Tatouage d'images par ondelettes et application à la couleur

Franck DAVOINE[1], François CAYRE[2]

[1]Laboratoire HeuDiaSyC, Université de Technologie de Compiègne
BP 20529, 60205 Compiègne, France

[2]Laboratoire TELE, Université catholique de Louvain
2, Place du Levant, 1348 Louvain-La-Neuve, Belgique
fdavoine@utc.fr, cayre@tele.ucl.ac.be

Résumé – Cet article introduit une méthode de tatouage pour la protection d'images fixes. La méthode permet de cacher une signature dans une image, sous la forme de w paquets de r bits. Le schéma de tatouage est multiplicatif, et la signature elle-même est calculée par addition de produits de couples de fonctions orthogonales. Nous montrerons comment le choix des fonctions orthogonales peut être fait, de façon à rendre le tatouage robuste face à différents types d'attaques. Puis, nous donnerons quelques résultats permettant d'apprécier la robustesse du tatouage, et discuterons des améliorations possibles pouvant être apportées à une telle méthode.

Abstract – This paper introduces an approach of watermarking for copyright protection. The goal of the method is to hide signatures composed of w segments of r bits in digital images. The framework itself is founded upon a wavelet transformed domain, and a multiplicative embedding rule using products of orthogonal basis functions. We will show how the choice of different kinds of orthogonal functions allows to improve the robustness of the watermarking scheme to signal processing or geometric attacks.

1 Introduction

Le tatouage d'images est une technique encore jeune, qui a pour but de dissimuler au sein même de l'information visuelle d'une image numérique, une signature identifiant son propriétaire, ou son contenu. La signature code un ou plusieurs bits, et ne doit pas être perçue par l'œil humain. Selon le cas, elle doit être indélébile, indétectable, et/ou illisible par une personne non autorisée et par quelque moyen que ce soit. Ces conditions ne peuvent bien sûr pas être rigoureusement toutes vérifiées en même temps, et les schémas de tatouage proposés doivent tenir compte de l'application visée. Le principe de l'algorithme de tatouage peut en outre être connu ou secret.
Notre objectif ici est de proposer une méthode de tatouage aveugle d'images fixes, basée sur une transformation en ondelettes discrète, et utilisant un ensemble de produits de fonctions orthogonales[1]. La méthode permet de dissimuler w paquets de r bits dans une image. La paramétrisation des fonctions permet d'adapter la robustesse du tatoueur à deux principaux types d'attaques : les attaques par traitement du signal (plus particulièrement le filtrage, et la compression JPEG), et les déformations géométriques locales du contenu de l'image. Nous décrirons le principe de la méthode et testerons sa robustesse face aux attaques visées. Enfin, nous testerons la méthode sur des images couleur.

1. Les auteurs remercient le RNRT pour avoir soutenu ce travail, dans le cadre du projet Aquamars.

2 Une méthode générique de tatouage

La méthode de tatouage d'images que nous décrivons ici utilise une transformée en ondelettes discrète. Elle consiste, comme l'ont proposé Barni *et al.* [1] en 1999, à ne marquer que les coefficients d'ondelette des trois images de plus fine résolution, et par conséquent, de tailles suffisamment grandes. La représentation d'une image par sa transformée en ondelettes est pratique puisqu'elle met en évidence l'information visuelle importante, telles que les régions fortement texturées et les contours. Lewis *et al.* [4] ont proposé en 1992 d'optimiser le calcul des seuils de décision d'un quantificateur scalaire des coefficients d'ondelettes, suivant un critère de perception psychovisuelle des dégradations engendrées sur l'image. Nous utiliserons ce schéma, pour calculer un masque de pondération psychovisuelle permettant d'accentuer l'insertion de la signature là où elle est peu perçue par l'œil humain. Introduisons maintenant les méthodes de tatouage d'images, puis de relecture des bits de la signature.

