAYA Sonia

Centre Bab Bhar d'Imagerie Médicale
Docteur Mounir MEHDI
Radiologue

مركز باب بحر للتصوير الطبي
حكيم منير مهدي
إختصاصي في التصوير بالأشعة

Sfax le 11/03/2008

ATTESTATION

Je soussigné docteur Mounir MEHDI atteste par la présente, et après avoir visualisé une série d'images originales et de la même série tatouées à plusieurs reprise, qu'il n'existe aucune déformation ou modification des données de ces images pouvant être à l'origine d'un changement ou d'une transformation du diagnostic.

Les modifications des bords périphériques de clichés en dehors de l'image n'altèrent pas la qualité de l'image et ne retentissent pas sur le diagnostic.

Cette attestation est délivrée à madame Imen FOURATI KALLEL pour servir et valoir ce que de droit.

Signature
Docteur Mounir MEHDI

Docteur Mounir MEHDI
Radiologue

RADIOLOGIE CONVENTIONNELLE - RADIOLOGIE DENTAIRE - MAMMOGRAPHIE - ECHOGRAPHIE DOPPLER COULE
49, Avenue Habib Bourguiba - 3000 Sfax - Tél. : 74 227 888 49، شارع الحبيب بورقيبة – 3000 صفاقس – الهاتف :

Attestation

D'après le travail de Madame Imen FOURATI KALLEL et des clichés présentés par cette dernière, le tatouage réalisé n'altère pas le contenu médical des images.

J'affirme, Dr Chaouki DABBECHE, médecin radiologue exerçant au service de radiologie du CHU Habib Bourguiba de Sfax qu'il n'y a pas de changement d'interprétations entre les images originales et les images tatouées.

Les tests de vérification d'intégrité ont prouvé l'aptitude de la technique développée par Mme FOURATI KALLEL à détecter et à localiser les zones de l'image altérées.

A propos des bords d'un cliché radiologique, ils ne comprennent généralement pas d'informations médicales, d'où leur modification ne change pas le contenu médical de l'image.

Figure 73. *Attestations des médecins*

Conclusion

Dans ce chapitre nous avons validé l'approche de tatouage réversible développée sur une base de 30 images en niveaux de gris de mélanome de taille 256x256 pixels et de résolution 8 bits par pixels.

La validation s'est étalée sur deux volets :

- un volet de validation technique permettant de vérifier la sensibilité de notre approche et son aptitude à détecter et à localiser les zones modifiées tout en garantissant une qualité d'image tatouée optimale,
- et un volet de validation clinique basée sur les avis des médecins spécialistes afin de vérifier que l'information médicale contenue dans l'image a été préservée après l'opération de tatouage.

Suite à cette validation clinique, le dermatologue nous a affirmé que la notion couleur est primordiale pour les images dermatologiques puisqu'elle fait partie du diagnostic.

D'où la nécessité d'étendre l'approche de tatouage réversible développée pour les images en niveau de gris au domaine des images couleurs.

Chapitre VII

Tatouage réversible des images couleurs

Introduction

Même s'il est parfois utile de présenter des images en noir et blanc ou en niveaux de gris, les nouvelles applications multimédias utilisent le plus souvent des images en couleurs.

Surtout pour les applications de télédermatologie dans lesquelles l'information couleur est primordiale puisqu'elle fait partie du diagnostic.

A partir de la forme géométrique et de la couleur de la lésion nævique ou du grain de beauté, le dermatologue évalue la nature de la lésion : bénigne ou maligne [JOl92].

Dans ce chapitre, nous nous intéressons à étendre l'approche développée pour les images en niveaux de gris au domaine des images couleurs [SHAR97].

1. Choix de l'espace colorimétrique

Plusieurs espaces colorimétriques [BOU02] existent d'après la commission International d'Eclairage CIE [CIE86]. Une étude exhaustive sur ces différentes espaces et leurs caractéristiques est présentée dans l'annexe du manuscrit.

Pour la plupart des études consacrées au choix de l'espace colorimétrique dans différents cadres d'application de traitement d'images numériques la conclusion générale montre que le choix d'un système couleur dans le cadre d'un traitement donné reste un problème largement ouvert. Même si quelques auteurs privilégient tel ou tel espace pour effectuer un type de traitement donné, il est aisé de trouver la contradiction dans un autre ouvrage.

En effet, le choix d'un espace dépend à la fois de l'application et du type d'images à traiter. De plus, la comparaison des résultats de traitements d'images obtenues à l'aide de différents espaces n'est pas une tâche aisée. On trouvera dans certains ouvrages, tel que dans [TRE04] une analyse détaillée des avantages et inconvénients de plusieurs espaces couleurs, selon l'application visée.

L'espace RGB est certainement l'espace le plus utilisé non pas parce qu'il apporte des avantages particuliers par rapport à d'autres modèles mais simplement parce qu'il dérive de la technologie la plus souvent employée dans l'environnement numérique. Cet attachement à ce système de primaires s'explique principalement par la dépendance aux matériels (cartes d'acquisition, cartes vidéos, caméras, écrans) qui effectuent leurs échanges d'informations uniquement en utilisant des triplets (R, G, B) voir figure 74.

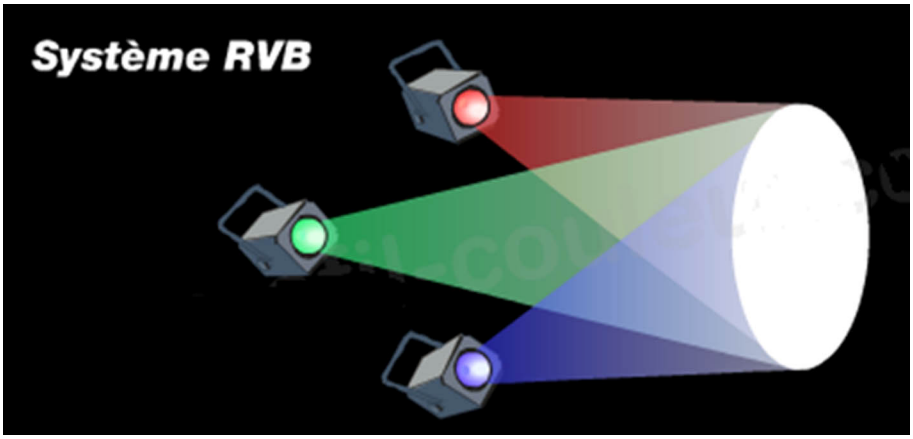


Figure 74. *Modèles RGB*

Le cube en couleur RVB est illustré sur la Figure 75. Aux trois primaires R, G, B, on fait correspondre respectivement trois vecteurs directeurs formant le repère d'un espace vectoriel. Ainsi, l'origine du cube, ou 0_R 0_G 0_B, représente l'absence totale de couleur, ce qui correspond au noir. L'extrémité la plus éloignée de l'origine est la somme des intensités les plus élevées de rouge, de vert, et de bleu, ou 255_R 255_G 255_B ceci produit la couleur blanche.

