Tatouage des Images Médicales en Vue d'Intégrité et de Confidentialité des Données

Mohamed Ali Hajjaji, Hajjaji Ridha, Mtibaa Abdellatif, Bourennane El-Bey

TATOUAGE DES IMAGES MEDICALES EN VUE D'INTEGRITE ET DE CONFIDENTIALITE DES DONNEES

Hajjaji Mohamed Ali[1.3], Hajjaji Ridha[1.2], Mtibaa Abdellatif[1.2], Bourennane El-Bey[3]

1 : Laboratoire d'EμE, Faculté des Sciences de Monastir, Boulevard de l'environnement 5000 Monastir-TUNISIE.
2 : Ecole Nationale d'Ingénieurs de Monastir, Avenue Ibn El Jazzar, 5019 Monastir – TUNISIE
3 : Laboratoire LE2I, Université de Bourgogne, Dijon – FRANCE
daly_fsm@yahoo.fr; rdhajjaji@gmail.com; abdellatif.mtibaa@enim.rnu.tn; ebourenn@u-bourgogne.fr

RESUME

Dans l'objectif de contribuer à la sécurité de partage et de transfert des images médicales, nous présentons dans ce travail la méthode de tatouage multicouche. Cette dernière consiste à insérer dans l'image médicale les informations qui concernent la signature de centre hospitalier et les données du patient. Elle doit permettre d'assuré l'intégrité, la confidentialité des données lors de leur partage, et la robustesse aux différents types d'attaques (compression JPEG, Copier-coller, transformations géométriques,…).

MOTS CLES

tatouage, images médicales, télémédecine, méthode multicouche, fonctions de hachage MD5, etc.

1. Introduction

L'imagerie médicale joue un rôle important et vital dans l'aide au diagnostic et la prise des décisions. A ce propos, plusieurs techniques différentes et complémentaires sont utilisées : Imagerie par Résonance Magnétique (IRM), Scanner, Computer Tomographie (CT), Tomographie par Emission des Positrons (TEP), Mammographie, Echographie, etc.

D'autre part, avec l'évolution des maladies, plusieurs diagnostiques restent insuffisante, d'où la nécessite de la coopération de plusieurs confrères afin d'aboutir à un diagnostique correcte c'est ce qu'on appel dans le domaine de la santé aide au diagnostic médical (télémédecine). Cette dernière ne cesse de prendre une place importante dans les différentes applications médicales, mais le problème majeur reste au niveau de l'échange des données, sur le réseau Internet, tout en conservant leurs intégrités ainsi que leurs confidentialités contre l'apparition considérable des pirates. Dans ce contexte plusieurs solutions informatiques basées sur l'utilisation des techniques de contrôle d'accès existent mais elles restent insuffisantes, d'où l'apparition de tatouage numérique dans le but de contribuer à la sécurité des images médicales partagés sur le réseau.

Dans ce cadre, nous proposons une technique de tatouage « multicouche » qui permet de :

- Contrôler l'intégrité et l'authenticité des informations médicales ;
- Garder la confidentialité des données relatives au patient ou de centre hospitalier.

Cette méthode, inspirée des travaux de B.Vassaux [1], se base sur l'utilisation de la technique CDMA (Code Division Multiple Acces). Dans la deuxième section nous présentons les mesures utilisées pour évaluer la qualité de l'image ainsi que des exemples d'attaques que pourrait subir une image médicale partagée sur le réseau. La troisième section est réservée à la représentation du schéma de tatouage proposé. Les résultats du travail sont présentés dans la section 4. Le présent travail est clôturé par des conclusions et des perspectives.

2. Evaluation des algorithmes de tatouage

Vu les multiples applications envisagées ainsi que les critères qui rentrent en jeu, il est difficile d'évaluer un algorithme de tatouage, toutefois il est possible d'identifier quelques éléments essentiels pour l'évaluation de tatouage tels que la qualité de l'image tatouée et la robustesse de la technique contre les différentes attaques.

