الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Projet de Fin d'Études

présenté par

GHRIBI Khadidja & ABDELLAOUI Asmaa

pour l'obtention du diplôme de Master en électronique spécialité Réseaux et Télécommunications.

Thème

Tatouage des images pour aide au télédiagnostic

Proposé par : Mme. BENBLIDIA Nadjia *Co-promotrice :* Mme. REGUIEG Fatma Zohra

Année Universitaire 2011-2012

Remerciements

Nous remercions ALLAH de nous avoir donné le courage, la patience, la santé, et la motivation d'entamer et de finir ce mémoire de fin d'études dans les meilleures conditions.

Nous tenons à remercier très chaleureusement les personnes qui ont contribué de près ou de loin à la réalisation de ce travail et particulièrement « nos parents ».

Notre promotrice Mm.BEN BLIDIA Nadjia de nous avoir proposé ce sujet, et pour son soutiens et ses conseils tout au long de ce projet. Ce projet qui a développé en nous une capacité de recherche et d'adaptation.

Nos sentiments de profonde gratitude vont à nos professeur qui tous au long de notre cursus nous ont transmis leur savoir sans réserve.

Tout notre respect et nos remerciement les plus sincères vont vers les membres de jury qui ont pleinement consacré leur temps et leur attention pour évaluer ce travail, qui espérons le sera à la hauteur de leur attente.

ABDELLAOUI Asmaa et GHRIBI Khadidja.

التي الهجمات بعض من لحمايتها الطبية الصورة في مائية علامة لوضع مخطط تنفيذ هو الأطروحة لهذه الهدف في المستخدمة التقنيات لمختلف النظرية الدراسة بعد،بعد عن التطبيب شبكة في نقلها أثناء لها تخضع أن يمكن المجال.

تم .والمتانة الإختفاء الهشاشة، مبدأ على العلامة تعتمد .ما صورة في علامة إدخال أساس على تعريفها يمكن يكون الثلاث الحالات في المائية العلامة واستخراج .ومتعددة وهشة، قوية لإدراجها أنماط ثلاثة إلى تقسيمها ,الواردة الصورة على المصادقة في الهشة التقنية كفاءة النتائج وأظهرت .الأصلية العلامة بوجود منظور نصف مبرمجة رسومية واجهة باستخدام النتائج هذه تستخرج .الهجمات بعض مع والمتعددة القوية والتقنية بMATLAB

المائية والعلامة القوية، المائية التوقيعات،الهجمات،العلامة الطبية، الصور حماية بعد، عن التطبيب :البحث كلمات الهشة.

Résumé :

L’objectif de ce mémoire, est la mise en pratique d’un schéma de tatouage pour la problématique de la sécurité des images médicales contre quelques attaques qu’elles peuvent subir lors de leurs transmission dans les réseau de télédiagnostic en télémédecine . Puis une étude théorique sur la sécurité des images médicales et l’état de l’art des techniques de tatouage. Le tatouage d’image se décrire comme l’insertion d’une marque dans une image. Dans de cadre de notre travail la signature à insérer repose sur les principes de l’invisibilité, la fragilité et la robustesse.il est décomposé en trois sous schémas ; l’insertion robuste, fragile, et multiple. L’extraction du tatouage dans les trois cas va être semi aveugle à la présence de la signature originale. Les résultats obtenus montrent une efficacité de la technique fragile pour la vérification de l’authentification, la technique robuste au but d’amélioration de PSNR pour quelques attaques simulées ainsi pour la technique multiple. Les résultats sont obtenue a partir d’une interface graphique programmée en MATLAB.

Mots clés : la télémédecine, la sécurité des images médicale, signature, attaques, robuste, tatouage fragile

Abstract : The objective of this thesis is the implementation of a watermarking scheme for the problem of security of medical images against some attacks that can undergo during their transmission in the network diagnostics to telemedicine, after a theoretical study on security of medical images and the state of the art of watermarking techniques.

Watermarking image be described as the insertion of a mark in the image. In framework of this proposed scheme, the insertion of the signature based on three principles; invisibility, fragility and robustness. It is decomposed into three schemas; insertion robust, fragile, and multiple. The extraction of the watermark in the three cases will be half blind on the presence of the original signature. The results of a fragile technique are performance in verification of authentication. The robust technique in view to improve PSNR for some simulated attacks the same with the multiple technique. The results are obtained from a graphical interface programmed in MATLAB.

Keywords: security of medical images, signatures, attacks, robust watermark, frangible watermark**.**

Listes des acronymes et abréviations

ATM	mode de transfert asynchrone
BMP	BitMaP
EEG	électro-encéphalo-gramme
EPS	Encapsulated Post Script
GIP	GraphicalInterchange Format
IDCT	transformation inverse en cosinus discrète
JPEG	Joint Photographic Experts Group
LPM	Log Polar Maping
LSB	Least Significant Bit
MSB	MediumSignificant Bit
MSE	medium square error
ORL	oto-rhino-laryngologie
PET	Positron émission tomographie
pixels	Picture element
PPP	pixels par pouce
PS	PostScript
PSNR	Peak Signal to Noise Ratio
RMN	résonance magnétique nucléaire
SRM	spectroscopie par résonance magnétique
SVH	système visuel humain
TCD	la transformation en cosinus discrète
TEP	tomographie par émission de positons

TFD	transformation Fourrier discrète
TFM	la transformée de Fourier Mellin
TIFF	Tagged Image File Format
TOD	Transformée en Ondelettes Discrète
TWD	transformation ondelette discrète
WPG	Word PerfectGraphic

Sommaire

Chapitre2 .*tatouage numérique des images*

Chapitre3 .*schéma proposé*

Chapitre4. *Implémentation des résultats*

Liste des figures

Liste des tableaux

Introduction générale

Suite au développement des technologies de l'information et de la communication, en particulier l'internet qui a facilité le partage et le transfert des données numériques , et grâce aux nouvelles formes de piratage de documents, la sécurité de l'information deviens un défi majeur. Parmi ces technologies la télémédecine, qui permet le partage et la reconnaissance des images médicales reçues, ce qui est primordiale d'avoir un système de sécurité qui protège ces images contre les attaques qui peuvent être subir lors de transmission par des malveillants.

Les images médicales sont des outils d'aide de décision pour les médecins, selon cette importance le système de protection doit être le plus possible robuste. D'autre part, il est important aussi de détecter n'importe quelle attaque pour l'authentification et l'intégrité de ces images, donc, le système doit être aussi le plus possible sensible.

Dans ce cas la question qui se pose : Est ce qu'il y a un compromis entre la fragilité et la robustesse d'un système de protection ?

Parmi les systèmes de sécurité, le tatouage numérique qui se repose sur l'insertion d'une marque (signature) qu'elle est une séquence semi aléatoire codé avec une clé sécrète k, ou bien un logo ou une image quelconque, soit une partie ou un niveau de l'image elle-même. Cette marque est insérée dans un plan bien précis de l'image médicale, le choix du plan est basé sur la robustesse et fragilité de tatouage ainsi que la visibilité de la marque. La séparation des plans de bites de l'image, c'est à dire la séparation des fréquences, se fait par l'application d'une transformation à l'image originale (TFD, TCD, TOD….), et l'insertion de la signature se fait par deux méthodes : additives et substitutives, à la réception ; la présence des informations sur l'image et le filigrane originale ainsi que la clé k dépend de mode d'extraction de tatouage. Le Choix d'un mode repose sur la complexité d'implémentation. Donc, Pour

garder la notion d'authenticité d'une image médicale reçue avec celle émise, il faut qu'on applique un tatouage fragile. Et pour garder l'importance d'envoyer une image médicale plus protégée et de recevoir une image moins altérée nous à prendre à appliquer un tatouage robuste.

Plus spécifiquement, on va essayer d'analyser un simple système de tatouage jouant sur la fragilité et la robustesse, et de trouver le compromis entre eux. A la fin on va conclure la méthode la plus performante pour l'application d tatouage en imagerie médicale.

En effet, Ce mémoire se décompose en quatre chapitres :

Dans le premier chapitre on définit les concepts de base d'une façon générale, débutants par la télémédecine (définition, types, matériels utilisées…etc.).En suite les différents concepts des images numériques et médicales; les différents attaques appliqués, et enfin les solutions proposées pour la bonne protection de ces images.

Dans le deuxième chapitre on va spécialisée sur une méthode de sécurité d'image médicale ensuite sur le schéma générale des blocs d'insertion et de détection du tatouage ainsi que l'état de l'art des techniques et des méthodes existantes.

Le schéma proposé sera détaillé dans le troisième chapitre, le système opère dans le domaine fréquentiel par transformée l'image en ondelette. Ce chapitre comporte également les différents tests et expérimentations réalisées afin de valider les méthodes d'insertion et d'extraction de la marque.

Le dernier chapitre présentera les différents résultats d'évaluation face aux différentes attaques ; évaluera le choix de la technique prenant en considération les paramètres qui ont des influences sur la technique proposé. Et nous allons décrire l'environnement de programmation ''MATLAB'' ainsi que l'interface d'application et les différentes fonctionnalités offertes par le système.

Nous terminerons par une conclusion générale en énonçant quelques perspectives.

Chapitre 1 la sécurité des images médicales

1.1 Introduction sur la télémédecine

L'évolution technologique dans le secteur des communications est en voie de changer les relations entre les individus et les collectivités ; C'est le cas de la télémédecine.

L'avènement des nouvelles technologies de l'information et des télécommunications permet d'envisager de nouvelles façons d'exercer la médecine, et d'offrir des services médicaux spécialisés ou ultra spécialisés dans des régions qui, jusqu'à maintenant, n'ont pu en bénéficier. Au cours des années à venir, des technologies de l'information et le déploiement, à grande échelle des réseaux de télécommunications, influencera considérablement les comportements individuels et collectifs. La télémédecine pourrait notamment modifier en profondeur les pratiques médicales et l'organisation des soins de santé offerts à la population. [1].

Le terme TÉLÉMÉDECINE signifie littéralement « médecine à distance » et a été inventé dans les années 70. Elle est définie par l'Organisation Mondiale de la Santé (OMS) en 1997 comme, la partie de la médecine qui utilise la transmission par télécommunication d'information médicale (images, comptes rendus, enregistrements, etc.), en vue d'obtenir à distance un diagnostic [2].

1.1.1 Définition général

La télémédecine est désormais considérée comme un acte médical à part entière. Il s'agit plus précisément, d'une forme de pratique médicale à distance en utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé [3].

1.1.2 Spécialités de la télémédecine

- Téléconsultation : consultation, diagnostic et suivi du patient à distance ;
- Télé-Expertise : demande d'un deuxième avis à un médecin référent (Médecin Expert) ;
- Téléassistance à domicile : téléalarme pour personnes âgées, femmes enceintes, handicapés...
- Téléassistance des voyageurs isolés : nautisme, montagne,...
- Télésurveillance : surveillance du patient à distance ;
- Téléformation (e-learning) : formation et enseignement médical à distance ;
- Télé-Medico-Social : encadrement du patient maintenu à domicile ;
- Télétransmission : transferts d'informations médicales entre professionnels de santé et patient (Réseaux de soins) ;
- Télé-Radiologie : interprétation d'examens radiologiques à distance (diagnostic et expertise) ;
- Télé-Chirurgie : opération chirurgicale assistée à distance par ordinateur ;
- Télé-Psychiatrie : consultation, diagnostic et suivi d'un patient par un psychiatre ;
- Télé-Staff : réunion de professionnels de santé en visioconférence.

1.1.3 Techniques de transmission utilisées en télémédecine

Les techniques suivantes ne s'excluent pas mutuellement : une application ou un service de télémédecine peut en employer une seule ou toute combinaison des trois [2].

a Transmission audio

La transmission audio est une application courante et bien connue, utilisée par exemple pour une consultation médicale entre un patient et son médecin, ou pour un échange d'avis entre deux médecins.

L'idée est simple mais efficace, et pourrait être appliquée dans n'importe quelle région un tant soit peu équipée en téléphones.

b Transmission de données

La transmission de données permet d'acheminer des données médicales de type statique (dossier médical, matériel de formation...) ou dynamique (fonctions vitales telles que rythme cardiaque, pression sanguine...).

c Transmission d'images

La transmission d'images concerne les images fixes (radiographies, etc.) ou animées (vidéo, etc.) qui ont des fins de consultation, d'interprétation diagnostique ou de visioconférence. Les plus couramment échangées dans la pratique actuelle de la télémédecine sont les images radiologiques, qui comprennent les différents types, l'image produite est analogique mais doit être numérisée pour une transmission efficace [2].

1.1.4 Avantages et inconvénient de la télémédecine

a Avantages

- Influx sur le développement de la volonté politique, professionnelle et industrielle et Facilite la collaboration et améliore les différents réseaux de soins en incitant la bonne volonté.
- Permet accès à des compétences sortant du cadre de connaissances de son médecin et avoir plusieurs avis en même temps et en temps réel avec formation continue des médecins.
- Evite les déplacements inutiles et élimine la redondance des actes et des examens avec un meilleur control de dépenses.
- la télémédecine trouve une solution pour les pays sous-développés. [4]

b Inconvénients

- Hétérogénéité des besoins ; Budget disponible, Spécialisation du médecin, Préférences d'interfaces

- Problèmes d'infrastructure aux niveaux gouvernementaux ; Equiper les villes de réseaux, Subvention d'équipements
- Problèmes habituels des nouvelles technologies, Scepticisme quant à son intérêt et son utilité, Le manque de volonté de changer de médecins, Beaucoup de questions juridiques et éthiques. [4]

1.1.5 Conclusion

La télémédecine est la technologie qui s'occupe d'envoyer un dossier médicale d'un patient, dans notre travail on s'intéresse à la transmission des images médicale ; par la connaissance de l'image médicale.

1.2 Image numérique

1.2.1 Définition

L'image numérique est définie par le nombre de points dite la composant. Cela correspond au nombre de pixels qui compose l'image en hauteur (axe vertical) et en largeur (axe horizontal).

Il existe deux sortes d'images numériques : les images vectorielles et les images matricielles (figure1.1). Dans une image vectorielle les données sont représentées par des formes géométriques simples qui sont décrites d'un point de vue mathématique (exemple : un cercle définit par la position de son centre ainsi que son rayon).L' image matricielle est formée d'un tableau de points ou pixels. Plus la densité des points sont élevées, plus le nombre d'informations est élevé et plus la résolution de l'image est aussi élevée en effet, les images vues sur un écran de télévision ou une photographie sont des images matricielles) [5].

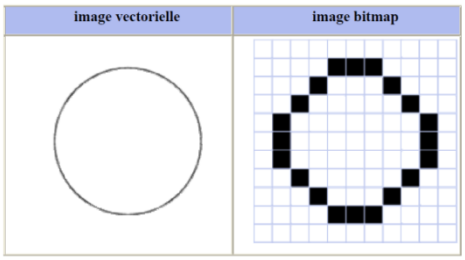


Figure1. 1Comparaison d'un grossissement d'une image vectorielle et d'une image Bitmap

1.2.2 Notion de pixel

L'image numérique est découpée en de nombreux petits points appelés **pixels**, abréviation de " picture element " qui signifie " élément d'image ". Pour chaque élément, on attribue une intensité lumineuse. La qualité de l'image dépend d'une part du nombre de pixels, et d'autre part du nombre de valeurs possibles pour l'intensité (tons).la figure1.2 montre l'effet de changement de nombre de pixel.

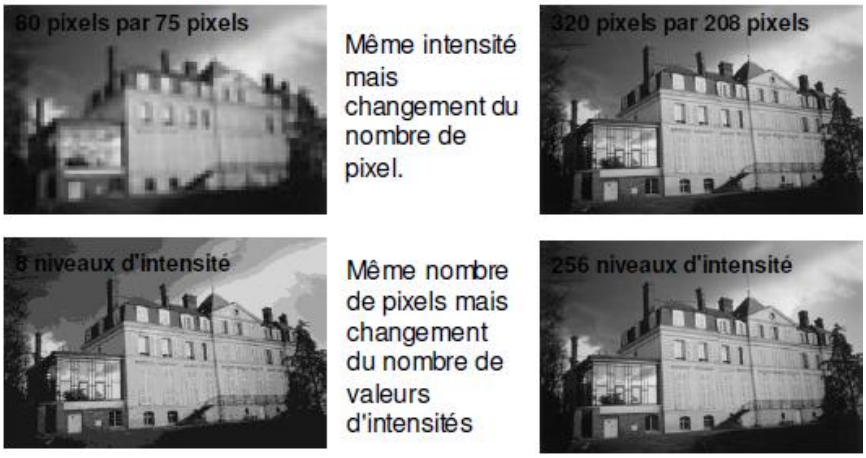
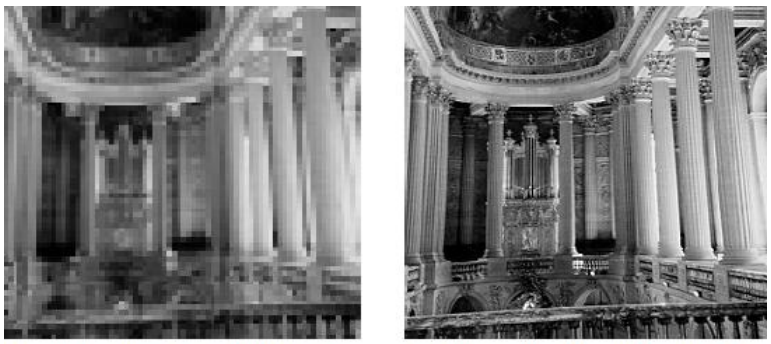


Figure1. 2 Influence de nombre de pixel et niveaux d'intensités sur une image numérique

1.2.3 Résolution d'une image

La résolution d'une image est le nombre de pixels par pouce (ppp) sachant que 1 pixel mesure 0,1 mm (figure 1.3) [5]



18 pixels par pouce soit environ 7 pixels par cm dans ce cas on observe l'effet de pixelisation

72 pixels par pouce soit environ 30 pixels par cm.

Figure1. 3 Même image avec deux résolutions différentes.

1.2.4 Plages de couleur d'une image

La plage de couleur (plage dynamique) est la gamme de différence tonale entre le blanc le plus clair et le noir le plus foncé d'une image. Plus la plage est large, plus le nombre de valeurs pouvant être représentées est grand [5].

Selon la figure 1.4 l'image est obtenue par superposition de trois rayonnements lumineux : le rouge (R), le vert (V) et le bleu (B). Une image couleur est typiquement représentée par une profondeur de bit variant de 8 à 24 bits ou plus. Dans une image 24 bits, les bits sont souvent divisés en 3 groupes : Huit pour le rouge, Huit pour le vert et Huit pour le bleu. Les combinaisons de ces bits servent à représenter les autres couleurs, ainsi qu'une image à 24 bits offre 16,7 millions de valeurs de couleurs.

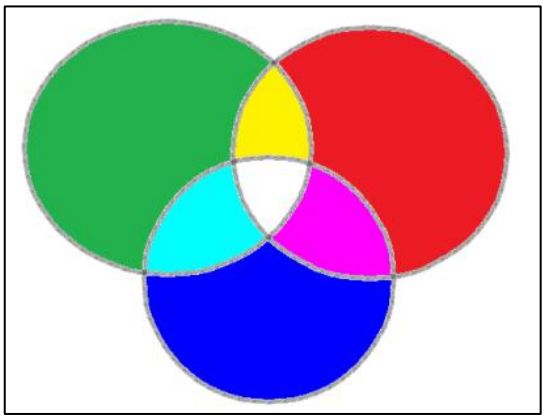


Figure1. 4 Schéma des couleurs principales dans une image numérique

1.3 Image médicale

1.3.1 Introduction

L'imagerie médicale regroupe ensemble des techniques utilisées par la médecine pour le diagnostic mais aussi le traitement d'un grand nombre de pathologies. Elle a révolutionné la médecine en donnant un accès immédiat et fiable à des informations jusqu'alors « invisibles » au diagnostic clinique, comme par exemple aux caractéristiques anatomiques, voire même à certains aspects du Métabolisme (imagerie fonctionnelle) des organes [6].

1.3.2 Principes physiques des différents procédés utilisés en imagerie médicale

a Rayons X

Les rayons X (RX) sont des ondes électromagnétiques (de même nature que les ondes de lumière mais plus énergétiques). Ils ont la propriété d'être atténués par toutes sortes de substances, y compris les liquides et les gaz. Ils peuvent traverser le corps humain, où ils seront plus ou moins atténués suivant la densité électronique des structures traversées [6].

b Ultrasons

Les ultrasons sont des ondes sonores imperceptibles à l'oreille humaine. Ils sont absorbés ou réfléchis par les substances qu'ils rencontrent. Le temps qu'ils mettent à revenir à la sonde qui les a émis (écho) est fonction de la distance à laquelle se trouve l'objet. [6].

c Résonance magnétique nucléaire

Sous l'effet d'un champ magnétique intense, la résonance des noyaux d'hydrogène, élément présent en abondance dans l'eau et les graisses (80% du corps humain), on peut visualiser la structure anatomique de nombreux tissus (IRM anatomique). La résonance des noyaux d'hydrogène induite par la présence d'hémoglobine permet par exemple de suivre le trajet du sang dans le cerveau [6].

d Isotopes radioactifs

En introduisant des molécules radioactives dans le corps humain, il est possible de suivre leur trajet au moyen d'une caméra qui détecte leur rayonnement lumineux. Les éléments qui émettent de simples photons sont détectables par des gamma-caméras [6]

1.3.3 Matériels utilisé pour l'imagerie médicale

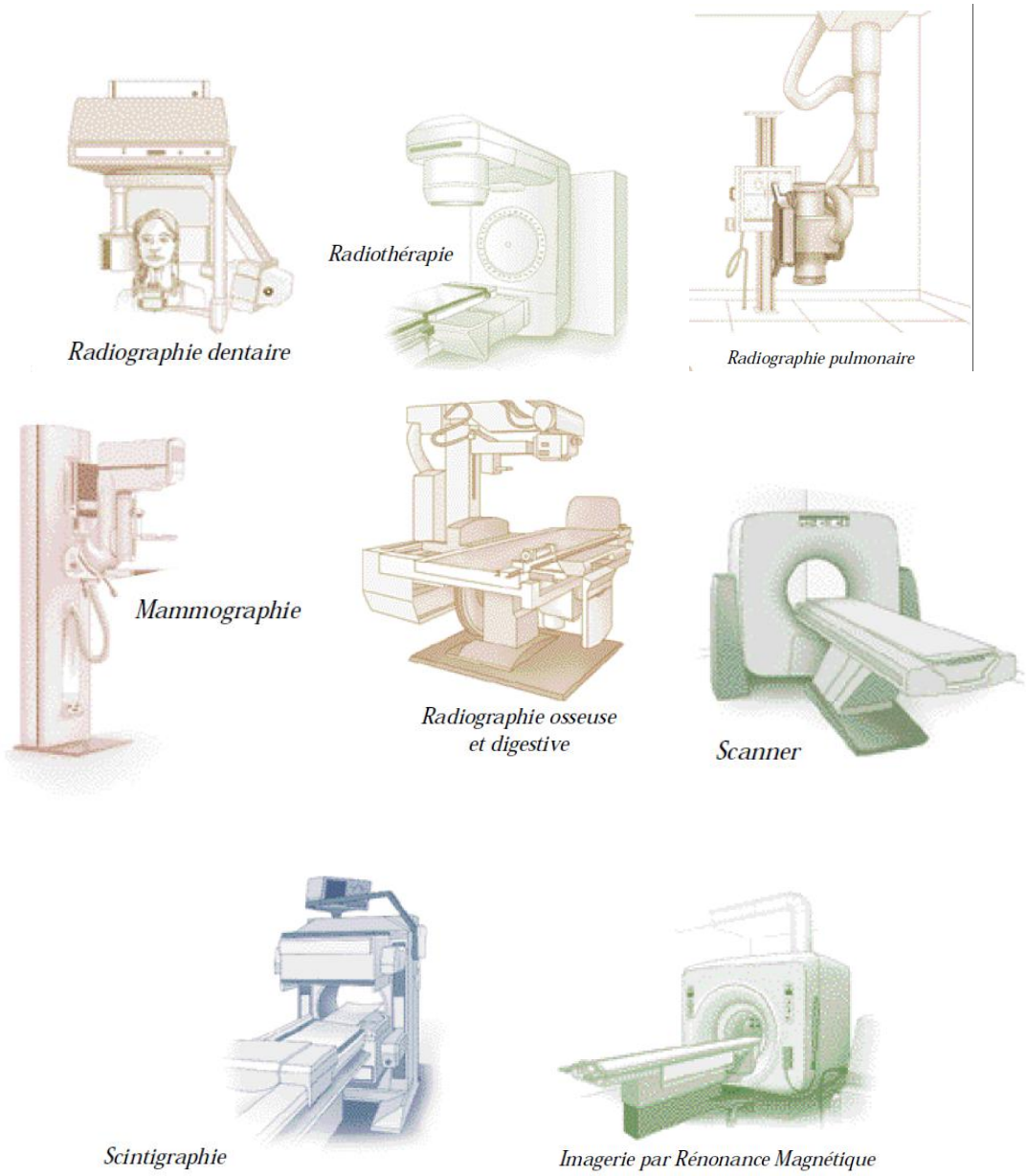


Figure1. 5 matériels utilisés pour l'image médicale

La protection des images médicales lors de leurs transmissions est un facteur nécessaire pour la confidentialité, l'authentification et l'intégrité contre les attaques ; pour cela des services de sécurité devraient être placés

1.4 Attaques sur les images dans les réseaux de télédiagnostic

Les attaques sur les images dans les réseaux de télédiagnostic Sont toute manipulation de l'image qui risque de nuire au processus de détection ou d'extraction de la marque qui s'y cache est considérée comme une attaque du système de marquage. Il se classifie en quatre catégories [7]

1.4.1 Attaques destructives

Ce type d'attaques vise à effacer la marque de l'image. Ces approches considèrent la marque comme un bruit additif au niveau de l'image et appliquent des transformations afin de réduire ou d'éliminer ce bruit tout en préservant une qualité acceptable de l'objet. Parmi les méthodes utilisées on retrouve le dé-bruitage, la compression avec perte et la quantification.

1.4.2 Attaques géométriques

Parmi ces types d'attaques on peut citer les zooms, les décalages, les changements d'échelle et les rotations. Ce type d'attaque dénature peu une image conservant ça qualité visuelle. Plusieurs outils permettant de simuler ce type d'attaques sont actuellement disponibles; le plus connu est Stirmark et UnsignStirmark crée des déformations géométriques locales.

1.4.3 Attaques cryptographiques

Ce type d'attaques s'appuie sur une recherche exhaustive et approfondie afin de trouver le secret de la marque ou une faiblesse du système de marquage.

1.4.4 Attaques de protocole

Ce type d'attaques ne vise ni la destruction de l'information insérée ni l'empêchement de sa détection. Par contre, il vise le concept même de l'application du «watermarking» en introduisant de l'ambiguïté dans le processus de détection et de décision. Ainsi, si la marque insérée apporte la preuve du droit d'auteur, l'attaquant

peut rajouter sa propre marque aux données du document et prétendre être le propriétaire de ces données, ce qui peut créer l'ambiguïté quant à l'identification du véritable propriétaire.

1.5 Services de sécurité

La Cryptographie, stéganographie, hachage et tatouage sont les garants actuels de l'authentification, de l'intégrité et de la confidentialité des données médicales (Figure1.6) [8].

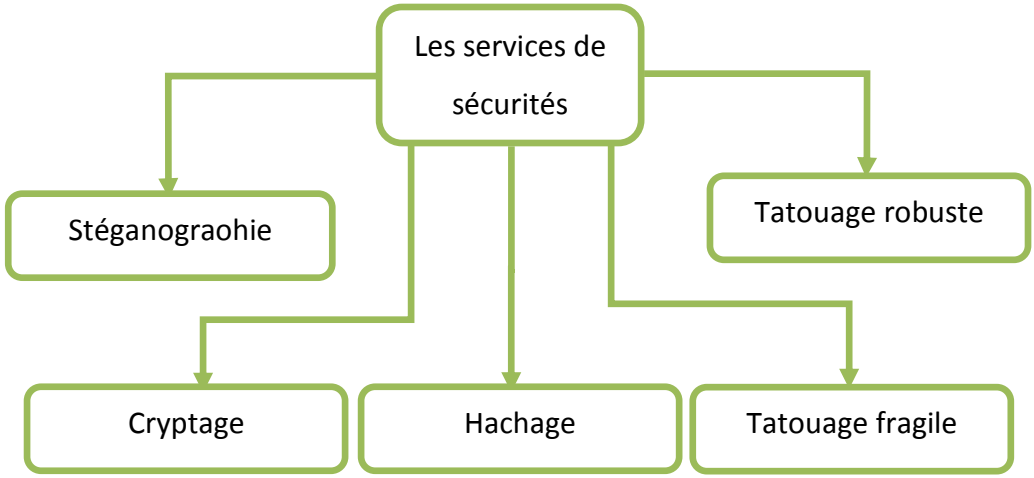


Figure1. 6 Services de sécurité de l'image médicale

1.5.1 Stéganographie

La stéganographie [9] [10] 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.

1.5.2 Cryptage

Le cryptage consiste à transformer un texte normal en un texte inintelligible appelé texte chiffré montré dans la Figure1.7 [11] [12] [13]. 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.