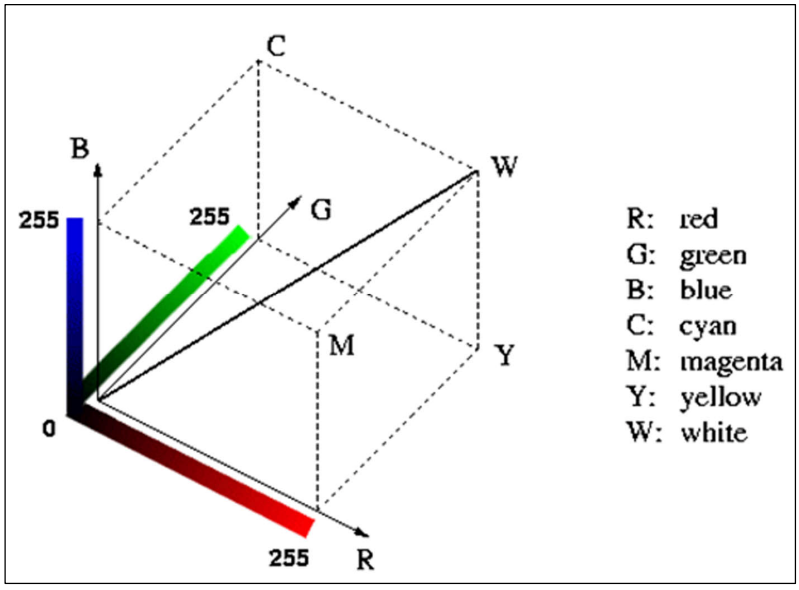


Figure 75. *Le Cube de Couleurs RVB*

La droite passant par les points Noir et Blanc est appelée axe des gris ou axe des couleurs neutres. Les points de cette droite représentent les nuances de gris allant du noir au blanc. Chaque axe du cube représente des valeurs de rouge, de vert, ou bleu dans l'intervalle [0 255]. Les valeurs entre 0 et 255 représentent les graduations dans l'intensité de couleur. Les couleurs peuvent être combinées par l'addition et la soustraction pour obtenir d'autres couleurs dans le cube.

2. Choix de l'approche d'adaptation de l'algorithme des images en niveau de gris aux images couleurs.

Il est souvent possible d'adapter les algorithmes, réalisés dans le cadre d'images en niveaux de gris, aux images couleurs. Dans ce contexte on peut distinguer trois approches [CHA98] [LAM02]: scalaire, vectorielle et marginale.

2.1. L'approche scalaire

Dans l'approche scalaire, (Figure 76) les trois composantes du vecteur couleur sont associées dans une première phase de fusion pour former un attribut scalaire, et le problème se ramène au traitement d'un signal scalaire. Cet attribut définit une variable, capable de résumer l'information portée par les trois composantes couleurs, dite variable de résumé. En général, c'est une combinaison linéaire des trois composantes.

Par exemple, la luminance Y=0.299R+0.587V+0.114B

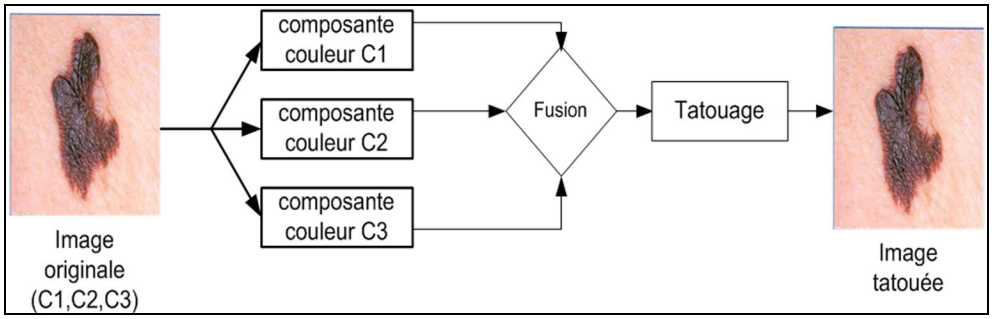


Figure 76. *Approche scalaire de tatouage de l'image couleur*

2.2. L'approche vectorielle

Dans l'approche vectorielle (figure77), le vecteur couleur est considéré globalement et le traitement doit alors être réellement vectoriel. Il n'y a pas dans ce cas d'étape de fusion explicite.

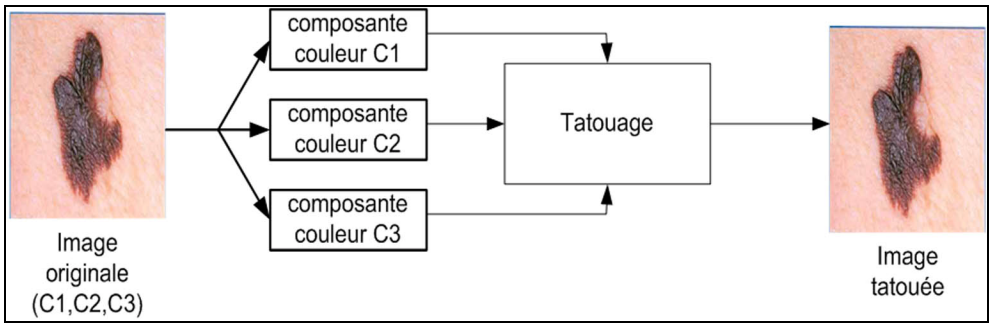


Figure 77. *Approche vectorielle de tatouage de l'image couleur*

2.3. L'approche marginale

L'approche marginale (figure78) consiste à tatouer indépendamment chaque composante de l'espace couleur, puis à fusionner les trois résultats obtenus pour construire l'image couleur tatouée.

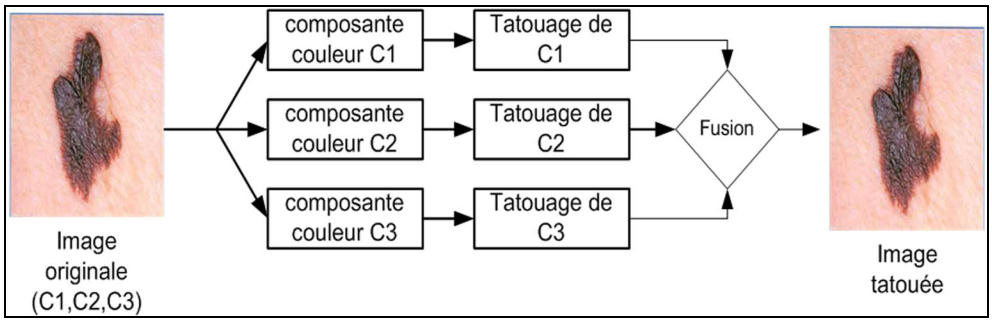


Figure 78. *Approche marginale de tatouage de l'image couleur*

L'utilisation de l'approche marginale donne plus de liberté de choix des pixels à tatouer par plan de couleur. En effet, les pixels tatoués dans le premier plan de couleurs peuvent être différents de ceux tatoués dans le second plan.

Notre choix s'est donc dirigé vers l'approche marginale pour effectuer l'adaptation de l'approche proposée en niveaux de gris à celle appliquée sur les images en couleurs.

L'approche marginale en tatouage soulève la question : quelle(s) composante(s) doi(ven)t être marquée(s) ?

L'utilisation d'un marquage marginal couleur doit être particulièrement contrôlée. En effet, chaque composante offre un équilibre différent concernant l'invisibilité de la marque.

Il faut aussi tenir compte du fait que le marquage simultané des trois composantes offre bien sûr un taux plus important [FLE97], mais il risque de faire rapidement baisser la qualité de l'image tatouée.

Une des premières solutions envisagées en tatouage d'images couleurs marginales consiste à utiliser le canal bleu comme espace d'insertion car c'est le canal qui est le moins sensible à la

décomposition RVB. Ainsi dans [KUT97], l'insertion s'effectue en modifiant la composante bleue de certains pixels dont les positions sont définies à partir d'une clef secrète.
Dans la rétine de l'œil humain il existe 3 sortes de cônes qui réagissent à des longueurs d'ondes différentes : bleu (450 nm), vert (540 nm) et rouge (580 nm).

Les longueurs d'ondes associées aux primaires sont illustrées dans le tableau 5 ci-dessous :

	Rouge	Vert	Bleu
Longueur d'onde λ	580 nm	540 nm	450 nm

Tableau 5. *Les longueurs d'ondes associées aux primaires*

Dans la figure 79, nous présentons le comportement des cônes humains suivant les longueurs d'ondes auxquelles ils sont sensibles.

