Un Algorithme de Tatouage d'Images Numériques reposant sur les Changements d'Horloge Périodiques

Vincent MARTIN[1], Marie CHABERT[1], Bernard LACAZE[2]

[1]ENSEEIHT/IRIT, Institut National Polytechnique de Toulouse
2 Rue Camichel, BP 7122, 31071 Toulouse Cedex 7, France

[2]INSA/IRIT
Vincent.Martin,Marie.Chabert,Bernard.Lacaze@enseeiht.fr

Résumé – Cet article s'intéresse à l'insertion d'un ou plusieurs tatouages dans une image numérique selon la technique d'étalement de spectre. L'algorithme proposé utilise les Changements d'Horloge Périodiques, qui sont une alternative originale aux méthodes classiques de tatouage inspirées des communications multi-utilisateurs par étalement de spectre. Cet article fournit une étude théorique des performances de la méthode proposée, ainsi que des résultats expérimentaux présentant une comparaison détaillée avec un algorithme de référence, en fonction de diverses conditions d'insertion et de diverses attaques. Un masque perceptuel et l'utilisation des propriétés statistiques locales de l'image sont pris en compte dans les résultats théoriques et expérimentaux.

Abstract – This paper deals with the embedding of single or multiple watermarks into digital data. The proposed algorithm is based on Periodic Clock Changes, which are an alternative to classical pseudo-noise modulation methods. This study presents theoretical results and an experimental comparison between the performance of the proposed algorithm and of the classical one, in terms of embedding conditions and of robustness to several attacks. The theoretical and experimental results take into account the use of a perceptual mask and the use of local statistical properties of the image.

1 Introduction

La protection de l'intégrité des images, sons et vidéos numériques et la gestion de leurs droits d'auteurs suscite actuellement un grand intérêt. Le tatouage numérique consiste à insérer une marque dans les composantes perceptuelles du document numérique avant sa diffusion auprès des usagers. Cette marque est constituée d'un ou plusieurs messages secrets. La technique d'insertion peut être publique mais utilise une clé secrète. La marque doit être imperceptible pour l'usager, robuste aux attaques et doit pouvoir être détectée et décodée en réception par une personne munie de la clé. Dans le cadre du tatouage aveugle étudié dans cet article, l'image originale n'est pas nécessaire à la détection. Certaines techniques de tatouage, telles que l'étalement de spectre, s'inspirent d'une analogie avec les communications numériques [6]. En effet, l'insertion et le décodage d'un tatouage peuvent s'interpréter comme la transmission d'un message dans un canal bruité. Le bruit représente alors l'image hôte et les attaques.

Cet article étudie l'insertion additive et simultanée d'un ou plusieurs messages dans une image numérique, selon le principe du tatouage par étalement de spectre [10]. A l'insertion, on étale le spectre du message afin de le dissimuler et au décodage, on étale le spectre du bruit pour mieux l'éliminer. Par analogie avec les méthodes d'accès à répartition par code, on peut effectuer du tatouage multiple. Celui-ci est en effet nécessaire dans certaines applications comme le *fingerprinting*, où chaque utilisateur est identifié par une empreinte unique dans le but de détecter les copies illégales du document. Pour améliorer les performances en réception, différents domaines d'insertion sont possibles. Par ailleurs, l'utilisation d'un masque basé sur les caractéristiques psychovisuelles de l'image permet d'assurer l'imperceptibilité du tatouage.

Cette étude se focalise sur la technique d'étalement en elle-même. L'étalement de spectre est le plus souvent obtenu en modulant le message par une séquence pseudo-aléatoire appelée séquence directe. La séquence directe fait office de clé secrète. Cette technique sera notée dans la suite DS-CDMA (pour *Direct Sequence Code Division Multiple Access*). Dans cet article, les Changements d'Horloge Périodiques (PCC, pour *Periodic Clock Changes*) sont proposés comme technique alternative d'étalement de spectre. Les PCC possèdent des propriétés d'étalement intéressantes et ont été appliqués avec succès aux communications multi-utilisateurs [8].

La partie 2 présente le principe général des PCC et propose un algorithme de tatouage basé sur cette technique. Dans la partie 3, on compare au travers de simulations les performances au décodage de DS-CDMA et PCC par rapport au bruit introduit par l'image hôte et à diverses attaques.