2.1 Insertion de la signature

Soit une clé K dite *privée*, utilisée pour interdire la relecture sans autorisation d'une signature M. Les conditions suivantes sur K et M doivent être vérifiées :

$$M = \bigoplus_{i=1}^{w} M_i^r \ , \quad M_i^r \in \{0;1\}^r \ , \ \forall i \in [1;w] \qquad (1)$$

$$K = \bigoplus_{i=1}^{w} K_i^l \ , \quad K_i^l \in \{0;1\}^l \ , \ \forall i \in [1;w] \qquad (2)$$

$$\text{et } \forall (i,j) \in [1;w]^2 \quad K_i^l \neq K_j^l \qquad (3)$$

où $\bigoplus$ est l'opérateur de concaténation. La clé et la signature sont donc respectivement découpées en w paquets (segments binaires) de l et r bits. Notons ici que la construction des segments K_i^l (resp. M_i^r) pourrait se faire en choisissant aléatoirement les bits dans K (resp. M), pour augmenter la sécurité globale du système de tatouage, comme nous le verrons par la suite. Les segments de clé doivent également être tous différents (3), de façon à éviter toutes interférences. Soit une image originale I de taille $2m \times 2n$, et deux ensembles de fonctions de base :

$$F_{M,k} \ : \ [0;m] \times [0;n] \to \mathbb{R} \ , \quad k \in \mathbb{N} \qquad (4)$$

$$F_{K,k} \ : \ [0;m] \times [0;n] \to \mathbb{R} \ , \quad k \in \mathbb{N} \qquad (5)$$

avec les contraintes d'orthogonalité intra- et inter-ensembles suivantes :

$$\forall (\alpha,\beta) \in \mathbb{N}^2 \quad \langle F_{M,\alpha} \ , \ F_{M,\beta} \rangle = \delta_{\alpha,\beta} \qquad (6)$$

$$\forall (\alpha,\beta) \in \mathbb{N}^2 \quad \langle F_{K,\alpha} \ , \ F_{K,\beta} \rangle = \delta_{\alpha,\beta} \qquad (7)$$

$$\forall (\alpha,\beta) \in \mathbb{N}^2 \quad \langle F_{M,\alpha} \ , \ F_{K,\beta} \rangle = 0 \qquad (8)$$

Chaque segment binaire est vu comme un index, de la manière suivante : le segment M_i^r de la signature indexe une des 2^r fonctions $F_{M,k}$, le segment K_i^l de la clé indexe une des 2^l fonctions $F_{K,k}$. Soit $b_\nu : \{0,1\}^\nu \to \mathbb{N}$ une bijection, permettant d'associer une valeur d'index à un segment binaire. L'équation suivante définit une fonction de marquage W permettant de "porter" la signature M composée de $w \times r$ bits :

$$W(i,j) = \frac{1}{w} \sum_{p=1}^{w} F_{K,b_l(K_p^l)}(i,j) \times F_{M,b_r(M_p^r)}(i,j) \qquad (9)$$

Soit l'image I, sur laquelle nous calculons une transformée en ondelettes discrète. Notons I_s ($s \in HL, LH, HH$) les trois images de plus fine résolution, chacune de taille $m \times n$, et composées des coefficients d'ondelettes $I_s(i,j)$. L'insertion de la signature dans l'image se fait selon un schéma multiplicatif, pour accentuer le marquage des coefficients d'ondelettes les plus significatifs. Soit I_s^W la version tatouée de I_s, et ω_s un masque de pondération psychovisuelle [4] calculé à partir de la représentation multirésolutions de l'image I. Pour chacune des trois images I_s, le masque ω_s fournit une valeur de pondération réelle par coefficient d'ondelette. Soit enfin le coefficient α permettant de contrôler la force du tatouage. L'insertion de la signature se fait de la façon suivante :

$$I_s^W(i,j) = I_s(i,j) + \alpha \times \omega_s(i,j) \times |I_s(i,j)| \times W(i,j) \qquad (10)$$

L'image tatouée I^W est ensuite obtenue par transformation en ondelettes inverse, à partir des images de coefficients I_d^W.

2.2 Lecture de la signature

La lecture des w paquets de r bits à partir de l'image I^W peut se faire assez facilement, si les conditions d'orthogonalité (éq. 6, 7 et 8) sont vérifiées. Nous proposons ici la méthode simple suivante : soit une clé K et une image tatouée. La clé est découpée selon (2), pour extraire chacun des segments K_p^l. Il reste à calculer les corrélations entre I_s^W et les produits $\omega_s' \times F_{K,b_l(K_p^l)} \times F_{M,b_r(M_q^r)}$ pour chaque $q \in \{1, 2^r\}$. Le masque ω_s' est recalculé sur l'image tatouée et éventuellement attaquée. Pour un segment K_p^l donné, on ne conserve que les fonctions $F_{M,b_r(M_q^r)}$ qui retournent la corrélation maximale $C1_{F_M}^{max}(K_p^l)$, et la deuxième corrélation $C2_{F_M}^{max}(K_p^l)$, maximum des $2^r - 1$ corrélations restantes. La fonction $F_{M,b_r(M_q^r)}$ associée au segment K_p^l est jugée correcte si la différence $(C_1 - C_2)$ est supérieure à un seuil fixé, calculé de la façon suivante :

$$C_1 - C_2 > \mathcal{T} \times C_1, \quad \text{avec } 0 < \mathcal{T} < 0.3 \qquad (11)$$

