Crypto-Compression d'Images Médicales par Cryptage Partiel des Coefficients DCT

William Puech, José Marconi Rodrigues

CRYPTO-COMPRESSION D'IMAGES MÉDICALES PAR CRYPTAGE PARTIEL DES COEFFICIENTS DCT

W. Puech et J.M. Rodrigues.

Laboratoire LIRMM, UMR CNRS 5506, Université Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE

william.puech@lirmm.fr, jose-marconi.rodrigues@lirmm.fr

ABSTRACT

The traffic of digital images has increased rapidly in the Internet. Security of image becomes important for many sectors mainly for medical applications. Nowadays, the transmission of medical images is a daily routine, especially over wireless (battlefields, traffic accidents, etc). Partial encryption is an approach to reduce the computational resources for huge volumes of multimedia data in this kind of network. This paper presents a method of partial or selective encryption for medical JPEG images. It is based on encryption of the quantified DCT coefficients. The purposed method results in a significant reduction in encryption and decryption processing time. It is fast and does not reduce the compression performance of the JPEG algorithm.

1. INTRODUCTION

Le transfert d'images est encore actuellement peu sécurisé. Les algorithmes standards de chiffrement ne conviennent pas au cas particulier des images. L'idéal serait de pouvoir appliquer des systèmes de chiffrement asymétriques afin de ne pas avoir de clef à transférer. Du fait de la connaissance de la clef publique, les systèmes asymétriques sont très coûteux en temps de calcul, et donc pas envisageable pour un transfert sécurisé d'images. Les algorithmes symétriques imposent de transférer la clef secrète. Les méthodes classiques de chiffrement d'images nécessitent le transfert de la clef secrète par un autre canal ou un autre moyen de communication [2, 1, 5].

Les algorithmes de chiffrement par blocs appliqués aux images présentent deux inconvénients. Premièrement, quand l'image contient des zones homogènes, tous les blocs identiques sont également identiques après chiffrement. Dans ce cas, l'image cryptée contient des zones texturées et l'entropie de l'image n'est pas maximale. Le second problème est que les méthodes de cryptage par blocs ne sont pas robustes au bruit. En effet, une erreur sur un bit chiffré va propager des erreurs importantes dans tout le bloc courant.

Pour le transfert d'images les algorithmes de chiffrement d'images doivent pouvoir être combinés avec les algorithmes de compression d'images tel que JPEG [4]. Le problème est que les algorithmes de cryptage ont pour objectif de supprimer toutes les redondances afin d'éviter des attaques statistiques alors que les algorithmes de compression cherchent les redondances contenues dans les images afin de réduire la quantité d'information.

Dans ce résumé nous proposons une méthode cryptant partiellement le contenu d'une image afin de garder une certaine quantité de redondance permettant de comprimer l'image partiellement cryptée. Pour cela nous intégrons notre algorithme de cryptage partiel dans la chaîne de l'algorithme de compression JPEG. A ce jour, peu de travaux proposent des solutions de cryptage partiel. En combinant compression et cryptage par AES, Norcen *et al* [3] concluent que pour obtenir un haut niveau de confidentialité, au minimum 12.5% de données doivent être chiffrées.

Après avoir rappeler les bases de l'algorithme JPEG Section 2, nous présentons notre stratégie de cryptage partiel. Section 3 nous présentons les résultats de notre méthode appliquée à une image échographique.

2. COMPRESSION JPEG ET CRYPTAGE PARTIEL

L'algorithme JPEG est une méthode de compression fortement utilisée en traitement et transmission d'images[4]. Le principe de compression est décrit Figure 1. Les parties importantes sont la transformée cosinus discrète (DCT) et la phase de quantification des coefficients fréquentiels.

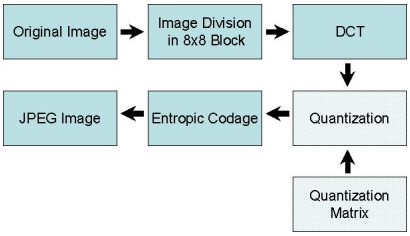


FIG. 1 – Compression JPEG

La DCT permet d'obtenir une représentation fréquentielle particulière de l'image à partir de sa matrice de pixels. A partir des intensités de blocs de $N \times N$ pixels $p(i,j)$, nous obtenons les coefficients DCT associés $F(u,v)$:

$$F(u,v) = \frac{2}{N}C(u)C(v)\sum_{i=0}^{N-1} \sum_{j=0}^{N-l} p(i,j)cos\left(\frac{\pi(2i+1)u}{2N}\right)cos\left(\frac{\pi(2j+1)v}{2N}\right), \quad (1)$$

avec : $C(x) = \frac{1}{\sqrt{2}}$ si $x = 0$ et $C(x) = 1$ si $x \neq 0$, et le support supposé de taille $N \times N$, généralement, $N = 8$.

Pour chaque bloc de pixels les coefficients fréquentiels sont rangés des fréquences basses, à partir de la composante continue $F(0,0)$, aux très hautes fréquences $F(7,7)$. Après la DCT, la phase de quantification a pour objectif de réduire la quantité d'information en divisant chaque coefficient fréquentiel par un coefficent de quantification fonction d'un facteur de qualité.