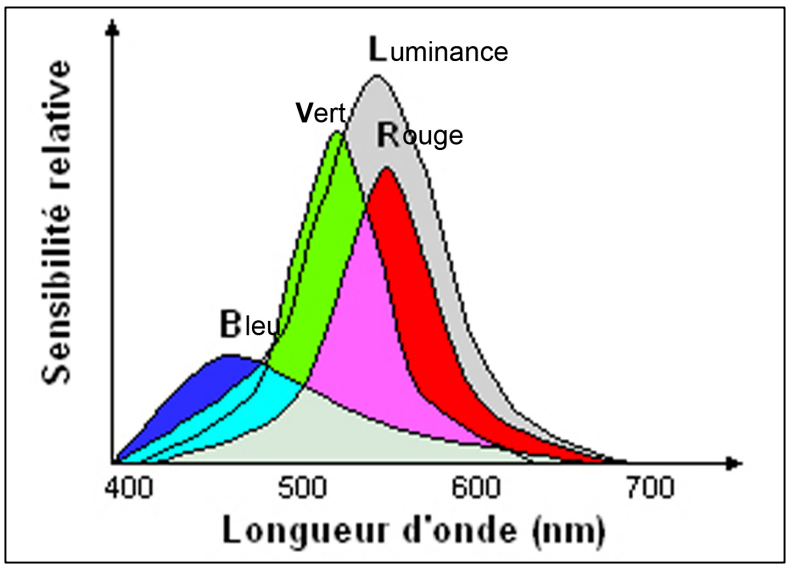


Figure 79. *Représentation de la courbe de sensibilité spectrale*

Approximativement 65% des cônes sont sensibles au rouge, 33% sont sensibles au vert et seulement 2% sont sensibles au bleu.

3. L'approche développée pour les images couleurs

Pour les images couleurs nous utilisons le même principe que pour les images en niveaux de gris. Nous précisons les composantes de l'image originale dans lesquelles nous insérons la signature ; nous appliquons à l'image une fonction de hachage permettant de prendre des informations sur l'image même.

La signature est ensuite insérée dans les blocs 8x8 de l'image originale d'une façon réversible.

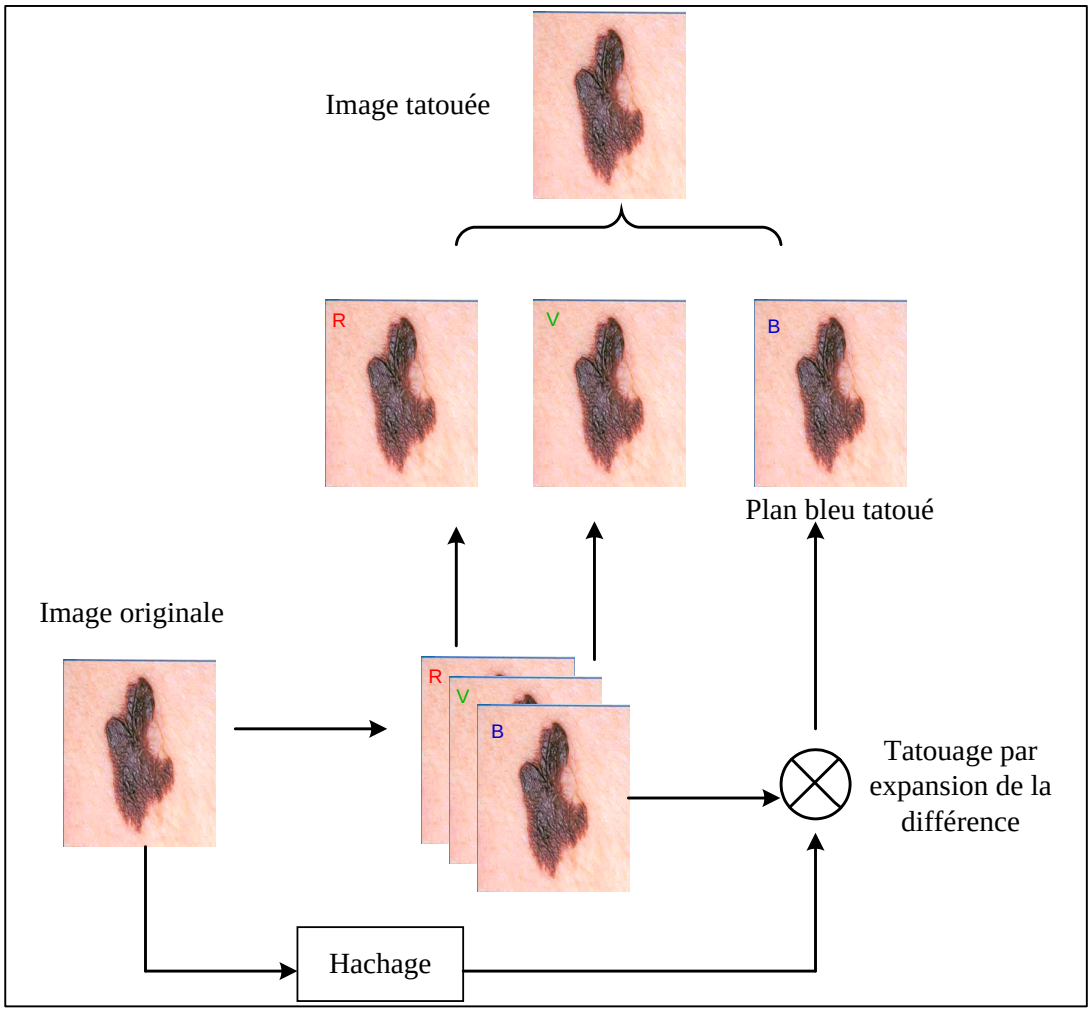


Figure 80. *Principe du tatouage couleur*

Nous avons commencé par décomposer l'image originale en trois composantes et par la suite nous avons tatoué indépendamment chaque composante de l'espace couleur. Enfin, nous avons fusionné les trois résultats obtenus pour construire l'image couleur tatouée.

Le tatouage des trois composantes de l'image nous offre une capacité d'insertion importante. Cependant, la qualité de l'image médicale tatouée risque de baisser excessivement.

Afin d'assurer une bonne qualité de l'image tatouée, nous utiliserons uniquement la composante couleur bleue pour l'insertion de la signature (voir figure 80).

4. Validation de l'approche développée pour les images couleurs

Nous appliquons l'approche développée à 30 différentes images médicales couleurs de taille 256x256 pixels avec une résolution de 8 bits par pixel et par composante couleur ce qui correspond à 24 bits par pixel et un codage sur 256 niveaux de chacune des trois composantes R, V et B.

Dans cette partie nous évaluons la qualité de l'image tatouée, et nous vérifions la sensibilité de l'approche par rapport aux différentes attaques, la précision de la localisation des zones modifiées et sa réversibilité.

4.1. Fragilité par rapport aux différentes attaques

La fragilité d'une approche de tatouage et son aptitude à détecter et à localiser les différentes modifications est vérifiée en appliquant à l'image tatouée différentes attaques.

Il s'agit d'insérer la signature dans l'image selon l'approche de tatouage réversible proposée, puis d'attaquer l'image et enfin de vérifier la présence de la signature.

