Transfert sécurisé d'images par combinaison de techniques de cryptographie et de tatouage

William Puech et Michel Dumas
Laboratoire CEM2, UMR CNRS 5507
Université Montpellier II, Les Carmes, Pl. Gabriel Péri, 30021 Nîmes Cedex 1, France
puech@univ-montp2.fr, dumas@univ-montp2.fr

1 Introduction

La mise en place d'interfaces de visualisation à distance connaît actuellement une forte demande dans le cas de transfert de données textuelles et images. Le premier problème rencontré 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, dans certaines applications, il ne faut absolument pas qu'une image soit dissociée des informations textuelles. De plus, pour des raisons de confidentialité, ces données doivent être rendues illisibles et non déchiffrables, donc cryptées.
Nous présentons dans cet article une technique de cryptage, puis une technique de tatouage d'images qui combinées permettent un transfert sécurisé. Après avoir généré une clef permettant de crypter l'image, il est alors possible de tatouer celle-ci avec deux composantes qui sont la clef de cryptage et les données textuelles associées à l'image.

2 Cryptage

2.1 Méthode

Pour pallier au problème de transmissions d'informations au travers des réseaux des techniques de chiffrement de messages plus ou moins robustes ont été développées [8]. Parmi ces algorithmes, nous pouvons citer le chiffrement de Vigenère [2], l'algorithme DES à clefs secrètes [1] et l'algorithme RSA à clefs publiques et privées [5].

Dans notre méthode de cryptage d'images, nous utilisons un algorithme récursif dérivé de celui de Vigenère qui consiste à employer une clef éventuellement aussi longue que la longueur du message. Le message est alors découpé en bloc de longueur identique à celle de la clef pour pouvoir être codé.
Soit une image composée de N pixels, pour chaque pixel de l'image originale $p(n)$, nous calculons la valeur du pixel $p'(n)$ en utilisant l'équation suivante :

$$\begin{aligned} p'(n) &= p(n) + \alpha(1)p'(n-1) + \alpha(2)p'(n-2) \\ &\quad +\alpha(3)p'(n-3) + ... + \alpha(k)p'(n-k), \end{aligned} \tag{1}$$

avec n l'indice du pixel dans l'image, $n \in [k, N]$, $k \in [1, n]$ et $\alpha(i)$, étant une séquence de nombres aléatoires générant la clef de cryptage, $i \in [1, k]$.
L'équation (1) peut alors s'écrire :

$$p'(n) = p(n) + \sum_{i=1}^{i=k} \alpha(i)p'(n-i), \tag{2}$$

où k est l'ordre de récurence, donc l'ordre de la clef de cryptage. Notons qu'à la séquence aléatoire $\alpha(i)$, il faut associer une séquence de k pixels virtuels cryptés $p'(i)$.
Pour crypter à l'ordre k les pixels $p(n)$ d'une image de taille N et obtenir une image de même taille composée de pixels cryptés $p'(n)$, il faut donc une clef de cryptage composée de $2k$ éléments générée par les séquences $\alpha(i)$ et $p'(i)$, $i \in [1, k]$.

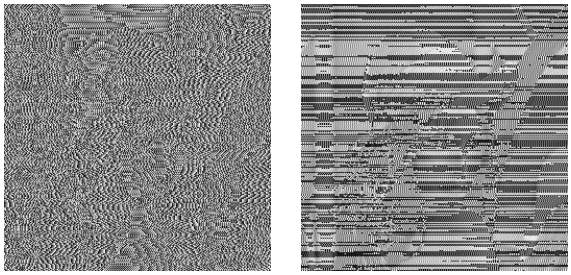
2.2 Résultats

Dans cette section, nous illustrons notre technique de cryptage aux ordres 1, 2 et 3 avec une

image de taille 256×256 pixels. Pour chacune des clefs de cryptage, nous avons utilisé pour les pixels virtuels les valeurs $p(-1) = 108$, $p(-2) = 203$ et $p(-3) = 47$.

(a) (b)

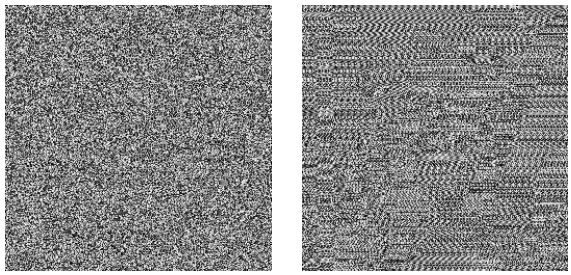
Figure 1: (a) Image originale, (b) Image cryptée à l'ordre 3, $k = -2$, $l = 2$, $m = 1$.



(a) (b)

Figure 2: (a) Image cryptée à l'ordre 1, $k = -1$, (b) Image cryptée à l'ordre 1, $k = 1$.

