Stéganographie d'images basées sur le théorème chinois des restes

Dinu COLTUC[1], Alain TRÉMEAU[2]

[1]FIE, Université Valahia de Targoviste
BP 16-296, Bucarest, Roumanie

[2]LIGIV, Université Jean Monnet
10, rue Barrouin, 42000 Saint Etienne, France
coltuc@valahia.ro, tremeau@ligiv.org

Résumé – Dans ce papier nous nous intéressons au problème de cacher dans une image, moyennant une seule opération, de multiple messages provenant de multiples utilisateurs. L'idée est d'utiliser le théorème chinois des restes. Sur le plan théorique, il est établi qu'un nombre illimité de messages peuvent être insérée dans l'image elle-même. Une des limites de l'approche vient du fait que ces multiples messages ne doivent être ni détectables, ni visibles. Par construction, la première condition est naturellement satisfaite, par contre toute la difficulté consiste à satisfaire la seconde condition. Un atout de cette approche est que chaque utilisateur peut disposer d'une clé différente pour détecter une des marques superposée à l'image.

Abstract – This paper investigates the problem of embedding, in the same cover image, multiple messages for multiple receiving parties. A solution based on the Chinese Reminder Theorem is given. Theoretically, an unlimited number of messages can be inserted. The security of the scheme is provided by distinct secret key for each receiver. Experimental results are provided.

1 Introduction

Dans ce papier nous nous intéressons au problème de cacher dans une image, moyennant une seule opération, de multiple messages provenant de multiples utilisateurs. Chaque utilisateur dispose d'une clé secrète qui lui est propre.

Pour illustrer l'insertion de multiple messages prenons tout d'abord un des cas d'étude les plus simples; celui de deux messages (*codewords*) que l'on veut superposer à un couple de pixels a et b. Soit m_1 et m_2 les deux clés secrètes considérées, et r_1 et r_2 les deux messages associés. Considérons que $r_1 < m_1$ et $r_2 < m_2$. L'idée est d'ajouter une certaine quantité à l'un des pixels (e.g. a) de façon que le reste de la différence entre les deux pixels (i.e. a - b) divisé par m_1 soit égal à r_1. Ensuite, il suffit d'ajouter une certaine quantité à chacun des deux pixels (e.g. a et b) de façon que le reste de la somme des deux pixels (i.e. a + b) divisé par m_2 soit égal à r_2. Un tel approche permet l'insertion simultanée de deux messages dans tout groupe de deux pixels.

Ce papier propose une méthode pour superposer K messages à une image, avec $K \geq 2$. Notre approche est basée sur le principe du théorème chinois des restes [1]. Reste ensuite, comme dans tout processus de stéganographie sécurisé, à s'assurer que les messages transmis n'ont pas été altérés par un processus donné. Nous verrons que compte tenue de la stratégie de marquage que nous avons utilisé, la résolution de ce dernier point est par définition immédiate.

Le plan de ce papier et le suivant. Le théorème chinois des restes est brièvement rappelé dans la deuxième section. Dans la troisième section, nous donnons les principes de base de notre approche. Des résultats expérimentaux sont fournis dans la quatrième section. Finalement, dans la cinquième section nous présentons nos conclusions.

2 Théorème chinois des restes

Le théorème chinois des restes démontre l'existence d'un nombre inconnu qui, divisé par un ensemble de diviseurs, donne un ensemble de restes souhaités. Soit N ce nombre, m_i les valeurs de chacun des diviseurs, et r_i, $i = 1, \ldots, K$ chacun des restes modulo les valeurs des diviseurs, on a alors :

$$N \bmod m_i = r_i,\ i = 1, \ldots, K \tag{1}$$

Selon le théorème chinois des restes, si l'ensemble des valeurs de modulo (i.e. les m_i) forme un ensemble de nombres premiers entre eux alors le système d'équations donné par (1) possède une solution unique N, $1 \leq N \leq M$ où :

$$M = m_1 m_2 \ldots m_K \tag{2}$$

L'existence et l'unicité de N peut être facilement démontrée mathématiquement en trouvant un ensemble de K nombres M_i ayant les deux propriétés suivantes :