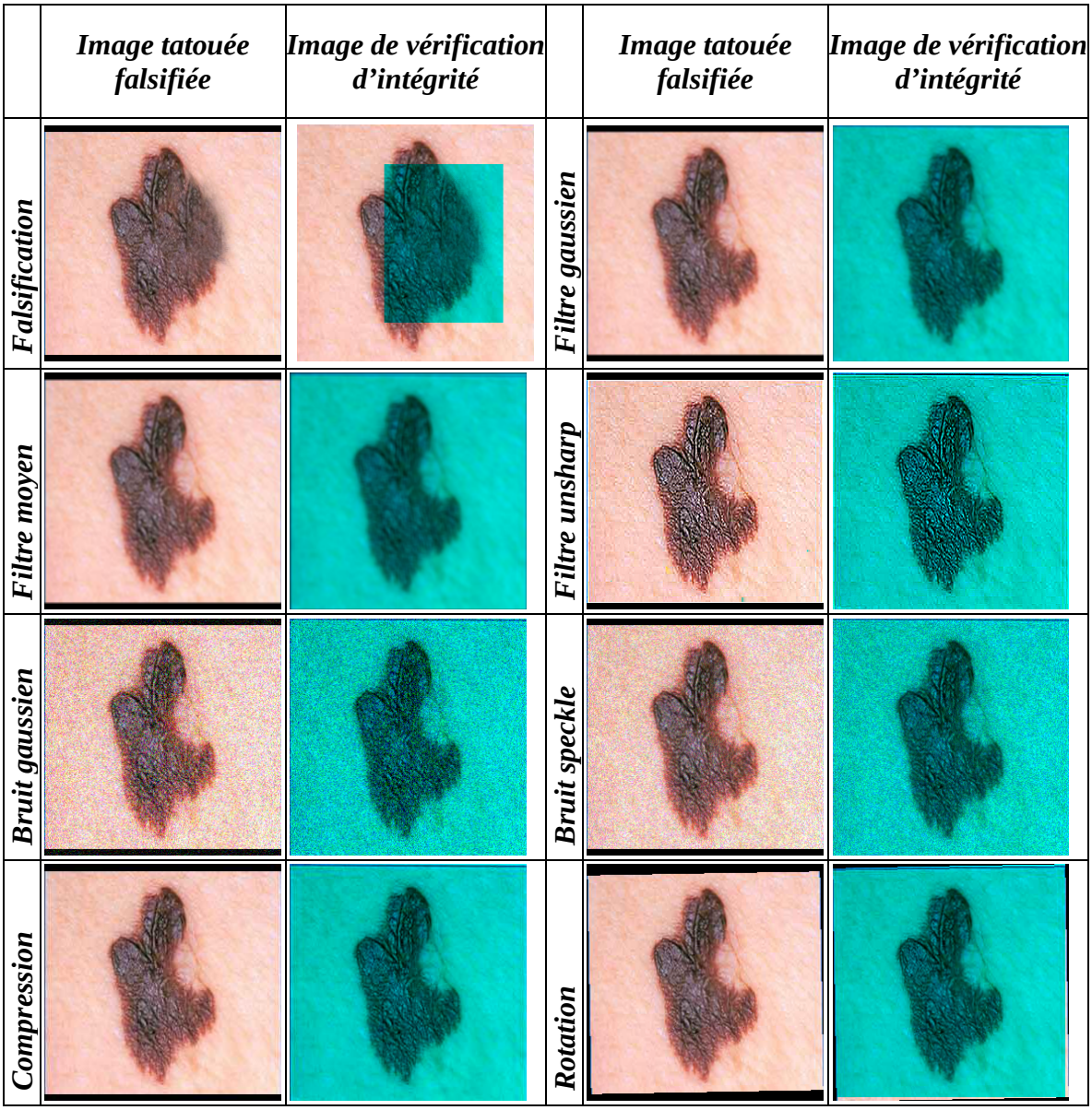


Figure 81. *Fragilité par rapport aux différentes attaques*

Les résultats obtenus dans la figure 81 montrent l'efficacité de notre approche et son aptitude à détecter et à localiser les différentes attaques que peut subir l'image tatouée lors de sa transmission.

La couleur joue un rôle majeur pour la précision de la nature de la lésion ; dans ce contexte nous avons changé la couleur du grain de beauté comme l'illustre la figure 82 et nous avons testé l'aptitude de notre approche à détecter et à localiser la modification apportée à l'image.

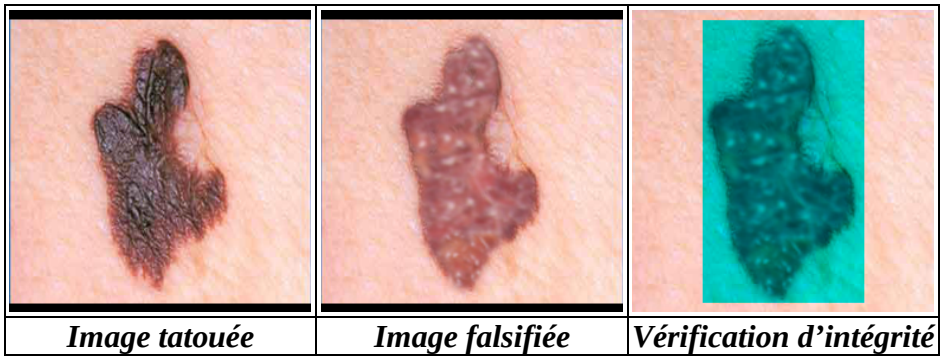


Figure 82. *Localisation des zones modifiées*

La partie dont la couleur est modifiée se présente bien sur l'image de vérification d'intégrité comme étant une zone colorée en cyan localisant la falsification avec une précision remarquable.

4.2. Qualité de l'image tatouée

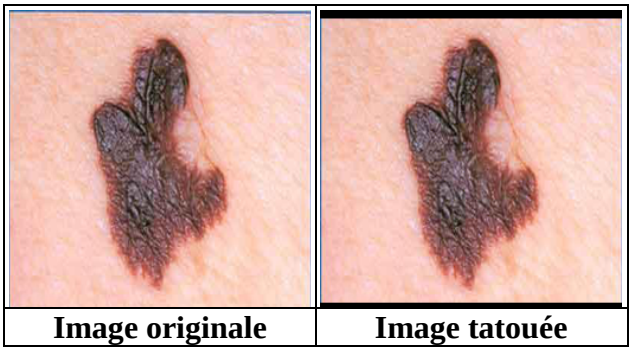


Figure 83. *Image originale et Image tatouée*

Pour les images médicales la signature doit être imperceptible : comme l'illustre la figure 83 : l'image tatouée devra être globalement similaire à l'image originale pour ne pas conduire à des interprétations erronées.

Il est également nécessaire d'évaluer la dégradation de l'image engendrée par le tatouage. Pour ceci nous effectuons des mesures de la qualité de l'image tatouée par calcul de PSNR pour chaque composante de l'image (cf figure 84).