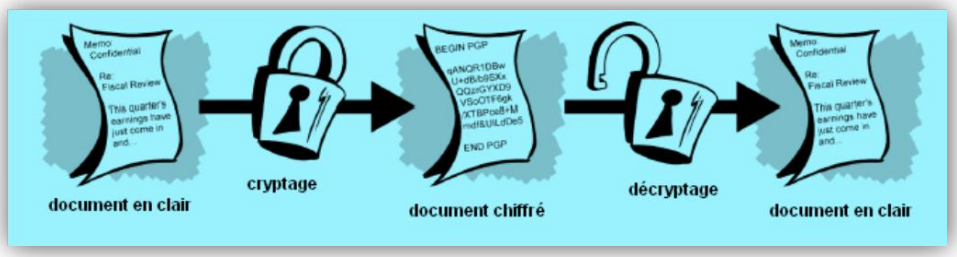


Figure1. 7 Schéma de cryptage

1.5.3 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) [14] [15].la Figure 1.8 montre L'ensemble haché est le résumé du document et le document est transmis. Il est impossible de récupérer le résumé d'un document pour le joindre à un autre document ou d'altérer le document original. La moindre modification apportée entraîne l'échec du processus de vérification.

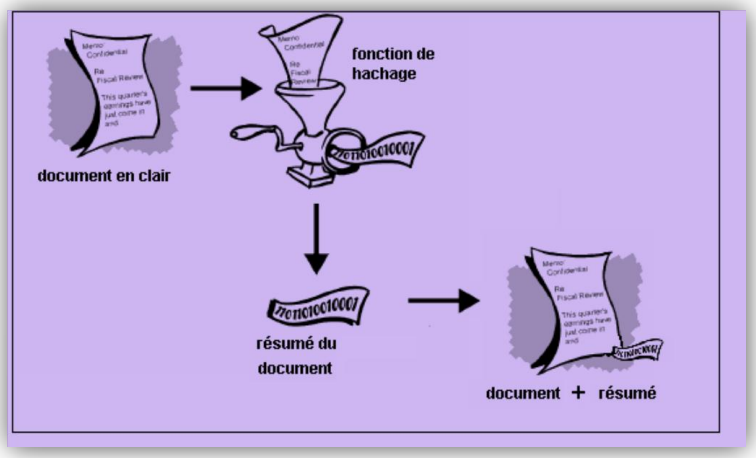


Figure1. 8 Schéma de hachage

1.5.4 Tatouage

Le tatouage numérique est l'art de cacher une signature dans un document [16] [17] [18]la Figure 1.9 résume le procédé d'insertion. Cette marque invisible ou non aura des caractéristiques propres à chaque domaine d'utilisation (robustesse,

réversibilité, capacité ...). 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.

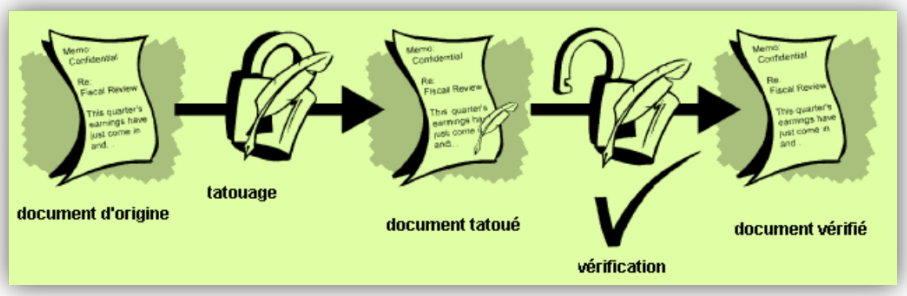


Figure1. 9 Schéma de tatouage

1.6 Classification des services de sécurité

On peut classer les différents services de sécurité selon les facteurs ;confidentialité, intégrité et authentification le tableau 1.1 résume la comparaison entre ces services :

1.6.1 Confidentialité

Action de conserver le caractère privé et secret d'un élément pour toutes les Personnes non autorisées

1.6.2 Intégrité

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

1.6.3 Authentification

C'est d'insérer dans un document image une marque qui puisse authentifier le document ou apporter la preuve que le contenu de ce document n'a pas été modifié depuis cette insertion.

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

Tableau1. 1 Comparaison entre les différents services de sécurité

1.7 Conclusion

Dans ce chapitre on a présenté les différents concepts de la télémédecine, des notions principales sur l'image numériques et l'image médicale et les différents services de sécurité des données médicale. Ce chapitre pose une problématique sur la sécurisation des échanges des images médicales en télémédecine dont trois méthodes sont proposées.

Le prochain chapitre s'interesse au tatouage d'image comme service de sécurité par présentation l'état de l'art des différentes techniques existantes.

Chapitre 2 Tatouage des images

2.1 Introduction

L'apparition de la révolution numérique et l'accessibilité des nouvelles technologies de l'information au grand public ont entraîné un volume d'échange de documents multimédias de plus en plus grandissant. Malgré les mécanismes de sécurité classiques, tels que la cryptographie, qui protègent les données multimédias lors de leur acheminement, les risques de fraude, de manipulation et de piratage constituent de réelles menaces lorsque les données sont à la source ou à la destination. Ces données sont faciles à pirater, à modifier et à rediffuser sans aucune perte de qualité perceptible. La protection des données multimédias est une nécessité incontournable si on veut assurer la qualité des services offerts. En ce sens, les développements récents qu'ont connus les techniques de marquage numérique ou watermarking des données sont prometteurs.

2.2 Définition de tatouage d'image

Le tatouage d'images est une technique récente apparue à la fin des années 80. Le premier article introduisant le terme tatouage, digital watermarking en anglais, fut présenté par Komatsu et Tominaga [19] en 1988. Le début des années 1990 a vu la publication d'un nombre modéré d'articles, entre 5 et 10 par an, jusqu'en 1995. Ensuite, un nombre croissant d'articles fut publié avec un doublement tous les ans [20]. L'International Society for Optical Engineering (SPIE) a créé dès lors une conférence spécifique dédiée à la sécurité et au tatouage pour les contenus multimédia en 1999. L'exploitation commerciale des techniques de tatouage a réellement commencée avec la création de la société Digimarc en 1995. [21] a sorti son premier logiciel de tatouage en 1996 et a depuis réussi à l'imposer à de nombreuses sociétés telles que Adobe, Macrovision ou encore Philips Electronics. En

outre, Digimarc fournit aussi ses solutions de tatouage à des sociétés gérant des bases de données images telles que Corbis [22] ou Getty Image [23].

Le tatouage d'image peut être décrit comme l'insertion d'une marque (une signature, un message, une image...) dans une image la figure 2 .1 montre un exemple de tatouage visible et invisible.

Figure2. 1 Exemples de tatouage invisible et visible

Des logiciels ont donc été développés dans le but de tester la résistance des signatures insérées dans les images. On peut citer Stirmark et Unzign qui sont les plus utilisés. Le logiciel Stirmark fait subir à l'image des déformations géométriques dans le but de tester la robustesse du tatouage. Le Logiciel Unzign permet quant à lui de modifier la valeur locale des pixels de l'image. La variation des pixels est aléatoire, ce qui correspond à un ajout de bruit sur l'image [24] [25].

2.3 Propriétés d'un système de tatouage

Il existe trois propriétés généralement utilisées pour décrire les systèmes de tatouage .

2.3.1 Robustesse

La robustesse représente la capacité du tatouage à résister à une modification intentionnelle ou non de l'image et qui permet encore la détection de la signature.

Un marquage robuste garantit une protection de la marque en résistant à des manipulations qu'elles soient malicieuses ou innocentes. Si la marque robuste a été détruite, il faut que cette opération entraîne une détérioration significative de l'image en question. En général, la robustesse de la marque est renforcée en augmentant l'intensité (ou l'énergie) de la marque insérée. Cependant, cette amélioration se fait au

détriment de l'invisibilité, d'où le compromis invisibilité-robustesse à prendre en compte dans tout algorithme de marquage [26].

a Notion de fragilité

Étant donné une image marquée avec la marque W, cette marque W est dite fragile si sa détection échoue à la moindre modification des pixels de l'image. Cette marque est dite semi fragile si sa détection échoue lorsque l'image a subi une modification majeure ou une manipulation non acceptable. Il est clair qu'une marque fragile ne peut être en même temps robuste puisque les deux contraintes sont contradictoires. Les algorithmes de marquage fragile utilisent souvent des fonctions de hachage ou de signature numérique [26].

2.3.2 Imperceptibilité

L'imperceptibilité est le fait que l'image signée est plus ou moins proche, au sens visuel, de l'image originale. La qualité de l'image tatouée peut aussi être évaluée à l'aide d'outils tels que le PSNR. Etant donné la recherche d'invisibilité de la marque, il est important d'évaluer la différence de perception visuelle entre l'image originale et l'image tatouée [26].

- ***Notion d'invisibilité***

L'invisibilité de la marque représente un critère important. Il s'agit de faire en sorte que l'impact visuel du marquage soit le plus faible possible afin que l'image marquée soit perçue comme fidèle à l'image originale. Plusieurs auteurs proposent de mesurer le degré d'invisibilité en calculant le PSNR (Peak Signal to Noise Ratio) de l'image marquée. Il s'agit de comparer l'image originale et l'image marquée pixel à pixel et de mesurer la distorsion entre les deux par la formule (2.1) et (2.2).

$$\mathrm{PSNR}_{\mathrm{dB}} = 10\log_{10}\frac{MN\max I(m,n)^2}{\sum_{m,n}(I(m,n)-I^*(m,n))^2} \qquad 2.1$$

ou bien

$$\mathrm{PSNR}_{\mathrm{dB}} = 10\log_{10}\frac{MN(255)^2}{\sum_{m,n}(I(m,n)-I^*(m,n))^2} \qquad 2.2$$

Les images sont de taille *S=M* x *N*et *I (m, n)* est la valeur du pixel *(m, n). I* et *I** indiquent l'image originale et l'image marquée respectivement. Généralement une valeur de *PSNR* supérieure à 34 dB représente une image marquée de bonne qualité.

2.3.3 Capacité

La capacité du schéma de tatouage doit aussi être prise en compte. Elle représente la quantité d'informations que l'on peut insérer. Les besoins en capacité d'insertion ne sont pas les mêmes en fonction du but recherché lors du tatouage de l'image [26].

- ✓ Ces trois propriétés, la robustesse, l'imperceptibilité et la capacité sont intimement liées. Un compromis doit être trouvé entre ces 3 paramètres. En effet, lorsque l'on augmente la quantité d'informations du message inséré, on aura tendance à dégrader plus fortement l'image originale ou à diminuer la résistance du message. P.Bas propose le schéma si dessous (figure2.2) illustrant l'imbrication de ces trois propriétés. Il montre comment ces trois paramètres influent les uns sur les autres. Il explique que si une image tatouée I1 appartient à une surface S1, l'ajout de robustesse diminuera la capacité et l'imperceptibilité de la signature. De plus, si la contrainte d'imperceptibilité est moindre (surface S2), une même diminution de l'imperceptibilité δi permettra d'obtenir des gains en capacité et en robustesse (δc et δr) plus importants que dans le premier cas [26].

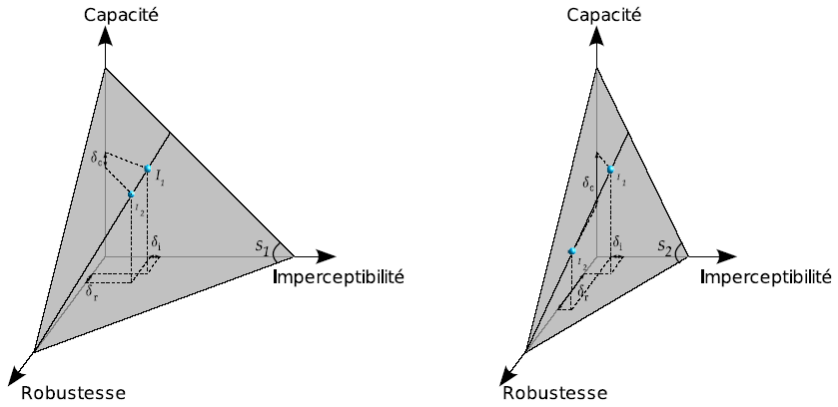


Figure2. 2 Illustration graphique du triangle des contraintes en tatouage d'images selon Bas

2.4 Schéma général du tatouage d'images

La plupart des algorithmes de tatouage reposent sur le même modèle et diffèrent seulement par des stratégies spécifiques à certains niveaux du processus d'insertion ou de détection. Il est donc possible de présenter d'une façon générique le tatouage d'images. Selon la figure 2.3 on peut diviser le processus de tatouage en quatre blocs principales : le bloc de création et d'insertion de marque, le bloc d'extraction et en fin, le bloc de détection. Les blocs de l'insertion et l'extraction de la marque décident les caractéristiques des autres blocs et ils sont les plus importants [27].

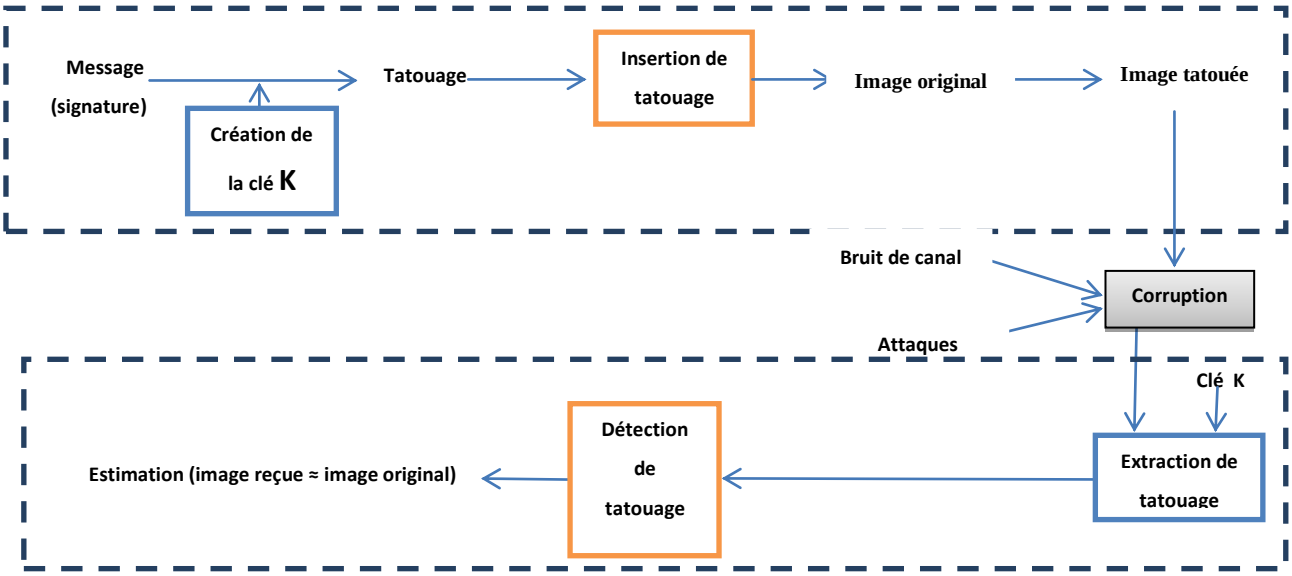


Figure2. 3 Schéma général de tatouage d'image.

Remarque

- Le tatouage informé est d'utilisé l'image original dans la construction de signal tatoué.
- Dans le tatouage multiple plusieurs tatouage sont insérés (plusieurs utilisateurs).

2.4.1 Bloc d'insertion de tatouage

a Création de la marque

Le tatouage est soit un logo soit une séquence de bits aléatoire. Il existe beaucoup d'algorithmes utilisant une séquence ayant la distribution Gauss comme sa

marque. Par exemple, ce sont des algorithmes de Marco Corvi&GianucaNiochiti, Rakesh Dugad, … Un autre type de marque le plus utilisée par son évidence est un logo. C'est une petite image qu'on traite comme une marque. Avant d'insérer à une image, on applique souvent un codage avec une clef K pour augmenter le secret .la fonction de génération de la marque est en fonction de message informatif et la clé K une clé privée contrôlant le processus de génération et structuration [27].

b Insertion de tatouage

La marque est insérée directement à l'image ou sa forme transformée. Pour obtenir la robustesse de tatouage Il faut insérer à la forme transformée. Il existe de nombreuses transformations différentes, on peut noter ici la transformation Fourrier discrète (TFD), la transformation cosinus discrète (TCD), la transformation ondelette discrète (TWD)… et chacune d'elles a des avantages pour contre quelques types d'attaques, Les deux dernières transformations possèdent plusieurs fortes caractéristiques dans laquelle on peut exploiter afin d'obtenir un bon algorithme de tatouage. A côte d'utilisation de domaines transformés, pour plus renforcer la robustesse, le modèle de psychovisuels humaine s'applique pour accroître l'invisibilité de la marque. Ce modèle vient de la recherche de la capacité de vision humaine et en basant des points faibles des yeux, on peut l'insérer plus d'information mais sans conduire à l'observation des changements [27]. Quelques auteurs ont combiné ces caractéristiques en vue de créer un masque afin de déterminer le maximum nombre de bits qui peuvent être changé dans chaque région de l'image.

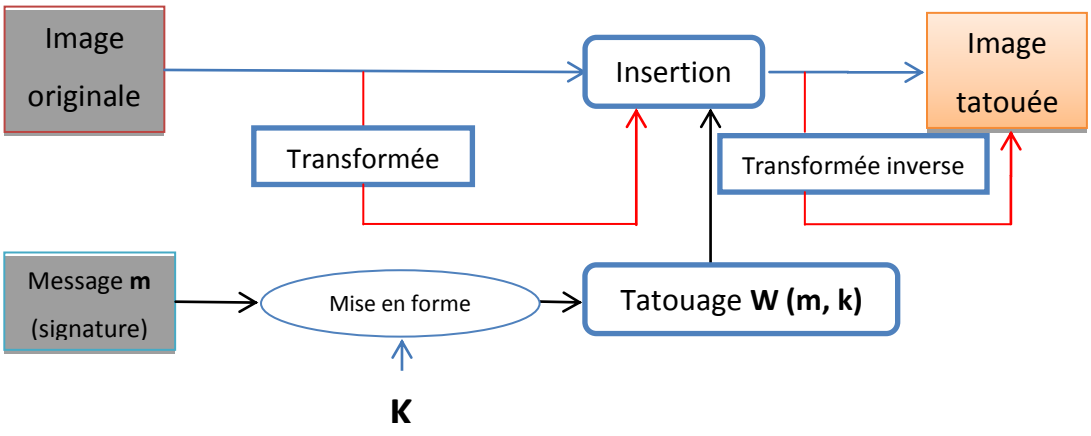


Figure2. 4 Procédé d'insertion

2.4.2 Bloc de détection de tatouage

a Extraction de tatouage

Il existe plusieurs modes pour l'extraction du tatouage : le mode non-aveugle, le mode semi-aveugle et le mode aveugle. Ces modes spécifient l'information a priori dont le module d'extraction pour la vérification du tatouage. L'utilisation de tel ou tel mode dépendra de l'application visée et des protocoles utilisés [28].

Mode non-aveugle : (ou tatouage privé) le récepteur dispose de l'image ainsi que du tatouage original. Ce contexte est montré dans la figure 2.5 .Il est incompatible avec des applications visant à vérifier l'intégrité de l'image, ou à assurer la vérification en temps réel du copyright (problème de temps d'accès à la base de données contenant les informations originales).

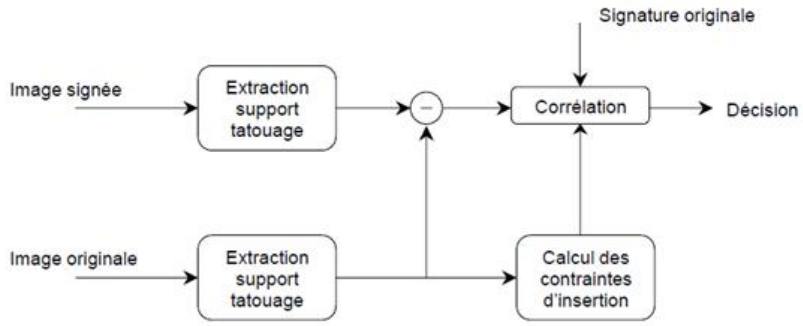


Figure2. 5 Mode d'extraction non-aveugle

Mode semi-aveugle : (ou tatouage semi-privé) le tatouage original est supposé connu lors de l'extraction et utilisé le plus souvent via un score de corrélation(Figure2.6)[28].

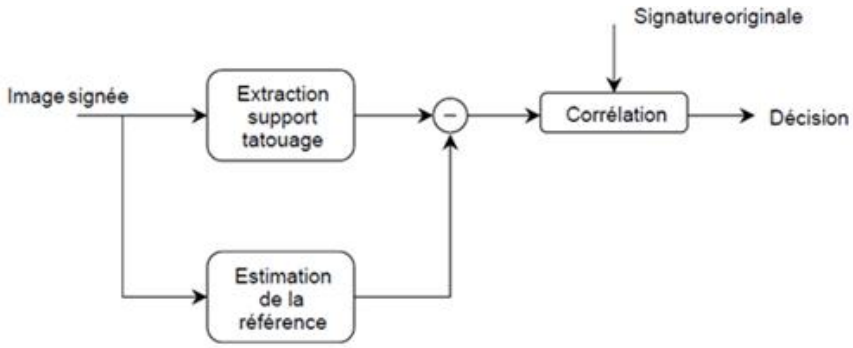


Figure2. 6 Mode d'extraction semi-aveugle.

Mode aveugle : (ou tatouage public) il s'agit du seul mode où l'on peut réellement parler d'extraction du tatouage puisque l'on ne présuppose ni la connaissance du tatouage, ni la connaissance de l'image originale (Figure2.7). C'est le mode d'extraction le plus intéressant, mais également le plus difficile à mettre en œuvre [28].

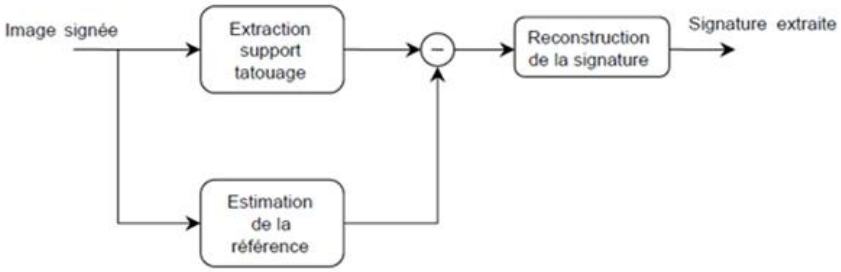


Figure2. 7 Mode d'extraction aveugle

b Détection de tatouage et décodage

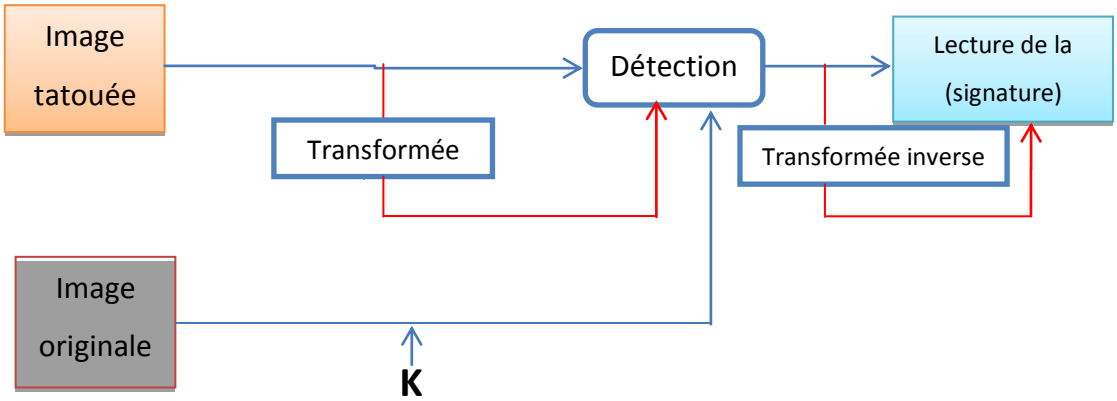


Figure2. 8 Procédé de détection

La figure2.8 représente un schéma générale de détection .Si on utilise un logo dans le procédé d'insertion, le procédé de détermination d'existence de marque est réalisé facilement. Si la marque est basée par une séquence aléatoire ayant la distribution gaussienne, il faut identifier la distribution de séquence obtenue et comparer le résultat pour donner une conclusion.

2.5 Techniques de tatouage d'image

2.5.1 Introduction

Le but de cette partie est de présenter les méthodes les plus significatives du domaine, afin de familiariser le lecteur avec les notions clés classiquement utilisées en tatouage

d'image. Même si la plupart des techniques présentées ici ont connu des améliorations significatives ces dernières années, elles permettent néanmoins d'appréhender la problématique, les difficultés et les limites inhérentes au tatouage d'image.

Les algorithmes de tatouage se distinguent les uns des autres essentiellement par les quatre points clés suivants :

- La manière de sélectionner les points (ou blocs) dans le document hôte qui porteront l'information cachée.
- Le choix d'un espace de travail pour réaliser l'opération d'enfouissement (dans le domaine spatial ou transformé comme DCT, ondelettes, Fourier-Melin, etc.) ;
- La stratégie utilisée pour mettre en forme l'information à cacher avant son enfouissement : redondance, codes correcteurs, bits de resynchronisation
- La manière de mélanger intimement le message avec le signal hôte (modulation) ; l'idée de base consiste le plus souvent à imposer une relation binaire entre les bits du message et des caractéristiques choisies de l'image porteuse.

Il existe principalement deux grandes familles de méthodes : celles qui opèrent dans le domaine spatial et celles qui opèrent dans un domaine transformé ; plus quelques méthodes originales

2.5.2 Techniques additifs

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter un bruit à l'image [29]. La figure 2.9 montre le schéma complet d'une méthode additive. La première étape est la génération d'une marque *W* qui est composée d'un bruit blanc *bb* de générateur *K* modulant parfois un message *M.* La seconde étape est la pondération de cette marque par un facteur *a* issu du calcul d'un masque psychovisuel (Ma). La troisième étape est l'addition de la marque à l'image. Cette incrustation peut se faire directement sur l'image *I* (dans le domaine spatial) ou sur une transformée *Tr* de celle-ci (TFD, TCD, TOD,…etc.) pour obtenir l'image tatouée [29].

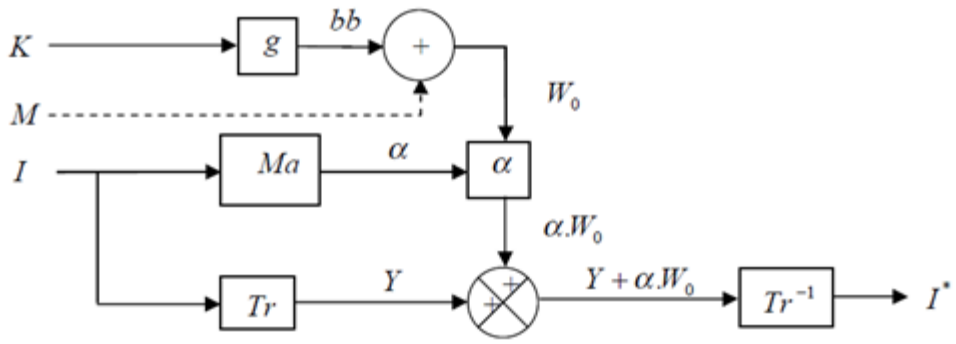


Figure2. 9 Schéma de tatouage d'une méthode additive

a Le domaine spatial

Il existe deux méthodes principales du tatouage additif dans le domaine spatial :

- ✓ La première consiste à ajouter une séquence aléatoire modulée par un message.
- ✓ La deuxième consiste à modifier le PATCHWORK de l'image.

- **Etalement du spectre**

Cette technique consiste à insérer plusieurs bits dans une image, chaque bit à insérer prend la valeur –1 ou +1, et est associé à une région de l'image. Le message complet est donc réparti sur toute l'image et modulé par une séquence aléatoire. Le signal résultant est ensuite pondéré par un masque représentant l'activité de l'image, la pondération est alors plus faible dans les régions homogènes que dans les régions texturées. La séquence obtenue est ensuite ajoutée à l'image pour obtenir enfin une image marquée par la séquence aléatoire 2D. Cette technique s'appelle étalement du spectre [30].

- **Patchwork**

La technique du PATCHWORK consiste à diviser l'image en deux ensembles disjoints de pixels A1 et A2 de même taille qui dépendent d'une clef secrète. Chaque pixel Pi,j ensuite est modifié selon la règle 2.2 :

$$Si \;\; P_{i,j} \in A_1 : P'_{i,j} = P_{i,j} \qquad 2.2$$

$$\text{Si } P_{i,j} \in A_2 : P'_{i,j} = P_{i,j} + \alpha$$

La détection de la signature se fait en calculant la différence β entre la moyenne des pixels des deux ensembles A1 et A2, la signature est détectée si β est > à un certain seuil fixé au préalable [31,32 ,33].

b Domaine fréquentiel

- **La transformée en cosinus discrète(DCT)**

De nombreuses méthodes ont été développées à partir des connaissances acquises auparavant en codage de source. Les auteurs de ces méthodes espèrent ainsi en travaillant dans le domaine DCT [34], anticiper et prévenir au moins les attaques liées à une compression JPEG. Ils espèrent également pouvoir travailler plus rapidement car le tatouage est réalisé directement sur le flux compressé. Le dernier point opérant en faveur d'un tatouage dans le domaine DCT est qu'il est possible de bénéficier, au moins en partie, des études psychovisuelles déjà menées en codage de source pour gérer les problèmes de visibilité. L'algorithme proposé par Koch et Zhao en 1995 [35] est à la base de nombreux travaux, notamment de projets de recherche européens comme le projet Talisman [36].