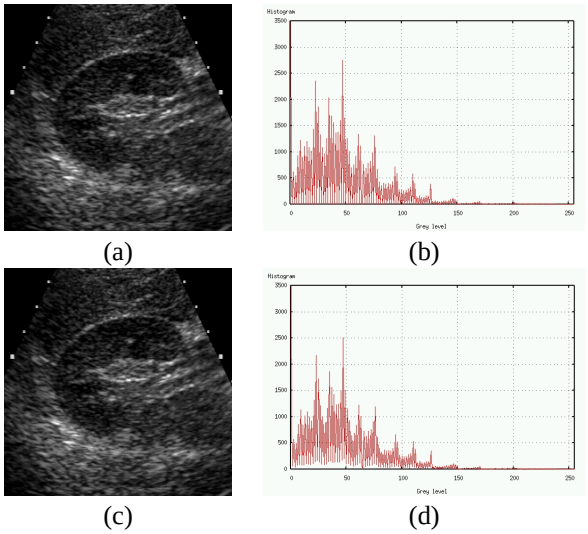
$$F'(u,v) = \left[\frac{F(u,v)}{Q(u,v)}\right], \quad (2)$$

avec [x], la valeur entière la plus proche de x.

Notre méthode de cryptage partiel se propose de chiffrer que les coefficients fréquentiels quantifiés relatifs aux basses fréquences. Chaque coefficient fréquentiel quantifié en basse fréquence est chiffré à partir d'un générateur de nombre pseudo-aléatoire modulo le spectre de chaque coefficient fréquentiel :

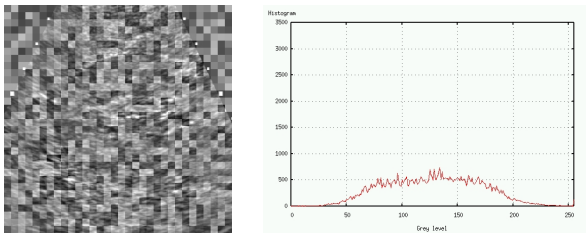
$$E(u,v) = \big(rand() + F'(u,v)\big)\, modulo \left(\frac{2NC(u)C(v)}{Q(u,v)}\right). \quad (3)$$

3. RÉSULTATS



(a) (b) (c) (d)

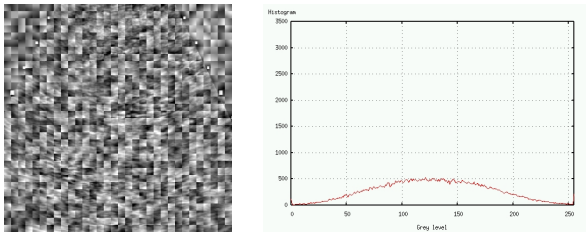
FIG. 2 – a) Image échographique originale, b) Histogramme de l'image originale, c) Image comprimée, d) Histogramme de l'image comprimée.



(a) (b)

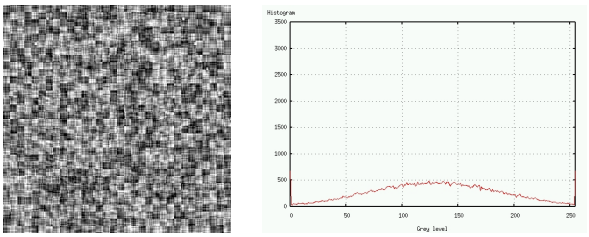
FIG. 3 – a) Image crypto-comprimée partiellement (F(0,0)), b) Histogramme.

A partir de l'image originale Figure 2.a, de taille 256×256 pixels, soit $64Ko$, nous avons tracé Figure 2.b son histogramme mettant en évidence les redondances de l'image. Cette image comprimée avec JPEG pour un facteur de qualité de 100% est illustrée Figure 2.c. L'histogramme de l'image comprimée est très proche de celui de l'image originale, mais la taille de l'image comprimée est de $45.9Ko$. En chiffrant uniquement le coefficient $F(0,0)$ de chaque bloc, l'image illustrée Figure 3.a dissimule fortement l'information initiale de l'image. L'histogramme correspondant, Figure 3.b, montre qu'une grande partie des redondances a disparu. La taille de l'image crypto-comprimée est alors de $46.9Ko$. En chiffrant également les coefficients F(1,0) et F(0,1), nous obtenons l'image de la Figure 4.a et l'histogramme correspondant Figure 4.b. Notons que l'histogramme est plus plat que le précedent. La taille de l'image crypto-comprimée est alors de $48.6Ko$.



(a) (b)

FIG. 4 – a) Image crypto-comprimée partiellement (F(0,0), F(1,0) et F(0,1)), b) Histogramme.



(a) (b)

FIG. 5 – Image crypto-comprimée partiellement (F(0,0), F(u,0) et F(0,v)), b) Histogramme.

En chiffrant en plus tous les coefficients de la première colonne et de la première ligne des blocs 8×8, nous obtenons l'image de la Figure 5.a et l'histogramme correspondant Figure 5.b. Notons que l'histogramme est encore plus plat que le précédent. La taille de l'image crypto-comprimée est alors de $59.8Ko$. Dans ce cas nous perdons en taux de compression.

4. CONCLUSION

Dans cet article, nous avons présenté une méthode permettant de combiner cryptage et compression d'images. L'approche par cryptage partiel permet de laisser dans l'étape de compression des zones homogènes dans les hautes fréquences. Nous envisageons maintenant de développer cette approche au niveau des hautes fréquences en utilisant des méthodes de cryptage par mélange de données. Nous pensons également mettre en place une cryptanalyse de l'approche proposée.

REFERENCES

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

[2] F. Li, J. Knipe, and H. Cheng. Image compression and encryption using tree structures. *Pattern Recognition Letters*, 18 :1253–1259, 1997.

[3] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. Confidential storage and transmission of medical image data. *Computers in Biology and Medicine*, 33 :277–292, 2003.

[4] W.B. Pennebaker and J.L. Mitchell. JPEG : Still Image Data Compression Standard. *Van Nostrand Reinhold*, 45, 1993.

[5] A. Sinha and K. Singh. A technique for image encryption using digital signature. *Optics Communications*, 218 :229–234, 2003.