Puisque l'on a seulement tatoué la composante bleue afin de quantifier la dégradation de l'image tatouée, nous ne calculons uniquement que le PSNR pour la composante bleue ***"B"*.**

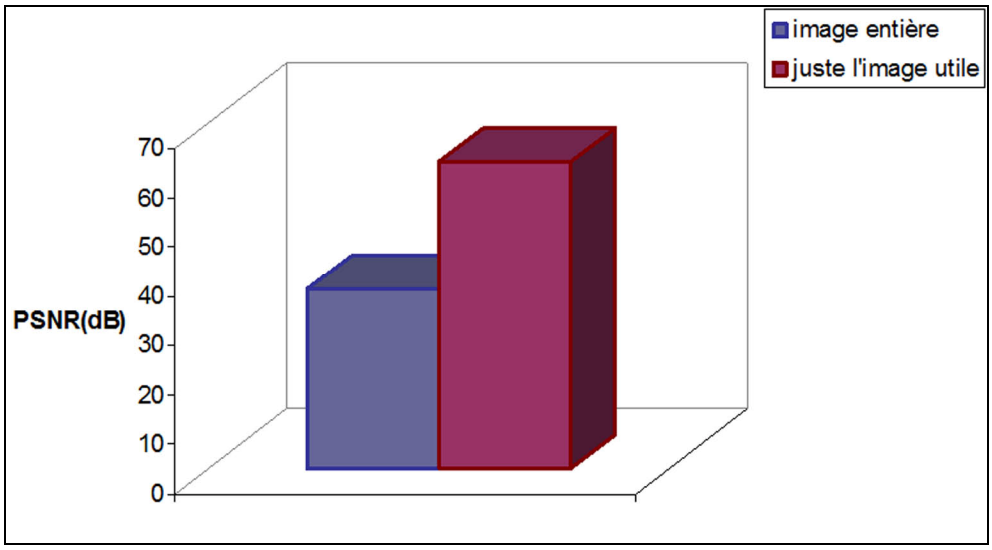


Figure 84. *Les valeurs moyennes du PSNR pour la composante "B" des 30 images tatouées*

Si l'on tient compte de la composante bleue de l'image tatouée entière (avec les bords modifiés), la valeur moyenne du PSNR pour la composante bleue des 30 images de mélanome tatouées reste toujours supérieure à 41 dB, ce qui donne une image qui peut être exploitable.

Pour l'image utile comportant l'information médicale ; la qualité de l'image tatouée est de très bonne qualité.

4.3. Réversibilité

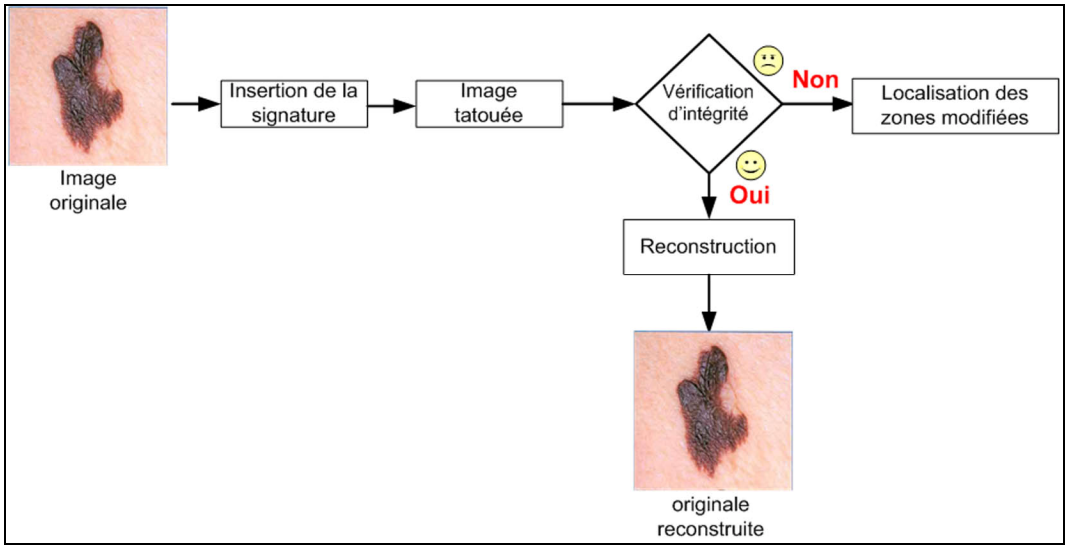


Figure 85. *Test de réversibilité*

Suite à la vérification d'intégrité, l'utilisateur est certain que l'image reçue est intacte et qu'elle n'a subit aucune modification au cours de sa transmission.

Grâce à la notion de réversibilité de notre approche, l'utilisateur est capable de reconstruire l'image originale (cf figure 85) pour faire ses interprétations en se basant sur cette dernière en

s’assurant qu’aucun détail (même infime) n’est modifié ou n’a disparu suite à l’insertion de la signature.

Conclusion

Dans ce chapitre nous avons étendu l’approche développée pour les images en niveaux de gris au domaine des images couleurs. Nous avons commencé par choisir l’espace colorimétrique d’insertion. Nous avons opté pour l’espace RGB compte tenu de sa dépendance aux matériels (cartes d'acquisitions, caméras, écrans, ...) qui effectuent leurs échanges d'informations en utilisant des triplets (R, G, B).

Par la suite nous avons choisi l’approche d’adaptation adéquate au passage du niveau de gris à la couleur. Nous avons utilisé l’approche marginale qui donne plus de liberté de choix des pixels à tatouer par plan de couleur.

Nous avons également validé l’approche développée pour les images couleurs en l’appliquant à plusieurs images médicales couleurs et en évaluant la qualité de l’image tatouée obtenue, la sensibilité de l’approche par rapport à différentes attaques, la précision de la localisation des zones modifiées et enfin la réversibilité.

Conclusions et Perspectives

Conclusion

Actuellement, plusieurs efforts se concrétisent pour développer de plus en plus les outils médicaux alliant technologies et médecine. Cette modernisation a permis une manipulation plus sûre et plus pratique, une transmission plus rapide, un stockage plus économique et une indexation plus efficace des informations médicales. Mais ce développement n'est pas sans dérive : le numérique a participé à la large expansion de la falsification et du piratage d'où la nécessité de chercher à développer des moyens et des techniques de protection. Le tatouage se présente ainsi comme étant une solution qui consiste en l'insertion d'une marque dans l'image permettant de vérifier son intégrité.

Dans le cadre de cette thèse de doctorat, nous avons présenté une méthode de tatouage réversible qui a permis d'assurer la vérification d'intégrité des images médicales tout en offrant aux utilisateurs (médecins) une copie intacte de l'image originale.

Dans la première partie de ce travail, nous avons commencé par étudier les problèmes de sécurité des images médicales, nous avons exposé les services de sécurité. Nous avons aussi mis l'accent sur le tatouage fragile, ses caractéristiques et les contraintes auxquelles il est soumis pour passer par la suite à démontrer la nécessité du tatouage réversible Nous avons présenté en détail ses caractéristiques, le schéma d'insertion, celui de détection pour ensuite énumérer les techniques de tatouage réversible les plus connues.

Dans la deuxième partie de notre travail nous avons développé dans un premier temps une nouvelle approche de tatouage réversible basée sur l'expansion de la différence entre deux pixels voisins. Puis nous avons appliqué cette technique sur 30 images médicales de 256 niveaux de gris de taille 256x256 pixels.

Nous avons pu montrer l'efficacité de cette technique pour la vérification de l'intégrité des images médicales et la localisation des zones modifiées tout en assurant une bonne qualité visuelle.

Dans un deuxième temps, nous avons prouvé que les performances de cet algorithme peuvent être améliorées significativement en tenant compte du voisinage du pixel. Dans ce cadre, nous avons testé les différents modèles de prédiction afin de trouver la technique optimale dans notre cas : pour notre objectif. En effet, nous avons appliqué les modèles linéaire, linéaire avec pondération et non linéaire. Nous avons prouvé que le modèle linéaire avec pondération est le modèle le plus adéquat. Nous avons utilisé différents critères d'évaluation dont en particulier le PSNR, l'EQM et le RFA.

Enfin, nous avons terminé cette partie par une comparaison de notre méthode avec cinq autres méthodes de tatouage réversible pour mettre en évidence les résultats très prometteurs issus de ce travail.

Dans la troisième partie, nous avons validé l'approche développée dans le cadre du projet Européen DECOPREME (DEpistage COllaboratif PREcoce des MElanomes).

Dans un premier temps, nous avons validé notre travail techniquement, une simulation d'un ensemble d'attaques est effectuée pour vérifier la présence de la signature après chaque attaque et s'assurer de l'aptitude de notre approche à détecter et à localiser les zones modifiées. Une étude de la qualité de l'image tatouée et de la réversibilité de notre approche est aussi effectuée.