A partir de l'image présentée figure 1.a, nous réalisons un cryptage à l'ordre 3, avec $k = -2$, $l = 2$, $m = 1$, afin d'obtenir l'image cryptée de la figure 1.b.
Dans le cas d'un cryptage basé sur l'algorithme à l'ordre 1, nous obtenons les images des figures 2.a et b, respectivement cryptées avec $k = 1$ et $k = -1$. Nous remarquons dans les deux cas que le cryptage n'est pas satisfaisant. En effet, une partie de l'information contenue dans l'image originale reste visible. Dans le cas d'un chiffrement à l'ordre 2, la qualité des résultats diffère selon les valeurs de k et l. En effet, des cas particuliers de valeurs pour k et l, figures 3.a et b, se rapprochent fortement des coefficients utilisés en filtrage d'images.
A partir d'un chiffrement d'ordre 3, il devient



(a) (b)

Figure 3: (a) Image cryptée à l'ordre 2, $k = -1$, $l = 1$, (b) Image cryptée à l'ordre 2, $k = 1$, $l = -1$.

difficile de lire le contenu de l'image cryptée quelles que soient les valeurs de la clef générée aléatoirement. Nous illustrons, figure 4.a, que la qualité du cryptage obtenue avec des valeurs élevées de k, l et m n'est pas différente de celle obtenue avec des valeurs entières proches de zéro, figure 1.b. Par contre, en augmentant ces valeurs, nous augmentons la taille de la clef de cryptage. Au moment du décryptage, quelles que soient les valeurs de k, l et m, nous obtenons le résultat présenté figure 4.b, qui ne diffère en aucun point de l'image originale.

(a) (b)

Figure 4: (a) Image cryptée à l'ordre 3, $k = -25$, $l = 64$, $m = 58$, (b) Image décryptée.

3 Tatouage

3.1 Méthode

Pour des applications nécessitant parallèlement le transfert de données textuelles et d'images, le tatouage est une solution intéressante. Le tatouage consiste en l'insertion d'une information invisible et indélebile dans une image pour

la transmission de celle-ci via le réseau par exemple [3, 4]. A la réception, cette information doit pouvoir être extraite de l'image pour différentes utilisations. La longueur du message peut être relativement importante selon l'application. Nous montrons ici une méthode de tatouage dans le domaine spatial, qui du fait de la transmission via le réseau doit résister à la compression JPEG. Les méthodes classiques de tatouage dans le domaine spatial modifient les bits de poids le plus faible (LSB) au niveau des pixels pour y insérer des bits du message à transmettre [6, 7]. Ces méthodes considèrent que les LSB n'apportent pas une information significative dans l'image, et que la vision humaine n'est pas capable de détecter plus de 60 niveaux de gris. Cependant, la modification seule du LSB par pixel n'est pas robuste pour des applications nécessitant une compression. En effet dans le cas d'une compression JPEG, des composantes hautes fréquences sont supprimées et le message contenu dans les LSB est perdu.
Pour augmenter la robustesse, nous proposons une technique de tatouage spatial par blocs de 8×8 pixels. Dans chaque bloc, nous modifions, le LSB de la moyenne des niveaux de gris du bloc de manière à y insérer la valeur d'un bit du message. Nous montrons ensuite qu'il est possible d'insérer le message en utilisant le deuxième ou le troisième bit de poids le plus faible de la valeur moyenne du bloc de manière à augmenter la robustesse de la méthode sans dégradrer la qualité de l'image.
Dans le cas d'un tatouage par blocs sur le LSB, nous calculons la valeur moyenne des niveaux de gris des pixels composant le bloc courant. Si nous souhaitons marquer un 0 ou un 1, nous augmentons ou diminuons le niveau de gris des 64 pixels du bloc de manière à ce que le LSB de la valeur moyenne du bloc corresponde à la valeur souhaitée. Pour le LSB, 4 cas sont possibles.
Dans le cas par exemple d'un tatouage par blocs sur le troisième LSB de la valeur moyenne des blocs, nous avons

$$\underline{\text{pour obtenir ——0– :}}$$

$$p(i) = \begin{cases} p(i)+1 & si \quad --000 \\ p(i) & si \quad --001 \\ p(i) & si \quad --010 \\ p(i)-1 & si \quad --011 \\ p(i)-2 & si \quad --100 \\ p(i)-3 & si \quad --101 \\ p(i)+3 & si \quad --110 \\ p(i)+2 & si \quad --111 \end{cases} \tag{3}$$

$$\underline{\text{pour obtenir ——1– :}}$$

$$p(i) = \begin{cases} p(i)-2 & si \quad --000 \\ p(i)-3 & si \quad --001 \\ p(i)+3 & si \quad --010 \\ p(i)+2 & si \quad --011 \\ p(i)+1 & si \quad --100 \\ p(i) & si \quad --101 \\ p(i) & si \quad --110 \\ p(i)-1 & si \quad --111 \end{cases} \tag{4}$$

3.2 Résultats

	original	100 %	90 %	75 %
bit 1	OK	×	×	×
PSNR dB	57.85	55.19	41.16	36.73
bit 2	OK	OK	×	×
PSNR dB	52.08	51.19	40.91	36.64
bit 3	OK	OK	OK	OK
PSNR dB	49.74	49.21	40.68	36.56