2 Changements d'Horloges Périodiques

2.1 Définitions et propriétés

Un filtre Linéaire Périodique Variant dans le Temps (LPTV) est un filtre dont la réponse impulsionnelle est une fonction $h(n,k)$ T-périodique ($T \in \mathbb{N}$) du temps indexé par $n \in \mathbb{N}$. Sa fonction de transfert $H_n(\omega)$ est définie par :

$$H_n(\omega) = \sum_{k=-\infty}^{+\infty} h(n,k) e^{-ik\omega}, \qquad H_n(\omega) = H_{n+T}(\omega) \quad (1)$$

Les filtres LPTV ont été appliqués à l'entrelacement, à l'égalisation aveugle et aux communications par étalement de spectre [3].

Soit f une fonction T-périodique de n. Dans un cadre stochastique, si $Z = \{Z(n), n \in \mathbb{Z}\}$ est un processus stationnaire alors on appelle Changement d'Horloge Périodique le nouveau processus

$$U(n) = Z(n - f(n)), \qquad f(n) = f(n + T) \qquad (2)$$

Les PCC sont des cas particuliers de LPTV ($H_n(\omega) = e^{-i\omega f(n)}$).

Supposons désormais que $f(n)$ est une permutation aléatoire T-périodique définie par $f(n) = \underline{n} - q_{\underline{n}}$, où q est une permutation de $(0, 1, 2, ..., T-1)$ et $\underline{n}$ le reste de la division euclidienne de n par T ($n = \overline{n}T + \underline{n}$). Le PCC inverse est $f^{-1}(n) = \underline{n} - q_{\underline{n}}^{-1}$. Pour T suffisamment grand, le spectre de V s'approche de celui d'un bruit blanc [8].

Les communications multi-utilisateurs utilisant les PCC transmettent pour chaque message M_j le résultat d'une permutation aléatoire f_j de période donnée T. L'application successive de deux PCC quelconques $f_i \circ f_j$ est un PCC et étale le spectre. Seul le PCC inverse f_j^{-1} permet de retrouver le spectre d'entrée. Les performances des PCC et du DS-CDMA ont été comparées dans [11] pour les communications multi-utilisateurs, en fonction du nombre d'utilisateurs. Les estimations du TEB (Taux d'Erreur Binaire) montrent des résultats similaires pour un grand nombre d'utilisateurs et une légère supériorité des PCC pour un faible nombre d'utilisateurs.

2.2 Application au tatouage

Les LPTV utilisés dans le cadre du tatouage doivent blanchir le spectre, être inversibles, sûrs cryptographiquement et éventuellement former un ensemble orthogonal pour le tatouage multiple. Les permutations aléatoires périodiques remplissent toutes ces conditions pour un faible coût calculatoire.

La littérature contient plusieurs références à l'utilisation des permutations aléatoires dans le cadre du tatouage, le plus souvent comme entrelaceur préalable du message pour améliorer la sécurité [5], mais aussi pour l'entrelacement d'une information à spectre coloré dans le cadre du tatouage audio asymétrique [1].

Changements d'Horloge Périodiques Monodimensionnels :

Le tatouage W_j est obtenu en appliquant un PCC T_{1D}-périodique f_j (la clé secrète) à une version redondante M'_j du message M_j : $W_j = f_j(M'_j)$, avec

$$m'_j(l + (p-1)L) = m_j(l), l \in \{1, ..., L\}, p \in \{1, ..., P\} \quad (3)$$

La redondance ainsi introduite permet d'obtenir de bonnes performances en réception malgré le rapport élevé entre la puissance du document et celle du tatouage (DWR, pour *Document to Watermark Ratio*) qu'impose la contrainte l'imperceptibilité.

Après transmission l'image reçue est l'image tatouée et attaquée $I'_W = I + B + \alpha \sum_{j=1}^{J} W_j$, où I est l'image support et B le bruit. Lors du décodage, le PCC inverse est appliqué à I'_W et étale le spectre de I et de B. La Fig.1 montre les propriétés d'étalement des PCC sur l'exemple d'une image numérique (Lena).