2.1 Mesure de qualité de l'image

Pour évaluer la qualité de l'image, on fait recourt à des mesures soit objective soit subjective.

Les mesures subjectives

Il est très intéressant, surtout dans le cas des images médicales, d'utiliser le critère subjectif pour la mesure de la qualité des images. Les images originales et modifiées sont présentées à un groupe d'observateurs composé

d'experts. La distance de présentation requise est de 4 fois la hauteur de l'écran. Le tableau 1présente les applications possibles de la qualité de l'image [2] [3].

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

Tableau 1 : Indice d'appréciation de la qualité de l'image

Les mesures subjectives sont toutes fois coûteuses, notamment si on travaille avec un échantillon important des images médicales.

Les mesures objectives

Les mesures objectives sont basées sur la comparaison pixel par pixel entre l'image originale et l'image marquée. Parmi ces mesures nous retrouvons l'Entropie relative, l'Erreur quadratique moyenne, l'Erreur moyenne absolue, le rapport signal sur le bruit (PSNR) et PSNR pondéré.

Le Rapport Signal sur le Bruit

Parmi les mesures de distorsion les plus populaire en traitement d'image est le rapport signal sur le bruit SNR (Signal to Noise Ratio) et le PSNR (Peack Signal to Noise Ratio). Elles sont définies respectivement par les formules suivantes :

$$(SNR)_{dB} = 10 \log_{10} \left\{ \left[\frac{\sum_{i,j} I^2(i,j)}{\sum_{i,j} [I(i,j) - I_w(i,j)]^2} \right] \right\} \quad (1)$$

$$(PSNR)_{dB} = 10 \log_{10} \left\{ N * M \left[\frac{\max I^2(i,j)}{\sum_{i,j} [I(i,j) - I_w(i,j)]^2} \right] \right\} \quad (2)$$

Le PSNR pondéré

On remarque bien qu'aucune des méthodes précédentes ne tient compte du HVS (Système Visuel Humain), elles sont basées sur la comparaison pixel par pixel, alors que le HVS tient compte du voisinage. Le wPSNR (PSNR pondéré) a été proposé par Voloshy noviski et Al. [4].

$$(wSNR)_{dB} = 10 \log_{10} \left\{ \frac{M * N \max I^2(i,j)}{\sum_{i,j} \left[\frac{I(i,j) - I_w(i,j)}{1 + Var_I(i,j)} \right]^2} \right\} \quad (3)$$

Avec Var_I (i,j) représente la variance locale du pixel(i,j) et I(i,j) est la valeur de luminance du pixel (i,j) de l'image originale et I_w(i,j) celle de l'image à testé.

Les deux images étant de taille [M*N].

3. Les attaques

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors de son extraction [5].

On distingue plusieurs types d'attaques telles que les attaques intentionnelles, ces dernières ne visent pas forcement à attaquer le tatouage. Parmi ces attaques classiques nous retrouvons [6] :

- L'addition d'un bruit ;
- Le filtrage ;
- La compression avec pertes essentiellement le JPEG ;
- Les transformations géométriques (décalage, rotation, zoom, découpage…) ;
- La conversion Analogique Numérique etc.

De plus, on peut distinguer un autre type d'attaque qu'on l'appelle souvent « les crackers » [7]. Ce type d'attaque vise à perturber et désynchroniser l'image dans le but de rendre le message inséré très difficile à détecter sans recours à l'image originale. Dans le cadre de tatouage des images médicales, ces dernières peuvent subir, particulièrement, des attaques qui peuvent conduire à un diagnostique erroné ou à une erreur d'authentification. A titre d'exemple on cite :

L'attaque de « la signature multiple » [8]

C'est la présence de plusieurs signatures sur l'image, elle conduit à une ambiguïté dans la détection de propriétaire de l'image (centre médicale, médecin…).