$$M_i \bmod m_i = 1,\ i = 1, \ldots, K \tag{3}$$

et

$$M_i \bmod m_j = 0,\ i \neq j,\ i, j = 1, \ldots, K, \tag{4}$$

Donc, N est calculé par :

$$N = \left(\sum_{i=1}^{K} M_i r_i \right) \bmod M \tag{5}$$

La preuve est immédiate: les équations (1) peuvent être établies en prenant $N \bmod m_i$, $i = 1, \ldots, K$, et en utilisant les équations (3) et(4).

Dans le but de trouver l'ensemble M_i, on peut remarquer que M_i est divisible par tous les modulo à l'exception de m_i, c'est à dire :

$$M_i = A\frac{M}{m_i} \tag{6}$$

De plus, la division de M_i par m_i donner un reste égal à 1 :

$$M_i = Bm_i + 1 \tag{7}$$

Les équations (6) et (7) entraînent que :

$$A\frac{M}{m_i} - Bm_i = 1 \tag{8}$$

ou, évidement, $\frac{M}{m_i}$ est un entier.

L'équation (8) est équivalente à l'équation classique :

$$Ap + Bq = 1. \tag{9}$$

L'algorithme Euclidien décrit dans [1] peut être ensuite utilisé pour trouver les valeurs A et B. Enfin, en utilisant l'équation (6), (ou l'équation (7)), l'ensemble M_i est trouvé et, par conséquence, on détermine N.

3 Principes de base de l'algorithme

Soit K le nombre de messages. Supposons que chaque message R_i, $i = 1, \ldots, K$, soit de même longueur P. Soit r_i^j la $j^{\text{ème}}$ valeur ($j = 1, \ldots, P$) du $i^{\text{ème}}$ ($i = 1, \ldots, K$) message. Pour chaque message, un diviseur m_i est associé. Afin de satisfaire le théorème chinois des restes, tous les diviseurs m_i doivent former des nombres premiers entre eux et tous les restes doivent vérifier $r_i^j < m_i$, $j = 1, \ldots, P$.

Partitionnons tout d'abord l'image en groupes de p pixels, avec $p \geq 1$. Considérons, pour des raisons de simplicité, que le nombre de groupes que l'on va définir est égal à la longueur des messages P que l'on veut appliquer. Pour chaque message (et chaque utilisateur) une fonction de permutation secrète Π_i est définie, $\Pi_i : \{1, 2, \ldots, P\} \rightarrow \{1, 2, \ldots, P\}$. Considérons que Π_0 corresponde à la permutation identité.

3.1 Clé secrète

L'algorithme de marquage que l'on propose repose sur l'utilisation d'une clé secrète qui porte sur trois éléments:

1. le partitionnement du plan image en P groupes de p pixels, quand $p \geq 1$;
2. la fonction de permutation Π_i;
3. les diviseurs m_i.

La partition est identique quelque soit l'utilisateur. Ce dispositif présente deux niveaux de sécurité. Le premier, global au système, vient du fait que l'image est partitionnée en groupes de p pixels (quand $p \geq 1$), l'autre spécifique à l'utilisateur, vient des valeurs m_i et Π_i.

Les valeurs m_i ne permettent pas un haut degré de sécurité puisque le nombre de possibilité quant au choix de ces valeurs est extrêmement limité. Par contre, la fonction de permutation Π_i et la fonction de partition renforcent nettement cette sécurité. Pour le moment, le nombre de permutations est en $P!$ ou P est le nombre de groupes pixels dans l'image. De même, un très grand nombre de partitions en groupes de p pixels peut être défini pour un ensemble donné de P groupes. L'ordre dans lequel sont traités ces p pixels à l'intérieur du groupe a aussi une répercussion sur le nombre de combinaisons.

FIG. 1: Image de test.