Le calcule de la DCT sur une matrice NxN illustré dans la formule 2.3, tant que le calcule de la DCT inverse (IDCT) est illustré dans la formule 2.4 .

$$DCT(i,j) = \frac{1}{\sqrt{2}}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} pixel(x,y)cos\left(\frac{(2x+1)i\pi}{2N}\right) cos\left(\frac{(2y+1)j\pi}{2N}\right) \quad 2.3$$

$C(x) = \frac{1}{\sqrt{2}}$ si x vaut 0, et 1 si x>0.

$$pixel(x,y) = \frac{1}{\sqrt{2N}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(i)C(j)DCT(i,j)cos\left(\frac{(2x+1)i\pi}{2N}\right) cos\left(\frac{(2y+1)i\pi}{2N}\right) \quad 2.4$$

$C(x) = \frac{1}{\sqrt{2}}$ si x vaut 0, et 1 si x>0.

- **la transformée de Fourier Mellin (TFM)**

Des transformations géométriques de l'image tatouée conduisent fréquemment à l'impossibilité d'extraire le tatouage pour de nombreux algorithmes. Ce constat a conduit à envisager l'implantation du tatouage dans un espace transformé présentant une invariance aux opérations géométriques usuelles de l'image. Ruanaidh *et al.* Préconisent l'usage de la transformée de Fourier-Mellin pour assurer la restitution du tatouage malgré qu'elle ait subi une translation et/ou une rotation et/ou un changement d'échelle. L'espace invariant est obtenu ; d'une part grâce à la propriété de la transformée de Fourier qui répercute une translation de l'image exclusivement sur la phase et laisse invariant l'amplitude ; et d'autre part, par un changement de repère **(LPM** : Log Polar Maping), de cartésien vers logarithmique-polaire, qui ramène les opérations de rotation et de changement d'échelle à une translation [37].

- **Le domaine multirésolution (Transformée en Ondelettes Discrète TOD)**

Les transformées en ondelettes qui, tout comme la transformée DCT fait l'objet de nombreuses études dans le contexte du codage, ont également trouvé un écho dans la communauté du tatouage d'image. Cet intérêt repose d'une part sur les analyses en termes psychovisuels menées afin d'optimiser les tables de quantifications des codeurs, d'autre part sur l'aspect multi-échelle de telles transformées propice à une répartition plus robuste du tatouage [38,39, 40,41].

2.5.3 Tatouage substitutif

La classe des schémas substitutifs peut être représentée par des schémas où la signature n'est pas ajoutée mais substituée des composantes de l'image [42]. Une clé secrète *K* associée à un générateur aléatoire permet de sélectionner les différentes composantes $C(I)_K$ de l'image. Ces composantes peuvent désigner les pixels d'une image, ou une transformée de celle-ci (TCD, TFD,…etc.). La signature à insérer est obtenue en appliquant une contrainte sur $C(I)_K$ en fonction du message à insérer. On procède ensuite à l'étape de substitution L'image *tatouée I** est reconstruite à partir des composantes propres à la signature.

La détection de la signature s'effectue en comparant le degré de similitude entre le message retrouvé à partir des composantes extraites de l'image tatouée $C(I^*)_K$ et le préambule utilisé lors de l'insertion (figure2.10).

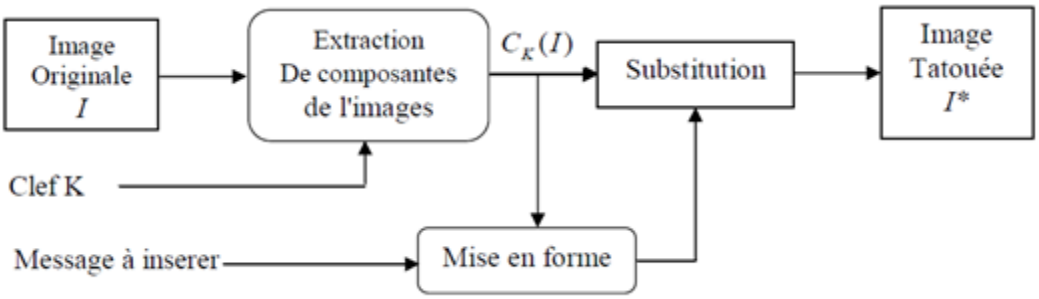


Figure2. 10 Principe de l'insertion par substitution

a Le domaine spatial

- **(L.S.B)**

La technique de modification de bits de poids faible (LSB : Least Significant Bit) est bien connue en tatouage substitutif. Le message à insérer est tout simplement substitué aux bits de poids faible d'une composante quantifiée de l'image (Chrominance, Luminance, DCT) [43].

- **Quantification**

La quantification des composantes de l'image peut aussi être utilisée pour insérer un message selon un dictionnaire de valeurs quantifiées. Ces valeurs différentes selon la valeur du symbole que l'on veut transmettre. Le nombre de dictionnaires envisagé est fonction de la quantité d'information contenue dans le message. La variété des mots de chaque dictionnaire détermine la distorsion produite par l'insertion du message. La détection du message est accomplie en vérifiant que les blocks de l'image appartiennent bien au dictionnaire utilisé lors de l'insertion [44].

- **Substitution de caractéristiques géométriques**

Les caractéristiques géométriques de l'image peuvent aussi être substituées pour permettre l'insertion d'une marque. L'insertion de la signature se fait en déplaçant légèrement certains coins ou bords de l'image originale. La signature est composée d'un réseau dense de droites. L'image est ensuite décomposée en blocs dans chacun desquels un ensemble de points d'intérêt est extrait. La signature est

insérée en effectuant des déformations géométriques locales autour de ces points caractéristiques pour les placer chacun aux abords d'une des droites du réseau. La détection de la signature se fait ensuite en examinant la proportion de points d'intérêt qui sont placés sur les réseaux de droites [45].

b Domaine fréquentiel

- **Modification des coefficients DCT**

La quantification de certains coefficients DCT, les effets visuels résultant de cette manipulation sont parfois difficilement maîtrisables. Le laboratoire de Traitement des Signaux de l'EPFL propose une nouvelle approche reposant sur le codage fractal [46]. Le codage fractal est basé sur la définition d'une association entre différentes régions de l'image. Cette association est réalisée selon un critère d'auto-similitude fondé sur la minimisation de l'erreur quadratique entre les blocs cibles et les blocs sources transformés. La recherche du bloc source associé s'effectue dans deux fenêtres de recherche centrées sur le bloc cible, selon une certaine convention et de la valeur du bit à cacher.

L'intérêt de cette approche est de mettre à profit certaines propriétés d'invariance propres aux fractales afin de pouvoir prévenir certaines attaques et récupérer la marque sans avoir recours à l'image originale.

- **Méthodes Psychovisuelles**

L'utilisation de modèles psychovisuels permet d'augmenter la force de la signature sans que les dégradations soient visuellement perceptibles. L'objectif de ces techniques est de prendre en défaut le système visuel humain (SVH) et d'exploiter les différentes propriétés de masquage. Le masquage a lieu lorsqu'un signal (la signature) est rendu imperceptible par la présence d'un autre signal dit masquant (l'image). Plusieurs modèles de masque ont été utilisés en tatouage d'image, certains modèles sont dans le domaine spatial, d'autres dans le domaine fréquentiel. F. Autrusseau et A. Saadane [47], ont proposé un masque permettant d'allier des caractéristiques fréquentielles du SVH et des caractéristiques spatiales de l'image traitée.

les méthodes additives							
		Le domaine spatial		Le domaine fréquentiel			
		Insertion par l'étalement de spectre	Division de l'image en "patchwork"	La TFD	la TCD		
robustesse		contrôle efficace de la robustesse.	Pas évidement robuste	Robuste	Robustesse augmente si on diminue la visibilité		
Invisibilité		généralement sous forme *invisible*	Augmentée modifiant les luminances de n couple de pixel	Invisible	Invisibilité augmente si on diminue la robustesse		
complexité		facile	simples à comprendre et à réaliser	Complexe à la détection et d'insertion Pose un problème au discontinuée de signale	Complexité de régler le compromis entre la robustesse et l'invisibilité		
La capacité		faible *capacité*		La *capacité* de l'algorithme est toutefois limitée	Limitée car il utilise la notion de blocs.		
La sécurité		Résoudre les problèmes de communication sur les canaux bruités	compenser les effets du bruit blanc additif ne résiste pas à de petites déformations géométriques, ni même à la compression JPEG	Résiste à l'attaque géométrique	Résiste à l'attaque géométrique Résiste à une compression JPEG		
Le cout		N'est pas couteuse	N'est pas couteuse		moyen		

Tableau 2.1 tableau comparatif de différentes techniques de tatouage des images

les méthodes additives						Les méthodes substitutives					
Le domaine fréquentiel	Le domaine multi résolution		Le domaine spatial								
La transformée FOURIER-MELLIN	Transformée en Ondelettes Discrète		L.S.B	Quantification	Substitution de caractéristiques géométriques						
Robuste Domaine invariant	Robustesse élevée		Robustesse inexistante	Robuste	robuste						
Généralement sous forme invisible	Généralement invisible (lignes de discontinuité on force un contour est peu visible)		Généralement visible ou invisible	Généralement visible ou invisible	Invisibilité augmente si les blocs sont les fines le max						
Difficulté de reconnaissance la forme de tatouage Couteuse en temps de calcule	Complexité de construction d'une ondelette (algorithme complexe)		Simple	Généralement simple	Simple						
Capacité d'insertion limitée	Elevé car elle bien décrire un grand nombre des signaux		Limité car l'insertion au niveau des bits a poids faible	En fonction de nombre de dictionnaires envisagé	Capacité importante						
invariante aux distorsions asynchrones et au mouvement	Résiste très fort au changement d'échelle et au bruit additif et aux erreurs de quantification		la marque ne résistera pas à une compression jpeg où à un bruit blanc gaussien additif	Résiste aux petites variations	Faible résistance à la transformation géométrique						
moyen			Cout faible	Cout faible							

Tableau2.1 tableau comparatif de différentes techniques de tatouage des images

Les méthodes substitutives							Les Méthodes Psychovisuelles	
Le domaine fréquentiel		Le domaine multi résolution						
Modification des coefficients TCD	Quantification des coefficients ondelettes							
Robustesse augmentée modifiant les valeurs quantifiant les coefficients basse fréquence	Robustesse augmentée par l'emploi de code correcteur	Très robuste						
Généralement invisible	Généralement invisible	Assurent L'invisibilité						
Complexité de modifier les paramètres des coefficients DCT	Complexité supplémentaire au décodeur	Complexe (allier les caractéristiques spatiales et fréquentielles de SVH)						
Limitée car il utilise la notion de blocs.	Forte capacité	Forte capacité						
résiste attaque géométrique	résiste attaque géométrique	Résiste a les attaque JPEG Fragile aux attaques géométriques						
résiste aux attaques liées à la compression JPEG	Plus résiste aux attaques liées à la compression JPEG 2000							
Cout moyen	Un Peu couteuse	couteuse						

Tableau 2.1. Tableau comparatif de différentes techniques de tatouage des images

2.6 Conclusion

Ce chapitre a décris l'état de l'art des différents techniques utilisées dans le tatouage des images, avec les deux méthodes principale ; additives et substitutives dans les deux domaines spatial et fréquentielle. On a essayé de faire une comparaison entres ces différents techniques comptant les facteurs ; la robustesse, l'invisibilité, la capacité d'insertion, la complexité d'implémentation et le cout, ce qui nous permettra de choisir notre système proposée dans le chapitre suivant.

Chapitre 3 le système proposé

3.1 Introduction

Nous aborderons les différents concepts utilisés pour la réalisation du système proposé de tatouage des images médicales.

En effet, on va essayer de protéger ces images contre les différentes attaques par l'insertion d'une marque (signature) qui prend la propriété d'invisibilité (cas des images médicales).Le processus d'insertion sera dans le domaine fréquentiel par transformée en ondelette. Dans cette partie on va décrire trois techniques de tatouage selon la force d'insertion de la marque : fragile, robuste et multiple, en montrant l'architecture globale du système.

3.2 Schéma général des systèmes de tatouage proposés

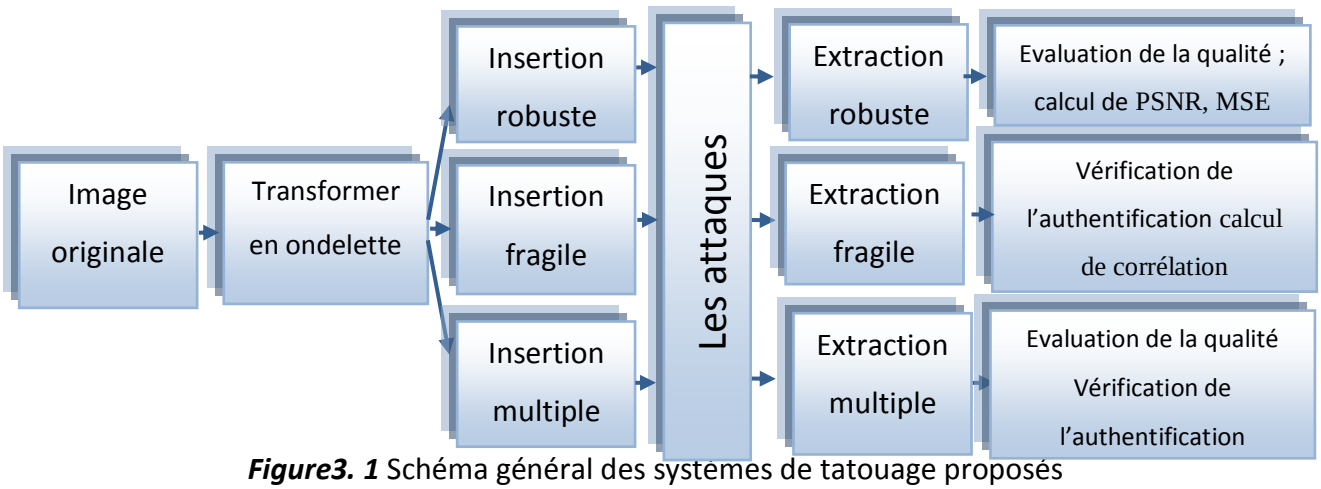


Figure3. 1 Schéma général des systèmes de tatouage proposés

Ce schéma proposé (Figure3.1) est basée généralement sur la décomposition en ondelette. Il est décomposé en trois méthodes selon la force d'insertion de la marque.

La première méthode est robuste qui sert à protéger l'image tatouée contre les attaques, l'évaluation de la qualité d'une image extraite à la réception se fait par un calcul de deux paramètres PSNR et MSE. La deuxième méthode, la signature sera fragile ; la technique sert à détecter une attaque via un score de corrélation calculer entre la signature originale est la signature extraite. La troisième méthode est l'insertion multiple des deux marques : robuste et fragile, a comme but la protection et la détection au même temps.

3.3 Choix de l'espace de travail

3.3.1 Domaine fréquentiel

Le travail sur le domaine fréquentiel consiste à insérer la marque, non pas directement dans l'image mais, dans sa transformée. Afin de retrouver l'image marquée, on effectue la transformée inverse. La séparation fréquentiel pour l'insertion de tatouage se fait par la transformer en ondelette.

a Utilisation de la transformée en ondelettes

L'intérêt de cette transformée est l'optimisation du choix des emplacements et la force du marquage de la signature dans l'image ainsi que son aspect multi-échelle qui offre une répartition plus robuste au tatouage. Les ondelettes sont l'un des outils les plus efficaces actuellement dans le traitement des images. Il est avéré que les ondelettes apportent des meilleurs résultats, Contrairement, à la DCT, la DWT qui s'applique à la totalité de l'image et non pas à des blocs de pixels, ce qui permet d'éviter l'apparition de carrés uniformes.

b Transformée en ondelettes

La transformée en ondelettes vue comme une décomposition dyadique de l'image, réalisée à l'aide d'une paire de filtres QMF (filtres quadratiques miroirs) montrer dans la figure 3.4, l'un étant passe haut (H) et l'autre passe bas (L). Ces deux filtres sont successivement appliqués sur toute l'image qui, à leurs sorties, subissent un

sous échantillonnage [47][48].la figure3.2 montre la décomposition on multirésolution en 4 niveaux.

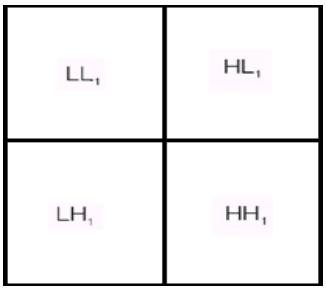


Figure3. 2 Niveaux de fréquence pour la transformé en ondelette

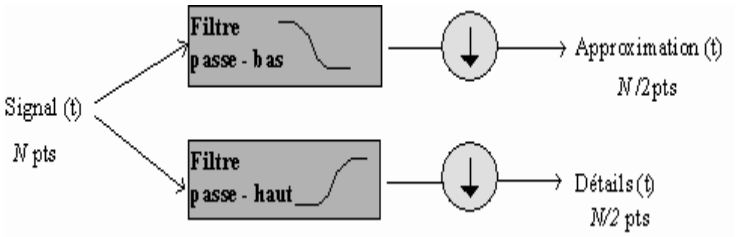


Figure3. 3 schéma des filtres de la transformé en ondelette

Où le symbole  représente l'opération de sous-échantillonnage : on ne prend qu'un point du signal sur deux.

c Transformée inverse

Pour de nombreuses applications, Il est intéressant, de pouvoir reconstruire le signal à partir des coefficients d'ondelettes : les signaux d'approximation et de détails. Cette opération est appelée *reconstruction* ou *synthèse*[48].

On passe donc de l'approximation A_j à l'approximation A_{j-1} par l'opération montrée dans la figure3.4.

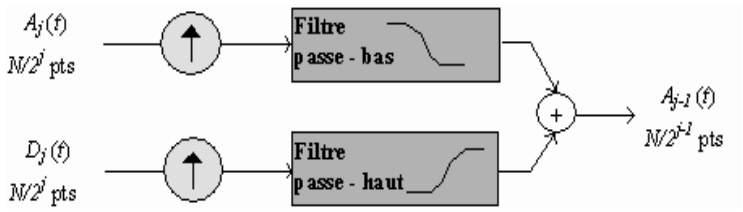


Figure3. 4 Schéma des filtres de la transformé inverse en ondelette.

Si x(t)est une fonction réelle de variable réelle la transformée en ondelettes de f est:

$$g(a,b) = \frac{1}{\sqrt{a}} \int_{t=-\infty}^{t=\infty} x(t)\ \bar{\psi}_{a,b}(t)\ dt \qquad 3.1$$

a est différent à 0 La fonction $\psi_{a,b}(t)$est obtenue par translation et dilatation d'une fonction particulière appelée ondelette mère:

$$\psi_{a,b}(t) = \Psi(\frac{t-b}{a}) \qquad 3.2$$

B détermine la position et a donne l'échelle.

Cas d'un signal :a est la fréquence et b le temps.

- La fonctionΨdoit être oscillante et d'intégrale nulle.
- Ψdoit être de carré intégrable.
- Ψpeut être à valeurs complexes.
- Il existe de nombreuses ondelettes mères Ψpossibles.
- Ainsi définie c'est une transformation continue à
- rapprocher de la transformation de Fourier continue.
- La transformation en ondelette est une transformation

3.3.2 Avantage de la transformé en ondelette

- Bien adaptée aux signaux non-stationnaires ;
- Permet une décomposition spatio-fréquentielle de l'image ;
- permet une décomposition multirésolution ;
- pas d'effets de bloc ;
- permet la transmission progressive.

3.3.3 Types d'ondelettes

a Ondelette de Haar

On la considère que c'est la première ondelette connue. Elle est la plus simple à comprendre et à implémenter [50].

C'est une fonction dilatée et/ou translatée de la fonction mère ψ qui vaut :

$$\psi(t) = \begin{cases} 1 & \text{pour } 0 \leq t < \frac{1}{2} \\ -1 & \text{pour } \frac{1}{2} \leq t < 1 \\ 0 & \text{sinon} \end{cases}$$

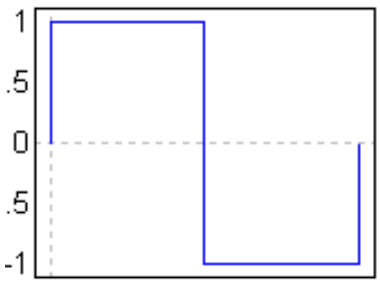


Figure3. 5 Ondelette de Haar

b Ondelette chapeau mexicain

$$\psi(t) = \frac{2}{\sqrt{3\sigma}\pi^{\frac{1}{4}}} \left(1 - \frac{t^2}{\sigma^2}\right) e^{\frac{-t^2}{2\sigma^2}} \qquad 3.3$$

En mathématiques et en analyse numérique, l'ondelette chapeau mexicain, est le négatif normalisé de la dérivée seconde d'une fonction gaussienne, c'est-à-dire à l'échelle et à la normalisation près, la seconde d'un polynôme d'Hermite. C'est un cas particulier de la famille des ondelettes continues (l'ondelette utilisée dans la transformée en ondelettes continue) connue sous le nom d'ondelettes hermitienne. Elle est généralement dénommée "chapeau mexicain"(Figure3.6) aux États-Unis, car la forme de sa courbe rappelle un chapeau typique du Mexique, le "Sombrero".

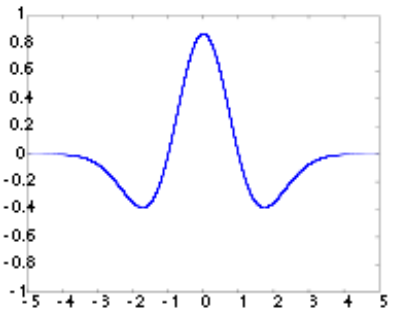


Figure3. 6 Ondelette chapeau mexicain

c Ondelette de morlet

En mathématiques, l'ondelette de Morlet montrée dans la figure 3.7 (Gabor ondelettes de Gabor) est une ondelette composée d'une exponentielle complexe (transporteur), multiplié par une fenêtre gaussienne (enveloppe). Cette ondelette est étroitement liée à la perception humaine, à la fois l'audience et de la vision.

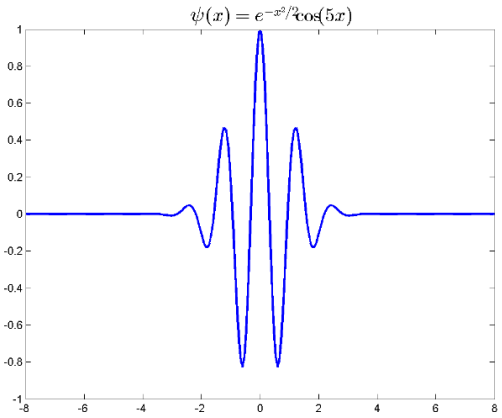


Figure3. 7 Ondelette de Morlet.

d Ondelette de Daubechies

Nommées d'après leur créatrice Ingrid Daubechies, les ondelettes de Daubechies sont une famille d'ondelettes orthogonales définissant une transformée en ondelettes discrète, caractérisées par une nombre maximal de moments dissipant pour un support donné. Pour chaque type d'ondelette de cette classe, il existe une

fonction d'échelle (appelée aussi ondelette mère) qui génère une analyse multirésolution orthogonale.

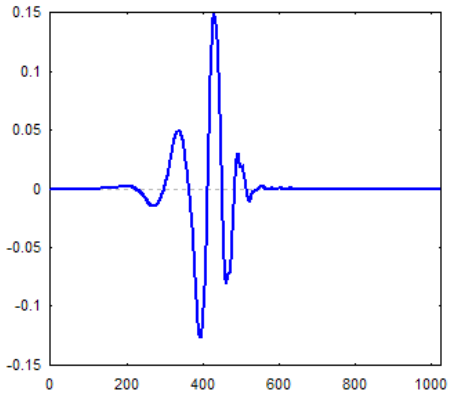


Figure3. 8 Ondelette de Daubechies

3.3.4 Comparaison des types d'ondelette

Type d'ondelette	Avantage	Inconvénient
ondelettes de Haar	une complexité très faible	n'est pas continu et donc pas différentiable.
ondelette chapeau mexicain	gagner un temps de calcul très important	la réduction inhérente du contraste global de l'image traitée.
Ondelette daubechies	la compacité des supports, en préservant l'ortho-normalité	l'abandon de la symétrie
Ondelette de morlet	Optimalement localisée dans le plan temps-fréquences	La taille dépend également de la fréquence.

Tableau3. 1 Comparaison des ondelettes

Le tableau 3.1 exprime les différentes caractéristiques des ondelettes existantes .le choix de l'ondelette se fait selon le compromis entre l'efficacité et la simplicité.

Dans notre schéma on a utilisé l'ondelette de Daubechies pour sa compacité des supports, en préservant l'ortho-normalité; et sont inconvénient (l'abandon de la

symétrie) n'influe pas sur les transformations de l'image médicale surtout dans le domaine fréquentiel.

3.4 Signature

On a utilisé dans notre technique un schéma additif qui consistent principalement à ajouter une signature à l'image, pour le facteur de visibilité on a appliqué (ajouté) plusieurs types de marque pour qu'on aura une signature invisible avec une bonne qualité d'image tatouée et image extraite.

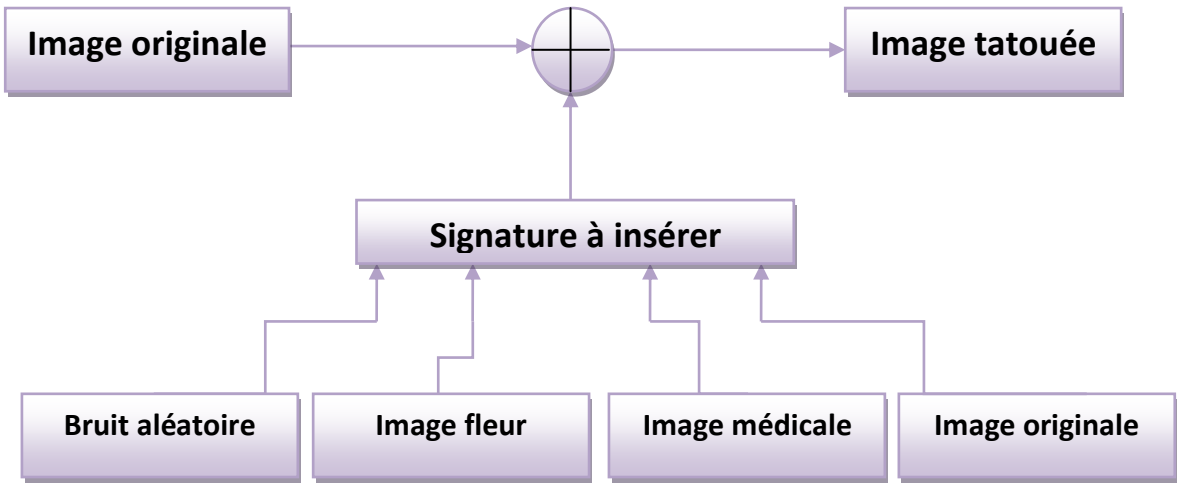


Figure3. 9 Les différents types de signature

Dans le cas du tatouage robuste, la signature est insérer dans les basses fréquences (les plan à poids lourds) par contre dans la technique du tatouage fragile on insère les détails de l'image, la signature dans ce cas doit être invisible.

3.5 Insertion de la signature

La technique de tatouage est choisie selon la manière d'insertion de la marque.

3.5.1 Schéma d'insertion de la signature robuste

Les étapes d'insertion de marque du tatouage robuste sont présentées dans le schéma de la figure 3.10.

