Tatouage d'images cryptées pour l'aide au télédiagnostic

William PUECH[1], Michel DUMAS[1], Jean-Claude BORIE[1] et Magali PUECH[2]

[1] Centre d'Electronique et de Microoptoéléctronique de Montpellier, UMR CNRS 5507,

STINIM, Université Montpellier II, Les Carmes, Pl. G. Péri, 30021 Nîmes Cedex 1, France.

[2] Centre Commun de Mesures Imagerie Cellulaire,

Université Lille I, 59655 Villeneuve d'Ascq Cedex, France.

puech@univ-montp2.fr, dumas@univ-montp2.fr, borie@univ-montp2.fr, puech@univ-lille1.fr

Résumé - Le développement d'interfaces de visualisation à distance pour des images médicales rencontre des problèmes de sécurité de données. Dans ce papier, nous présentons une combinaison des techniques de cryptage et de tatouage d'images. Nous proposons un système permettant de transférer des images médicales de manière sécurisée en générant une clef pour crypter l'image, puis en tatouant l'image avec la clef de cryptage et les données concernant le patient.

1. Introduction

La mise en place d'interfaces de visualisation à distance de données médicales connaît actuellement une forte demande. Ces interfaces permettent d'accéder aux dossiers des patients contenant des données textuelles et images. Le développement de ces systèmes rencontre deux types de problèmes. Le premier concerne la qualité des données transmises. En effet, pour des raisons de temps de transfert au travers du réseau toutes les données, et en particulier les images, sont comprimées. Le deuxième problème concerne l'aspect sécurité. Pendant le transfert des données, il ne faut absolument pas qu'une image soit dissociée du nom du patient concerné pour éviter toute confusion d'appartenance à la réception de celle-ci. De plus, pour des raisons de confidentialité, pendant le transfert, ces données doivent être rendues illisibles et non déchiffrables, donc cryptées.

Dans cet article, nous proposons un système permettant de transférer des images médicales de manière sécurisée. Pour cela, à l'émission, dans un premier temps nous générons une clef permettant de crypter l'image, puis de tatouer celle-ci avec deux composantes. La première de ces deux composantes concerne la clef utilisée pour le cryptage, alors que la deuxième partie du message tatoué concerne les principales données du patient.

Dans la section 2, nous présentons le type de données à transmettre concernant les images médicales en introduisant le format DICOM. Dans la section 3, après avoir présenté les principes de la cryptographie et du tatouage, nous développons une technique combinant cryptographie et tatouage. Dans la section 4, nous présentons alors les différents résultats obtenus sur une image médicale.

2. Aide au télédiagnostic

2.1 Le format DICOM

Le format DICOM (Digital Imaging and COmmunication in Medicine) est le standard utilisé dans le milieu médical [5]. Il permet grâce à sa structure de transférer les images numériques médicales à travers un réseau. En effet, ce format dispose de protocoles d'échange et d'une interface de communication réseau, soit OSI (Open Systems Interconnect), soit TCP/IP (Transmission Control Protocol / Internet Protocol). Le format DICOM fournit d'une part l'image numérique et d'autre part une information texte relative à l'examen effectué. Les niveaux de gris des pixels de l'image sont codés sur 12 bits. Il est possible de mettre en évidence les zones que le médecin spécialiste désire analyser en ne gardant qu'une partie de l'information haute résolution.

2.2 Application Client/Serveur

La visualisation à distance de ce genre d'image nécessite des visualiseurs performants, vu la taille de celles-ci qui est comprise entre 512x512 et 2000x2000 pixels, avec un codage sur 12 bits de niveau de gris par pixel. Des travaux permettant la consultation de bases de données en ligne sont d'actualité [3, 10].

Pour palier à ce problème, nous proposons une application Client/Serveur qui permet de consulter ces images à partir d'un simple navigateur Web [1]. Le développement de notre application, a nécessité l'utilisation de code HTML et PHP pour la partie formulaire et interrogation du serveur et Javascript pour les actions et événements du coté client. Le Javascript est également utilisé pour l'apparence graphique.