Les propriétés statistiques de l'image ou des coefficients de sa transformée permettent d'établir des stratégies de décodage

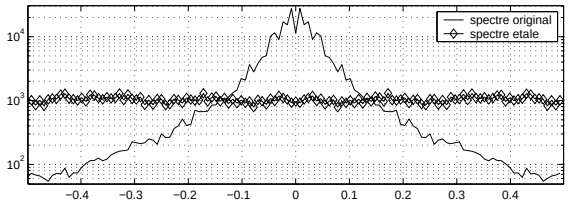

FIG. 1 – Propriétés d'étalement des PCC (Lena)

optimal [5]. En particulier, le décodage par corrélation ou par filtrage adapté est optimal dans le cas de distributions gaussienne de l'image et du bruit. Le message reçu est $\hat{M}_j$:

$$\begin{aligned} \hat{m_j}(l) &= \frac{1}{\alpha P} \sum_{p=1}^{P} (f_j^{-1}(i'_W))(l + (p-1)L) \\ &= m_j(l) + \frac{1}{\alpha P} \sum_{p=1}^{P} (f_j^{-1}(i+b))(l + (p-1)L) \end{aligned} \qquad (4)$$

Soient σ_I^2, σ_B^2, σ_{MAI}^2 les variances dues respectivement à l'image support, au bruit et aux interférences multi-utilisateurs (dans le cas du tatouage multiple). D'après le théorème Central-Limite, $\hat{M}_j$ est gaussien de moyenne $E[\hat{M}_j] = M_j + \mu(I)$ (où $\mu(I)$ est la moyenne de I) et de variance $(\sigma_I^2 + \sigma_B^2 + \sigma_{\text{MAI}}^2)/\alpha^2 P$. Alors $\hat{m_j}(l)$ est une statistique suffisante pour le décodage et la règle de décision est

$$D_j(l) = [\text{signe}(\hat{m_j}(l) - \mu(I_W))]_{l \in \{(1,...,L\}}. \qquad (5)$$

Le théorème Central-Limite montre que

$$\text{BER} \simeq Q(\alpha\sqrt{P}/\sqrt{\sigma_I^2 + \sigma_B^2 + \sigma_{\text{MAI}}^2}) \ , \qquad (6)$$

où $Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du$. Les résultats expérimentaux présentés dans la partie 3 vérifient cette estimation théorique des performances.

Ce récepteur est préférable dans les conditions du tatouage ($\sigma_{\text{MAI}}^2 << \sigma_{I_W}^2$) à d'autres récepteurs (décorrélateur par exemple) utilisés dans le cadre de la détection multi-utilisateurs [12] et repris dans des publications concernant les permutations aléatoires [9].

Il existe $T!$ permutations équiprobables de période T. Dès que $T > N/8$, 1D-PCC offre donc de meilleures garanties sur l'entropie de la clé que la modulation de type DS, où l'on peut générer 2^N clés équiprobables.

Changements d'Horloge Périodiques Bidimensionnels :

Le tatouage est le résultat de l'application successive d'une permutation f_j^1 sur les colonnes et d'une seconde permutation f_j^2 sur les lignes du message redondant, pris sous forme matricielle. L'insertion et le décodage suivent le même principe que pour 1D-PCC. A la réception, on applique successivement les PCC inverses $(f_j^2)^{-1}$ et $(f_j^1)^{-1}$ sur l'image tatouée. L'objectif est d'obtenir des performances similaires à celles de 1D-PCC pour une période plus faible : l'association de deux PCC au décodage devrait davantage réduire la corrélation spatiale présente dans l'image support.

3 Simulations

3.1 Implantation

Domaine d'insertion : W peut être inséré dans la luminance I ou dans une transformation inversible de I (DFT, DCT [10],

transformée en ondelettes [2]...). DS et PCC ont été comparés dans le domaine spatial (luminance) (L-DS, L-PCC) et dans celui de la Transformée en Cosinus Discrète (DCT) par blocs 8x8 (DCT-DS, DCT-PCC), qui est le plus utilisé du fait de son rôle dans le format de compression JPEG.