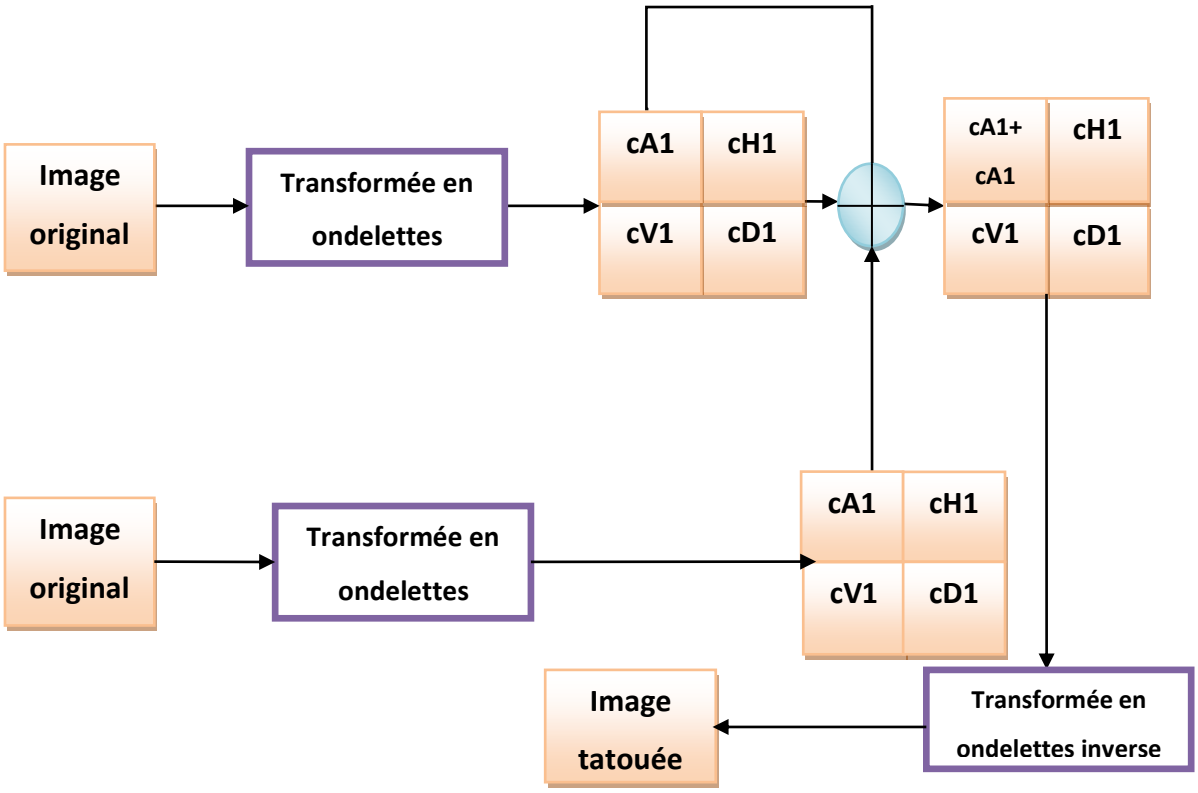


Figure3. 10 Schéma d'insertion dans la technique de tatouage robuste.

a Algorithme d'insertion

- Transformation de l'image en ondelette en quatre plans cA1, cH1, cV1, cD1. cA1 représente les basses fréquences, et (cH1, cV1, cD1) représentent les hautes fréquence, tel que cH1 : sont les détails horizontales, cV1 : les détail verticales et cD1 : sont les détails diagonale.
- Choix de la signature à insérer ; on va choisir à insérer la même image.
- Insertion du niveau choisi, dans ce cas on va insérer les basses fréquences (cA1).
- Application de la transformée en ondelette inverse pour obtenir une image tatouée prête à transmettre.

3.5.2 Schéma d'insertion de la signature fragile

Le schéma de la figure3.12 résume les étapes d'insertion pour tatouage fragile :

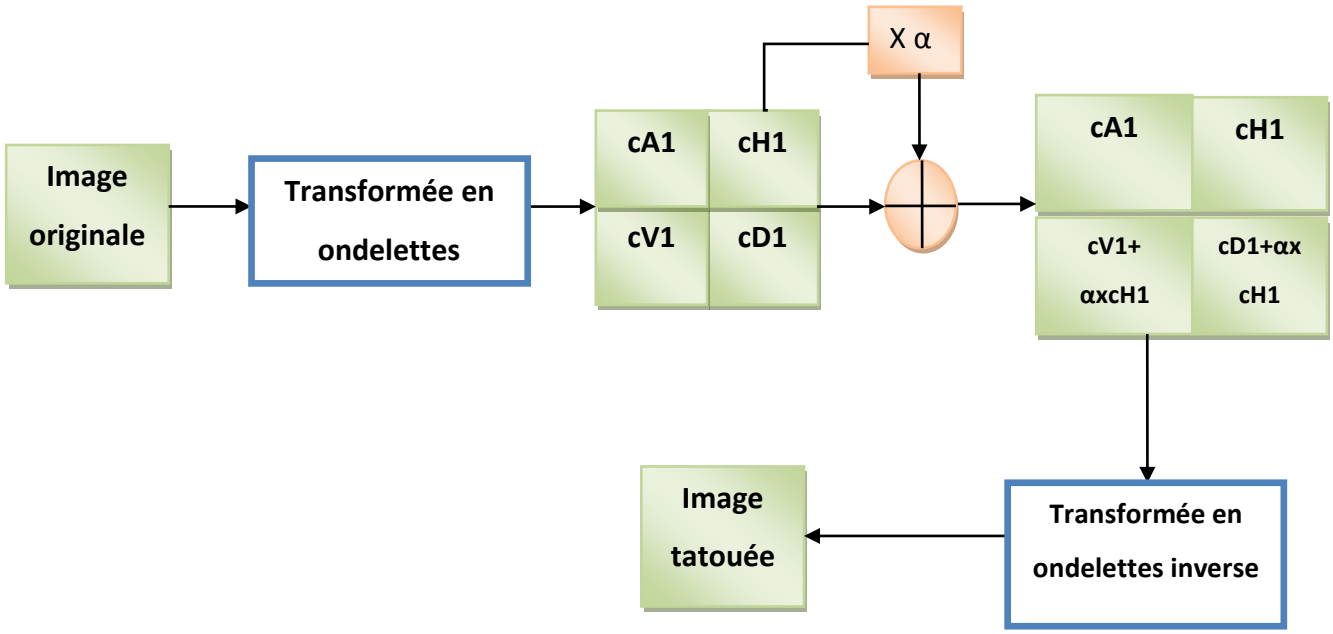


Figure3. 11 Schéma d'insertion dans la technique de tatouage fragile

Algorithme d'insertion

- Transformation de l'image en ondelette en quatre plans cA1, cH1, cV1, cD1.
- Multiplication du niveau d'insertion par un facteur d'invisibilité α qui prend des valeurs entre [0 et 1], le choix de la valeur de α respecte le critère « l'image ne doit pas être altérée par la signature ».
- Insertion du niveau choisi comme un filigrane dans les niveaux hauts fréquence, cV1, cD1.
- Application la transformer inverse.
- En fin obtention une image tatouée prête à transmettre.

3.5.3 Schéma d'insertion de la signature multiple

Les étapes d'insertion de marque du tatouage multiple sont présentées dans le schéma de la figure3.12.

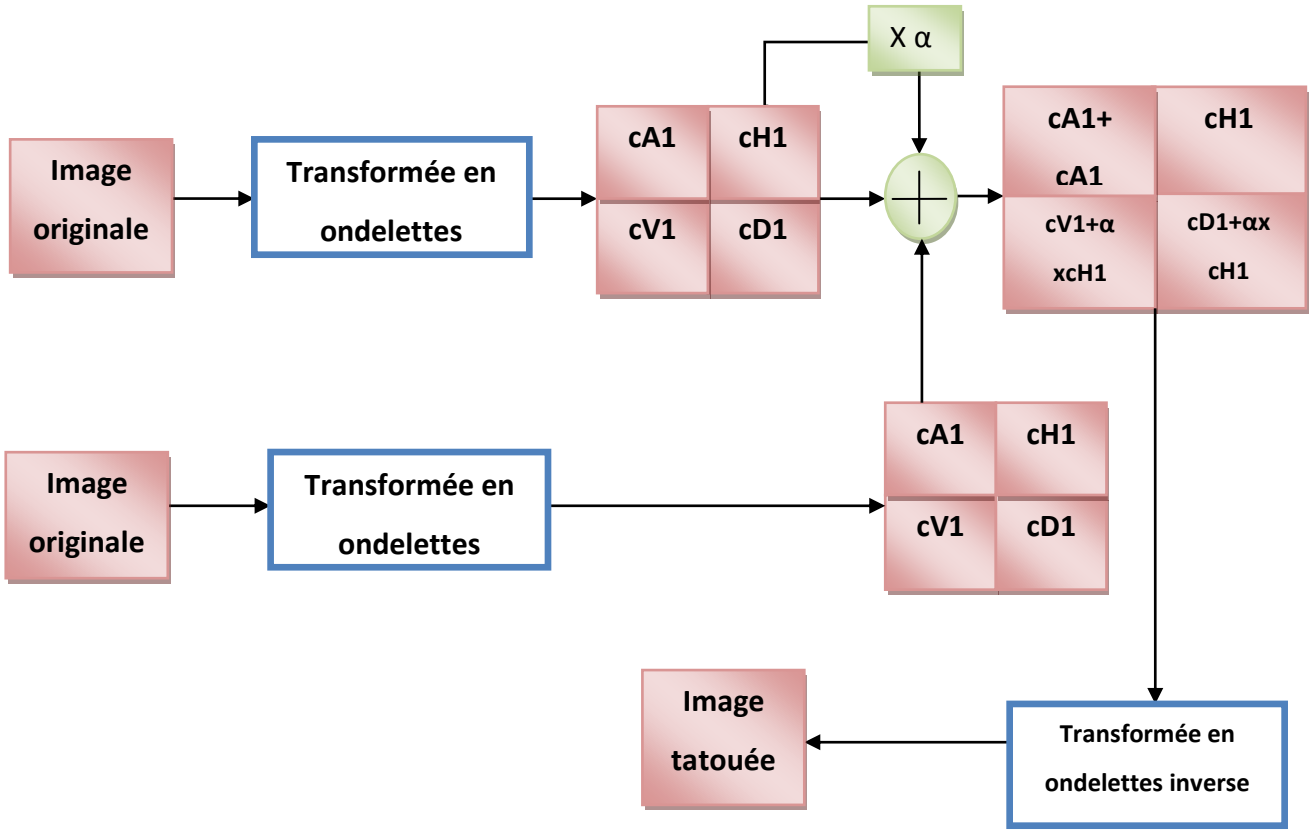


Figure3. 12 Schéma d'insertion dans la technique de tatouage multiple

a Algorithme d'insertion

- Transformation du l'image en ondelette en quatre plans cA1, cH1, cV1, cD1.
- Multiplication du niveau d'insertion par un facteur d'invisibilité α qui prend des valeurs entre [0 et 1], le choix de la valeur de α respecte le critère de l'image ne doit pas être altérée par la signature.
- Insertion du niveau choisi comme un filigrane dans les niveaux hauts fréquence, cV1, cD1.
- Ajout du niveau CA1 de signature à celui de l'image médicale (la marque robuste).
- Application la transformer inverse.
- En fin obtention une image tatouée prête à transmettre.

3.6 Contrainte des attaques

L'image 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.

3.6.1 Ajout de bruit

a Bruit blanc

C'est un bruit aléatoire uniformément distribué.

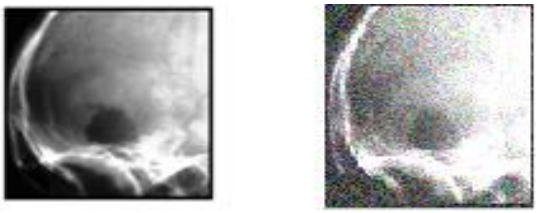


Figure3. 13 Image attaquée par ajout de bruit blanc

b Bruit gaussien

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

$$f_X(x,t_k) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{1}{2}\frac{(x-m)^2}{\sigma^2}\right) \quad 3.4$$

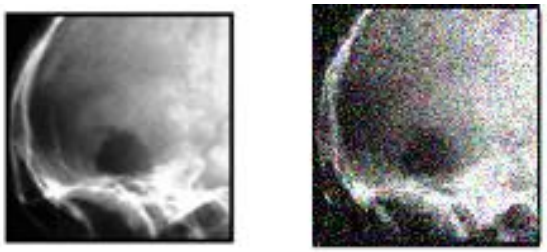


Figure3. 14 Image attaquée par ajout de bruit gaussien.

3.6.2 Filtrage

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).

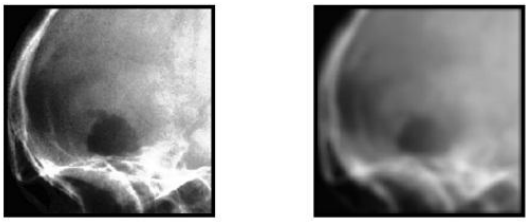


Figure3. 15 Image attaquée par un filtre moyen

3.6.3 Compression avec perte

Le but de la compression avec perte (attaque) est de réduire la taille des fichiers images. Elle est basée sur la quantification, ce qui permet de perdre une partie l'information utile.

a Compression jpeg

Le format JPEG est le standard classique le plus utilisé pour la compression des images (basée sur la transformer en DCT). Cette compression est basée sur l'élimination des hautes fréquences (les détails) de l'image

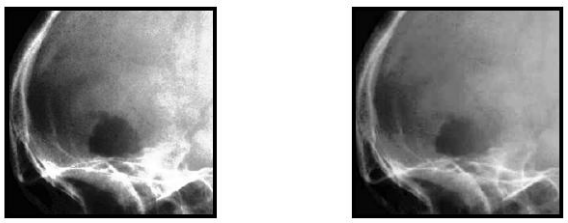


Figure3. 16 Image attaquée par compression jpeg

b Compression jpeg2000

La compression par jpeg2000 est plus performante que celle du Jpeg classique à poids de fichiers égaux. Elle produit des images moins dégradées : elle est fondée sur la transformer en ondelette.

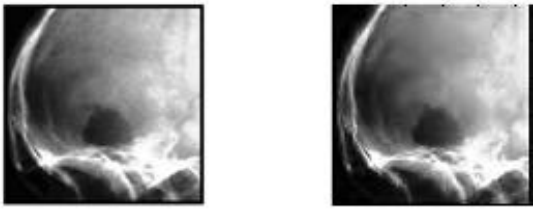


Figure3. 17 Image attaquée par compression jpeg2000.

3.6.4 Rotation

La rotation autour de l'origine est une déviation de l'image d'un certain angle. Les intensités des pixels ne peuvent jamais revenir à leurs valeurs initiales.

$x = x\cos(\theta) - y\sin(\theta)$; $y = y\cos(\theta) + x\sin(\theta)$, avec θ angle de rotation 3.5

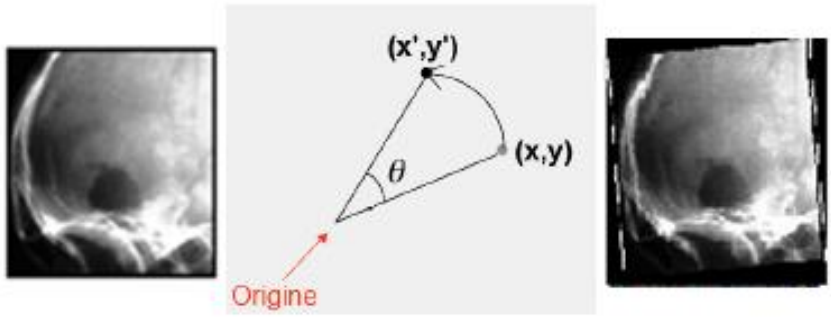


Figure3. 18 Image attaquée par rotation

3.7 Extraction de la marque

À la présence de la signature originale, L'extraction de la marque va être en mode semi aveugle.

3.7.1 Méthode robuste

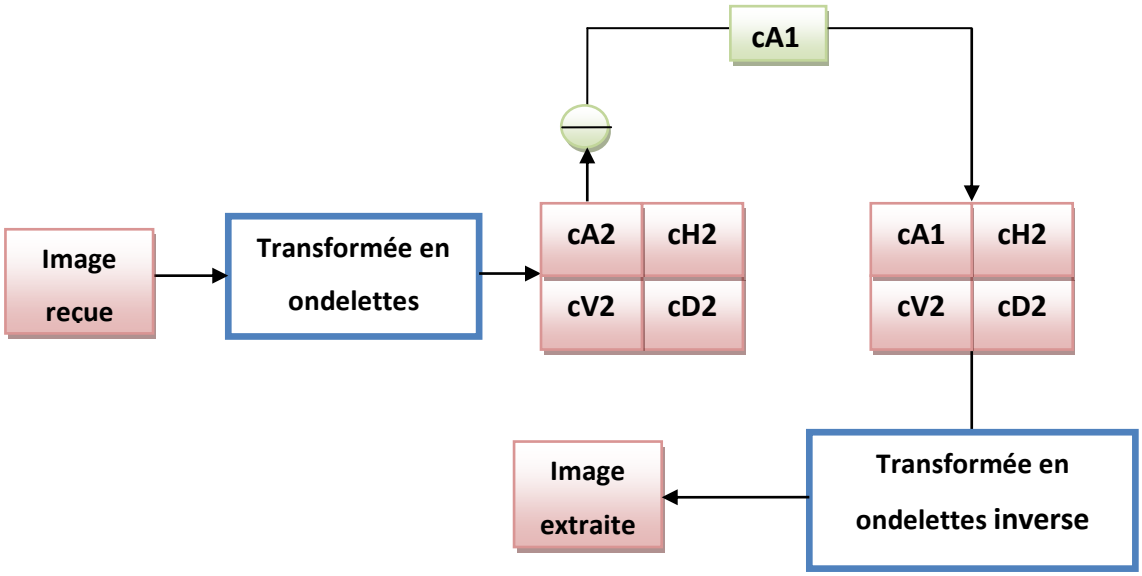


Figure3. 19 Schéma d'extraction dans la technique de tatouage robuste.

a Algorithme d'extraction de la signature

L'algorithme de l'extraction montré dans la figure 3.20 est fondé sur :

- La transformation de l'image reçue en ondelettes : c'est une étape importante pour l'extraction de la signature. Elle permet la séparation des niveaux de fréquences.
- L'extraction de la signature inversant le processus d'insertion (substituer le plan CA1).
- L'application de la transformation inverse.

3.7.2 Méthode fragile

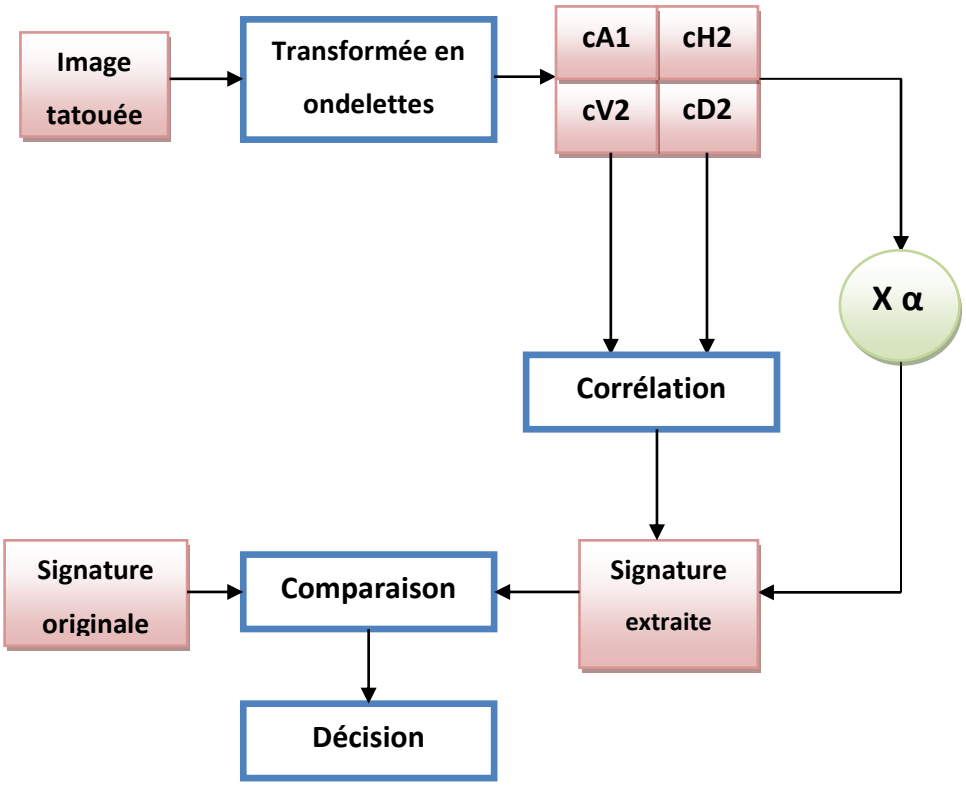


Figure3. 20 Schéma d'extraction dans la technique de tatouage fragile

a Algorithme de détection de tatouage

L'algorithme de l'extraction montré dans la figure 3.21 est fondé sur :

- Transformation de l'image reçue en ondelette.
- Calcule de corrélation entre les niveaux de détails et la signature originale,
- Multiplication la valeur moyenne des corrélations foi le même niveau insérer à la réception de l'image reçue.
- Multiplication de résultat par la valeur de α afin d'obtenir une signature extraite.
- Calcule une deuxième corrélation entre la signature extraite et la signature originale si elle est supérieur un facteur f (appelé un facteur de fragilité) l'image est authentique sinon l'image est non authentique.

3.7.3 Méthode multiple

Schéma suivant résume les étapes d'extraction de marque de la marque multiple.

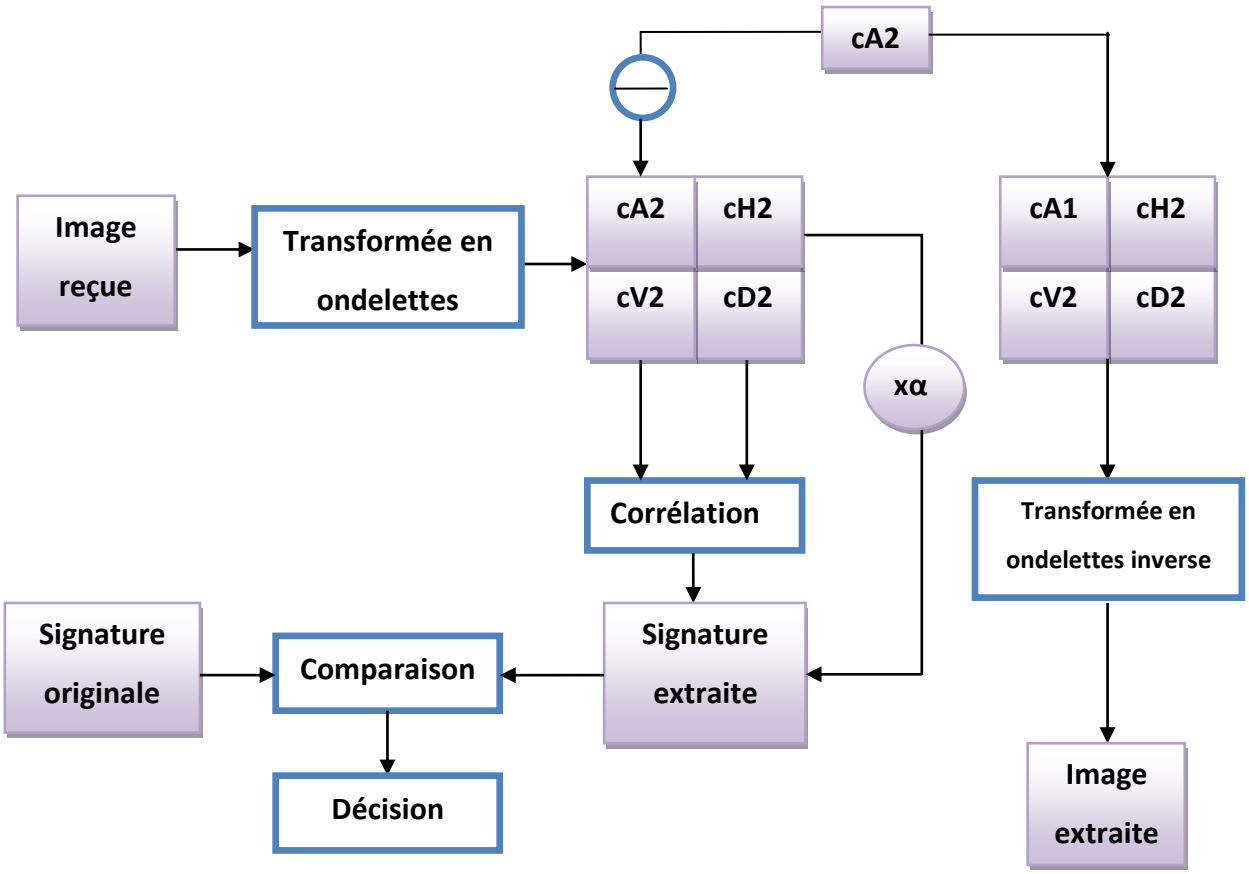


Figure3. 21 Schéma d'extraction dans la technique de tatouage multiple.

a Algorithme de détection de tatouage

L'algorithme d'extraction montré dans la figure3.21 est basé sur :

- Transformation l'image reçue en ondelette.
- Application du processus d'extraction du tatouage robuste et extraire la signature fragile, de la même façon des techniques précédentes.
- Application de la transformation en ondelette inverse.
- Vérification de l'authentification de l'image extraite.

3.8 Corrélation

La mesure de la corrélation a pour objectif, la détection d'une attaque via un score de corrélation précis. Ainsi, l'image A est une image primaire et l'image B est image secondaire, les valeurs de la corrélation entre les deux images pour les trois vecteur RGB sont calculés selon l'équation de la corrélation 3.6

$$r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \overline{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \overline{B})^2\right)}} \qquad 3.6$$

(A barre et B barre représentes les moyennes)

3.9 Evaluation des schémas

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

Pour évaluer les images résultantes, on va calculer le PSNR« Peak Signal-to-Noise Ratio » et le MSE « Medium Square Error».

Le PSNR est calculé à partir de l'erreur quadratique moyenne (MSE) 3.6

$$MSE = \frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{M} |p(m,n) - \hat{p}(m,n)|^2 \qquad 3.6$$

où M et N sont les dimensions horizontale et verticale de l'image, $p(m,n)$ et $\hat{p}(m,n)$ sont respectivement les valeurs du pixel à la position (m, n) pour l'image initiale et pour l'image restaurée. Le PSNR dont l'unité est le dB (décibel) a pour équation 3.7

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \qquad 3.7$$

Une valeur faible du MSE signifie qu'il y a très peu de différence entre les deux images comparées. Comme le PSNR est calculé à partir de l'inverse du MSE. Donc, logiquement, plus la valeur du PSNR est faible et plus les images diffèrent.

3.10 Conclusion

Le tatouage robuste sert à éliminer ou minimiser l'effet des attaques sur l'image reçue. En contre partie, le tatouage fragile sert à prouver l'intégralité des images reçues basé sur l'insertion dans les détails. Le tatouage multiple regroupe les propriétés de la technique robuste et fragile.

Dans ce chapitre on a essayé d'expliquer ces trois techniques de tatouage proposées, la simulation et l'efficacité de ces technique se voie dans le prochaine chapitre.

Chapitre 4 Implémentation et résultats

4.1 Introduction

Après la présentation des schémas et des techniques de tatouage proposées, Dans ce chapitre on va les mettre en œuvre, et analyser les résultats obtenus en présentant d'abord l'environnement de programmation utilisé, ainsi que l'interface de l'application. Enfin on termine par le compromis entre les techniques proposées.

4.2 Environnement de programmation

Pour implémenter notre application, on a utilisé le langage de programmation MATLAB 7.8(2009), qui est un environnement riche en outils comportant toutes les fonctionnalités nécessaires pour créer des projets. En effet, le MATLAB (« matrix laboratory ») est un langage de programmation de quatrième génération et un environnement de développement ; il est utilisé à des fins de calcul numérique. Développé par la société (MathWorks), MATLAB permettra la manipulation de matrice, l'affichage des courbes et des données, la mise en œuvre des algorithmes, la création des interfaces utilisateurs, et peut s'interfacer avec d'autres langages comme le C, C++, Java, et Fortran.

Les utilisateurs de MATLAB sont de milieux très différents comme l'ingénierie, les sciences et l'économie dans un contexte aussi bien industriel que pour la recherche. Matlab peut s'utiliser seul ou bien avec des toolbox (« boite à outils »).

4.3 Interface de l'application

L'interface graphique a pour but la simplicité de l'analyse de techniques proposées.

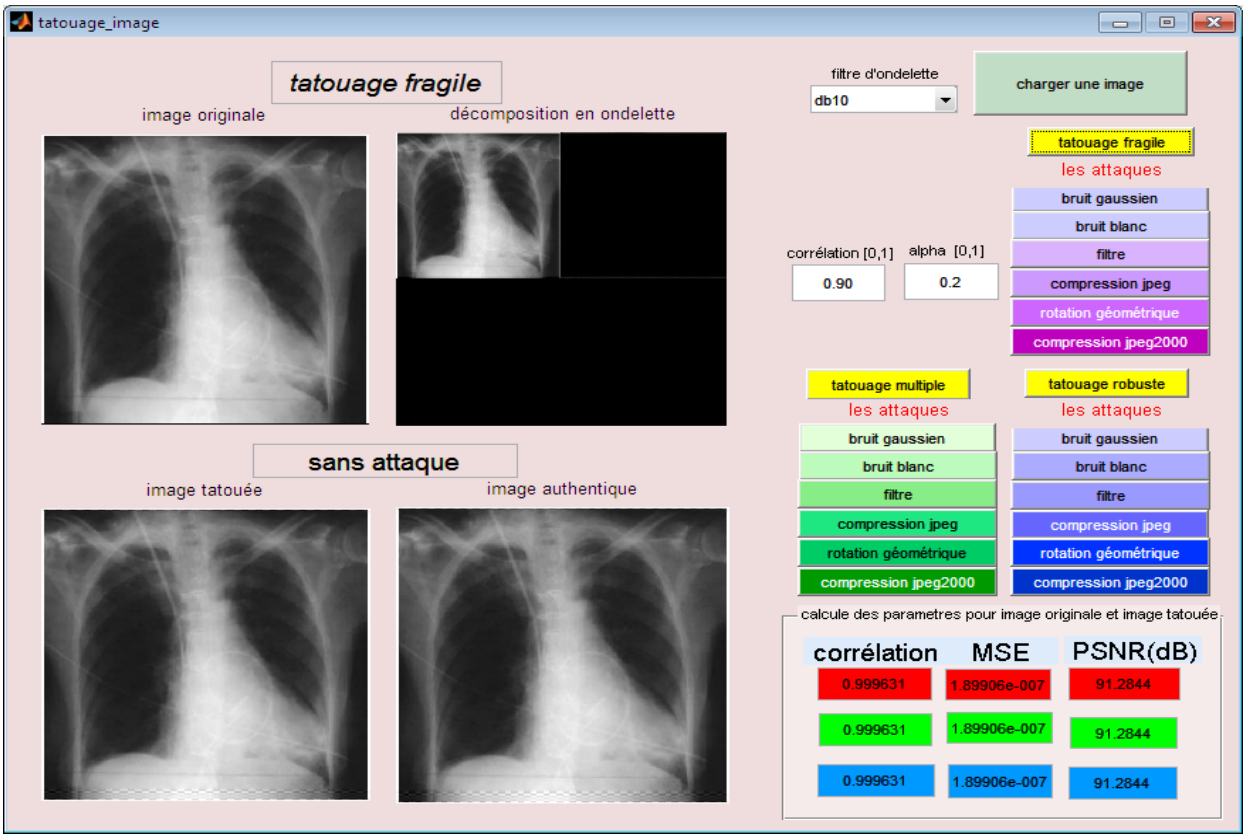


Figure4. 1 l'interface de l'application

Le menu principale de l'application présenté dans la *figure4.1* nommé « tatouage-image», il permet le chargement de l'image à traiter (niveaux de gris ou bien en couleurs)en utilisent le bouton « charger une image ».