2.3 Confidentialité

En intranet, la confidentialité est obtenue grâce à la structure hiérarchique du format DICOM. Celle-ci se retrouve en pratique, au sein d'une base de données identifiant séparément et dans l'ordre : le patient, les propriétés de l'examen, les séries de l'examen, les paramètres des images et enfin le chemin exact vers ces images. A chaque élément d'un tableau est associé un numéro d'identification unique, ainsi qu'un pointeur sur l'élément correspondant du tableau suivant. En parcourant cette structure, on peut reconstituer séquentiellement toute l'information relative à un examen.

Bien que le format DICOM ne soit pas conservé pour la phase de transfert, la confidentialité et la sécurité des informations doivent être préservées. Pour cela, nous proposons, section 3, une technique permettant de sécuriser en un seul bloc les données images et textes concernant un patient.

3. Techniques de Cryptographie et de tatouage

3.1 Cryptographie

L'utilisation des réseaux informatique pour la transmission d'informations médicales pose le problème de la sécurisation. Pour pallier à ce problème, des techniques de chiffrement de messages plus ou moins robustes ont été développées. Ces algorithmes utilisent des clefs de chiffrement et de déchiffrement soit identiques, soit différentes [2]. Parmi les plus courantes, nous pouvons citer le chiffrement de Vigenère [8] à une seule clef, l'algorithme DES à clefs secrètes [4] et l'algorithme RSA à clefs publiques et privées [6]. L'algorithme RSA, actuellement le plus performant utilise des clefs de 512 à 1024 bits.

Dans notre méthode de cryptage d'images médicales, présentée section 3.3, nous utilisons un algorithme dérivé de celui de Vigenère. Le principe de ce chiffrement consiste à employer une clef éventuellement aussi longue que le message. Le message est alors découpé en bloc de longueur identique à celle de la clef pour pouvoir être codé.

3.2 Tatouage

Le tatouage d'image consiste à insérer de manière invisible et indélébile une information dans une image puis de tenter de récupérer cette information après transfert de l'image. La contrainte d'indélébilité est propre au domaine du tatouage [7].

Les schémas de tatouage sont variés en fonction de leur domaine d'application. L'insertion de la signature se fera soit dans le domaine spatial [9] soit dans un domaine transformé. Dans un schéma additif, l'information à insérer est rajoutée dans l'image alors que dans un schéma substitutif l'information à insérée est substituée à des caractéristiques de l'image.

Dans notre méthode de tatouage d'images cryptées, section 3.3, nous utilisons un schéma additif dans le domaine spatial.

3.3 Insertion d'un message dans une image cryptée

3.3.1 Emission de l'image

Détaillons le principe combinant cryptage et tatouage. A l'émission, dans un premier temps nous générons une clef permettant de crypter l'image. Dans un deuxième temps, nous tatouons celle-ci avec deux composantes qui sont la clef utilisée pour le cryptage et les principales données du patient. L'image peut alors enfin être transmise.

Pour chaque pixel de l'image originale $p(i)$, nous calculons la valeur de $p'(i)$ de l'image cryptée en utilisant l'équation récurrente d'ordre 3 suivante :

$$p'(i) = p(i) + kp'(i-1) + lp'(i-2) + mp'(i-3),\ i \in [3,N] \quad (1)$$

où $p'(i-1)$, $p'(i-2)$ et $p'(i-3)$ sont les pixels précédemment cryptés, k, l et m sont trois coefficients, et N la taille de l'image.

Concernant les trois premiers pixels de l'image cryptée, nous avons besoin de fixer des valeurs précédentes de manière aléatoire :

$$\begin{aligned} p'(0) &= p(0) + ka + lb + mc \\ p'(1) &= p(1) + kp'(0) + la + mb \\ p'(2) &= p(2) + kp'(1) + lp'(0) + ma, \end{aligned} \quad (2)$$

où a, b et c sont ces trois valeurs aléatoires. Les paramètres a, b et c seront considérés comme des pixels virtuels de l'image cryptée $p'(-1)$, $p'(-2)$ et $p'(-3)$ et auront des valeurs aléatoires comprises entre 0 et 255.