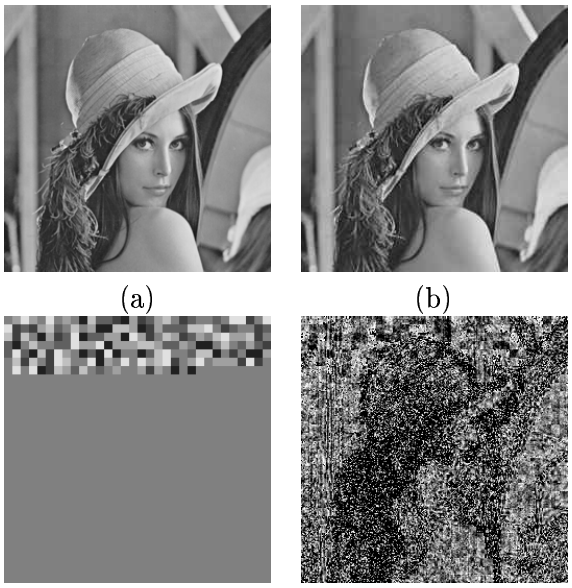
Table 1: Différents résultats, OK quand le message reçu est identique au message émis.

Pour un tatouage par blocs sur le LSB, avec un message composé de 888 bits et une compression JPEG de qualité 100%, seulement 5% des bits du message sont erronés. Par contre 30% des caractères du message sont faux, mais très peu de caractères faux ont plus d'un bit faux. Statistiquement le nombre de bits faux par caractère suit une loi de Poisson. Si nous diminuons le facteur de qualité de compression, statistiquement le nombre de bits faux par caractère suit une loi gaussienne. Par exemple pour un facteur de

qualité de 75%, 50% des bits sont faux et tous les caractères du message sont erronés.

(a) (b)

Figure 5: (a) Tatouage par blocs en utilisant le LSB de la valeur moyenne du bloc, (b) Différence entre l'image tatouée utilisant le LSB de la valeur moyenne du bloc comprimée à 100% et l'image originale.



(a) (b)

(c) (d)

Figure 6: *(a) Tatouage par blocs en utilisant le troisième LSB de la valeur moyenne du bloc, (b) Compression de l'image (a) avec un facteur de qualité de* 40%*, (c) Différence entre l'image (a) et l'image originale, (d) Différence entre l'image (b) et l'image originale.*

La figure 5.a illustre un tatouage d'image par blocs en utilisant le LSB. Le bruit rajouté par la compression est représenté figure 5.b. Dans le Tableau 1, nous montrons les différents résultats obtenus pour plusieurs taux de compression en utilisant le tatouage par blocs sur le premier, deuxième et troisième LSB. Ces résultats montrent les limites de cette technique. Le tatouage sur le troisième LSB est correct jusqu'à une compression de 48 %. Pour une compression à 50 %, le PSNR est égal à $33.77dB$. Le tatouage utilisant le troisième LSB est plus robuste car la compression modifie pricipalement les deux LSB de la valeur moyenne du bloc. En revanche, la qualité de l'image diminue, le tatouage devient visible aux frontières des blocs. Les figures 6 illustrent la perte de qualité due au tatouage et à une compression à 40%.

4 Conclusion

Nous avons présenté une technique récursive de cryptage d'images basée sur le chiffrement de Vigenère. La longueur de la clef dépend de l'ordre utilisé qui doit au moins être égal à 3. Pour insérer des informations textuelles, nous avons présenté une méthode de tatouage spatial par blocs. Celle-ci devant être robuste à la compression doit s'appuyer sur le troisième LSB afin de transmettre correctement le message. Nous travaillons actuellement sur des améliorations de cette méthode en utilisant les valeurs réelles des moyennes des blocs de pixels.

References

[1] NBS FIPS 46. Data encryption standard. Technical report, National Bureau of Standards, U.S. Department of Commerce, 1977.

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

[3] Leighton T. Cox I., Kilian J and Shamoon T. Secure spread spectrum watermarking for multimedia. Technical Report 95-10, NEC Research Institute, Princeton, NJ, USA, 1995.

[4] De Vleeschouwer C. Delaigle J.F. and Macq B. Watermarking algorithm based on a human visual model. *Special Issue on Watermarking, Signal Processing*, 66(3):319–336, 1998.

[5] Shamir A. Rivest R. L. and Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[6] Zhu B. Swanson M.D. and Tewfik A.H. Transparent robust image watermarking. In *International Conference on Image Processing, Lausanne, Switzerland*, 1996.

[7] Tyrkel A.Z Van Schyndel R.G. and Osborne C.F. A digital watermark. In *International Conference on Image Processing, Austin, Texas*, 1994.

[8] Diffie W. and Hellman M. E. New directions in cryptography. *IEEE Transactions on Information Theory*, 26(6):644–654, 1976.