Dans un deuxième temps, nous avons validé notre approche cliniquement en nous basant sur les avis des médecins spécialistes afin de vérifier que l'information médicale contenue dans l'image a été bien préservée après l'opération de tatouage.

Enfin nous avons généralisé aux images en couleur le schéma que nous avions élaboré pour les images en niveaux de gris.

Les principales contributions développées dans ce rapport concernent d'une part le développement d'un schéma de tatouage fragile réversible utilisant le domaine spatial, l'amélioration de l'imperceptibilité de la signature ainsi que le contournement du problème de dépassement. Et d'autre part, l'application de la nouvelle approche dans le cadre du projet Européen DECOPREME (DEpistage COllaboratif PREcoce des MElanomes). Ceci permet de

vérifier l'intégrité des images lors de leur transfert entre les points de connexion de la plateforme.

Perspectives

L'objectif de cette thèse et de mettre en place une nouvelle approche de tatouage réversible pour la vérification d'intégrité des images médicales utilisant une insertion de la signature dans le domaine spatial.

Le domaine spatial offrant une multitude d'avantages, il présente aussi des limitations et des inconvénients pouvant affecter l'efficacité du schéma du tatouage. D'ou la possibilité d'utiliser d'autre domaine comme le domaine multi-résolution : la transformée en ondelettes présente une haute flexibilité qui découle de la liberté de choix de la fonction d'ondelettes et de ses paramètres.

De ce fait, une **première perspective** consiste à utiliser ce domaine qui peut mener à des qualités de tatouages meilleures.

Comme le tatouage réversible est encore un domaine de recherche très récent, il convient de noter que ce type de tatouage offre plusieurs axes de recherche :

- D'une part, on peut étudier le tatouage réversible semi-fragile qui permet de tolérer des attaques bien définies, citons le cas des compressions JPEG et JPEG 2000 qui sont largement utilisées pour l'archivage et le stockage des images, notamment avec l'utilisation massive des modalités numériques en imagerie médicale qui engendre aujourd'hui des volumes de données de plus en plus importants.

- D'autre part, on peut également étudier le tatouage réversible pour des séquences vidéo. Cette extension paraît naturelle dans la mesure où l'on peut considérer une vidéo comme une succession d'images fixes.

  Cette représentation permet d'ajouter un niveau de redondance supplémentaire en répétant le tatouage dans les différentes trames de la vidéo ; ce qui nous offre un gain important en terme de capacité d'insertion. Mais il faudra tenir compte des problèmes de complexité et de temps de calcul si l'on souhaite tendre vers le temps-réel, indispensable pour les nouvelles applications numériques.

Un **autre volet de perspectives** touche l'adéquation des schémas de tatouage réversible dans le cas des images 3D qui sont de plus en plus omniprésents. Les modèles 3D sont utilisés par plusieurs applications et spécifiquement par la médecine (chirurgie assistée par ordinateur ou

à distance, aide au diagnostic, …). Ils peuvent être obtenus grâce à des procédés de numérisation tridimensionnelle d'objets physiques. Ils sont généralement représentés sous forme de maillages surfaciques ou volumiques. Ces modèles peuvent aussi être décrits par des nuages de points ou des surfaces implicites.

Enfin une **perspective sécurité** sera intéressante. La méthode de tatouage réversible proposée a permis en combinaison avec la fonction de hachage utilisée d'assurer l'intégrité de l'image médicale. On peut penser à introduire une technique de cryptographie dans le schéma de tatouage actuel assurant ainsi plus de confidentialité et plus de sécurité.

Bibliographie Personnelle

Articles en journaux

[FOU09] Imen FOURATI KALLEL, Mohamed Salim Bouhlel,Jean-Christophe Lapayre "Control of Dermatology Image Integrity using Reversible Watermarking“ *IJIST International Journal of Imaging Systems and Technology*,Vol 19,Issue 1, accepté en Novembre 2008,

[FOU08] Imen FOURATI KALLEL, Jean-Christophe Lapayre et Mohamed Salim Bouhlel "Medical Image semi fragile Watermarking In The Frequential Field" *JOTE Journal Of Testing and Evaluation* ,Vol 36,Issue 6,Novembre 2008 ISSN 0090-3973.

[FOU07a] I.Fourati , M.S.Bouhlel ,J.C Lapayre *"*Improved Tian's Method for Medical Image Reversible Watermarking*" ICGST International Journal on Graphics, Vision and Image Processing (GVIP),* Vol 7, Issue 2, July, 2007 ISSN 1687-3998.

Papiers en conférences

[FOU07b] Imen FOURATI KALLEL, Jean-Christophe Lapayre et Mohamed Salim Bouhlel "Nouvelle technique de tatouage réversible pour la vérification d'intégrité des images médicales" *Conférence Internationale: Sciences Electronique, Technologie de l'Information et des Télécommunications*, Hammamet 2007.

[FOU06a] Imen Fourati kallel, Mohamed Kallel, Mohamed Salim Bouhlel, "A Secure fragile Watermarking Algorithm for medical Image Authentication in the DCT Domain" *2nd IEEE International Conference on Information and Communication Technologies from Theory to Applications (ICTTA'06),* 24-28 April 2006, Damascus Syria, ISBN: 0-7803-9521-2

[FOU06b] Imen FOURATI, Jean-Christophe Lapayre et Mohamed Salim Bouhlel "Tatouage réversible des images médicales Communications Via Internet des documents numériques : Application: secteur médical": *Conférence Internationale. MCSEAI* 2006. 07-09-2006, Agadir, Maroc

[FOU06c] Imen FOURATI KALLEL, Mohamed Salim BOUHLEL "Tatouage semi fragile pour la vérification d'intégrité des images", *4ème International Conférence: Conférence Internationale. JTEA* 2006. 12-14 Mai 2006, Tunisie

[FOU05] Imen Fourati & Med Salim Bouhlel "Elaboration d'une nouvelle approche de Tatouage Fragile des images médicales" *Conférence Internationale : Sciences Electronique, Technologie de l'Information et des Télécommunications*, Mars 2005, Sousse. ISBN: 9973-51-546-3

Brevet

[BOU05] Mohamed Salim Bouhlel & Imen Fourati Kallel "Approche de tatouage semifragile "ATASEF" Brevet soumis à l'INNORPI, N° SN SN05335. Déposé le 31 Décembre 2005; Accépté le 30 Septembre 2007.

Bibliographie

[ABD03] Moez Abdelmoula, Mohamed Salim Bouhlel et Lotfi Kamoun "Nouvelle technique de crypto-compression pour la sécurisation de la transmission des images médicales" *Sciences Electronique," Technologies de l'Information et des Télécommunications*,M.S.Bouhlel, B.Solaiman et L.Kamoun ISBN 9973-41-685-6, Mars 2003.

[ADA00] ADAMS and KOSSENTINI, "Reversible Integer-to-Integer Wavelet Transforms for Image Compression: Performance evaluation and Analysis", IEEE *Transactions on Image Processing*, Vol 9, No 6, pp.1010-1024 June 2000.

[ALA04] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform, *" IEEE Transactions on Image Processing*, Vol. 13, No. 8, pp. 1147–1156, Aug. 2004.

[AMA89] M.AMADASUM, R. KING, "Textural features corresponding to textural properties" , *IEEE Transactions on systems, Man and Cybernetics*, Vol. 19, pp. 1264-1274,1989

[AND93] RJ.Anderson "The Classification of Hash Functions", *'Codes and Ciphers' , proceedings of Fourth IMA Conference on Cryptography and Coding*, pp83-93.