Masque perceptuel : l'insertion dans le domaine de la DCT par blocs 8x8 (DCT-DS, DCT-PCC) bénéficie de recherches sur l'analyse perceptuelle effectuées en compression d'image, car on l'utilise dans le format JPEG. Le masque perceptuel inspiré des travaux de Ahumada et Peterson [4] a été choisi dans le domaine de la DCT. Dans le domaine de la DCT, la variance de l'image support σ_I^2 dans (6) doit être recalculée en une nouvelle variance $\tilde{\sigma_I}^2$ pour tenir compte de ce masque qui limite notamment l'insertion à 22 coefficients choisis dans les moyennes fréquences (où la variance est moindre).

Préfiltrage au détecteur : dans le domaine spatial, l'image n'est pas stationnaire. Cependant, on peut estimer ses moments locaux à l'aide d'un filtre de Wiener [5] afin d'obtenir une estimation $\hat{I}$ de l'image originale au moment du décodage. L'image préfiltrée est $I''_W = I'_W - \hat{I}$ et σ_I^2 dans (6) devient $\sigma^2_{I'_W - \hat{I}}$, ce qui réduit considérablement l'influence du bruit dû à l'image.

Paramètres : les performances de DS et PCC sont comparées par simulations sur un ensemble de 5 images test. Dans le domaine de la DCT, cet ensemble est complété par des images hôtes I générées aléatoirement : les coefficients de chaque bloc suivent des distributions gaussiennes généralisées [5]. Pour une estimation précise du TEB, des messages sont générés aléatoirement jusqu'à ce qu'au moins 100 bits erronés aient été observés. Les valeurs par défaut ont été fixées à $N = 2^{18}$, $L = 100$ bits, $J = 1$, $T_{1D} = 2^{12}$, $T_{2D} = 2^6$ et DWR situé au seuil d'imperceptibilité (DWR=36 dB en moyenne).

3.2 Performances intrinsèques

Influence de la puissance d'insertion : lorsque le DWR augmente, l'imperceptibilité du tatouage est meilleure mais le TEB augmente également, pour les trois algorithmes comparés (cf Fig.2).

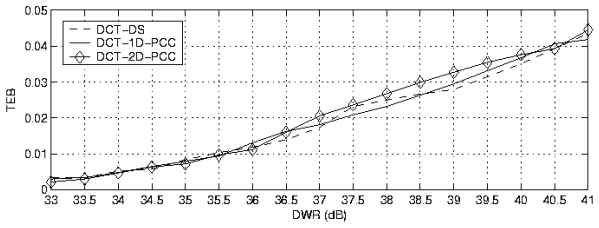

FIG. 2 – Performance au décodage par rapport à DWR (images simulées)

Choix de la période de la permutation : la période de la permutation influe sur les propriétés d'étalement, d'orthogonalité (dans le cas du tatouage multiple) et le coût calculatoire. Dans le domaine de la luminance, la corrélation entre les pixels joue un rôle important, ce qui n'est pas le cas dans le domaine transformé. On montre expérimentalement que les périodes $T_{1D} = 2^{12}$ et $T_{2D} = 2^6$ sont optimales pour une image comportant $N = 2^{18}$ pixels.

Influence du débit du message et du tatouage multiple : les performances de DS et PCC augmentent avec le nombre P d'échantillons insérés pour chaque bit d'information (Fig.3). Pour le tatouage multiple, les échantillons correspondant aux différents messages sont superposés, tout en respectant la contrainte d'imperceptibilité. Les PCC offrent des propriétés d'orthogonalité similaires à DS (cf Fig.4).

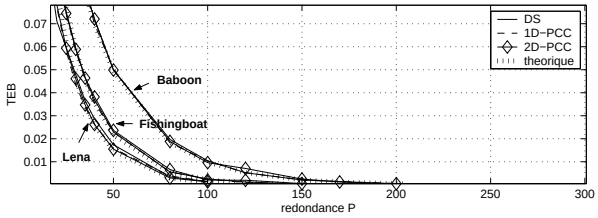

FIG. 3 – Performance au décodage par rapport à la redondance P

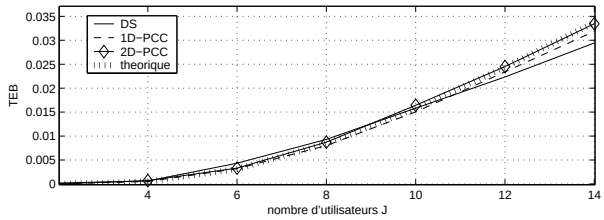

FIG. 4 – Performance au décodage par rapport au nombre d'utilisateurs J

3.3 Robustesse par rapport au bruit

Les performances de DS et PCC sont comparées en fonction du DWR (rapport entre la puissance de l'image hôte et celle du tatouage), puis du WNR (rapport entre la puissance du tatouage et celle du bruit, ou *Watermark to Noise Ratio*) dans le cas d'un bruit gaussien additif ou multiplicatif. Les PCC offrent une aussi bonne résistance au bruit que DS (cf Fig.5 et Fig.6).