A partir des équations (1) et (2), nous obtenons la clef de notre cryptage basée sur k, l, m, a, b et c.

Pour le tatouage, comme présenté section 3.2, nous utilisons un schéma additif dans le domaine spatial. Ce tatouage est effectué après avoir crypté l'image. Nous insérons le message en modifiant la valeur de la partie la moins significative de quelques pixels. Pour rester invisible, seul le bit de poids le plus faible est modifié. Par conséquent, pour chaque caractère à insérer, nous avons besoin de marquer huit pixels de l'image cryptée. Un pas constant, pourra par exemple être pris pour tatouer l'image.

3.3.2 Réception de l'image

A la réception, dans un premier temps, il faut récupérer l'information textuelle tatouée dans l'image. Grâce à cette information, dans un deuxième temps, il est alors possible de décrypter l'image. Notons que le pas de tatouage devra être connu pour récupérer l'information textuelle à la réception de l'image.

Analysons maintenant le répercussion du tatouage de l'image au moment du décryptage de celle-ci. En effet la combinaison cryptage-décryptage à elle seule n'induit aucune erreur dans l'image. Un pixel $p'(i)$ sera décrypté pour obtenir le pixel $q(i)$ selon l'équation suivante :

$$q(i) = p'(i) - kp'(i-1) - lp'(i-2) - mp'(i-3). \quad (3)$$

Au moment du décryptage, si le pas de tatouage est supérieur à 3, correspondant à l'ordre de récurrence de l'équation 3, un pixel $p'(i)$ à décrypter ne peut dépendre au maximum que d'un pixel tatoué. La variation du niveau de gris d'un pixel tatoué est comprise entre -1 et +1 par rapport à sa valeur originale car seul le bit de poids le plus faible est modifié. Si $p'(i)^*$ est un pixel crypté tatoué, alors $q(i)$ sera égal à $p(i)$ à plus ou moins 1 niveau de gris :

$$q(i) = p(i) + \alpha, \alpha \in [-1,0,+1]. \quad (4)$$

Pour le pixel suivant à décrypter, *p'(i+1)*, nous aurons *q(i+1)* qui sera égal à *p(i+1)* à plus ou moins *k* niveaux de gris:

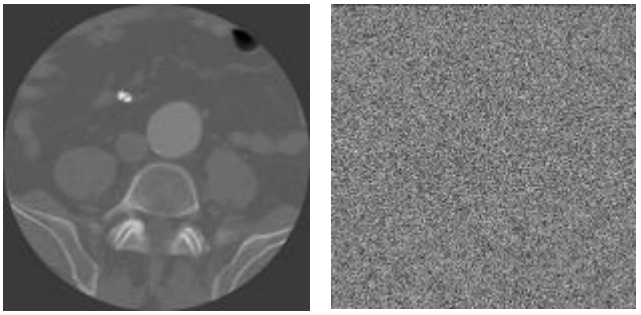
$$q(i+1) = p'(i+1) - kp'(i)^* - lp'(i-1) - mp'(i-2)$$
$$q(i+1) = p(i+1) + \beta, \beta \in [-k,0,+k]. \quad (5)$$

De la même manière, les pixels décryptés *q(i+2)* et *q(i+3)* seront respectivement égaux à *p(i+2)* à plus ou moins *l* niveaux de gris et *p(i+3)* à plus ou moins *m* niveaux de gris.

Notons donc qu'à partir de l'équation 3, un pixel tatoué peut modifier au moment du décryptage les valeurs de 4 pixels consécutifs. Nous en concluons aussi que les valeurs des trois coefficients *k*, *l* et *m* doivent rester des valeurs entières, petites et proches de 0. Dans le cadre de notre application, nous utiliserons pour *k*, *l* et *m* des valeurs aléatoires comprises entre -2 et +2.