[AUG83] August Kerckhoffs. "La cryptographie militaire". *Journal des sciences militaires*, vol. 9, pp. 5–38, January 1883.

[BAR97] J. M. Barton. "Method and apparatus for embedding authentication information within digital data".*US patent application*, vol5,pp 646 -997 1997.

[BEN96] W. Bender, D. Gruhl, and N. Morimoto. Techniques for data hiding. *IBM Systems Journal*, Vol 35, pp 131-336, 1996.

[BOR04] J. C. Borie. Sécurisation d'images par cryptage : applications aux images médicales. Thèse de doctorat Université de Nîmes, 2004.

[BOU02] M.S. Bouhlel, H.Trichili et L.Kamoun, "Etude évaluative des systéme colorimétrique et leur adaptation aux applications de l'imagerie", *Revue de la Faculté de Science de Bizerte*, Vol 1, pp.69-92, Juillet 2002.

[BOU03a] Mohamed Salim Bouhlel, Hanène Trichili et Lotfi Kamoun "A Review of Watermarking Techniques, Applications, Properties and Domains" *Journal of testing and evaluation for applied sciences and engineering.* ISSN 0090-3973. Vol 31, N°4, Juillet 2003.

[BOU03b] Mohamed Salim Bouhlel, Hanène Trichili & Lotfi Kammoun *"*A Review of Watermarking Techniques, Applications, Properties and Domains*" Journal of testing and evaluation for applied sciences and engineering*. ISSN 0090-3973. Vol 31, N°4, pp 357 – 360, Juillet 2003.

[CEL02a] M. Celik, G. Sharma, A.M. Tekalp, E. Saber, *"*Reversible data hiding, *" Proceedings of the International Conference on ImageProcessing 2002*, Rochester, NY, September 2002.

[CEL02b] M.Celik, G.Sharma, A.M.Tekalp, and E.Saber. "Lossless generalized-lsb data embedding". *IEEE Transactions on Image Processing*, July 2002.

[CEL03] M.Celik, G.Sharma, A.M.Tekalp, and E.Saber. "Localized lossless authentication watermark (law)".*Proceedings of SPIE: Security and Watermarking of Multimedia Contents* , Vol. 5020 pp 70,January 2003.

[CHA00] Y. Chahir., "Indexation et Recherche par le contenu d'informations visuelles". Thèse de doctorat, Ecole Centrale de Lyon, 2000.

[CHA05] C. C. Chang, W. L. Tai, and M. H. Lin, "A reversible data hiding scheme with modified side match vector quantization", *Proceedings of the International Conference on Advanced Information Networking and Applications*, Vol. 1, pp. 947–952, Taiwan, Mar. 2005.

[CHA98] J. Chanussot. "Approches vectorielles ou marginales pour le traitement d'images multicomposantes" Thèse de doctorat, Université de Stanford, France, novembre 1998.

[CHC01] C. C. Chang, M.S. Hwang, and T-S Chen. "A new encryption algorithm for image cryptosystems". *The Journal of Systems and Software*, Vol 58 pp 83-91, 2001.

[CIE86] Cie 15.2. "Colorimetry, Second edition". Rapport Technique, Commission Internationale de l'´Eclairage, Vienne, Autriche, 1986.

[COA00] G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, and R. Collorec. "Relevance of watermarking in medical imaging", *Proceedings of IEEE EMBS International Conference on Information Technology Applications in Biomedicine 2000*, pp. 250–255, 9-10 Nov. 2000

[COA01] G. Coatrieux, B. Sankur, and H. Maître, "Strict integrity control of biomedical images, " *Security and Watermarking of Multimedia Contents III*, Vol. 4314 of *SPIE Proceedings*, San Jose, Calif, USA, January 2001.

[CRA98] S.Craver, N.Memon, B-L.Yeo, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications", *IEEE Journal on selected areas in communications*, Vol. 16, No 4, Mai 1998.

[DAU90] I. Daubechies, "The wavelet transform, time-frequency localization, and signal analysis", *IEEE Trans. Inform. Theory*, Vol. 36, No5, pp.961-1005, Septembre 1990.

[ELB06] E. Elbasi and A. M. Eskicioglu. "A Semi-Blind Watermarking Scheme for Images Using a Tree Structure". *IEEE Sarno Symposium*, March 2006.

[EKI04] Ö. Ekici and B. Sankur. "Comparative Evaluation of Semi fragile Watermarking Algorithms". *Journal of Electronic Imaging*, Vol 13 No 1 ,pp 209-216, January 2004.

[FEN05] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, "A new multi-secret images sharing scheme using largrange's interpolation, " *Journal of Systems and Software*, Vol. 76, No. 3, pp. 327–339, June 2005.

[FLE97] D. Fleet et D. Heeger. "Embedding invisible information in color images". *IEEE-ICIP'97*, Vol 1, pp 532–535, Santa Barbara (Cal) Usa, 1997.

[FRI01] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication" *in Proc. SPIE Conf. Security and Watermarking of Multimedia Contents III*, Vol. 4314, pp. 197–208, San Jose, Calif, USA, January 2001.

[FRI02a] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats, *" in SPIE Proceedings of Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, Vol. 4675,pp. 572–583, San Jose, Jan. 2002.

[FRI02b] J.Fridrich, M. Goljan, and R.Du. "Lossless data embedding - new paradigm in digital watermarking." *EURASIP Journal of Signal Processing*, Vol. 2002, No. 2, pp. 185–196, Feb. 2002.

[FRI04] J. Fridrich, M. Goljan, Q. Chen, and V. Pathak. "Lossless data embedding with file size preservation". *Security, Steganography, and Watermarking of Multimedia Contents*, pp 354-365, 2004.

[FRI98] J. Fridrich, "Image watermarking for tamper detection", *Proc. IEEE International Conference on Image Processing*",Vol. 2,pp. 404–408, Chicago, Ill, USA, October 1998.

[FRI85] R. J. Friedman., "Early detection of malignant melanoma: the role of physician examination and self examination of the skin". *CA*, Vol 35 pp.130-51, 1985.

[GAR05] E. Garcia, H. Guyennet, J.-C. Lapayre, S. Ramadass, R. Budiarto, N. Kassim, and M. Bouhlel. "Collaborative Telemedicine Components Integration in a Multimedia Conferencing System", *20th APAN Meeting: Advanced Network Conference*, Taipei, pp 59-67, August 2005.

[GET06] G.S.El-Taweel, H.M Onsi, M.Samy, and M.G. Darwish. "Secure and Non-Blind Watermarking Scheme for Color Images". *ICGST International Journal on Graphics, Vision and Image Processing*, SI1, 2005

[GUI03] Guillod J, Schmid-Saugeon P, Décaillet F, Panizzon R, Kunt M, Thiran JP. "An Open Internet Platform to Distributed Image Processing applied to Dermoscopy". *Stud. Health Technol. Inform*. Vol 95, pp.107-12. 2003.

[HAL95] P.N. Hall., "Computer Screening for early detection of melanoma: is there a future?". *British Journal of Dermatology,* Vol 132, pp 225-338, 1995.

[HSU99] C. T. Hsu and J. L. Wu. "Hidden Digital Watermarks in Images". *IEEE Transactions on Image Processing*, Vol 8(1), pp 58-68, 1999.

[JOL92] P. Joly, Ph. Lauret., "Mélanome Malin, Prévention et Dépistage". *Mélanome Malin. M. DELAUNY, Ed MASSON*. PARIS, 1992.

[JPC97] H. Y. Jung, R. Prost, and T. Y. Choi. "A unified mathematical form of the walshhadamard transform for lossless image data compression", *Signal Processing*, Vol 63. EURASIP, Dec. 1997.