L'attaque par « copiage » [9]

Ce type d'attaque consiste à recopier une marque pour l'insérer dans une image non marquée, et dans ce cas, cette dernière peut être considéré commettant une image marquée.

4. Description de la méthode

Notre but est d'augmenter le nombre de bits de message à insérer (donnée du patient et signature de l'établissement de santé ou de médecin) dans l'image sans pour autant la dégrader visuellement. Cette approche est appeler « Méthode de Multicouche ». Cette méthode est basée sur le principe de CDMA. La méthode sera testée dans le domaine spatial. Les tests seront effectués sur trois types d'images médicales, des images IRM, radiographiques et échographiques, codées sur 256 niveaux de gris, format BMP. Les mesures de qualités de l'image nous permettrons de faire une étude comparative quant à l'adaptabilité de cette méthode à ces trois types d'images.

4.1 Les étapes d'insertion

L'insertion des données dans l'image va suivre les étapes suivantes :

1. Calculer la signature de l'établissement de santé ou de médecin en utilisant MD5 comme fonction de hachage.
2. Insérer les données nécessaires relatives au patient.
3. Concaténer la signature avec les données du patient et les convertir en binaire.
4. Découper l'image originale suivant le nombre de bits à insérer.
5. A l'aide d'une clé secrète, on génère une SBPA 2D (Séquence Binaire Pseudo Aléatoire à deux Dimensions) de taille égale à la portion de l'image, cette dernière est composée uniquement de +1 et -1 et à une moyenne nulle.
6. Remplir les blocs obtenus suite au découpage de l'image par (+SBPA2D), si un bloc correspond au bit «1» du message à insérer et par (–SBPA2D) s'il est correspond au bit «0 ».

La figure 1 illustre le schéma d'insertion de cette méthode.

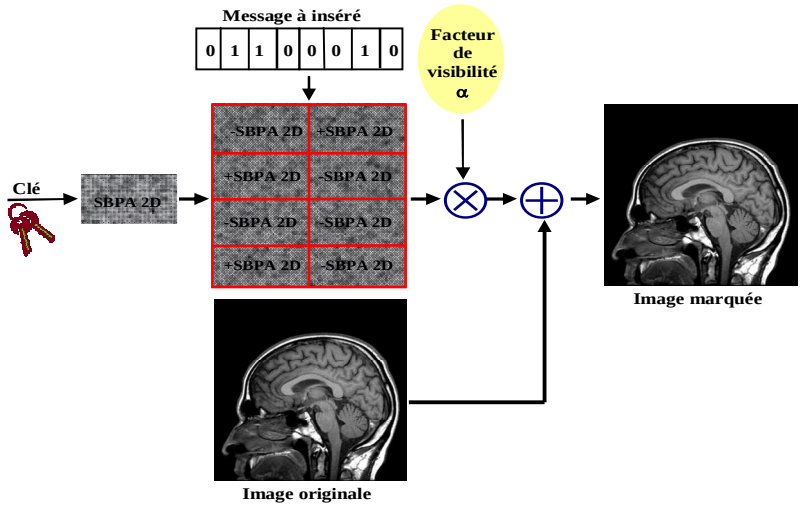

Figure 1. Insertion des données par découpage en blocs

4.2 Apport de la technique CDMA

On remarque bien que la dimension de la SBPA2D est inversement proportionnelle au nombre de bits à insérer, et que plus le nombre de bits à insérer est important, plus il est difficile de détecter les différents bits de message inséré. La technique de CDMA en communication consiste à mélanger plusieurs signaux à l'émission,

la détection se fait par calcul de corrélation. Suivant Vassaux au lieu d'insérer le message sur une seule couche, il est étalé sur plusieurs couches. La figure 2 illustre l'insertion d'une marque en utilisant la technique dite « Multicouche ».