Si le test (11) réussit, la séquence binaire M_q^r constituant une partie de la signature M est retrouvée à partir de la transformation inverse b_r^{-1}. On peut noter dès à présent que des compromis devront être trouvés sur les longueurs l (resp. r) des segments de clé (resp. signature). La longueur r ne doit pas être trop élevée car sinon, un nombre trop important de bits peut être perdu, en cas de fausse détection. La lecture de la marque par corrélations devient également trop coûteuse en temps de calculs. Et enfin il deviendrait difficile d'introduire un nombre trop important de fonctions orthogonales dans un support d'image de taille limitée (nous n'utilisons que les trois quart de la surface de l'image originale pour cacher la signature). Cette dernière remarque impose de limiter également la longueur l.

3 Implémentation

Nous présentons ici deux exemples d'implémentation de la méthode générique décrite dans la section 2, en utilisant deux types de fonctions de base, puis des résultats expérimentaux seront donnés dans la section 4. La transformation de l'image originale est calculée à partir d'ondelettes biorthogonales, selon un schéma "lifting". Nous nous fixons pour objectif d'introduire une signature de 64 bits dans une image monochrome de taille 256×256, codée sur 8 bits par pixel. Nous vérifierons les qualités de l'algorithme en terme de robustesse face à des attaques volontaires ou pas, de type JPEG ou géométriques.
Barni *et al.* [1] ont montré la robustesse de leur algorithme de tatouage par ondelettes et étalement de spectre, en utilisant des fonctions pseudo-aléatoires réelles centrées, de variance unité, et supposées être suffisamment orthogonales. De façon à tester la robustesse de notre algorithme face aux mêmes attaques que dans [1], nous avons utilisé le même type de fonctions pour F_M et F_K. Notons ici que ces deux ensembles de fonctions nous permettent de cacher w paquets de r bits dans une image, et non plus un seul bit, comme dans [1]. La lecture de la signature se fait par calcul de corrélations entre une fonction pseudo-aléatoire extraite de l'image tatouée et un ensemble d'autres fonctions, proposées par le propriétaire de l'image originale. Ceci impose donc que la géométrie globale de l'image ne soit pas trop modifiée après tatouage. Dans le cas contraire, les correspondances entre compo-

santes des fonctions sont perdues (les fonctions sont dites "désynchronisées") et le message ne peut pas être relu. Ce type de méthode de tatouage simple ne résiste donc pas à des déformations géométriques appliquées sur la totalité du support de l'image tatouée. Une solution proposée par différents auteurs est de cacher dans l'image des points ou motifs "d'encrage", faciles à retrouver avant lecture de la signature, et permettant de compenser les déformations géométriques. Mais ces points peuvent éventuellement être effacés de l'image tatouée.
Nous proposons ici d'utiliser des fonctions orthogonales pour F_M et F_K, plus régulières que des séquences pseudo-aléatoires, pour être moins sensibles aux problèmes de désynchronisation. C'est aussi pour cette raison que nous qualifions cette technique de *tatouage mou*. Les algorithmes d'attaque tels que *Stirmark* [6] appliquent des faibles déformations locales sur l'ensemble du support de l'image, tout en préservant une qualité visuelle suffisante. Nous proposons dans notre cas d'utiliser des sinusoïdes orthogonales de basses fréquences, horizontales pour F_M, et verticales pour F_K, de périodes suffisamment grandes par rapport à la taille des déformations locales introduites par exemple par *Stirmark*:

$$F_{M,k}(i,j) = \cos\left(\frac{2 \times \pi \times k \times i}{\beta_M}\right) \quad (12)$$

$$F_{K,k}(i,j) = \cos\left(\frac{2 \times \pi \times k \times j}{\beta_K}\right) \quad (13)$$

Nous choisissons arbitrairement les longueurs $l = r = 8$ et $\beta_K = 2 \times \beta_M = 256$. La signature sera introduite avec une force $\alpha = 0.35$ de façon à préserver la qualité visuelle des images marquées, et la valeur de $\mathcal{T}$ qui permet de relire chacun des segments de la signature est expérimentalement fixée à 0.10.