4. Résultats

Dans cette section, nous appliquons notre méthode sur une image de l'aorte issue d'un appareil tomodensitomètre à rayons X (scanner) de taille 512x512 pixels. A partir de l'image originale, figure 1.a, nous calculons le cryptage en utilisant la technique présentée section 3.3. Pour obtenir l'image cryptée, représentée figure 1.b, nous avons utilisé la clef indiquée dans le tableau 1. Après décryptage, nous pouvons constater que l'image décryptée, présentée figure 2.a, est identique à l'image originale. Il n'y a en effet aucune différence pixel à pixel entre les deux images du fait de la réversibilité de notre technique de cryptage.



(a) (b)

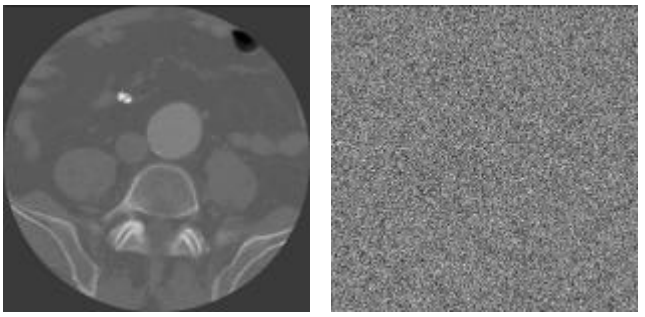
Figure 1 - (a) Image scanner originale.(b) Image cryptée.

TAB. 1 : composants de la clef de cryptage.

a	b	c	k	l	m
108	203	47	2	-2	-1

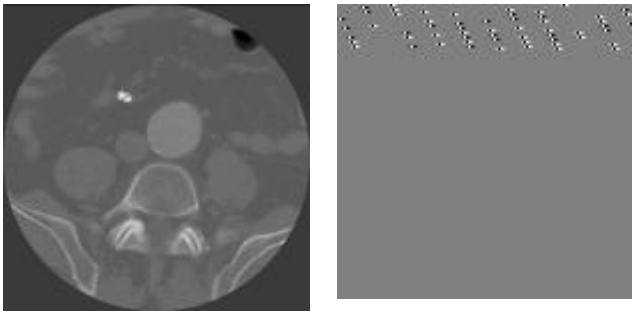
Nous pouvons alors réaliser le tatouage de l'image cryptée, figure 1.b, en utilisant un schéma additif dans le domaine spatial comme décrit section 3.3. Dans cette application, le message tatoué contient la clef de cryptage, les nom et prénom du patient, son âge ainsi que le lieu d'acquisition de l'image :
"*100_200_50_2_-2_-1_Bernard_Claude_60_ans_CHU_Laville*".

Le message, composé de 52 caractères nécessite donc la modification de 416 pixels de l'image. Si nous prenons un pas de 25, alors 20 pixels par ligne seront nécessaires pour le tatouage et cela sur les 21 premières lignes de l'image. Le résultat du tatouage de l'image cryptée est présenté figure 2.b. Nous pouvons alors transférer l'image et les données de manière sécurisée.



(a) (b)

Figure 2 - (a) Image décryptée à partir de la figure 1.b. (b) Tatouage de l'image cryptée figure 1.b.



(a) (b)

Figure 3 - (a) Décryptage de l'image tatouée figure 2.b. (b) Différence entre l'image originale figure 1.a et l'image tatouée décryptée (détail avec zoom x6).

Après le transfert, il est possible de lire la clef de cryptage à partir du tatouage et de décrypter l'image pour obtenir la figure 3.a. Le tatouage introduit une très petite détérioration de l'image originale. Nous montrons sur une zone agrandie, figure 3.b, la différence entre l'image originale et l'image tatouée décryptée. Ceci nous permet de montrer la position et l'espacement des pixels modifiés par le tatouage et le décryptage. La figure 4 illustre les variations des niveaux de gris des pixels sur une ligne de l'image différence de la figure 3.b. Nous pouvons alors vérifier que le tatouage d'un pixel sur l'image cryptée implique des variations de niveaux de gris par rapport à l'image originale sur 4 pixels voisins. Le tableau 2 indique les valeurs des différences des niveaux de gris des pixels au voisinage du pixel de la colonne 50. De plus, nous remarquons, figure 4, que même si le pas de tatouage est régulier et égal à 25, la fréquence de modification des pixels

n'est pas régulière. En effet, quand un pixel tatoué conserve la valeur du pixel original, alors il n'apparaît aucune différence dans l'image.