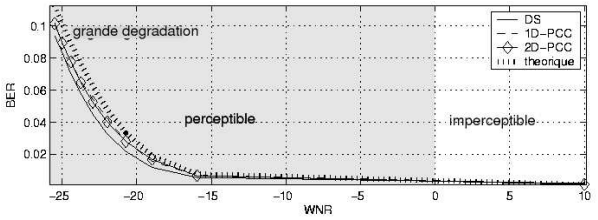

FIG. 5 – Robustesse au bruit additif

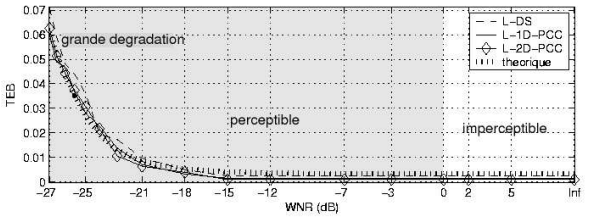

FIG. 6 – Robustesse au bruit multiplicatif

3.4 Robustesse à des attaques sophistiquées

Attaques désynchronisantes : les attaques dites géométriques (rognage, rotation, translation...) provoquent une désynchronisation entre l'image tatouée et la clé (code ou permutation). En effet, le calcul de la corrélation (DS) ou de la permutation inverse (PCC) conduisent à un décodage totalement erroné lorsqu'il est effectué sur des vecteurs ou matrices légèrement décalés. Plusieurs solutions (qui sortent du cadre de cette étude) utilisent l'insertion dans des domaines transformés appropriés ou l'insertion d'un signal de synchronisation [7]. Les deux méthodes peuvent être appliquées indifféremment à PCC ou à DS. Cependant, il n'existe pas encore de méthode de synchronisa-

tion robuste à des transformations géométriques locales et non affines et à l'élimination du signal de synchronisation.

Changement d'échelle, filtrage de Wiener, compression JPEG : les performances des trois algorithmes sont comparées par rapport à trois attaques sophistiquées classiques. Le changement d'échelle consiste à diminuer par 4 la taille de l'image transmise. A la réception, l'image est agrandie à sa taille originale par interpolation bilinéaire. L'attaque par filtrage de Wiener consiste à considérer que le tatouage est un bruit additif, et que l'image est le signal à débruiter. Les PCC offrent une aussi bonne résistance à ces attaques que DS (cf Fig.8, Fig.9). Les algorithmes sont plus robustes dans le domaine transformé.