Le bouton de pop menu à gauche montre la taille de filtre d'ondelette choisie (daubeshies10).

Pour chaque processus des méthodes de tatouage correspondantes (robuste, fragile, multiple), les différents boutons de l'interface sont associés, ce qui permet de les spécifier au préalable.

On doit spécifie après, la technique de tatouage qu'on veut l'appliquer, si on commence par le tatouage robuste, il suffit de cliquer sur le bouton de cette technique, l'image originale, sa transformé en ondelette, l'image tatouée ainsi que l'extraite doivent être affiché.

Le choix des attaques appliqués sur l'image originale et l'image tatouée sera à partir de la liste des boutons en dessous de la technique de tatouage choisis.

Dans tous les cas choisis les paramètres d'évaluation (PSNR, MSE, corrélation)des trois composantes de l'image (rouge, verte, bleu),seront calculés automatiquement et affichés au bous de l'interface à partir des espaces d'affichage « Edit » colorés selon les composantes ; ces valeurs seront égaux dans le cas des images en niveaux de gris.

Dans le cas du choix de la technique de tatouage fragile on doit saisir la valeur de facteur de visibilité « alpha »et celle de corrélation à partir des espaces de « Edit », qui appartient à l'intervalle mentionné en dessus du bouton.

L'application des attaques et les calculs des paramètres se fait de la même façon de la technique robuste.

Si on veut choisir un tatouage multiple il suffit, de cliquer sur le bouton de « tatouage multiple », et indiquer la valeur de facteur de visibilité et de corrélation, et appliquer le processus des techniques précédentes pour l'évaluation.

4.4 Choix de signature

La signature insérer est un facteur important dans le choix de technique de tatouage dont la visibilité et la robustesse caractérisent la technique utilisée. On doit trouver un compromis entre eux pour mieux utiliser la technique choisis.

Durant notre expérimentation différentes types de signature ont été appliqué pour tatouée l'image médicale.

Le tableau ci-dessous résume nos résultats:

Type de signature	Image quelconque	Image aléatoire	Image médicale quelconque	Insertion de la même image

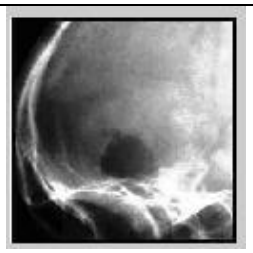
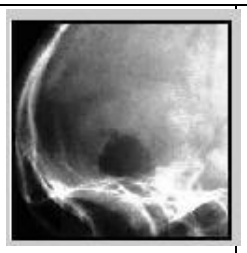
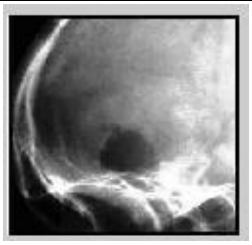
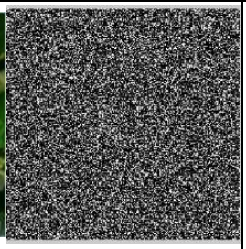
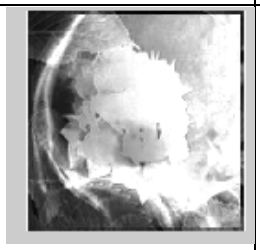
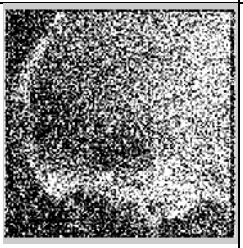
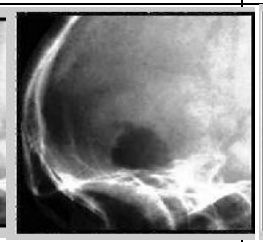
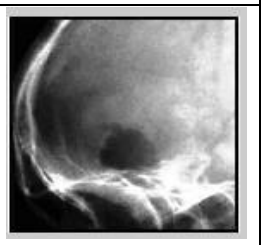
Image originale				
La signature				
Image tatouée				
Image extraite				
Calcul de PSNR	49.6	48.8	49.38	50.22
Calcul de MSE	0 .007	0.0075	0.0072	0.0066

Tableau4. 1 Insertion des différents types de signature.

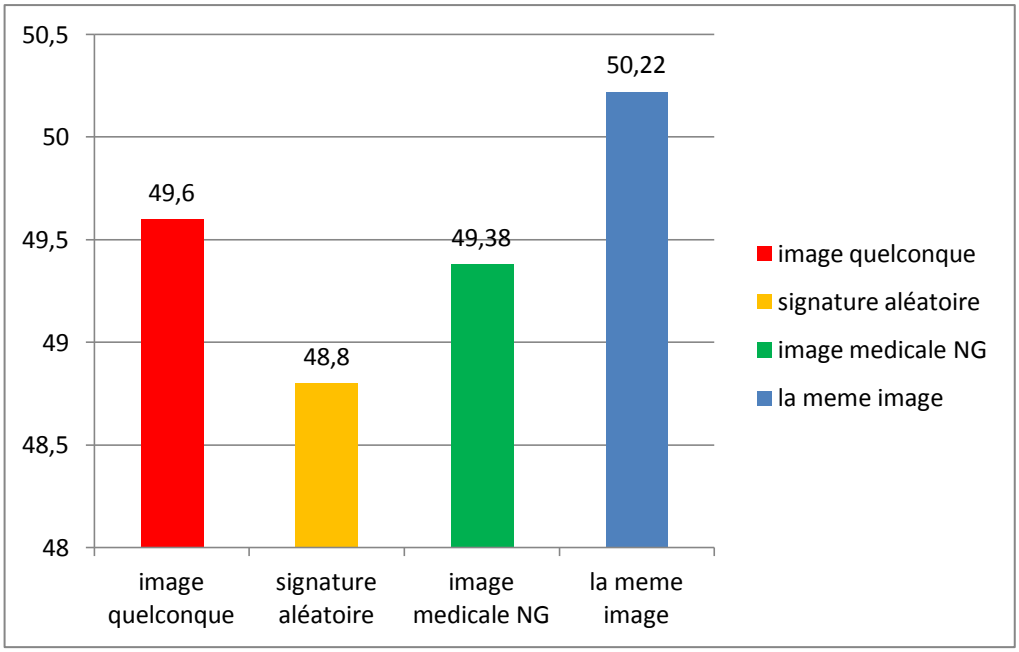


Figure4. 2 PSNR des différents types de signature.

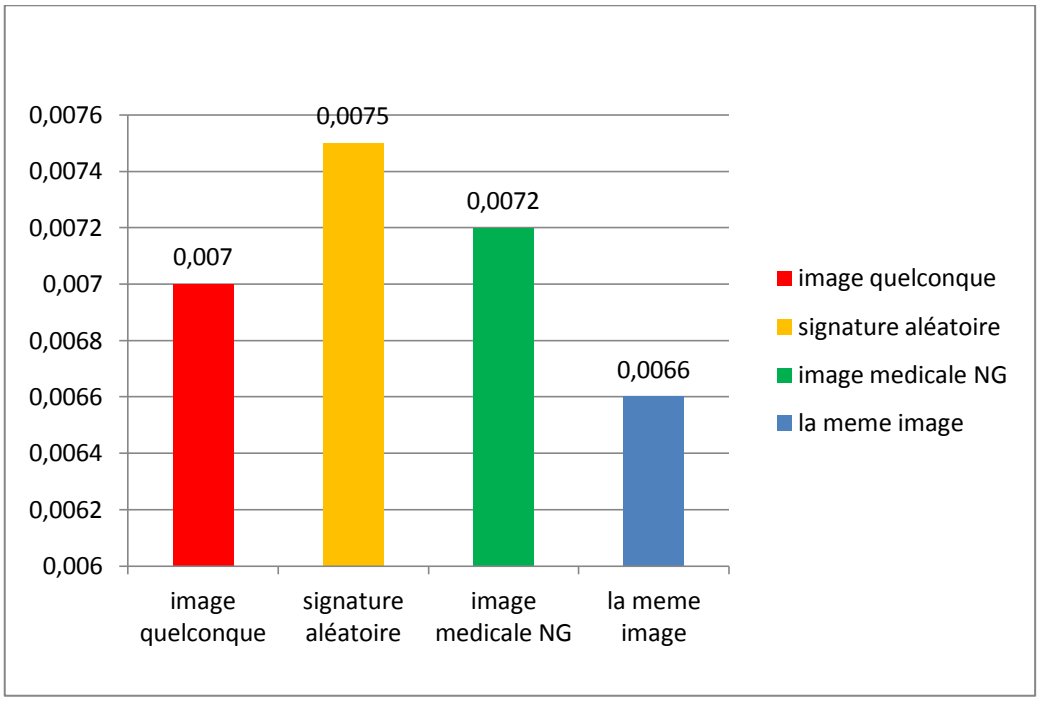


Figure4. 3 MSE des différents types de signature.

Le calcul de PSNR prouve que, si la marque insérée est la même l'image originale, l'image reconstruite a la meilleur qualité. La même marque présente la plus faible valeur de MSE ; c'est-à-dire l'image extraite est plus identique à l'originale.

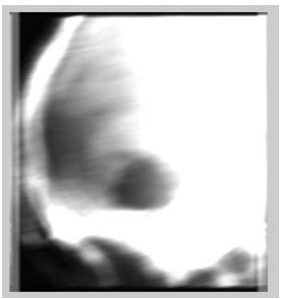
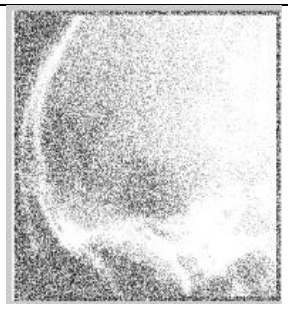
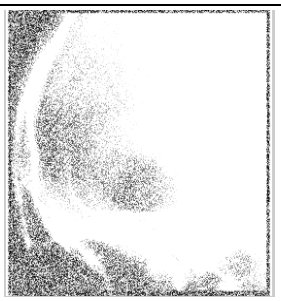
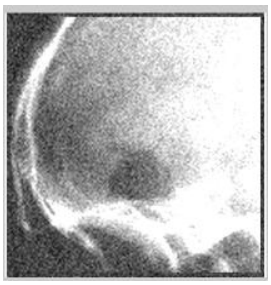
Pour les images médicales, on doit insérer la marque d'une manière invisible pour la bonne consultation du patient; de plus avoir une bonne qualité de l'image extraite (une valeur de PSNR élevée et faible pour celle de MSE).

4.5 Technique de tatouage robuste

Afin d'avoir une technique de tatouage robuste, on insère les basses fréquences de la marque dans celles de l'image médicale. Pour cela, on a appliqué différentes types d'attaques sur l'image médicale tatoué transmise une fois et autre sur l'image médicale.

Le calcul de PSNR et de MSE nous a permis de voir l'effet du tatouage robuste face aux attaques du canal de transmission.

Le tableau ci-dessous résume les résultats obtenus:

Les attaques	Image originale attaqué	Image tatoué attaqué	Image extraite
Un filtre circulaire			
Brui blanc Attaque			

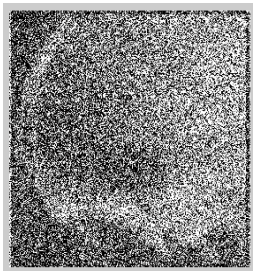
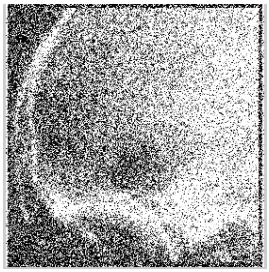
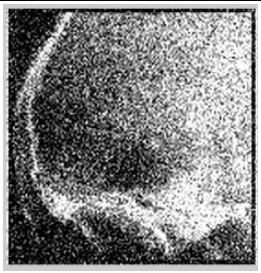
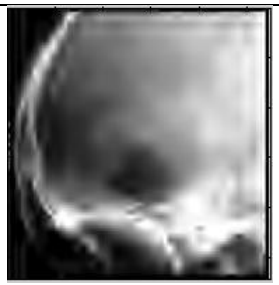
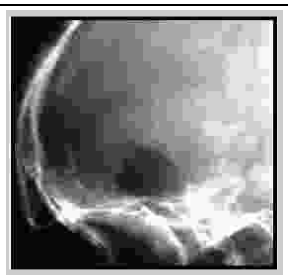
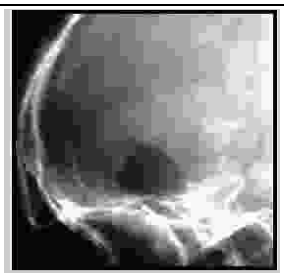
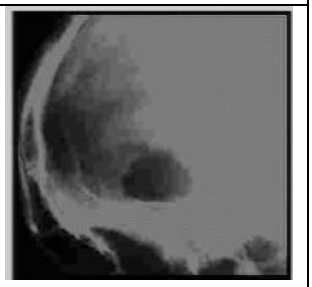
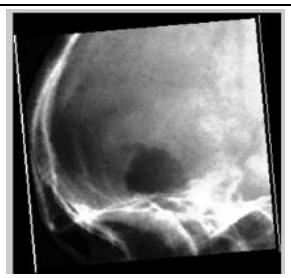
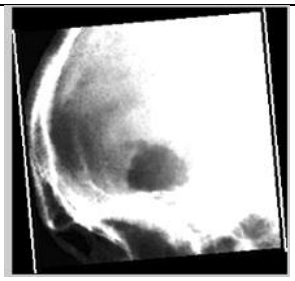
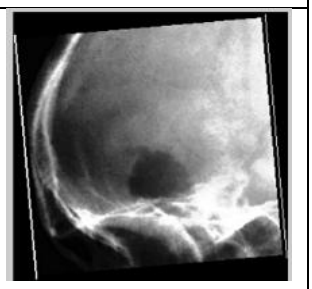
Bruit gaussien			
Compression JPEG 2000			
Compression JPEG			
Rotation géométrique			

Tableau4. 2 Différentes attaques appliquées sur l'image originale et l'image tatouée Avec une signature robuste

Les valeurs de PSNR et MSE obtenus après l'application des attaques ont été résumé dans le tableau 3.4 :

Les attaques	filtre	Bruit blanc	Bruit gaussien	Compression JPEG 2000	Compression JPEG	Rotation géométrique

PSNR (image originale/original attaqué)	44.4	10.99	11,15	34.66	22.47	25.29
MSE (image Originale/origina e attaqué)	0.001	0.33	0.99	0.032	0.070	0.079
PSNR (image originale/ image extraite)	43.8	24.92	26.05	35.03	30.24	25.34
MSE (image originale/ image extraite)	0.001	0.08	0.07	0.030	0.048	0.079

Tableau4. 3 Valeurs des PSNR et MSE obtenus en appliquant les attaques sur l'image tatouée avec une signature robuste

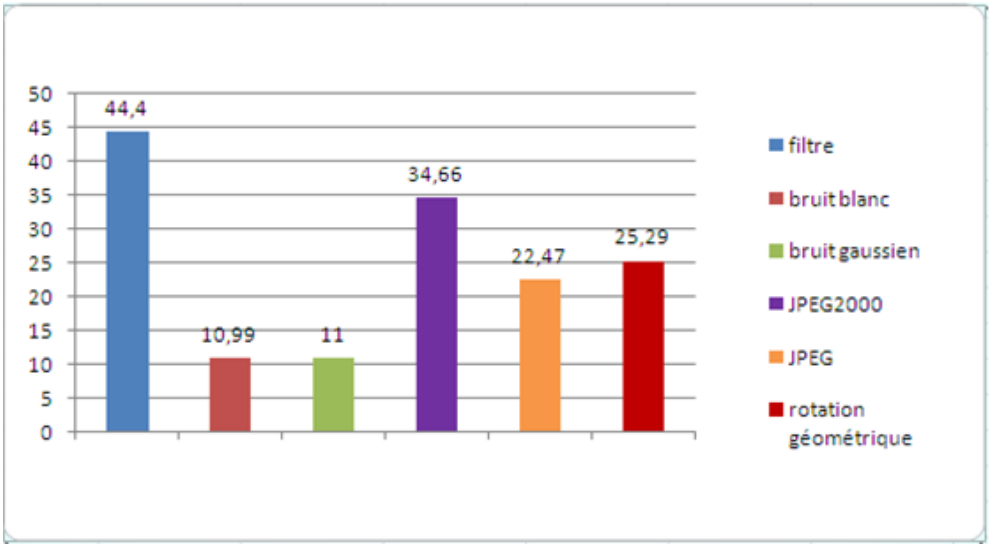


Figure4. 4 PSNR de l'image originale attaqué.

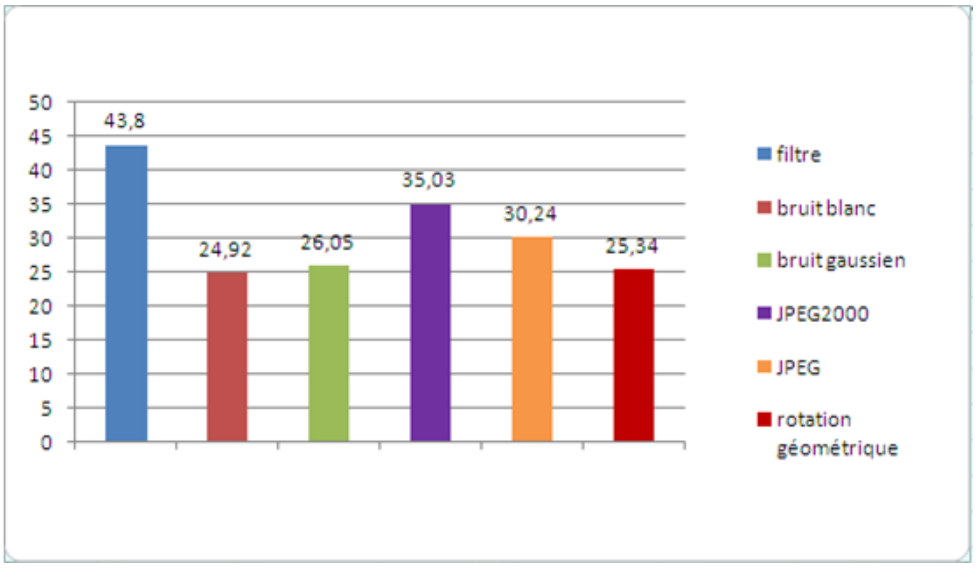


Figure4. 5 PSNR d'image extraite d'une signature robuste attaqué.

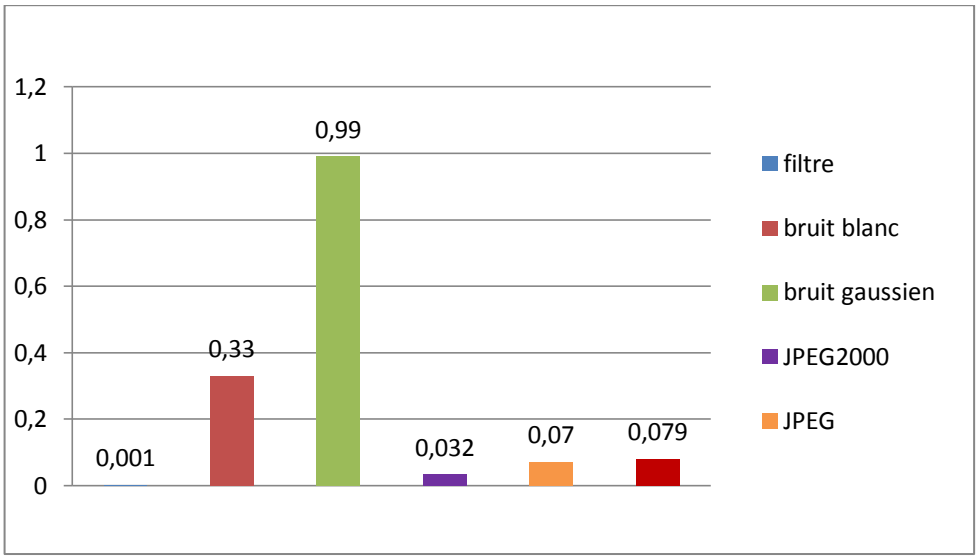


Figure4. 6 MSE d'image originale attaqué.

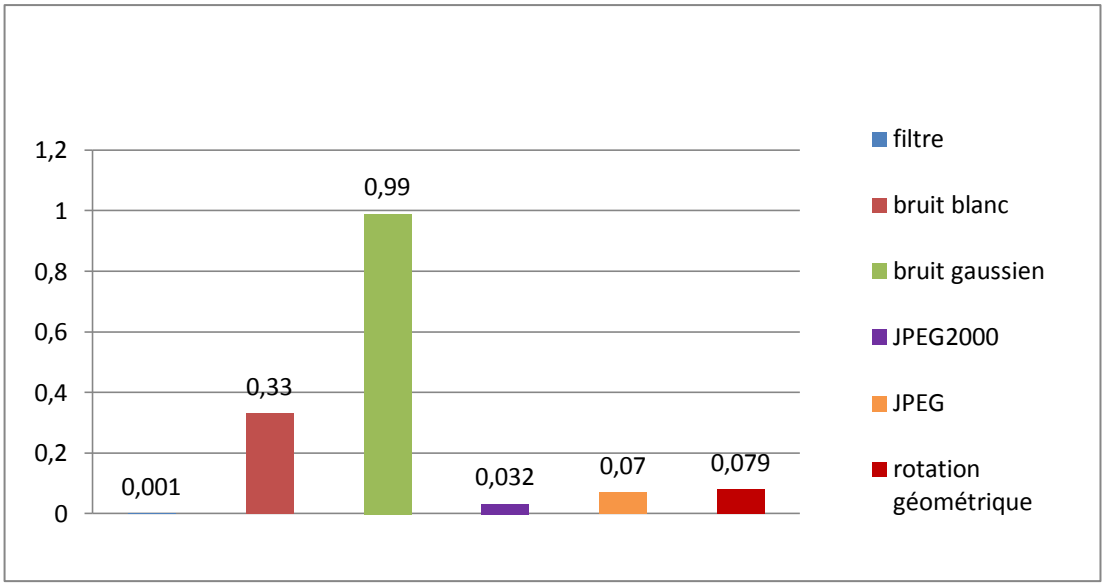


Figure4. 7 MSE d'image extraite d'une signature robuste attaqué.

Les figures en dessus, présentent L'analyse des résultats obtenus, et montrent que la technique utilisé est efficace pour les bruits (blanc, gaussien…etc.), ainsi que la compression avec perte, l'influence est faible dans le cas de compression sans pertes(JPEG2000), la technique utilisé n'empêche pas les filtres et la rotation géométrique.

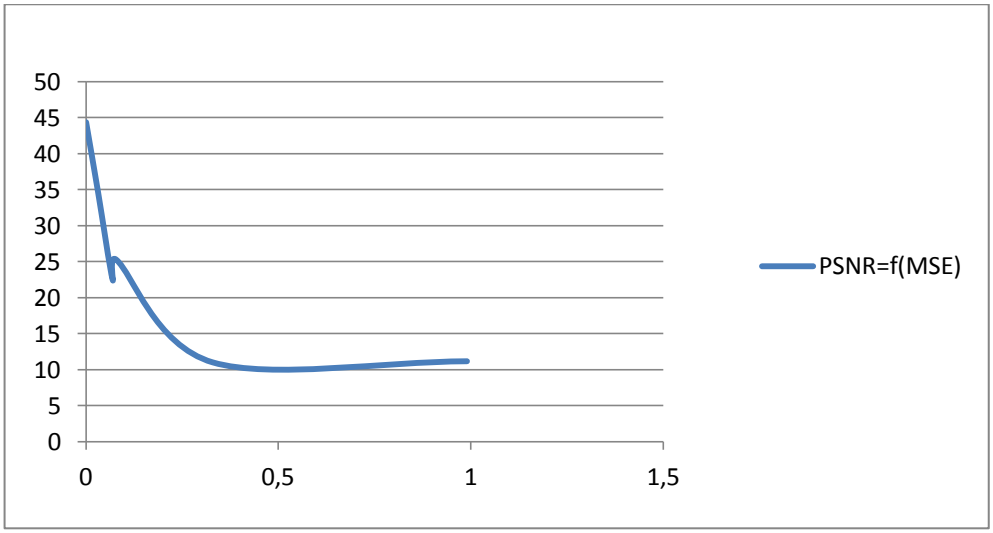


Figure4. 8 PSNR en fonction de MSE d'image originale attaqué.

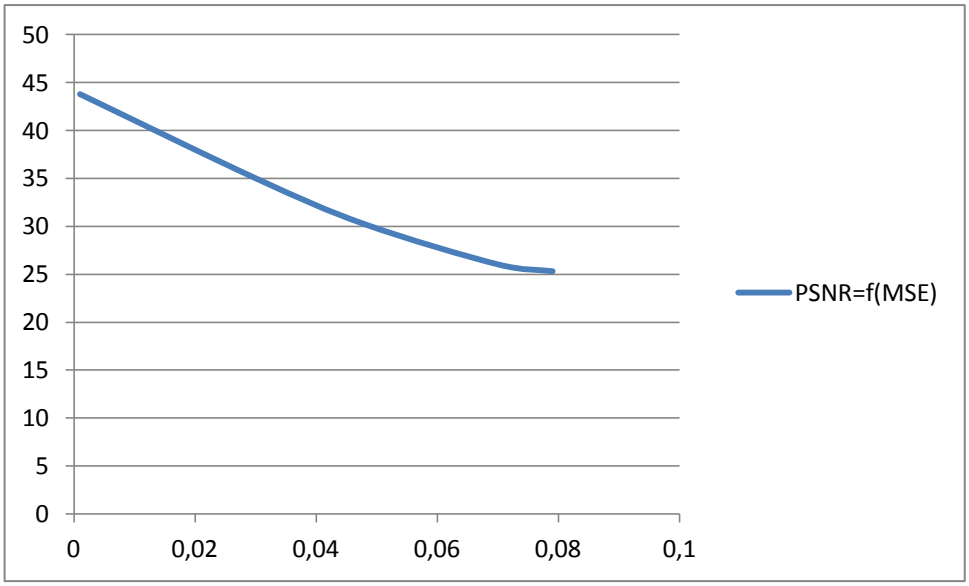


Figure4. 9 PSNR en fonction de MSE d'image extraite d'une signature robuste.

La relation entre les valeurs de PSNR et MSE dans les deux cas : l'image originale attaquée, ainsi que l'image extraite, est présenté dans Les graphes des *figures (4.8 et 4.9).*

Les valeurs de MSE se diminuent en fonction de l'augmentation de PSNR dans les deux cas. Pour l'image originale le PSNR est faible avec toutes les attaques ainsi que les valeurs de MSE sont grandes. L'allure des images tatoués extraites décrit une amélioration de PSNR pour quelque attaque come les bruit, et une diminution de l'intervalle du MSE de [0 à 1] jusqu'à [0 à 0 ,8].

4.5.1 Conclusion

La technique de tatouage robuste est efficace pour les types de bruit à grande puissance et peu à la compression avec perte (JPEG). Par contre dans le cas des filtres et les déformations géométriques, on ne voit pas l'efficacité de la technique utilisée (l'influe de la technique est nul).

4.6 Technique de tatouage fragile

Cette technique est caractérisée par le facteur d'invisibilité, et la capacité de détection de faible attaque, ainsi que les faibles déformations de l'image transmis.

4.6.1 Choix du bon plan d'insertion de tatouage

Dans ce cas on va insérer les détails de la marque dans l'image originale, pour le choix de plan d'insertion, on va insérer les différents plans et analyser les résultats. Le choix du plan d'insertion dépend d'une image à une autre.

a Insertion de cH1 dans ; cV1, cD1

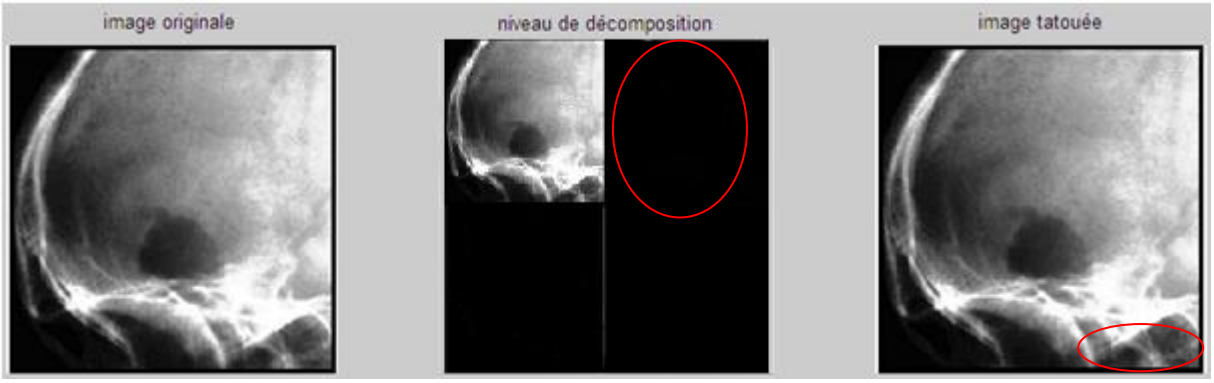


Figure4. 10 Insertion de cH1 dans ; cV1, cD1 sans attaque.