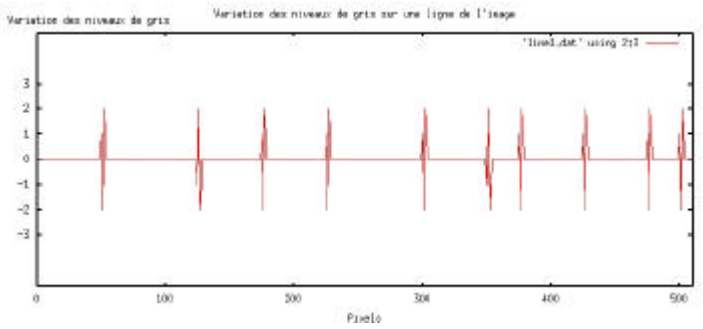


Figure 4 - Variation des niveaux de gris des pixels sur une ligne de l'image différence.

TAB. 2 : Variation des niveaux de gris des pixels autour d'un pixel tatoué colonne 50.

Pixel	47	48	49	50	51	52	53	54	55	56
Différence	0	0	0	1	-2	2	1	0	0	0

Pour quantifier la performance de notre méthode, nous calculons le PSNR (rapport signal à bruit crête "Peak Signal Noise Ratio") qui dépend de l'erreur quadratique moyenne (EQM) :

$$EQM = \frac{1}{N}\sum_{i=0}^{i=N-1}(p(i)-q(i))^2 = 0.0075.$$

Nous obtenons alors un PSNR de :

$$PSNR = 10\log_{10}(\frac{255^2}{EQM}) = 69.35 \quad dB.$$

5. Conclusion

Dans ce papier, nous avons présenté une méthode combinant des techniques de tatouage et de cryptographie. Nous avons montré que le tatouage d'une image cryptée influençait la qualité de l'image finale après décryptage. Pour notre application, nous ne cherchons pas à avoir une méthode de tatouage robuste. En effet, nous souhaitons juste préserver la confidentialité des données durant le transfert. Toutefois, si le tatouage est effacé de l'image, alors la clef de cryptage est perdue.

Nous avons illustré notre méthode avec une image scanner que nous avons cryptée et tatouée en insérant dans l'image la clef de cryptage et des données du patient. Dans notre application, nous avons montré que les modifications dues au tatouage et au décryptage ne détériorent pas fortement la qualité de l'image. Par conséquent, celles-ci ne perturbent pas le médecin spécialiste dans son télédiagnostic.

Références

[1] M. Bouchouicha, W. Puech, A. Kolesnikov, G. Passail and M. Dumas, "Visualisation d'images haute résolution au travers d'un arpenteur : application à l'imagerie médicale", *CORESA'00*, pp. 395-402, Poitiers, France, 2000

[2] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, IT-26, n° 6, pp. 644-654, 1976.

[3] D. Florescu, V. Issarny, P. Valduriez et K. Yagoub, "Caching strategies for data-intensive Web sites", *INRIA Rocquencourt, research report*, n° 3871, Le Chesnay, France, January 2000.

[4] NBS FIPS 46, "Data Encryption Standard", *National Bureau of Standards*, U.S. Department of Commerce, January 1977.

[5] NEMA, *Standards Publication Digital Imaging and Communications in Medicine (DICOM)*, 1993.

[6] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, 21, n° 2, pp. 120-126, 1978.

[7] J.J.K.O Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking digital images for copryright protection", *IEE Proc.-Vis. Image Signal Process.*, vol. 143, n° 4, pp. 250-256, 1996.

[8] B. Schneier, *Applied cryptography*,Wiley, 1995.

[9] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A digital watermark", *ICIP'94*, vol. 2, pp. 86-90, Austin, USA, 1994.

[10] S. Sclaroff, M. La Caxias, S. Sethi et L. Taycher, "Unifying textual and visual cues for content image retrevial on the World Wide Web", *CVIU*, Vol 75, pp. 86-98, August 1999.