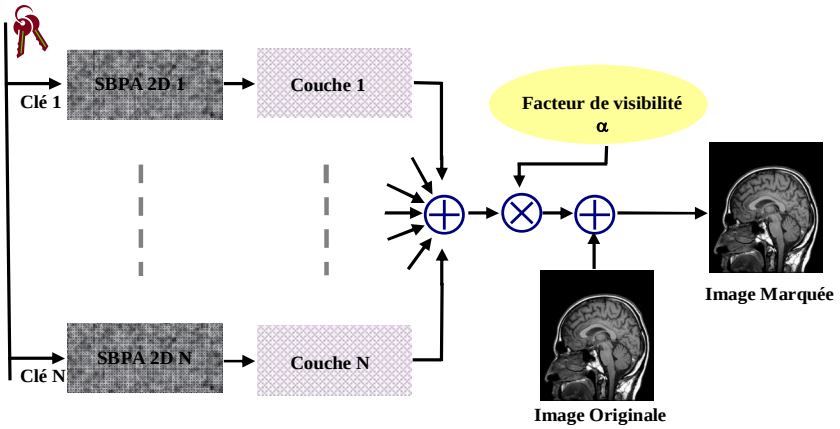

Figure 2. Schéma d'insertion en utilisant la méthode multicouche

4 .3. Les étapes de Détection

L'étape de détection consiste à extraire les données du patient ainsi que la signature de l'établissement hospitalier ou du médecin. L'algorithme de détection suivra alors les opérations inverses à l'insertion:

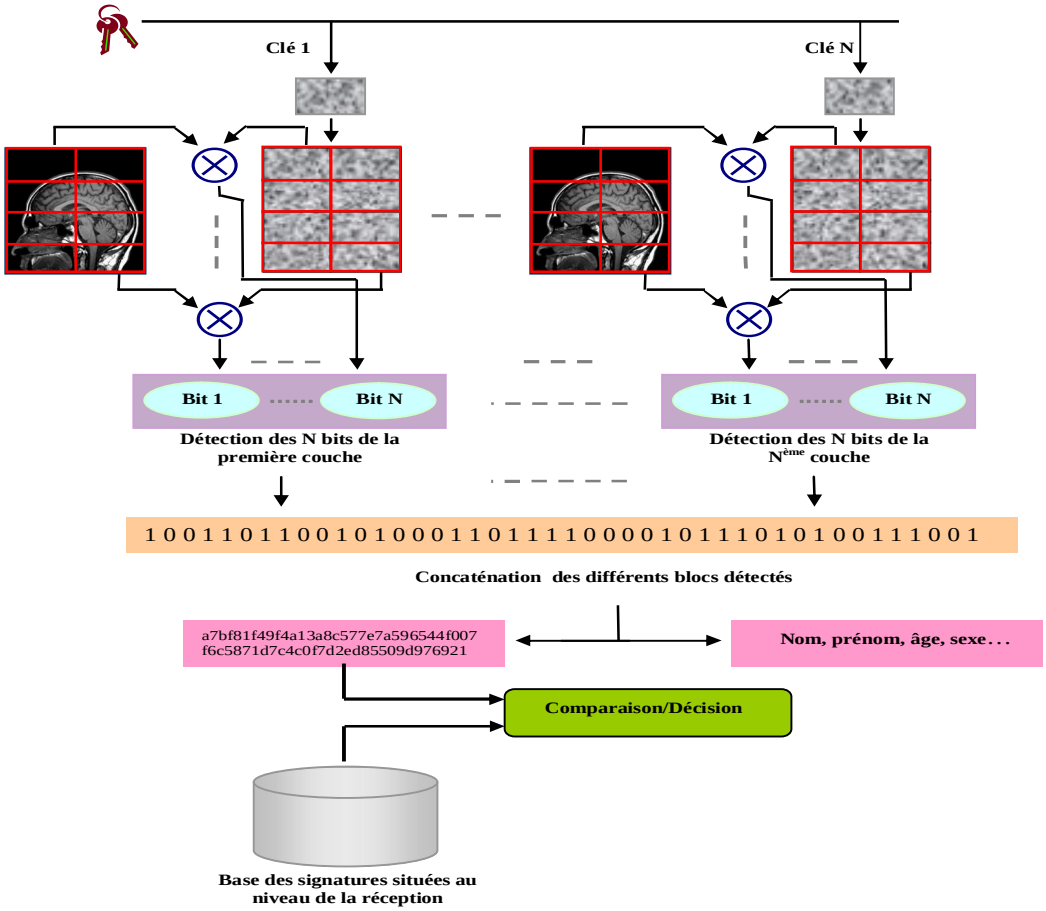

Figure 3. Schéma de détection de la méthode multicouche

5. Résultats

Pour évaluer les performances de la technique multicouches, plusieurs tests sont effectués sur 3 types d'images médicales (IRM, radiographie, échographie). Ces dernières sont codées sur 256 niveaux de gris, sous format BMP de taille 512x512. Les données insérées par l'utilisateur sont :

- La signature de l'établissement sur 128 bits (en utilisation MD5 comme fonction de hachage) ;

- Les données du patient : nom, prénom, âge et sexe ;
- La clé secrète K.

Pour pouvoir accéder aux données, dans l'image, l'utilisateur doit avoir :

- l'image tatouée ;
- la clé K ;
- le nombre de couches utilisées.

Dans le cas où les trois types d'échantillons d'images n'avaient subi aucune attaque, la détection de la totalité de la marque insérée se fait avec succès dans le cas de l'utilisation de 2, 4 et 8 couches et c'est qu'en choisissant le coefficient de visibilité adéquat.

On remarque bien que lorsqu'on applique une attaque «copier/coller», nous arrivons à extraire les données du patient ainsi qu'une valeur de signature. Cependant cette dernière est différente de la valeur de l'une des signatures situées dans une base de données au niveau de la réception ce qui démontre que l'image a subi des modifications. Ceci démontre que l'image partagée par le hôte a été soit attaquée ou bien changée par une autre. Dans ce cas on perd également l'information sur son authenticité. L'attaque de compression JPEG a été testée sur les trois types d'images médicales tatouées avec un message de 290 bits inséré sur 8 couches avec un coefficient de visibilité de 0.3. Les tests effectués montrent que l'augmentation du taux de compression (inversement proportionnel au facteur de qualité) entraîne une diminution du nombre de bits détectés. De plus, les images radiographiques semblent être plus robustes à l'attaque JPEG que les images échographiques ou IRM (Figure 4).

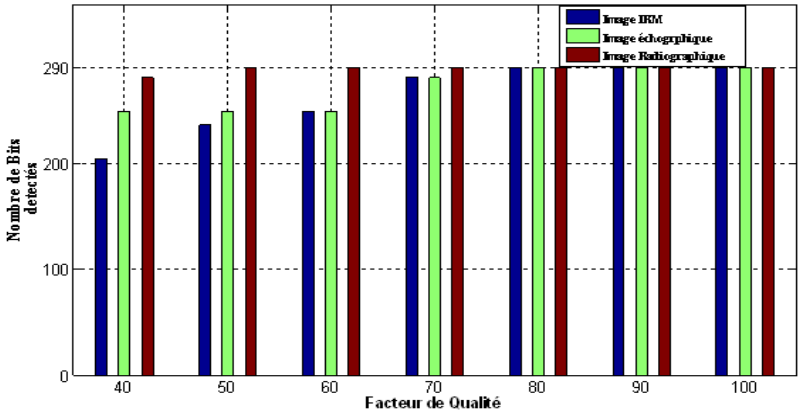

Figure 4. Nombre de bits détectés en fonction du facteur de qualité de la compression JPEG

Pour mesurer la qualité des images tatouées, nous avons calculé leurs wPSNR en faisant varier le nombre de couches ou le coefficient de visibilité. Les Figure 5.a et 5.b montrent les résultats obtenus pour les trois types d'images (radiographique, échographique et IRM).