L'insertion du niveau horizontale dans les autres niveaux des détails montre une petite déformation dans l'image.

b Insertion de cV1 dans ; cH1, cD1

Figure4. 11Insertion de cV1 dans ; cH1, cD1 sans attaque.

L'insertion du niveau verticale dans les autres niveaux des détails, montre une altération dans l'image tatouée.

c Insertion de cD1 dans ; cH1, cV1 sans attaque

Figure4. 12 Insertion de cD1 dans ; cH1, cV1 sans attaque.

Après l'insertion du niveau diagonale(CD1) dans les autres niveaux des détails, on aura une image tatoué parfaitement identique à celle originale de point de vue visuelle.

4.6.2 Calcule de corrélation pour la même image

Le calcule de corrélation permet d'analyser la ressemblance entre l'image originale et l'image tatouée, tant que la valeur de corrélation est grande, l'image tatouée est plus identique à celle originale.

Niveau	c H1	c V1	c D1
Corrélation	0,8015	-0,0417	0,0962

Tableau4. 4 Calcule de corrélation des différents niveaux insérer.

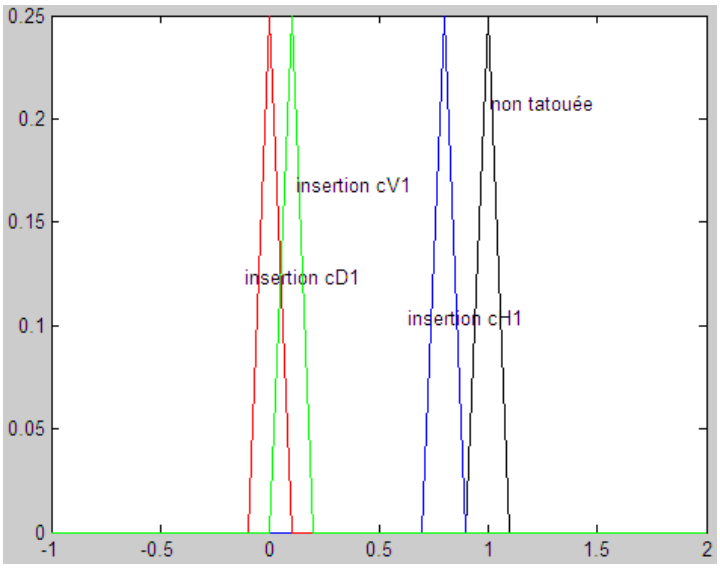


Figure4. 13 Histogrammes de corrélation.

Si le tatouage est visible ; altère l'image originale c'est le cas d'insertion des niveaux horizontale et verticale, mais le calcul de la corrélation montre une bonne ressemblance entre le niveau horizontale de l'image reçue et le niveau horizontale de l'image originale.

Pour cela on propose à insérer le niveau horizontale multipliée par un coefficient « alpha » appelé un coefficient d'invisibilité prend les valeurs de [0 à 1].

Pour que notre système détecte les petites altérations montrant que l'image est non authentique ; pour cela on fixe la corrélation en 0,75 si on veut une récupération de 75% de la signature originale est de 95% de l'image originale ce dernier est calculé par :

Signature de 100% de l'image ⟶ 80,15% de signature

95 % de l'image ⟶ 75 % de signature

Après le choix de la valeur « alpha » on applique la technique de tatouage fragile sur l'image non-attaquée ainsi que sur l'image qui a été affecté aux différentes attaques; l'analyse des résultats obtenus va nous permis de prendre la bonne valeur.

4.6.3 Utilisation d'une image médicale radiologique avec alpha=1

L'image radiologique est une image en niveau de gris ne contient pas beaucoup d'information qu'une image couleur (luminance seulement). On cherche à appliquer le tatouage sans perdre l'aspect visuel complet de l'image (l'information utile)

a L'image tatouée Sans attaque

La corrélation entre le niveau horizontal reçu et original pour ce type d'image est égale à 1 pour ce cas le facteur de corrélation choisi pour la comparaison sera 0,95.

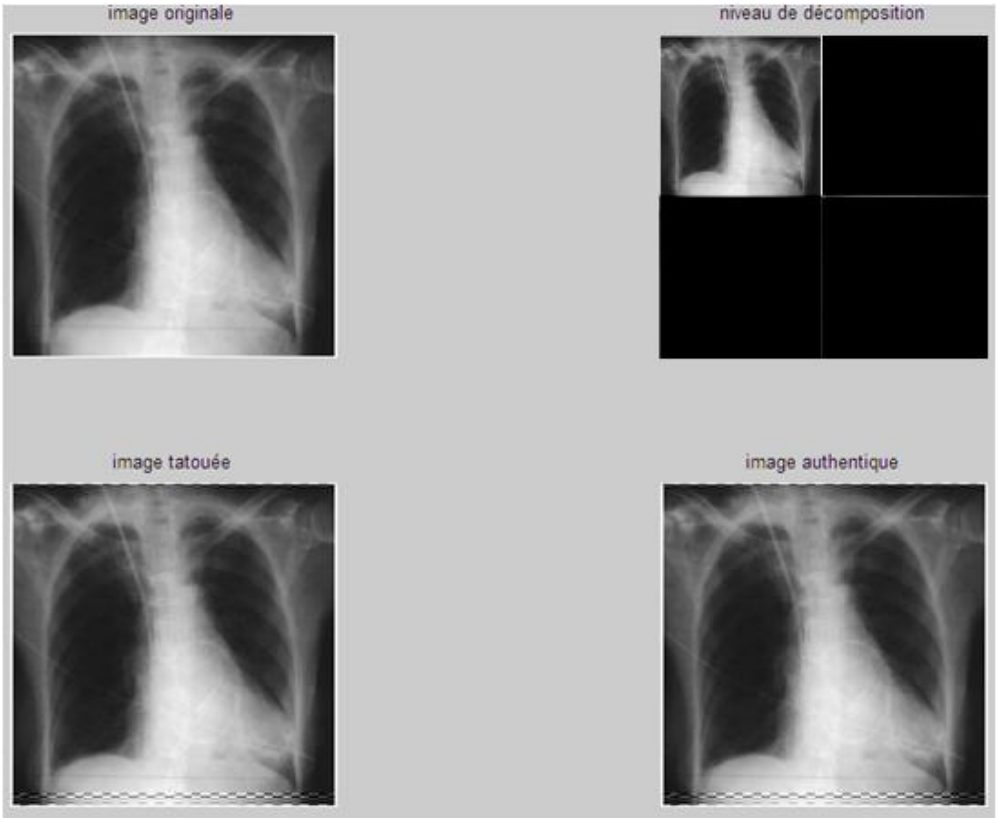


Figure4. 14 Image tatouée sans attaques (fragile, alpha=1).

b bruit blanc gaussien

Figure4. 15 Image tatouée attaquée par bruit gaussien (fragile, alpha=1).

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	57,16 dB	31,35 dB
MSE	0,0033	0,0432
La corrélation	0,43	

Tableau4. 5 paramètres d'insertion de tatouage fragile attaquée par un bruit gaussien

c Bruit blanc à une distribution pseudo aléatoire

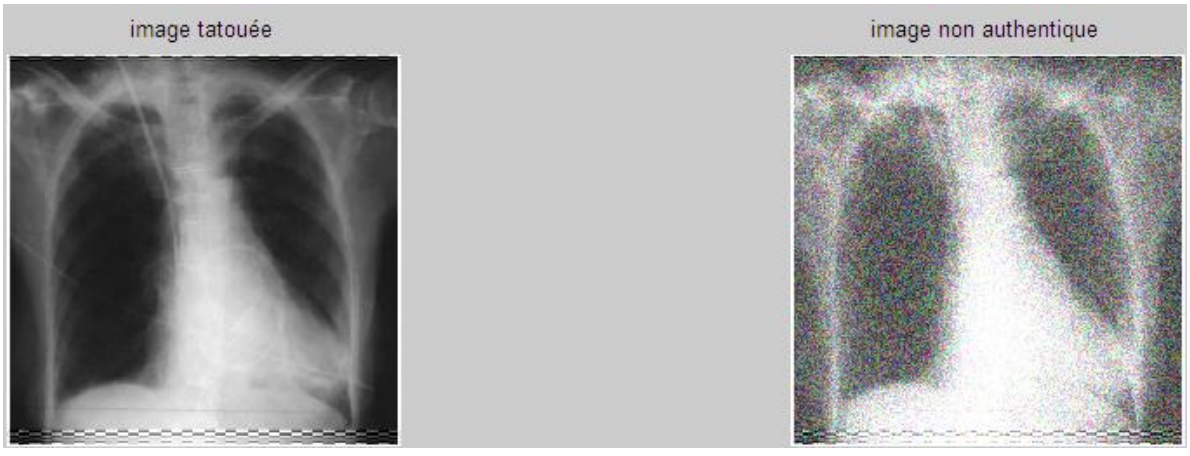


Figure4. 16 Image tatouée attaquée par bruit blanc (fragile, alpha=1).

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	57,16 dB	24,44dB
MSE	0,0033	0,0866
Corrélation	0,54	

Tableau4. 6 Image tatouée attaquée par bruit blanc (fragile, alpha=1)

d Filter

Figure4. 17 Image tatouée attaquée par un filtre circulaire (fragile, alpha=1).

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	57,16 dB	47,24dB
MSE	0,0033	0,0089
La corrélation	-0,017	

Tableau4. 7 Paramètres d'insertion de tatouage fragile attaquée par un filtre circulaire.

e rotation géométrique

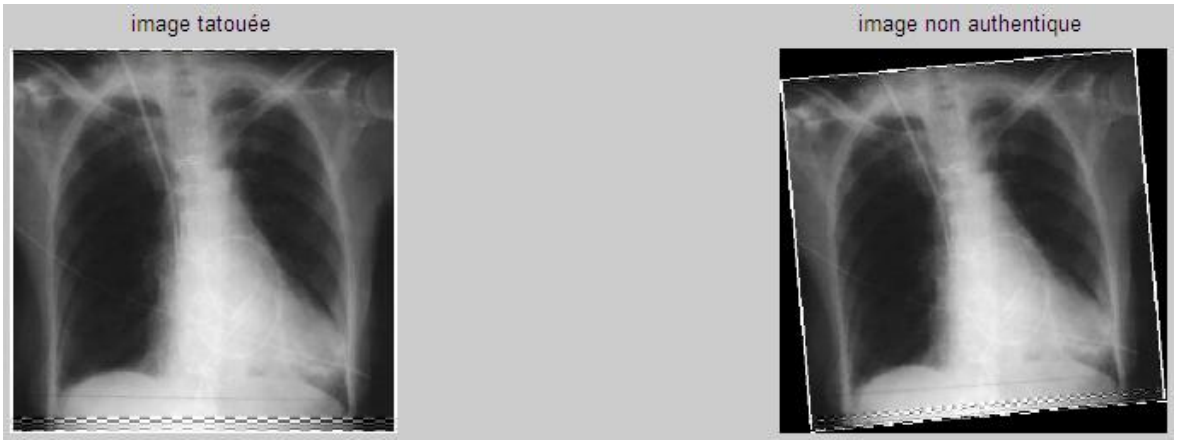


Figure4. 18 Image tatouée attaquée par une rotation (fragile, alpha=1).

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	57,16 dB	28,19dB
MSE	0,0033	0,0596
La corrélation	0,0024	

Tableau4. 8 Paramètres d'insertion de tatouage fragile attaquée par une rotation géométrique.

f compression jpeg avec perte avec un taux de 1%

Figure4. 19 Image tatouée attaquée par compression jpeg (fragile, alpha=1).

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	57,16 dB	56,61dB
MSE	0,0033	0,0035
La corrélation	0,79	

Tableau4. 9 Paramètres d'insertion de tatouage fragile attaquée par une compression JPEG.

g compression jpeg2000 avec perte avec un taux de 1,24%

Figure4. 20 Image tatouée attaquée par compression jpeg2000 (fragile, alpha=1).

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	57,16 dB	65,55dB
MSE	0,0033	0,0014
La corrélation	-0,88	

Tableau4. 10 Paramètres d'insertion de tatouage fragile attaquée par une compression jpeg2000.

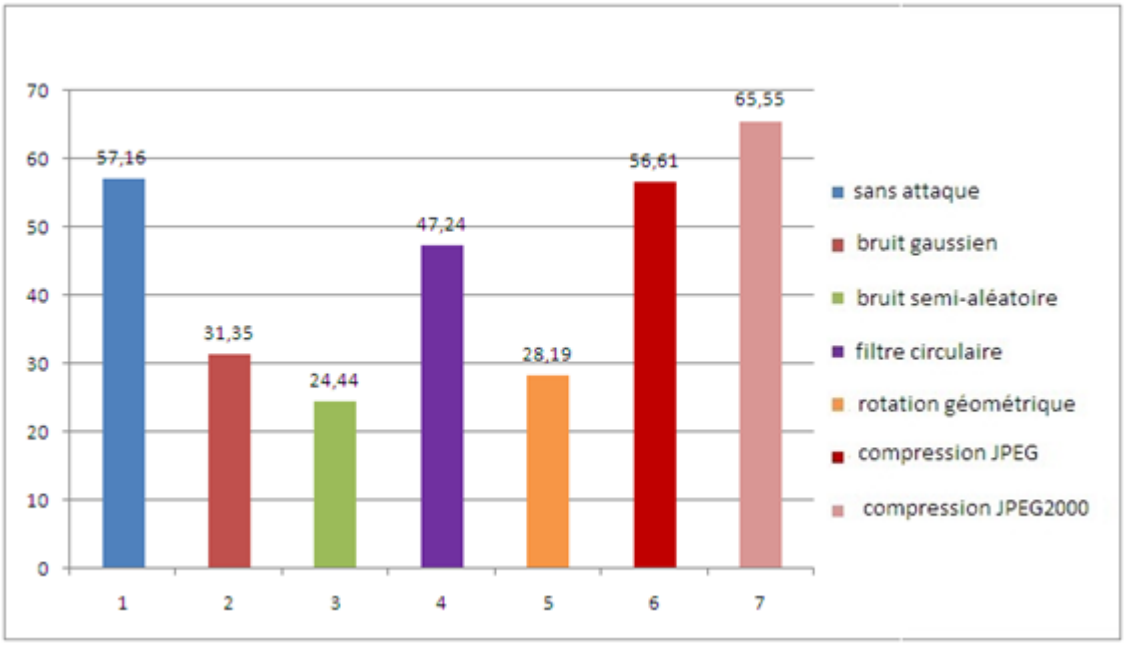


Figure4. 21 Valeurs de PSNR pour alpha=1.

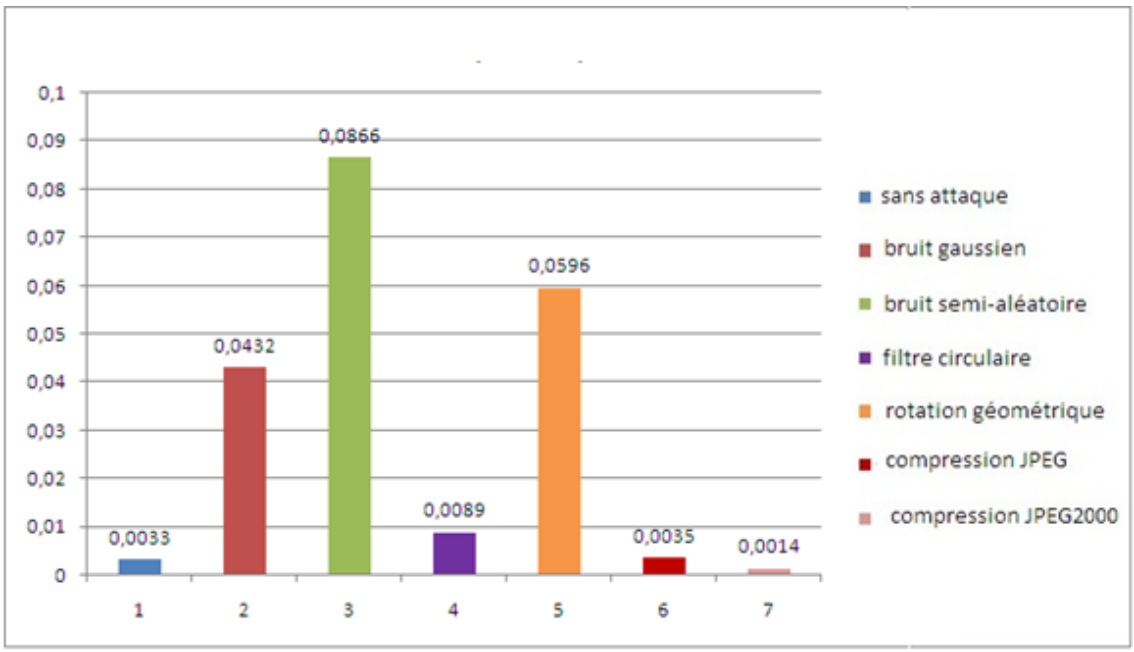


Figure4. 22 Valeurs de MSE pour alpha=1.

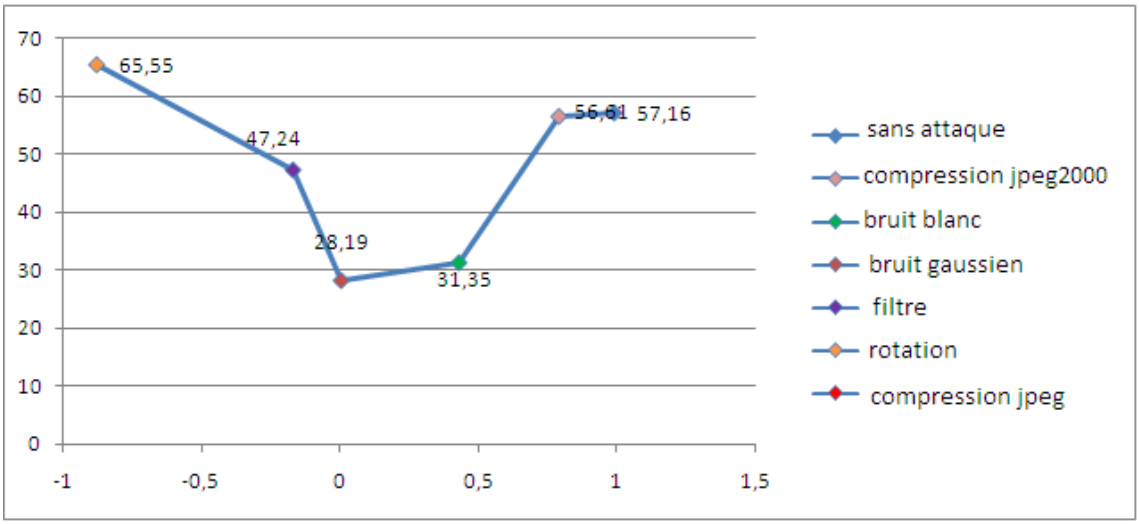


Figure4. 23 Valeurs de PSNR en fonction de MSE pour alpha=1.

Dans le cas de alpha=1, le graphe de PSNR en fonction de corrélation de la *figure 4.23* est non linéaire. On voit que dans le cas d'une image sans attaque la valeur de corrélation est petite par rapport à l'image attaquée malgré qu'elles soient un PSNR élevé ce qui implique que la détection n'est pas précise.

Pour une bonne détection des attaques la plus grande valeur de corrélation doit être correspondre à l'image sans attaque.

Pour trouver une solution de ce problème ainsi que le problème de visibilité de la marque on va changer la valeur de « alpha ».

4.6.4 Insertion de la marque avec : Alpha=0 ,2

a Sans attaque

Après la simulation du programme dans ce cas, l'image reçue est authentique à celle originale.

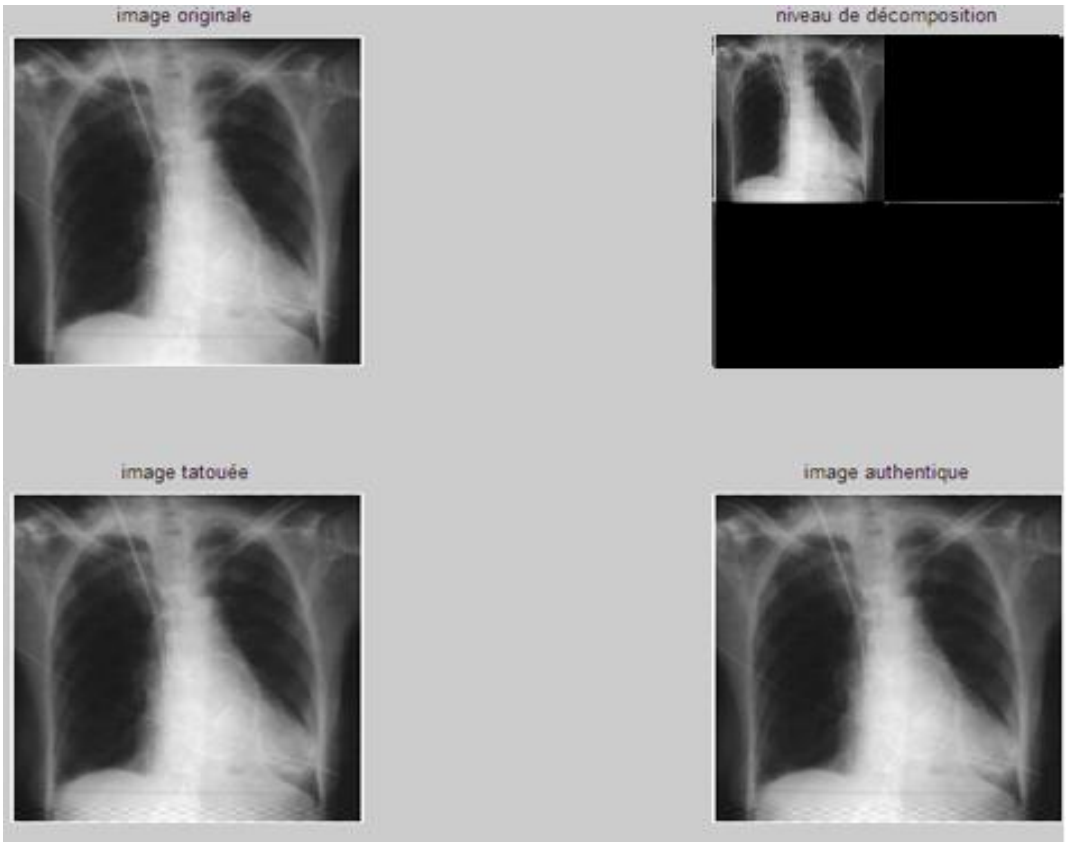


Figure4. 24 Insertion de la marque fragile avec alpha=0.2.

Calcul des paramètres

	Image originale et image tatouée	Image originale et image reçue
PSNR	89.35Db	89,35dB
MSE	$1,31x10^{-4}$	$1,31x10^{-4}$
La Corrélation	1	

Tableau4. 11 paramètres d'insertion de tatouage fragile avec alpha =0.2 sans attaques

b Application des attaques

Les attaques	Les paramètres	Image originale et image tatouée	Image originale et image reçue
Bruit gaussien	PSNR	89.35dB	32,12 dB
	MSE	$1,31x10^{-4}$	0,0402
	Corrélation, détection	0,42 image non authentique	
Bruit blanc	PSNR	89.35dB	24,79 dB
	MSE	$1,31x10^{-4}$	0,083
	Corrélation, détection	0,55 image non authentique	
filtre	PSNR	89.35dB	47,25 dB
	MSE	$1,31x10^{-4}$	0,0089
	Corrélation, détection	-0,0017 image non authentique	
Rotation géométrique	PSNR	89.35dB	28,32 dB
	MSE	$1,31x10^{-4}$	0,058
	Corrélation, détection	0,003 image non authentique	
Compression avec perte jpeg	PSNR	89.35dB	66,31 dB
	MSE	$1,31x10^{-4}$	0,0013
	Corrélation, détection	0,93 image non authentique	
Compression avec perte jpeg2000	PSNR	89.35dB	65,55 dB
	MSE	$1,31x10^{-4}$	0,0014
	Corrélation, détection	-0,88 image non authentique	

Tableau4. 12 Paramètres calculés d'une image tatouée attaquée (fragile, alpha=0,2) .

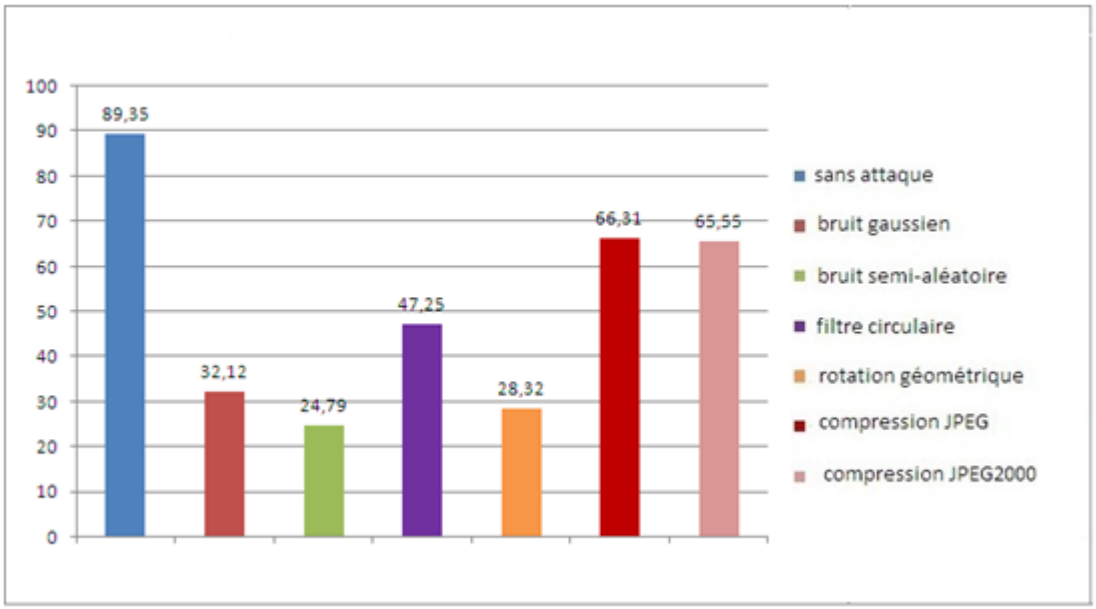


Figure4. 25 Valeurs de PSNR pour alpha=0.2 dans le tatouage fragile.

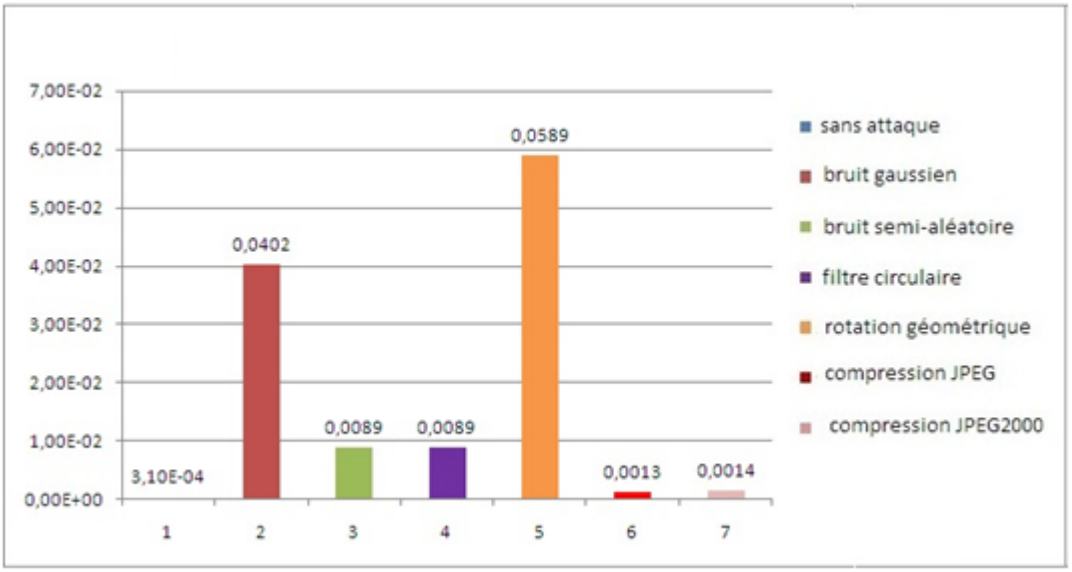


Figure4. 26 Valeurs de MSE pour alpha=0.2dans le tatouage fragile.