[KAM05] L. Kamstra and H.J.A.M. Heijmans. "Reversible Data Embedding Into Images Using Wavelet Techniques and Sorting". *IP*, Vol 14,No12 ,pp 2082-2090,December 2005.

[KUN99] Kundur and Hatzinakos, "Digital watermarking for telltale tamper proofing and authentification". *Proc of the IEEE*, Vol 87, N°7, pp.1167-1180, Juillet 1999.

[KUN99] Kundur and Hatzinakos, "Digital watermarking for telltale tamper proofing and authentification". *Proc of the IEEE*, Vol 87, N°7, pp.1167-1180, Juillet 1999.

[KUT97] M. Kutter, F. Jordan, et F. Bossen. "Digital signatures of color images using amplitude modulation". *SPIE,EI97 Proceedings*, pp 518–526, San Jose, California USA, Février 1997.

[LAM02] P. Lambert, "Etudes méthodologiques du filtrage et de la segmentation des images multi-composantes", mémoire HDR, Université de Savoie, Juillet 2002.

[LEE03] A. Leest, M. Veen, and F. Bruekers, "Reversible image watermarking, " *Proceedings of the ICIP International Conference on Image Processing*, Vol. 3, pp. II-731-4, Barcelona, Spain, Sep. 2003.

[LEN01] A. Lenstra and E. Verheul. "Selecting Cryptographic Key Sizes". *Journal of Cryptology*, Vol 14,pp.255-293, 2001.

[MER90] RC. Merkle″A Fast Software One_Way Hash Function″ *Journal of Cryptology* Vol 3, No 1, pp 43-58.

[MIN97] F. Mintzer, G. Braudaway, and M. Yeung, "Effective and ineffective digital

watermarks, " *Proceedings of the IEEE International Conference on Image Processing*, pp. 9-12, Santa Barbara, California, October 1997.

[MIT99] T.Mittelholzer. "An information-theoretic approach to steganography and watermarking". IHW'99, Dresden, Germany, September 1999.

[NIS03] Z. Ni, Y. Q. Shi, N. Ansari, and S. Wei, "Reversible data hiding, " *ISCAS Proceedings of the 2003 International Symposium on Circuits and Systems* , Vol. 2, pp. 912–915, Thailand, May 2003.

[NIK99] N. Nikolaidis and I. Pitas. " Digital Image Watermarking: An Overview" *ICMCS*, Vol 1, pp 1-6, 1999.

[PRE93] B Preneel, ″Analysis and Design of Cryptographic Hash Functions″ Thèse de doctorat, Catholic University of Leuven 1993.

[RAD07] Cours radiologie 2007 http://freeinfo.tuxfamily.org/

[RAM05] A. Ramalingam and S. Krishnan. "Robust image watermarking using a chirp detection based technique" *IEEE Proceedings Vision, Image and Signal Processing*,Vol 152 .pp771_778, December 2005.

[REY02] C. Rey and J.-L. Dugelay. "Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité". *Revue Traitement du Signal, numéro spécial*, Vol. 18, no 4, France, Jun. 2002.

[RIV92] R. Rivest, "The MD5 Message-Digest Algorithm", *DDN Network Information Center*, http://www.ietf.org/rfc/rfc1321.txt, April 1992.

[RUA96] J.J.K.O Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking digital images for copryright protection", *IEE Proc.-Vis. Image Signal Process.*, Vol. 143, No 4, pp. 250-256, 1996.

[SAI96] A.Said and W.Pearlman. "An image multiresolution representation for lossless and lossy compression". *IEEE Transactions on Image Processing*, Vol5.pp 13036-1310, September 1996.

[SAY96] K. Sayood, "Introduction to Data Compression", Morgan Kaufmann, 1996, pp. 87-94.

[SCH03] *Schmid-Saugeon P, Guillod J, Thiran JP*. "Towards a Computer Aided Diagnosis System for Skin Cancer". *Computerized Medical Imaging and Graphics. Computerized Medical Imaging and Graphics*,Vol27,No1,pp 65-78, January 2003.

[SHA49] C.E. Shannon. "Communication theory of secrecy systems" *Bell system technical journal*, Vol 28, pp 656–715, October 1949.

[SHA97] G. Sharma et H. J. Trusell. " Digital Color Imaging " *IEEE Transactions on*

Image Processing, Vol6,No7, pp 901- 932, juillet 1997.

[SSS94] T. Schindwolf, R. Schiffner, W. Stolz, R. Albert., "Evaluation of different image acquisition techniques for a computer vision system in diagnosis of malignant melanoma". *Journal Am. Acad. Dermatol*.Vol 31, pp 34-41, 1994.

[TIA03] J. Tian. "Reversible data embedding and content authentication using difference expansion". *IEEE Transaction on Circuits and systems for Video Technology*,February 2003.

[TIA02] J. Tian, "Wavelet-based reversible watermarking for authentication" *Proceedings of SPIE Sec. and Watermarking of Multimedia Cont*, "ol. 4675, Janvier. 2002.

[TRE04] TRÉMEAU, A., FERNANDEZ-MALOIGNE, C. et BONTON, P. (2004). "Image numérique couleur : de l'acquisition au traitement" Dunod.

[TRI02] Trichili, H., Boublel, M., Derbel, N., Kamoun, L., "A new medical image watermarking scheme for a better telediagnosis", *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics 2002, 6*-9 Oct. 2002, Vol.1, pp. 556–559, 2002.

[VAR05] G. Lo-Varco, W. Puech, and M. Dumas. "Content Based Watermarking for Securing Color Images". *Journal of Imaging Science and Technology*, Vol 49, pp.450-458, 2005.

[VLE03] C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management" *IEEE Transactions on Multimedia*, Vol. 5,No. 1, pp. 97–105, Mar. 2003.

[WOL96] R. Wolfgang and E. Delp, "A watermark for digital images," Proceedings of the IEEE International Conference on Image Processing, Vol. 3, pp. 219-222, 1996.

[WON99] P. Wong, "A watermark for image integrity and ownership verification, " *Final Program and Proceedings of the IS&T PICS 99*, pp. 374-379, Savanna, Georgia, April 1999.

[WSS96] M.J. Weinberger, G. Seroussi, and G. Sapiro. "Loco-I: a low complexity, contextbased, lossless image compression algorithm." *roc. Of the IEEE Data Compression Conference*, pp141–150, 1996.

[XIA97] X.G.Xia, C.Boncelet ang G.Arce, "A multiresolution watermark for digital images" *IEEE-ICIP'97*, Vol 1, pp 548-551, Santa-Barbara USA, 1997.

[XUA04] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding based on wavelet spread spectrum" *Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing*, pp. 211–214,Italy, Sept. 2004.

[YAN04] B. Yang, M. Schmucker, X. Niu, C. Busch, and S. Sun, "Reversible image watermarking by histogram modification for integer DCT coefficients"

Proceeding of the IEEE 6th Workshop on Multimedia Signal Processing, pp. 143–146, Siena, Italy, Sept.2004.

[YEU97] M. Yeung and F.Mintzer, "An invisible watermarking technique for image verification" *Proc. IEEE International Conference on Image Processing*, Vol. 2, pp. 680–683, Santa Barbara, Calif, USA, October 1997.

[YUL00] G. Yu, C. Lu, H. Liao, and J. Sheu. "Mean Quantization Blind Watermarking for Image Authentication". *Proc. IEEE Int. Conf. on Image Processing*, Vol 3, pp706_709, 2000.

[ZAI04] J.M. Zain, L. P. Baldwin, and M. Clarke, "Reversible watermarking for authentication of dicom images" *Proceedings of the 26th Annual International Conference of the Engineering in Medicine and Biology Society*, pp. 3237–3240, USA, 2004.

Annexes