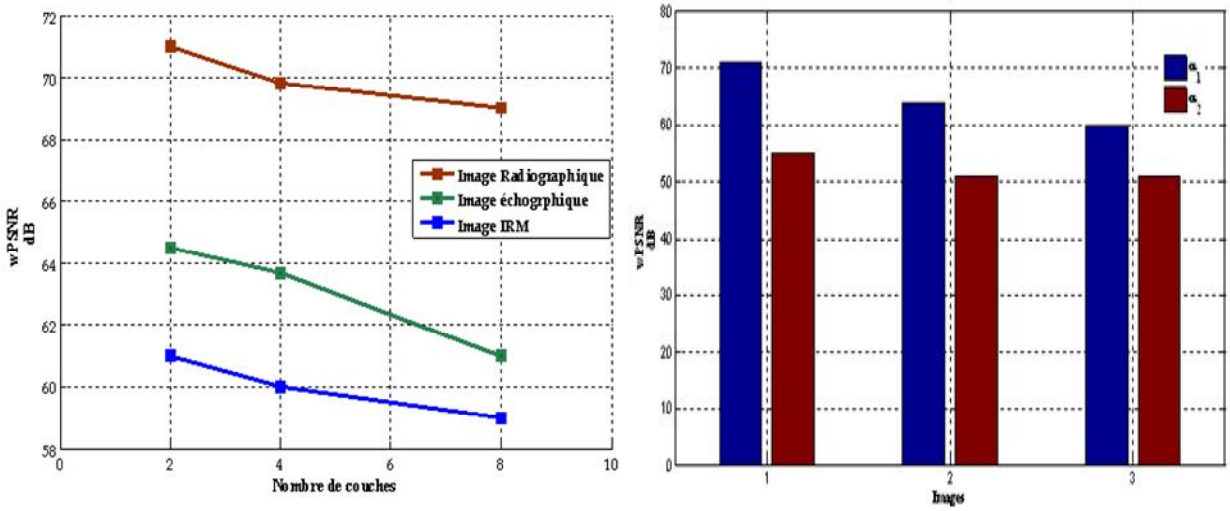

Figure 5. : (a) Mesure de la dégradation pour 2, 4 et 8 couches
(b)Mesure de la dégradation de trois images tatouées avec deux coefficients de visibilité α1(0.1) et α2 (0.5)

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

Enfin Nous avons effectué les tests sur dix échantillons de chaque type d'images médicales à fin de comparer leurs qualités en fixant la valeur du coefficient de visibilité, α=0.3, et le nombre de couches utilisées, 8 couches, (voir tableau 2).

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

Tableau 2. Valeur du wPSNR pour les trois types d'images médicales.
α=0.3, Nombre de couches : 8

6. Conclusion

Dans ce papier nous venons d'étudier l'utilisation de l'application de la méthode de « multicouche » dans le domaine de l'imagerie médicale, dans l'objectif de vérifier son authenticité. Nous avons également utilisé la fonction de hachage MD5 afin de vérifier son intégrité. Cette méthode, basée sur la technique CDMA vise à augmenter le nombre de bits insérés dans l'image sans pour autant la dégrader.

L'application de cette technique dans le domaine spatial donne de bons résultats pour l'insertion de 290 bits sur les plans qualité de l'image tatouée et robustesse du tatouage à la compression JPEG.

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

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

Références

[1] B.Vassaux, P. Bas & J.M. Chassery, "Tatouage d'images par étalement de spectre: Apport de la technique CDMA en mode multicouche", journées d'études et d'échanges compression et Représentation des Signaux Audiovisuels (CORESA), Oct. 2000.

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

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

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

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

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

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

[8] M. RAMKUMAR & A. AKANSU, "Robust Protocols for Providing Ownership of images", In IEEE 0-7695-0540-6/00, 2000.

[9] C.S.WOO, J.DU & B. PHAM, "Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images" in Proceedings APRS Workshop on Digital Image Computing, 2005, pp. 59-64.