En analysant les graphes ci-dessous, on remarque une amélioration importante dans les valeurs de PSNR et MSE, par rapport au choix de alpha=1.

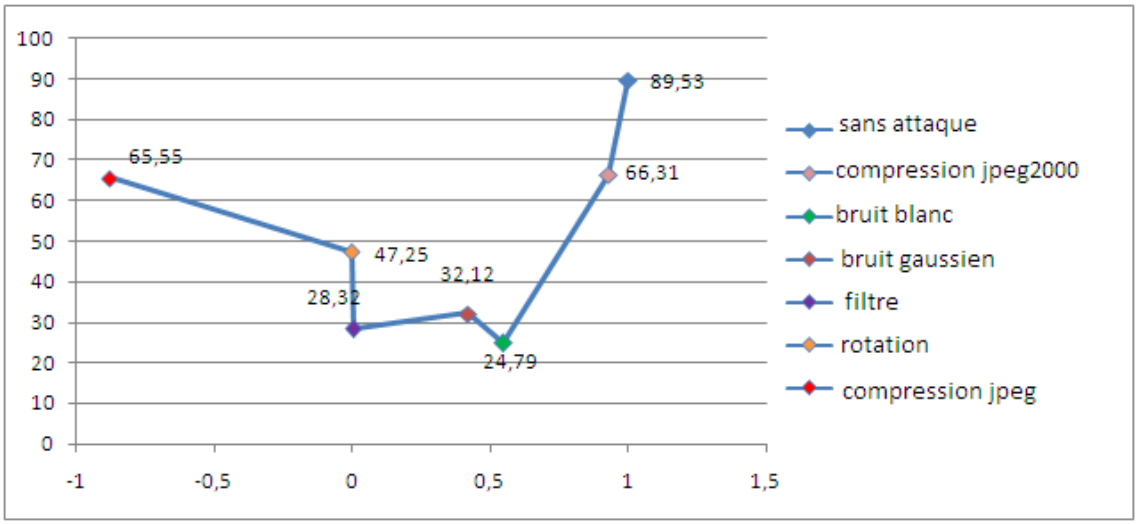


Figure4. 27 Valeurs de PSNR en fonction de corrélation pour le tatouage fragile et alpha=0.2.

L'allure des valeurs de PSNR en fonction de corrélation selon la *figure4.27*, décrit que la linéarité entre ces deux paramètres reste toujours un problème à poser, mai au même temps on remarque que la valeur la plus grande de corrélation correspond à la valeur la plus grande de PSNR, c'est à dire la détection dans ce cas est meilleur.

4.6.5 Conclusion

L'analyse des expériences montre que le choix de la valeur de alpha=O.2 ; donne le meilleurs effet de la technique choisis (bonne détection), soit pour l'image originale et même pour l'image tatouée dans les deux cas : attaqué et sans attaque.

4.7 Technique de tatouage multiple

Pour avoir un compromis des deux techniques de tatouages précédentes, on doit insérer une marque multiple (c'est-à-dire deux signature) : le niveau CA1 la signature robuste et CH1 la signature fragile, afin d'avoir une bonne protection et détection des altérations de l'image médicale transmis.

4.7.1 Analyse de tatouage sans attaque

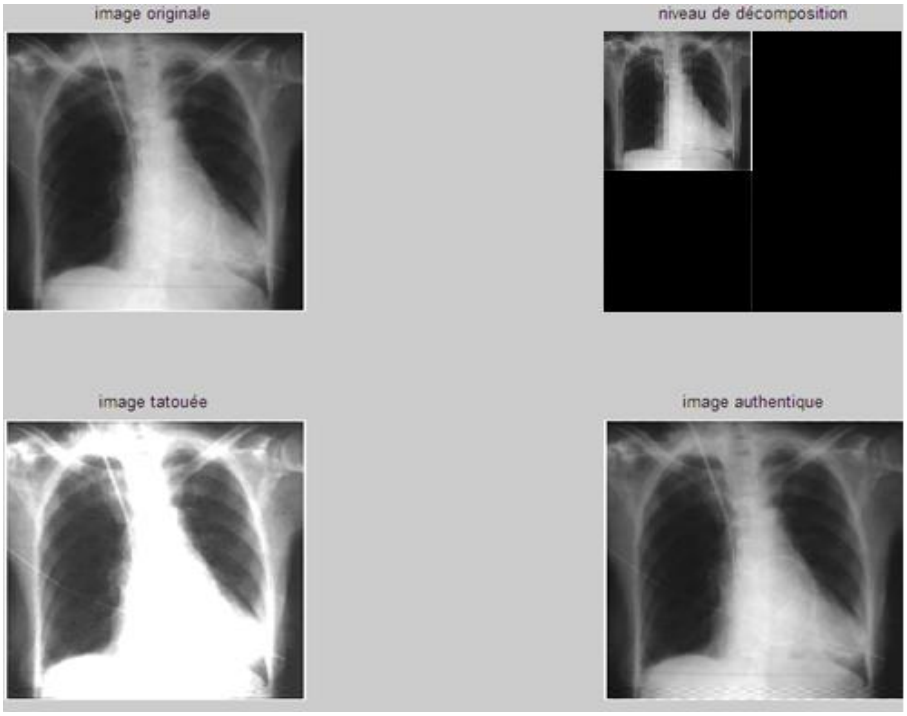


Figure4. 28 Insertion de signature multiple

PSNR (originale, extraite) dB	MSE (originale, extraite)	La Corrélation
88,73	$1,4x10^{-4}$	0 ,96

Tableau4. 13 Paramètres de signature multiple sans attaques

4.7.2 Application des attaques

a bruit gaussien

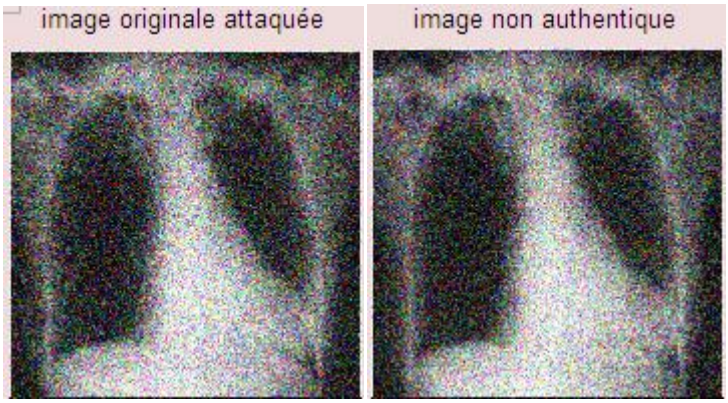


Figure4. 29 Comparaison entre image originale et image tatouée attaquée par bruit gaussien (multiple, alpha=0 ,2).

PSNR (originale, extraite) dB	MSE (originale, extraite)	Corrélation
34,22	0,0326	0 ,41

Tableau4. 14 Les paramètres calculés d'une image attaqué par bruit gaussien (multiple, alpha=0 ,2).

b bruit blanc

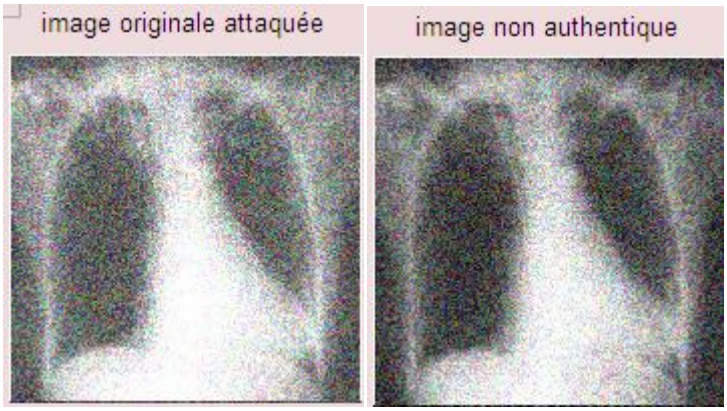


Figure4. 30 Comparaison entre image originale et image tatouée attaquée par bruit blanc (multiple, alpha=0 ,2).

PSNR (originale, extraite) dB	MSE (originale, extraite)	Corrélation
34,19	0,0327	0 ,53

Tableau4. 15 Paramètres d'une image attaqué par bruit blanc (multiple, alpha=0 ,2).

c filtre

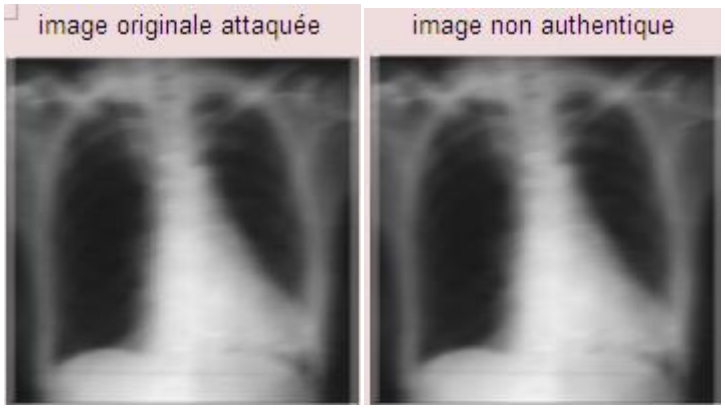


Figure4. 31 Comparaison entre image originale et image tatouée attaquée par un filtre (multiple, alpha=0 ,2).

PSNR (originale, extraite) dB	MSE (originale, extraite)	Corrélation
47,28	0,088	0 ,15

Tableau4. 16 Paramètres calculés d'une image attaqué par bruit blanc (multiple, alpha=0 ,2).

d rotation géométrique

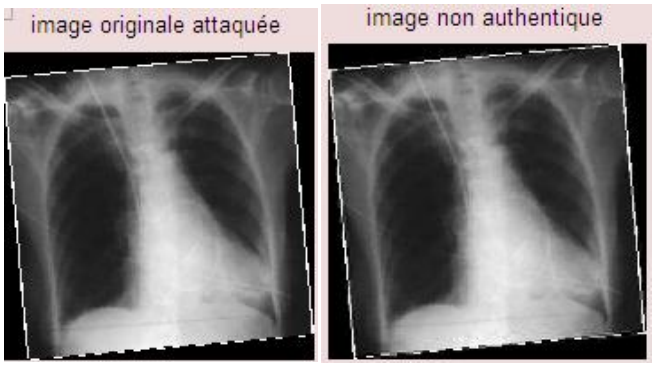


Figure4. 32 Comparaison entre image originale et image tatouée attaquée par rotation géométrique (multiple, alpha=0 ,2).

PSNR (originale, extraite) dB	MSE (originale, extraite)	Corrélation
27,85	0,0617	0 ,0046

Tableau4. 17 les paramètres d'une image attaqué par une rotation géométrique (multiple, alpha=0,2)

e compression JPEG

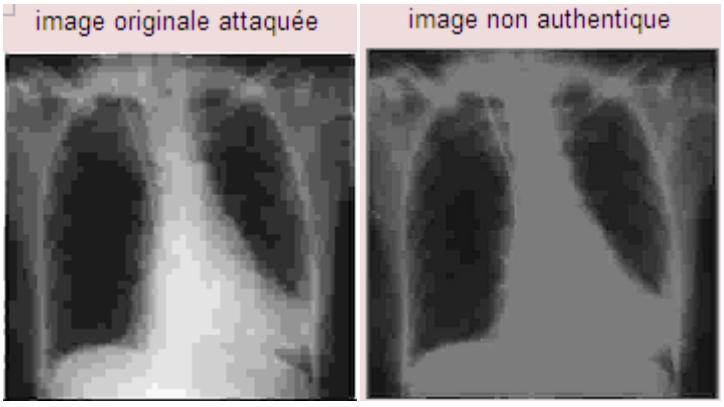


Figure4. 33 comparaison entre image originale et image tatouée attaquée par compression JPEG (multiple, alpha=0 ,2).

PSNR (originale, extraite)dB	MSE (originale, extraite)	Corrélation
35,78	0,0279	-0,66

Tableau4. 18 les paramètres d'une image attaqué par une compression JPEG (multiple, alpha=0,2)

ƒ la compression JPEG 2000

Figure4. 34 comparaison entre image originale et image tatouée attaquée par compression JPEG (multiple, alpha=0 ,2)

PSNR (originale, extraite) dB	MSE (originale, extraite)	Corrélation
36,28	0,0266	0 ,69

Tableau4. 19 les paramètres d'une image attaqué par une compression jpeg (multiple, alpha=0,2).

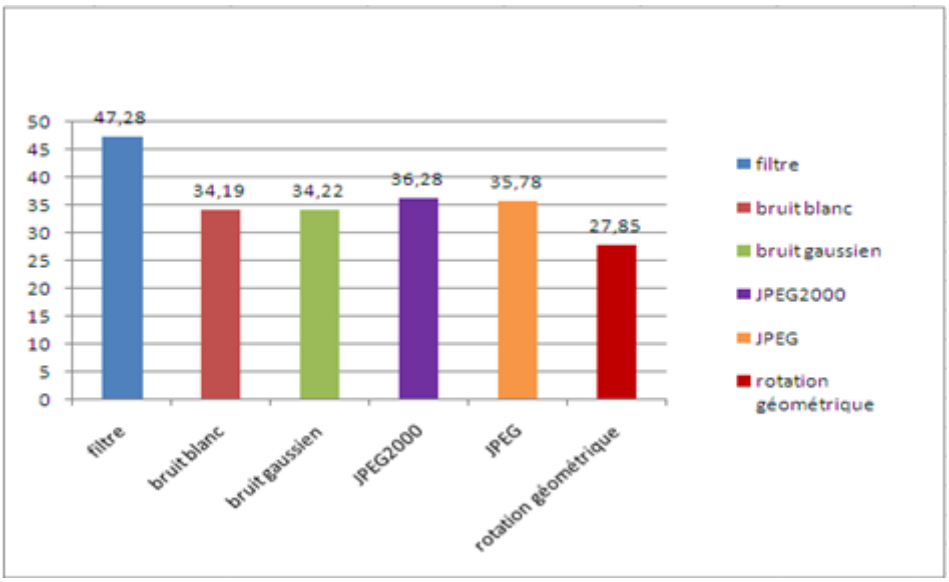


Figure4. 35 PSNR de l'image extraite d'insertion de signature multiple

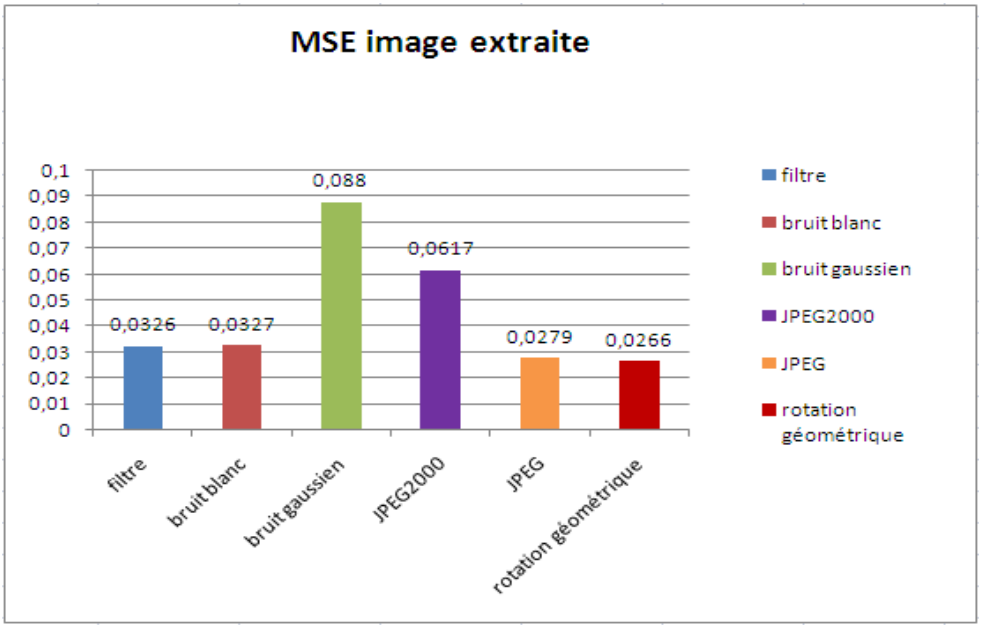


Figure4.36 MSE de l'image extraite d'une signature multiple.

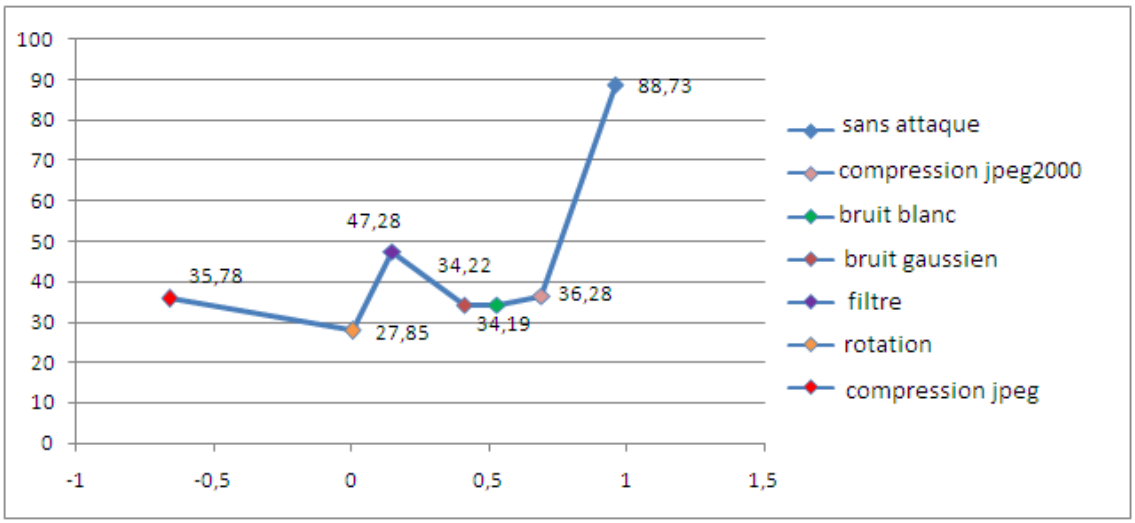


Figure4. 37 PSNR en fonction de corrélation d'une signature multiple

L'allure de graphe de *la figure 4.37* décrit que la valeur de PSNR supérieur est correspondante à l'image tatouée sans attaques ; ce qui prouve que détection est juste.

L'analyse des graphes des *figure (4.35, 4.36 et 4.37)* et les valeurs des facteurs d'évaluation (PSNR, MSE), ainsi que les images obtenus lors de tatouage, décrit l'intérêt de cette technique ; le but sera donc de détecter les attaque et les déformations de l'image médicale, et même de protéger sa qualité pendant sa transmission.

4.7.3 Conclusion

L'insertion d'une signature multiple (robuste et fragile), a pour rôle la détection et la robustesse face à différentes attaques qui altèrent l'image médicale transmis dans un réseau de la télémédecine.

4.8 Application du tatouage multiple à une image médicale couleur (rétinienne)

Dans cette partie on va mettre en œuvre le tatouage multiple sur une image rétinienne (image couleur), et calculer les différents paramètres d'évaluation en appliquant les différentes attaques sur l'image tatouée, pour décrire l'efficacité de la technique utilisé sur les images couleur.

Pour évaluer la technique appliquer sur une image couleur, on va analyser chaque composante de chrominance toute seul, car on est en train d'étudier trois matrices : pour la rouge, la verte, et la bleue.

4.8.1 Application de tatouage sans attaque

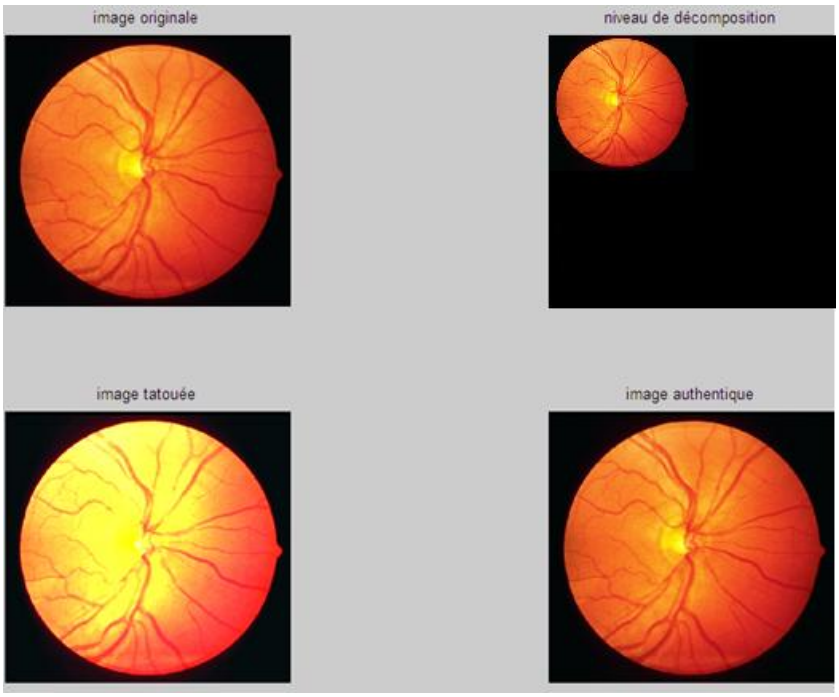


Figure4. 38 Tatouage multiple d'une image médicale couleur.

	PSNR (originale, extraite) dB	MSE (originale, extraite)	La Corrélation
rouge	78.32	$3.7499x10^{-006}$	0.9278
Vert	84.55	$8.9437x^{-007}$	0.9281
Bleu	74.47	$9.1125x^{-006}$	0.9257

Tableau4. 20 les paramètres d'image couleur tatoué par une signature multiple

4.8.2 Application de tatouage Avec attaque

a Bruit gaussien

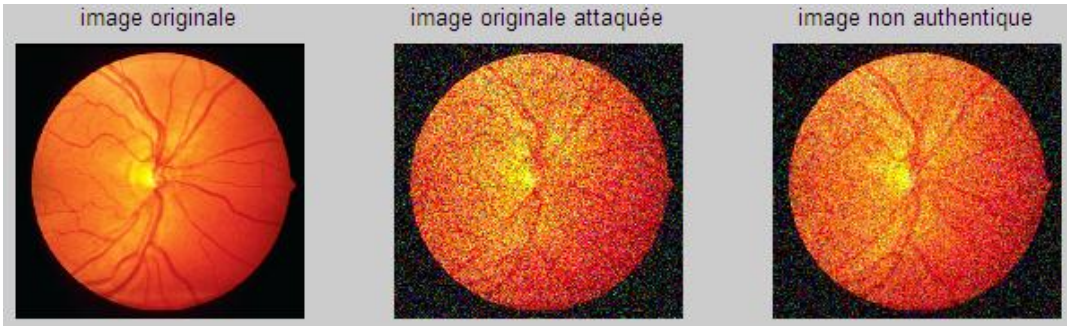


Figure4. 39 Image médicale couleur tatouée par une signature multiple attaqué par un bruit gaussien.

	PSNR (original avec attaque)	MSE (original avec attaque)	PSNR (originale, extraite)	MSE (originale, extraite)	Corrélation
rouge	32.1939	0.1540	36.6901	0.0546	0.0319
vert	32.2172	0.1532	36.7382	0.0542	0.0314
bleu	16.2645	6.0329	20.9207	2.1167	0.0336

Tableau4. 21 paramètres d'image médicale couleur tatoué par une signature multiple attaqué par un bruit gaussien.

b Bruit blanc

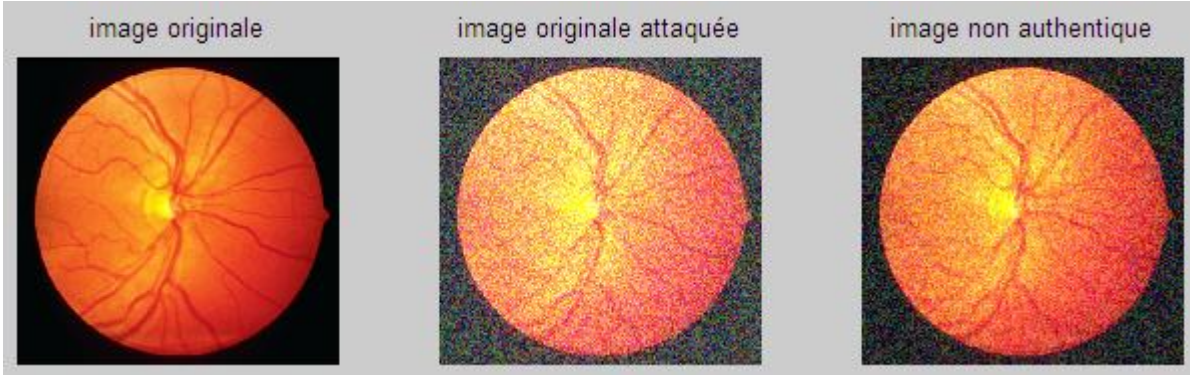


Figure4. 40 Image médicale couleur tatouée par une signature multiple attaqué par un bruit blanc.

	PSNR (original avec attaque)	MSE (original avec attaque)	PSNR (original, extraite)	MSE (originale, extraite)	Corrélation
rouge	24.8447	0.8366	35.5484	0.0711	-0.0528
vert	24.8491	0.8357	35.5021	0.0719	0.0488
bleu	8.9232	32.7081	19.5497	2.8314	0.0567

Tableau4. 22 Paramètres d'image médicale couleur tatoué par une signature multiple attaqué par un bruit blanc.

c Filtre circulaire

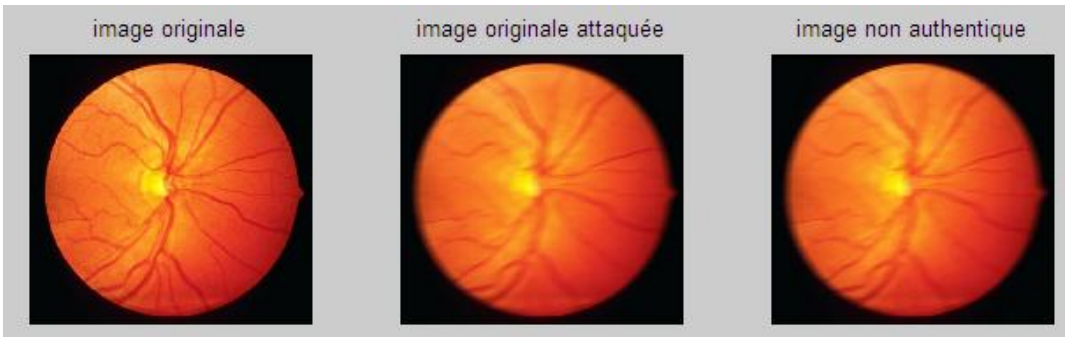


Figure4. 41 Image médicale couleur tatoué par une signature multiple attaqué par un filtre circulaire.

	PSNR (original avec attaque)dB	MSE (originale avec attaque)	PSNR(originale , extraite) dB	MSE (originale, extraite)	La Corrélation
rouge	64.3637	$9.3456x10^{-005}$	63.6579	$1.0995x10^{-004}$	-0.2665
vert	66.8742	$5.2427x10^{-005}$	66.6930	$5.4660x10^{-005}$	-0.2600
bleu	63.6800	$1.0939x10^{-004}$	63.5688	$1.1223x10^{-004}$	-0.2692

Tableau4. 23 paramètres d'image médicale couleur tatoué par une signature multiple attaqué par un filtre circulaire.

d la compression Jpeg

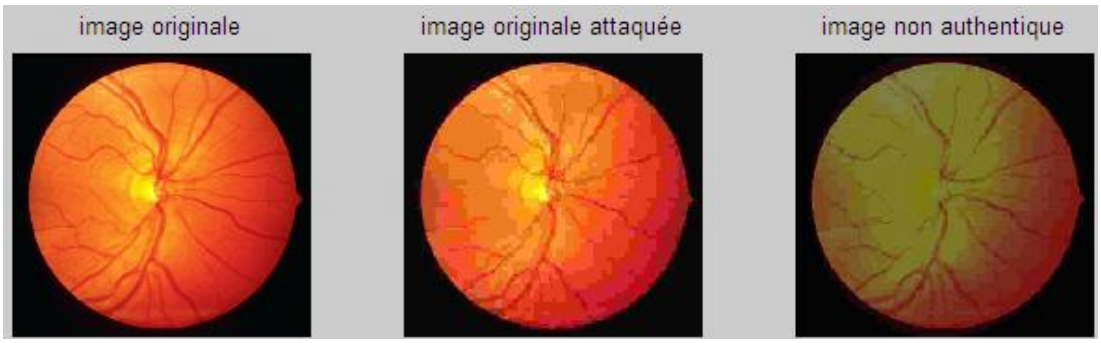


Figure4. 42 Image médicale couleur tatoué par une signature multiple attaqué par une compression JPEG.

	PSNR(original avec attaque)	MSE (originale avec attaque)	PSNR(originale ,extraite) dB	MSE(original e ,extraite)	Corrélation
rouge	62.4679	$1.4460x10^{-004}$	21.3284	1.8799	-0.0625
vert	66.5199	$5.6883x10-^{005}$	55.4169	$7.3331x10^{-004}$	-0.0410
bleu	43.8349	0.0106	52.9816	0.0013	-0.0093

Tableau4. 24 paramètres d'image médicale couleur tatoué par une signature multiple attaqué par une compression JPEG.

e la compression Jpeg2000avec le taux de compression=2,04

Figure4. 43 Image médicale couleur tatoué par une signature multiple attaqué par une compression jpeg2000.