4 Résultats

Afin d'évaluer l'influence de différentes attaques sur la lecture de la signature, nous choisissons d'illustrer nos résultats sur la seule image Lena, sachant que des résultats similaires ont été obtenus sur d'autres images "photographiques" de même taille.

4.1 Tatouage par étalement de spectre

Nous vérifions que des fonctions pseudo-aléatoires pour F_M et F_K permettent de retrouver les 8 paquets de 8 bits, dans l'image Lena, après des attaques simples de type "traitement du signal" telles qu'un filtrage passe-bas 3×3, une compression JPEG de *qualité 50%*, et la conservation d'un quart de la surface de l'image, choisi aléatoirement. La région extraite dans ce dernier cas doit bien sûr pouvoir être replacée à sa place sur le support de l'image originale pour resynchroniser les portions de signature (on parle dans ce cas de *pseudo-cropping*). La signature est également retrouvée si une partie seulement de l'image tatouée est déformée. Elle est par contre effacée (par désynchronisation) si la totalité de la géométrie de l'image est déformée, même faiblement avec des algorithme tels que *Stirmark*.

4.2 Tatouage mou

Afin de tester cette méthode, nous considérerons les deux attaques limites suivantes: une forte compression JPEG, et une déformation géométrique importante de la totalité de l'image tatouée.

Attaques JPEG

Nous vérifions expérimentalement que les 64 bits sont retrouvés, à partir de l'image Lena tatouée, puis compressée avec un facteur de qualité de 17%. L'image a bien sûr dans ce cas perdu toute valeur commerciale, mais le résultat laisse penser qu'une dégradation moindre permettra de retrouver la signature plus facilement. Nous constatons le même type de résultats sur d'autres images photographiques de même taille. La figure 1 illustre l'étape de lecture des huit paquets de huit bits de la signature. Pour un paquet donné, nous affichons à chaque instant les valeurs des corrélations maximales intermédiaires. Les deux derniers pics représentent donc les valeurs de corrélations maximales C_2 et C_1, que l'on compare selon (11).

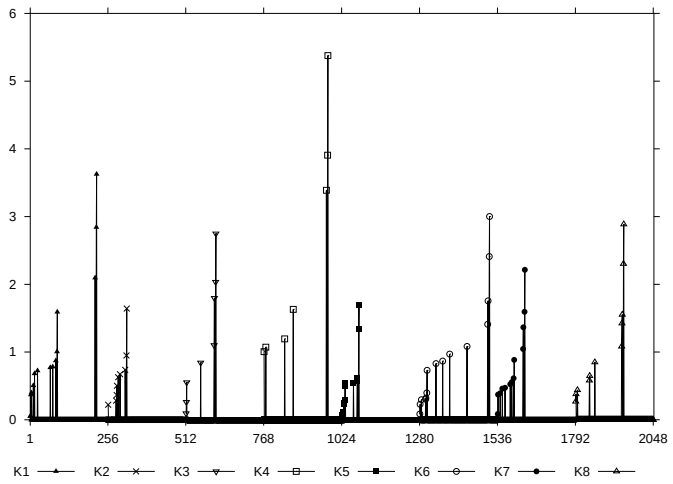

FIG. 1: *Lecture de la signature après attaque JPEG. Pour chaque paquet de la signature, nous affichons à chaque instant les valeurs des corrélations maximales intermédiaires. Les deux derniers pics représentent les valeurs de corrélations maximales C_2 et C_1, qui sont comparées.*

Attaques géométriques

Une transformation globale sinusoïdale d'une amplitude de 4 pixels et de période de 96 pixels est appliquée sur l'image Lena tatouée (Figure. 2, en haut à gauche). Cette déformation a été préférée à celles causées par *Stirmark*, moins visibles. L'utilisation de fonctions régulières pour F_M et F_K permet de retrouver les huit paquets de huit bits, dans l'image Lena de taille 256×256. Nous vérifions qu'il est possible de cacher puis relire une signature de 128 bits dans l'image Lena 512×512, attaquée par déformation cosinusoïdale, ou faiblement déformée par *Stirmark*. L'orthogonalité fréquentielle et spatiale des fonctions des ensembles F_M et F_K est dans ce cas mieux assurée.

La figure 2 montre des exemples d'attaques qui n'effacent pas les 8×8 bits cachés dans Lena 256×256.