3.2 Marquage

L'algorithme de marquage est alors le suivant :

1. générer les messages à partir des permutations secrètes $\Pi_i(R_i)$;
2. générer le $j^{\text{ème}}$ élément de la séquence N_j, $j = 1, \ldots, P$, à partir du théorème chinois des restes, i.e. en fonction de l'ensemble des valeurs de modulo précédemment utilisées;
3. insérer chaque message N_j dans chacun des groupes de p pixels à partir de la permutation identité Π_0.

Etant donné que $r_i^j < m_i$ et que le message N_j est inséré dans p pixels, la capacité du schéma est de :

$$C = \frac{\sum_{i=1}^{K} \log_2 m_i}{p} \text{ bpp} \tag{10}$$

On peut remarquer que M croit avec K. Donc, pour un p fixé, C croit également. L'effet de la croissance du taux d'information conduit évidement à une perte de qualité de l'image stéganographiée. Dans le but de contrôler cette qualité on peut restreindre le taux d'information par pixel a une certaine valeur q imposée et déterminer la taille de p :

$$p \geq \left\lceil \frac{\log_2 M}{q} \right\rceil \tag{11}$$

ou $\lceil x \rceil$ est le plus petit entier plus grand ou egal à x.

FIG. 2: Image stéganonographiée avec 2 messages par pixel, 2.58 bpp, 43 dB.

FIG. 3: Image stéganographiée avec 3 messages par pixel, 4.9 bpp, 29 dB.

3.3 Detection

L'algorithme de détection se définit assez facilement de la manière suivante pour l'utilisateur i :

1. extraire le $j^{\text{ème}}$ élément de la séquence N_j, $j = 1, \ldots, P$, à partir de la partition en groupes de p pixels (si $p > 1$) et de la clé secrète de permutation Π_i;
2. extraire le message $r_i^j = N_j \bmod m_i$, $j = 1, \ldots, P$.

Etant donné que la séquence N_j est accessible à tous les utilisateurs, on pourrait penser pouvoir détecter tous les messages destinés à tout autre utilisateur que soit même. Quand bien même un utilisateur pourrait retrouver à partir de sa valeur de modulo l'ensemble de la séquence des messages, i.e. l'ensemble des valeurs de modulo secrètes, il ne pourrait décoder celles-ci car il ne saurait pas dans quel ordre ceux-ci ont été constitués. Comme nous l'avons déjà indiqué, retrouver à partir de tests exhaustifs l'ensemble des permutations effectuées relève d'une opération d'une extrême complexité.

4 Résultats experimentaux

La méthode présentée dans la section précédente produit à partir de K messages une séquence de entiers N_j qu'on doit insérer dans un ou plusieurs pixels. Un grand nombre des méthodes ont été développées pour l'insertion des données [2, 3, 4]. Parmi ces méthodes, les méthodes spatiales qui remplacent les bits de poids faible sont les plus simples. Pour la mise en oeuvre de notre méthode nous allons utiliser une telle méthode. Dans ce papier nous avons choisi de présenter seulement quelques résultats illustratifs, ceux-ci ont été obtenus à partir de l'image test *Lena* de taille 512×512. (Fig. 1).

Dans un premier temps nous avons considéré l'insertion simultanée de deux messages en chaque pixel. Dans le premier exemple que nous donnons, nous avons utilisé les paramètres suivants : $m_1 = 2$, $m_2 = 3$ et $p = 1$. Afin d'insérer les N_j séquences dans chaque pixel de l'image une procédure assez simple a été utilisée. Les pixels ont été quantifiés de façon à avoir des multiples de M, on a ensuite ajouté à chaque pixel la valeur correspondante à N_j. Comme on peut le constater sur la Fig. 2, l'image stéganographiée résultante est de bonne qualité; son PSNR est de 43.1 dB. Le taux d'information cachée est ici de 2.58 bits par pixel.

Le second exemple que nous donnons porte sur l'insertion simultanée de trois messages. Dans cet exemple nous avons utilisé les paramètres suivants : $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ et $p = 1$. En ajoutant un troisième message on a augmenté du taux d'information cachée, passant ainsi de 2.58 bits par pixel à 4.9 bits par pixel. Comme cela était attendu la qualité de l'image stéganographiée résultante a diminué, l'image est devenue de moins bonne qualité (cf. Fig. 3); son PSNR est tombé à 29.16 dB.