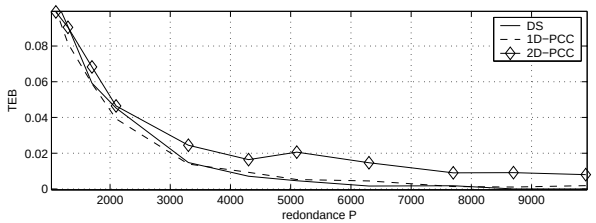

FIG. 7 – Robustesse au changement d'échelle en fonction de la redondance

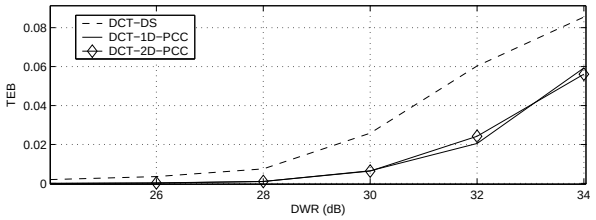

FIG. 8 – Robustesse au filtrage de Wiener

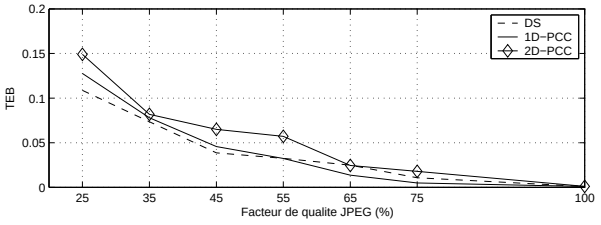

FIG. 9 – Robustesse à la compression JPEG

4 Conclusion

Les permutations aléatoires ont été introduites dans cette étude dans le cadre théorique général des PCC. Un tatouage par étalement de spectre PCC a été proposé et comparé à l'algorithme de référence DS, dans le domaine spatial et celui de la DCT par blocs. Les performances de PCC et DS sont globalement similaires et correspondent aux propriétés usuelles des techniques d'étalement de spectre : une grande robustesse au bruit additif et multiplicatif mais une vulnérabilité aux attaques désynchronisantes. Comme attendu, l'insertion dans le domaine de la DCT permet une meilleure robustesse aux attaques sophistiquées. 2D-PCC semble préférable à 1D-PCC du fait de son coût calculatoire plus faible et de ses meilleures performances pour une valeur adéquate de la période de la permutation.

A l'aide d'arguments théoriques et expérimentaux, cette étude montre que l'étalement par PCC offre des résultats globalement équivalents à ceux des techniques d'étalement classiques utilisant une modulation par un pseudo-bruit, ainsi qu'un bon niveau de sécurité. Elle justifie également l'emploi des permutations aléatoires en tant que technique d'étalement alternative dans les algorithmes existants. Les PCC basés sur les permutations aléatoires sont très simples de concept, d'implantation et de calcul et peuvent être introduits dans divers algorithmes de tatouage, concernant divers domaines transformés. On pourrait également conseiller l'utilisation d'étalement par PCC pour le tatouage de sons ou vidéos, où la redondance serait plus importante et la périodicité serait mieux exploitée. Les propriétés de filtres LPTV plus généraux, qui permettent d'effectuer simultanément un étalement et un modelage du spectre, sont à l'étude.

Références

[1] T. Furon, P. Duhamel. An asymmetric watermarking method. *IEEE. Trans. on Signal Proc.*, 51(4) :981–995, 2003.

[2] D. Kundur, D. Hatzinakos. Digital Watermarking Using Multiresolution Wavelet Decomposition. *IEEE ICASSP'98*, 5 :2659–2662, 1998.

[3] D. McLernon. One-dimensional Linear Periodically Time-Varying structures : derivations, interrelationships and properties. *IEE Proc.-Vis. Image Signal Proc.*, 146(5) :245–252, 1999.

[4] A.J. Ahumada, H.A. Peterson. Luminance-model-based DCT quantization for color image compression. *Proc. SPIE on Human Vision, Visual Proc., and Digital Display III*, 1666 :365–374, 1992.

[5] J.R. Hernández, F. Pérez-González. Statistical analysis of watermarking schemes for copyright protection of images. *IEEE Proc., Special Issue on Identification and Protection of Multimedia Information*, 87(7) :1142–1166, 1999.

[6] J.G. Proakis. *Digital Communications*. McGraw, NY, 4th edition, 2001.

[7] S. Pereira, T. Pun. Fast robust template matching for affine resistant image watermarking. *IEEE Transactions on signal proc.*, 51(4) :1045–1053, 2003.

[8] B. Lacaze, D. Roviras. Effect of random permutations applied to random sequences and related applications. *Signal Processing*, 82 :821–831, 2002.

[9] M. Coulon, D. Roviras. MMSE Joint Detection for an Asynchronous Spread-Spectrum System Based on Random Permutations. *IEEE ICASSP'04, Proc.*, 2 :17–21, 2004.

[10] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon. Secure spread spectrum watermarking for multimedia. *Image Processing, IEEE Trans. on*, 6(12) :1673–1687, 1997.

[11] D. Roviras, B. Lacaze, N. Thomas. Effects of Discrete LPTV on Stationary Signals. *IEEE ICASSP'02, Proc.*, 2 :1127–1220, 2002.

[12] S. Verdu. *Multiuser Detection*. Cambridge University Press, 1998.