FIG. 2: *Relecture de 64 bits dans des images differemment attaquées : warp global, warp local, flash, bruit gaussien, rehaussement de contraste, effet canvas.*

5 Images couleur

L'emploi de la couleur en tatouage d'images est un sujet encore peu exploré. La couleur d'un pixel, codée par un vecteur à trois composantes, peut être représentée dans différents espaces couleur. Ces espaces se calculent à partir de l'espace couleur RGB, par transformations linéaires ou non-linéaires.
La solution retenue ici est d'introduire des séquences de 64 bits indépendemment dans chacune des composantes d'une image couleur, et nous considérons les espaces de représentation RGB et YUV, le dernier étant largement utilisé par les normes de codage d'images fixes et animées. La force α est égale à 0.1, et les masques psychovisuels ω_s sont independamment calculés sur chaque composante. Les résultats (tableau 1) confirment qu'il est difficile d'introduire un nombre trop important de bits dans des composantes à faible entropie, telles que les composantes de chrominance U et V.

TAB. 1: *Extraction de* 3×64 *bits, à partir de l'image Lena en couleur,* 256×256*, compressée JPEG. Un "x" (resp. 64) indique que la détection des 64 bits a échoué (réussi).*

espace / qualité (jpeg)	R	G	B	Y	U	V
50	64	64	64	64	x	x
30	64	64	64	64	x	x
15	x	x	x	x	x	x

6 Conclusions et perspectives

Nous avons proposé dans cet article une nouvelle méthode générique de tatouage d'images, permettant de cacher une signature de w paquets de r bits (typiquement 8×8 bits) dans une image photographique monochrome de taille 256×256. La méthode insère dans l'image une somme de produits de fonctions orthogonales, et ces dernières peuvent être choisies en fonction du type d'attaques auxquelles le tatoueur devra faire face. La méthode s'est révélée être robuste face à des attaques simples de type traitement du signal, mais aussi à des attaques géométriques locales, réparties sur tout le support de l'image, et sur les composantes R, G et B d'une image couleur. La méthode générique peut bien sûr être améliorée. Nous proposons ici plusieurs solutions. L'utilisation de fonctions pseudo-aléatoires permet de calculer des seuils statistiques dépendant d'une probabilité fixée à l'avance de fausse détection des segments de la signature, comme l'ont déjà proposé différents auteurs, pour cacher un bit dans une image [2, 1]. Les fonctions régulières proposées dans l'article (des cosinus) sont orthogonales, mais elles perdent cette propriété s'il est nécessaire d'en cacher un grand nombre dans les trois quart de la surface de l'image à tatouer (les images des coefficients d'ondelette de plus fine résolution). Il reste donc à trouver des fonctions orthogonales régulières, plus locales, pouvant être disposées à différents endroits de l'image. Ces fonctions peuvent en outre être secrètes (ex: [3]), afin de rendre plus difficile la recherche de la signature. Il est également possible de considérer d'autres transformations en ondelettes, à base par exemple d'ondelettes complexes [5], qui présentent l'avantage d'être réversibles, et d'offrir un plus grand nombre de coefficients à tatouer (et donc "plus de place"). Les w paquets de r bits ont été introduits dans l'image, indépendamment les uns des autres. Des codes correcteurs d'erreurs par paquets (ex: Reed Solomon) pourraient donc être considérés. Enfin, une gestion plus efficace des clés et des messages en s'inspirant de résultats de cryptographie renforcerait la sécurité du schéma global de tatouage.

Références

[1] M. BARNI, F. BARTOLINI, V. CAPPELLINI, A. LIPPI and A. PIVA, "A DWT-based technique for spatio-frequency masking of digital signatures", *SPIE, vol. 3657, Conference on Security and Watermarking of Multimedia Content, Electronic Imaging,* San Jose, January 1999.

[2] M. BARNI, F. BARTOLINI, V. CAPPELLINI and A. PIVA, "A DCT-domain system for robust image watermarking", *Signal processing,* Vol. 66, pp. 357-372, 1998

[3] J. FRIDRICH, Lt.A.C. BALDOZA, R.J. SIMARD, "Robust digital watermarking based on key-dependent basis functions", *LNCS 1525, Intl. Information Hiding Workshop,* Portland, USA, April 1998.

[4] A. LEWIS and G. KNOWLES, "Image compression using the 2-D wavelet transform", *IEEE Transactions on Image Processing,* 1(2), pp. 244-250, April 1992.

[5] P. LOO and N. KINGSBURY, "Digital watermarking using complex wavelets", *IEEE Intl. Conference on Image Processing,* Vancouver, 10-13 Sept. 2000.

[6] F. PETITCOLAS and R. ANDERSON, "Evaluation of copyright marking systems", *Proc. of IEEE Multimedia Systems,* june 1999.