Les premiers tests que nous avons réalisés ont porté sur l'insertion de deux ou de plusieurs messages en chaque pixel. Afin d'améliorer la qualité de l'image stéganographiée ou d'augmenter le nombre de messages insérés dans l'image, nous avons ensuite étendu notre schéma d'insertion à un groupe de p pixels, $p > 1$.

Dans l'exemple que nous donnons, nous avons considéré l'insertion simultanée de trois messages pour tous les groupes de 2 pixels. Nous avons utilisé les paramètres suivants : $m_1 = 2$, $m_2 = 3$, $m_3 = 5$. Ces paramètres sont exactement les mêmes que ceux utilisés dans l'exemple précédent pour l'insertion de trois messages en chaque pixel. Etant donné que l'insertion porte, maintenant non

FIG. 4: Image stéganographiée avec 3 messages groupe de 2 pixels, 2.45 bpp, 40.72 dB.

FIG. 5: Image stéganographiée avec 4 messages par groupe de 2 pixels, 3.85 bpp, 32.57 dB.

plus sur chaque pixel, mais sur un groupe de 2 pixels, le taux d'information cachée a *a fortiori* diminué d'autant et la qualité de l'image stéganographiée a augmenté. Nous avons obtenu un taux d'information cachée de 2.45 bpp et un PSNR de 40.72 dB (cf. Fig. 4).

Nous pouvons augmenter le nombre de messages distincts que l'on peut superposer à des groupes de 2 pixels. L'exemple de la Fig. 5 est obtenu pour les paramètres suivants : 4 messages ($m_1 = 2$, $m_2 = 3$, $m_3 = 5$ et $m_4 = 7$). Dans ce conditions, pour une insertion dans des groupes de 2 pixels, nous avons obtenu un taux d'information cachée de 3.85 bpp et un PSNR de 32.57 dB.

5 Conclusion

Dans ce papier nous avons proposé une méthode d'insertion de multiple messages pour différents utilisateurs qui repose sur le principe du théorème chinois des restes. Afin d'illustrer le principe de notre méthode, un schéma d'insersion simple a été proposé. La sécurité de ce schéma est principalement assurée par l'utilisation d'une fonction de permutations secrète d'un ensemble de P éléments, ou P représente le nombre de pixels de l'image (ou une fraction de l'image). Un niveau supplémentaire de sécurité est assuré par l'utilisation d'une fonction de partition secrète de l'image pour le cas ou l'insertion porte non pas sur chaque pixel mais sur des groupes de p pixels. Différents exemples d'insertion simultanée de deux ou trois messages, en chaque pixel ou sur des groupes de 2 pixels ont été donné. Les résultats ainsi obtenus semblent prometteurs. D'autres travaux sont en cours, ceux-ci portent notamment sur la conception de schémas d'insertion plus complexes. L'objectif est d'optimiser le rapport capacité d'insertion / nombre de messages insérés, sous la contrainte de ne pas trop dégrader la qualité de l'image résultante, d'où la nécessité d'affiner la procédure d'insertion à partir de groupes de p pixels. L'extension aux images couleur constitue en ce sens une piste intéressante, en effet grâce à l'information couleur on peut plus facilement jouer sur une minimisation de la perte de qualité d'une image, compte tenu de la sensibilité du système visuel humain à percevoir plus facilement certaines différences images que d'autres.

References

[1] D. E. Knuth, *The Art of Computer Programming. Seminumerical Algorithms*, Third Edition, Addison Wesley, 1998.

[2] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Information Hiding: a Survey", *Proceedings of the IEEE*, vol. 87 no. 7, pp. 1062-1078, July 1999.

[3] F. Hartung, M. Kutter, "Multimedia Watermarking Techniques", *Proceedings of the IEEE*, vol. 87 no. 7, pp. 1079-1107, July 1999.

[4] B. Chen, G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", *IEEE Trans. on Information Theory*, vol. 47 no. 4, pp. 1423-1443, May 2001.