	PSNR(original avec attaque)	MSE(originale avec attaque)	PSNR(originale ,extraite) dB	MSE(original e ,extraite)	Corrélation
rouge	82.9471	$1.2950x10^{-006}$	19.9053	2.6088	-0.2153
vert	81.7947	$1.6885x10^{-006}$	35.4915	0.0721	-0.2496
bleu	67.3542	$4.6941x10^{-005}$	39.8961	0.0261	-0.2037

Tableau4. 25 paramètres d'image médicale couleur tatoué par une signature multiple attaqué par une compression jpeg2000.

f la Rotation géométrique

Figure4. 44 Image médicale couleur tatoué par une signature multiple attaquée par une rotation géométrique.

	PSNR (original avec attaque)	MSE (originale avec attaque)	PSNR(originale ,extraite) dB	MSE(originale,extraite)	Corrélation
rouge	28.8521	0.3325	28.5583	0.3558	-0.0078
vert	42.6975	0.0137	42.6570	0.0138	-0.0057
bleu	45.7948	0.0067	45.6325	0.0070	-0.0093

Tableau4. 26 Paramètres d'image médicale couleur tatoué par une signature multiple attaqué par une rotation géométrique.

Le calcul de PSNR dans ce cas sera sur les trois composante (rouge, verte, bleue), car leur distribution n'est pas identique comme le cas des images en niveau de gris.

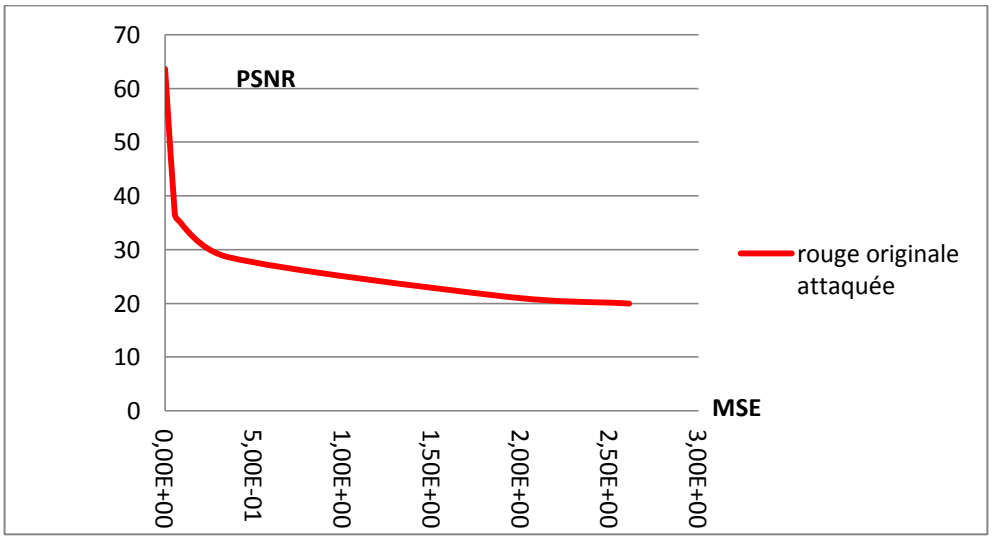


Figure4. 45 PSNR en fonction de MSE pour la composante rouge de l'image originale.

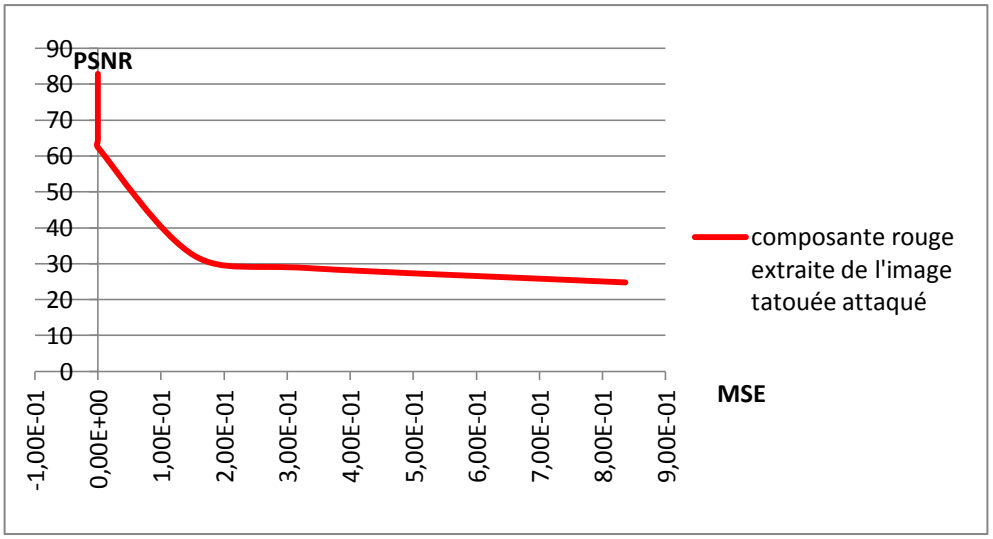


Figure4. 46PSNR en fonction de MSE pour la composante rouge de l'image extraite.

L'amélioration de PSNR en fonction de MSE pour la composante rouge se vue au milieu de l'intervalle par contre a l'extrémité selon *les figures (4 .45 et 4.46)*, elle montre un effet inverse de tatouage robuste pour quelques types d'attaques.

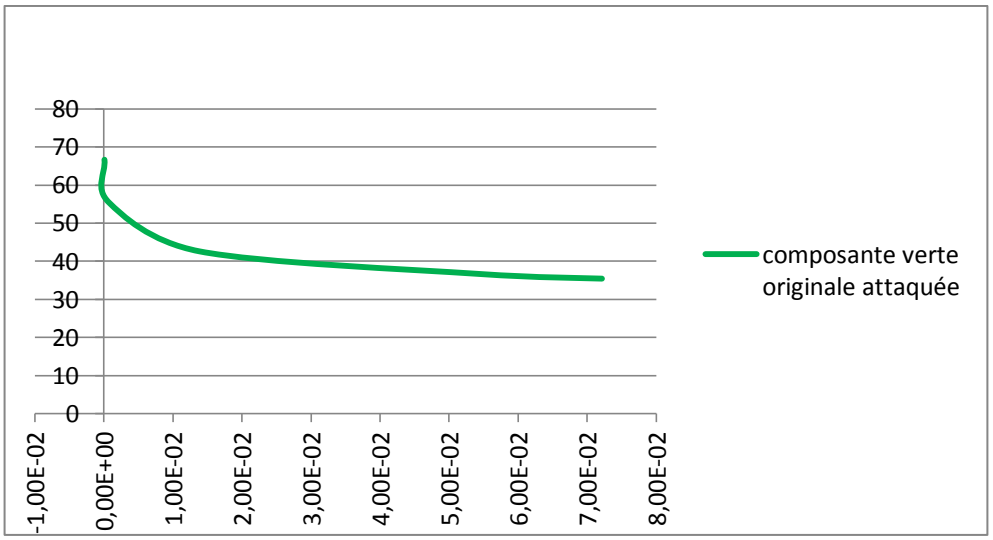


Figure4. 47 PSNR en fonction de MSE pour la composante verte de l'image originale.

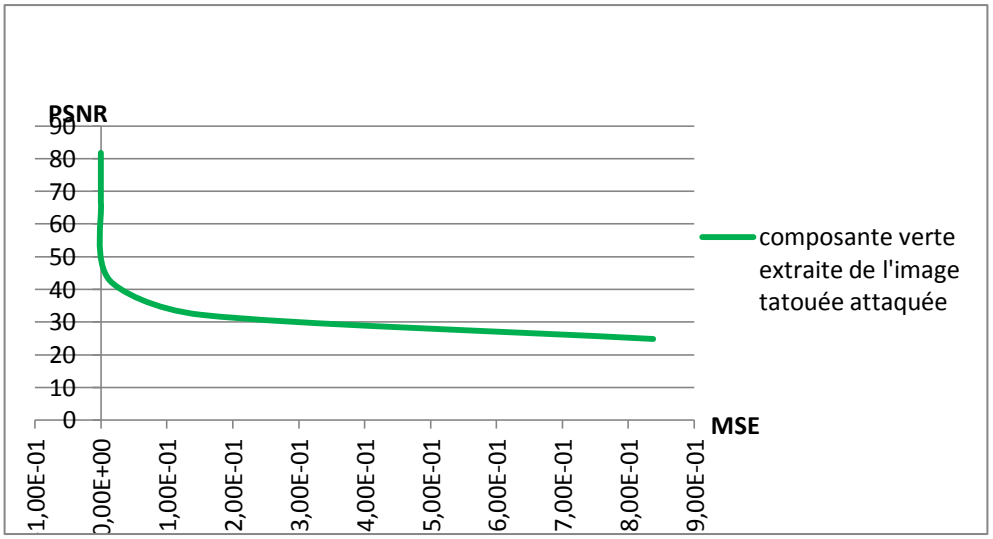


Figure4. 48 PSNR en fonction de MSE pour la composante verte de l'image extraite.

Pour la composante verte on remarque une linéarité de la courbe sans augmentation de MSE selon *les figures (4.47 et 4.48),* qui veut dire que l'influence des attaques sur la composantes verte est faible c'est dû que l'image contient une faible quantité d'information verte.

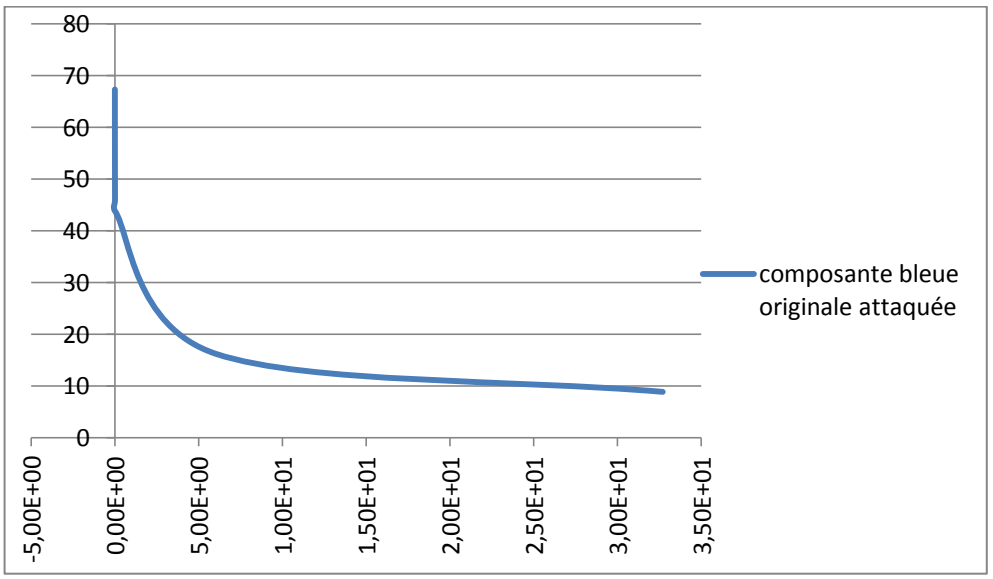


Figure4. 49 PSNR en fonction de MSE pour la composante bleue de l'image originale attaquée.

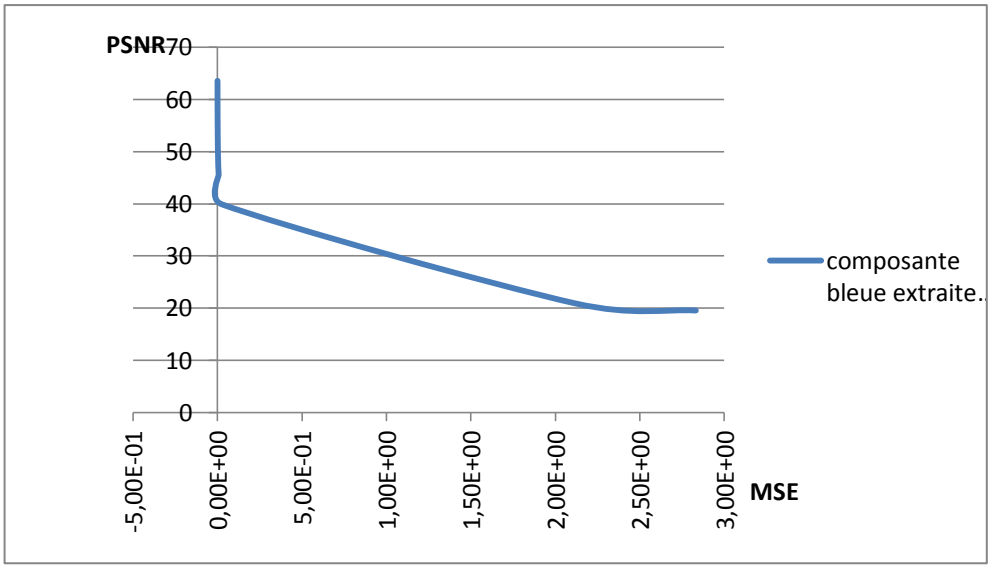


Figure4. 50 PSNR en fonction de MSE pour la composante bleue de l'image extraite attaquée.

L'application du tatouage sur la composante bleue est presque sans effet, les valeurs de PSNR et MSE montrés dans les graphes des figures (4.49 et 4.50) ne décrit aucun changement sensé, c'est dû au faible distribution de la couleur bleue dans l'image.

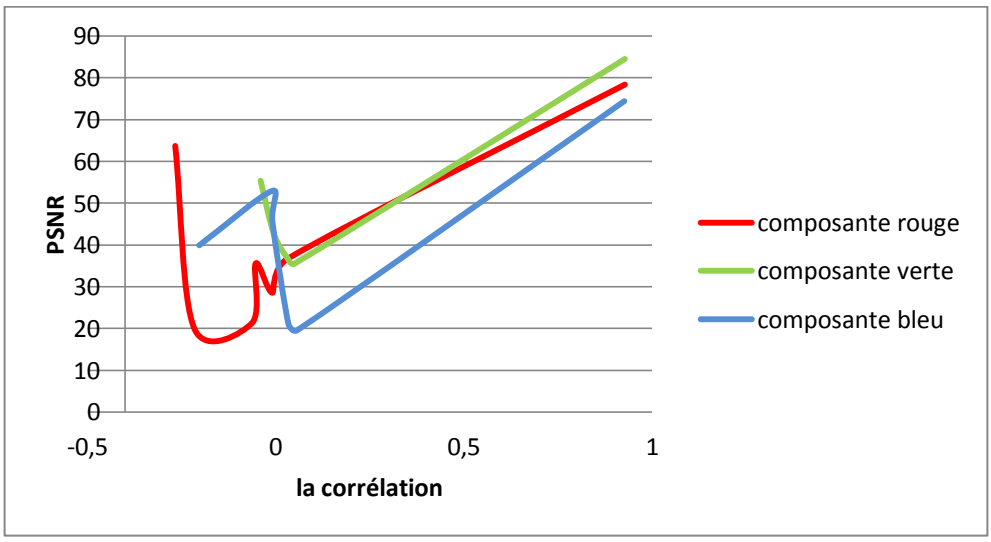


Figure4. 51 PSNR en fonction de corrélation pour les trois composantes de couleurs.

L'allure de graphe de la figure 3.51 des trois couleurs RVB, montre que le score de corrélation le plus grand correspond a la plus grande valeur de PSNR. On remarque

que l'intervalle de PSNR et de la corrélation de la couleur rouge plus large que d'autres couleurs.

On voit que la technique est efficace pour les images couleurs, en particulier la composante rouge dans ce cas. elle est plus influencée que les autres composantes, ce qui est montré dans les graphes obtenus. Cette dégradation des résultats causée par la distribution des couleurs de l'image choisie: la composante rouge est major.

4.9 Conclusion

Dans ce chapitre nous avons présenté les différents résultats obtenus lors de l'application des schémas des techniques proposées après une présentation de l'environnement de programmation, ainsi que l'interface de l'application avec toutes les fonctionnalités qu'elle permet d'accomplir à travers des prises d'écran, et cela dans le but de faciliter son utilisation.

L'analyse de ces différentes techniques de tatouage repose sur la sensibilité des images médicales par rapport aux images multimédia, donc l'amélioration des techniques de tatouages des images médicale ne se termine pas, malgré qu'on ait montré que la technique multiple est meilleure.

Conclusion générale

Le tatouage des images comme technique trouve sa place dans le domaine de la télémédecine. Dans ce contexte notre travail de recherche a pour objectif de comparer entre différentes techniques de tatouage avec les images médicales ;.

De ce fait, et comme technique, notre étude est basée sur l'utilisation des algorithmes de tatouage ainsi : robuste, fragile et multiple.

Plusieurs résultats ont été obtenus par différentes techniques :

En premier lieu, et par l'application de la technique robuste sur des images en niveaux de gris, les résultats montrent une amélioration de PSNR et MSE surtout pour le bruitage. Par contre et sur autres attaques ainsi : les déformations géométriques, les filtres, et la compression avec perte, les résultats de la technique robuste ne montrent pas une telle amélioration.

Donc, dans notre cas la protection par cette technique est insuffisante.

Pour cela, autres solutions ont été prospecté, comme la détection d'une attaque c'est le cas du tatouage fragile.

En deuxième lieu, et dans l'objectif de détecter si le document a subi des transformations, et plus spécifiquement si son intégrité a été préservée, On a utilisé la technique de tatouage fragile.

Les résultats montrent l'efficacité de cette technique pour tous types d'attaques appliquées, mais la variation de PSNR en fonction corrélation n'était pas linéaire. Donc, il est possibilité d'avoir une attaque presque insensée (PSNR élevé) avec

un facteur de corrélation très faible. On peu dire que, la détection dans ce cas n'est pas intéressante.

En dernier lieu, on a intéressé à mélanger le tatouage fragile avec celui robuste pour la détection et la protection en même temps. C'est le tatouage multiple.

Les résultats obtenus sont plus performants, et cette technique est la meilleure solution.

En effet, le résultat obtenu par, L'application de la technique multiple sur une image couleur (RVB) montre une différence entre chaque type d'attaque et pour chaque composante de couleur.

Ainsi l'image couleur contient plus d'information que l'image en niveau de gris (luminance, chrominance). Le calcule de PSNR est le meilleur pour le bruitage, et pour la composante de couleur major dans l'image.

L'extraction de la signature ou de l'image sera semi aveugle dans les trois cas à la présence de la signature originale, à la réception permet de garder le principe de la simplicité et l'efficacité au but d'estimer la meilleure technique de tatouage.

D'après tous ce qu'on a obtenus, on conclure que la protection des images médicale nécessite la détection de l'attaque. En effet, il est mieux de détecter seulement un ensemble donné de transformations (interdites). On peut par exemple autoriser certains taux de compression, des changements d'échelle. Dans ce cas, il est intéressant d'utiliser des méthodes de tatouage semi-fragile (il ne résiste pas des attaques autorisées qui ne perturbent pas l'information utile).

Comme perspectif, et Pour une bonne détection et protection dans le réseau de la télémédecine, il est nécessaire d'aider les médecins au diagnostic des images médicales.

Annexes

Formats des fichiers image

Un fichier informatique est une sorte d'enveloppe virtuelle qui contient des informations pour recréer l'image. On peut reconnaître ses fichiers (dans l'Explorateur Windows par exemple), par leurs extensions. Les extensions les plus courantes sont: BMP- DXF - EPS - GIF - JPG – PHOTO CD-PCX-PICT-PS-TIFF-WPG

- **BMP (BitMaP)** : Le format BMP est le format par défaut du logiciel Windows. C'est un format matriciel. Les images ne sont pas compressées.

- **DXF :** Le format DXF est un format vectoriel créé par la compagnie AutoDesk pour son logiciel de CAO AUTOCAD. Est un format très répandu dans le monde de la conception et du dessin assisté par ordinateur, et très peu répandu en d'autres domaines.
- **EPS (Encapsulated PostScript)** : Un document en format EPS vectoriel est un fichier en langage PostScript décrivant le contenu d'une image.

- **GIF (GraphicalInterchange Format)** : Le format GIF est un format qui a ouvert la voie à l'image sur le World Wide Web. C'est un format de compression qui n'accepte que les images en couleurs indexés codé sur 8 bits, soit en 256 couleurs.

- **JPEG (Joint Photographic Experts Group)** : Les images JPEG sont des images de 24 bits. C'est la meilleure qualité d'images disponible.

- **Photo CD:** Créé par la compagnie KODAK, ce format est utilisé par les laboratoires de photographies afin de transférer des négatifs de photos sous une forme numérique, généralement sur un CD-ROM.

- **PCX :** Le format PCX est utilisé par le logiciel Paintbrush sous Windows. C'est un format matriciel.
- **PICT :** Le format PICT est un format vectoriel interne au fonctionnement du Macintosh. C'est le format utilisé par le Presse-Papier du Macintosh. Il peut contenir des éléments graphiques ou des images numérisées.

- **PS (PostScript) :** Ce format est également une façon sûre de rendre disponible un document seulement pour impression sans droit de modification. Il s'agit toutefois d'un format très lourd à éviter lorsqu'il doit être transféré par Internet sur des liens à basse vitesse.

- **TIFF (Tagged Image File Format):** conçu à l'origine par la compagnie Aldus est un format matriciel. Conçu au départ pour n'accepter que les images en RGB, ce format permet de coder des images CYMK. Ainsi une image CYMK enregistrée en format TIFF peut être placée dans un logiciel de mise en pages et être envoyée à l'impression sans perte de qualité au niveau de l'image.

- **WPG :** Le format WPG est un format utilisé par les logiciels de la gamme de WordPerfect (WordPerfect, DrawPerfect, WP Presentations et autres) sous DOS, Windows ou Macintosh. C'est un format vectoriel qui donne un résultat acceptable lors de l'impression, mais qui doit surtout être utilisé en tant que format de travail. D'autant plus que ce n'est pas un format qui est reconnu par tous les logiciels.

Bibliographie

[1]. H. hocine, I.Oudjoudi, H.Ahmane, A. Abbassene, M.Boumaraf, L.Sekkai, la télémédecine pour le Désenclavement des zones Sahraoui en ALGERIE. Centre de développement des technologies avancées alger, page1, 2010.

[2]. Androuchko L. et W right D ;Les telecommunications et la santé., « Telemedicine and developing countries », Journal of Telemedicine and Telecar e, vol. 2, nºpage 2, 1996, RSM Press(Royal Society of Medicine Press) Ltd.

[3]. Anne-Sophie MAZEIRAT Juriste SHAM , Article La télémédecine est désormais considérée comme un acte médical à part entière. *7/04/2011*

[4]. Philippe Lefebvre et Michel Aka, Applications : Commerce électronique et Télémédecine, La Telemedecine 4 décembre 2000,

[5]. *Site de CRDP* Académie de *Grenoble* site d'autoformation à l'image numérique, les images numériques.

[6]. Pr Guy Frija, Secrétaire Général de la Société Française de Radiologie, · Pr Bernard Mazoyer, Directeur, Groupe d'Imagerie Neurofonctionnelle, UMR6095, CNRS, CEA, Universités de Caen et Paris 5 ; L'imagerie médicale .Texte rédigé par Clara Delpas pour le site web de la Fondation pour la Recherche Médicale Avril 2002

[7]. Ali JabeurBouzidi ;Développement de techniques de marquage d'authentification pour la protection de données multimédias MÉMOIRE pour obtention du grade de Maîtrise en informatique le 28/09/2009.

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

[9]. 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.

[10]. 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.

[11]. 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.

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

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

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

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

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

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

[18]. N.Komatsu et H.Tominaga authentication system using concealed image in telematics 1988

[19]. Cox Ingemar J., Miller Matthew L., Bloom Jeffrey A., "Digital Watermarking", *Academic Press*, 1st Edition, 2002.

[20]. site internet de la société digimarc 2005,

[21]. site internet de la société corbis 2005

[22]. site internet de la société gettyimages.2005.

[23]. F.A.P.Petitcolas, R.J.Anderson,et M.G.Kuhn. attacks on copyright marking systems. Dans *information Hiding. Second Internationnal Workshop,IHS98, pages 219-239.*

[24]. F.A.P.Peticolas. Watermarking schemes evaluation. Dans I.E.E.E.Signal Processing, volume vol.17,no,5,page5864,2000.

[25]. F.Hartung. et M.Kutter .multimedia watermarking techniques.Proceedings of IEEE(USA), 87(7):1079-1107,1999.

[26]. Vincent Martin ;thèse *:* École doctorale : Informatique et Télécommunications Spécialité : Signal, Image, Acoustique et Optimisation ,contribution des filtres LPTVET des techniques d'interpolation au tatouage numérique soutenue le 28 novembre 2006.

[27]. P. BAS: Soft-SCS : improving the security and robustness of the Scalar-Costa-Scheme by optimal distribution matching. In Proc. of the thirteenth Int. Workshop on Information Hiding, 2011

[28]. P. Bas, "Méthodes de Tatouage d'images fondées sur le contenu", Thèse de doctorat de L'INPG, Grenoble, Octobre 2000.

[29]. P. BASet F. CAYRE: Achieving Subspace or Key Security for WOA using Natural or Circular Watermar-king.In MM&Sec '06 : Proceedings of the 8th workshop on Multimedia and security, p. 80–88, New York, NY, USA, 2006. ACM.

[30]. G. R. BLAKLEY, C. MEADOWSet G. B. PURDY: Fingerprinting long forgiving messages. In Proc. Of Crypto'85, p. 180–189. Springer Berlin / Heidelberg, 1985.

[31]. D. BOESTEN et B. SKORIC: Asymptotic fingerprinting capacity for non-binary alphabets. Arxiv preprint arXiv : 1102. 0445, 2011.

[32]. D. BONEH et J. SHAW: Collusion-secure fingerprinting for digital data. Information Theory, IEEE Tran-sactions on, 44(5):1897 –1905, sep 1998.

[33]. K.R. Rao and P. Yip. Discrete cosinus transform: algorithms, advantages, applications. *Academic Press Inc.*, 1990.

[34]. E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. *IEEE Workshop on Nonlinear Signal and Image Processing*, Thessaloniki, Greece, 1995.

[35]. Site de TALISMAN ACTS Project AC019f.

[36]. J.J.K Ó Ruanaidh and T. Pun. Rotation, translation and scale invariant digital image watermarking. *IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97)*, vol. 1, pp. 536-539, Santa-Barbara, CA, Oct. 1997.

[37]. D. Kundur and D. Hatzinakos. Digital watermarking using multi-resolution wavelet decomposition. *In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 6, pp. 2969-2972, 1998.

[38]. H.-J. Wang and C.-C Jay Kuo. Image protection via watermarking on perceptually significant wavelet coefficients. *In Proceedings of IEEE Multimedia Signal Processing Workshop (MMSP'98),* pp. 279-284, Redondo Beach CA USA, Dec. 1998.

[39]. X.-G. Xia, C.G. Boncelet and G.R. Arce. Wavelet transform based watermark for digital images. *Optis Express*, 3(12): 497-511, Dec. 1998.

[40]. W. Zeng, B. Liu and S. Lei. Extraction of multi-resolution watermark images for claiming rightful ownership. *In Proceedings of SPIE, Electronic Imgaging'99, Security and Watermarking of Multimedia Contents*, vol. 3657, San-Jose, USA, Jan. 1999.

[41]. P. BAS: Soft-SCS : improving the security and robustness of the Scalar-Costa-Scheme by optimal distribu-tion matching. In Proc. of the thirteenth Int. Workshop on Information Hiding, 2011.

[42]. D. BONEHet J. SHAW: Collusion-secure fingerprinting for digital data. Information Theory, IEEE Tran-sactions on, 44(5):1897 –1905, sep 1998.

[43]. E. BERLEKAMP: Nonbinary BCH decoding. University of North Carolina. Dept. of Statistics, 1966.

[44]. M. Maes, C. M. Van overveld, 'Digital watermarking by digital warping', proceeding of the IEEE ICIP, vol. II, Chicago IL,p. 424-429,1998.

[45]. J. Puate and F. Jordan. Using fractal compression scheme to embeded a digital signature into an image. *Proc. of SPIE Photonics East Symposium*, vol. 1, Boston, USA, Nov. 18-22 1996.

[46]. F. Autrusseau, A. Saadane, and D. Barba. Psychovisual approach for watermarking. SPIEElectronicImaging,January2001

[47]. S. Chouchane, W. Puech : ntégration d'un nouveau marqueur dans le codeur d'images EZW basé sur les ondelettes.

[48]. Fred Truchetet ; ondelette pour le signale numérique, Editions Hermes, Paris, 1998

[49]. M. J. Y. Réveilles cours à l'Université Clermont -Ferrand II, France, dans le cadre du DEA d'Informatique-Productique-Imagerie Médicale, 1998-1999 publié dans wavelette par otium

[50]. YOUSSEF BENTALEB Analyse par ondelettes des signaux sismiques applications aux ondes de surface Soutenue publiquement le 18 mai 2007.

[51]. Imen FOURATIKALLEL ; Elaboration d'une nouvelle approche de tatouage réversible pour la vérification d'intégrité des images médicales. Dans la discipline Génie Electrique Doctorat en électronique 2009.

Sites :

- http://www.crdp.ac-grenoble.fr/image
- http://www.frm.org
- http ://www.digimarc.com
- http ://pro-corbis.com
- http://creative.gettyimages.com/source/home/home.aspx?country=fra.
- http://ns1.tele.ucl.ac.be/TALISMAN/ 1998.