Tatouage Numérique par Schéma de Costa à Structure Fractale Flottante

Ali KOMATY[1], Claude DELPHA[2], Aurélia FRAYSSE[2]

[1]Institut de Recherche de l'école Navale (IRENav), CC600,
29240 Brest cedex 9, France

[2]Laboratoire des Signaux et Systèmes (Université Paris-Sud, CNRS, Supélec),
3 rue Joliot Curie, 91192 Gif Sur Yvette, France

ali.komaty@ecole-navale.fr, claude.delpha@lss.supelec.fr,
aurelia.fraysse@lss.supelec.fr

Résumé – La dissimulation d'information par quantification scalaire fourni un bon outil pour le tatouage numérique. En effet, elle offre de bonnes propriétés en termes de robustesse et de capacité. Malheureusement, elle produit une très forte distorsion statistique donnant ainsi à l'attaquant des preuves de la présence de l'information dissimulée. Le but de cet article est d'améliorer les performances de ce schéma en terme de transparence statistique de l'information cachée. Pour cela, nous basons notre approche sur un quantificateur flottant, ayant une structure fractale. Ce travail s'appuie sur un schéma de tatouage à information adjacente à l'encodeur (schéma de Costa) en se basant sur une quantification flottante faite suivant une structure fractale. Après avoir présenté la méthode de tatouage utilisée, nous montrons que cette technique améliore les performances du schéma de Costa en termes d'invisibilité statistique, tout en gardant des propriétés satisfaisantes en termes de robustesse.

Abstract – Data Hiding schemes using scalar quantization has widely proved its efficiency in digital watermarking approaches. Indeed, it is well known that such kind of schemes provide good robustness and capacity performances. Nevertheless, it appears that these methods provide high statistical distortions on the watermarked signal probability density functions allowing the attacker to get the proof of the presence of the hidden information or not. The goal of this paper is to improve the statistical transparency performances of the embedded information for such schemes. For this purpose, our approach is based on the use of a floating quantizer with a fractal structure. For this work we start from the basic side-information based scheme (Costa's scheme) for which we use a floating quantizer with a fractal structure. We first present the used watermarking method and describe the technical improvements. Then we show that the proposed approach improves the statistical transparency of the watermark while keeping satisfying robustness.

1 Introduction

Les récents développements des médias numériques ont apporté un besoin croissant en termes de protection des données multimédia. Une solution proposée est l'utilisation de techniques de dissimulation d'informations. Le principe de ces techniques est d'insérer une marque (information secrète) dans un document hôte. Parmi ces techniques, le tatouage numérique se distingue par 2 propriétés importantes : la transparence perceptuelle, *i.e.* la marque ne doit pas être décelable par un tiers, et la robustesse aux attaques extérieures *i.e.* la résistance de la marque au transformations apportées, généralement appelées attaques. A ces notions de transparence visuelle on peut également ajouter la contrainte de capacité et celle d'invisibilité statistique pour l'utilisateur. L'idée serait alors d'avoir une classe de méthodes où l'attaquant aurait peu de preuves directes de la présence de la protection dans le document fourni. Tout laisse en effet penser qu'un attaquant serait moins tenter de faire subir des transformations illicites au document marqué s'il ne soupçonne pas l'existence de la marque. Parmi les méthodes de tatouage existantes, plusieurs utilisent la quantification du signal hôte pour insérer cette marque. Cette approche a déjà prouvé sa robustesse contre les attaques [1]-[2]. Le principe de ce marquage est introduit par Costa dans [3] et à été depuis mis en œuvre en pratique dans plusieurs schémas et notamment le SCS (Scalar Costa Scheme, [4]). Malheureusement, avec cette approche, il est introduit des distorsions importantes sur la densité de probabilité du signal après marquage, [5]-[6], qui rendent la marque statistiquement visible. Ces distorsions sont principalement dues à la régularité du quantificateur scalaire uniforme utilisé. Les méthodes proposées pour augmenter l'invisibilité statistique du schéma de Costa s'appuient soit sur la transformation du signal hôte comme dans [5], soit en modifiant le type de quantification utilisée (quantification codée treillis [7]-[6]). Ces dernières solutions relâchent les contraintes sur les paramètres de fonctionnement de la première technique et augmentent significativement l'invisibilité statistique mais ont jusque là montré des faiblesses en terme de robustesse sauf si elles s'appliquent dans un domaine spécifique [8], [9].
Nous proposons ici de mettre en oeuvre un schéma de tatouage à information adjacente utilisant un quantificateur flottant à structure fractale. Le but de cette méthode est d'améliorer les perfor-

mances du schéma classique en termes d'invisibilité statistique tout en conservant un niveau de robustesse significatif face aux attaques. Le quantificateur que nous utilisons est basé sur une approche fractale qui s'inspire des travaux de P. Bas [10]. Nous montrons comment améliorer ce quantificateur pour le rendre efficace dans le cadre d'une solution de tatouage robuste aux attaques additives. Avec un tel quantificateur, le principal avantage pour nous réside dans le fait que sa structure est flottante, au sens où le pas de quantification est irrégulier et est déterminé grâce à des échantillons du signal hôte. On se base pour cela sur la forte corrélation de pixels voisins dans une image. Nous montrons l'utilisation d'un tel quantificateur dans un schéma de Costa noté Schéma de Costa à Structure Fractale flottante et décrivons les performances obtenues pour des images réelles tant en terme de robustesse que de transparence statistique.

2 Tatouage basé sur la Quantification

Considérons un message m à cacher dans un signal hôte x. Nous devons produire un signal marqué s, de sorte que la différence $w = s - x$ représente la marque. Pour cela, les techniques basées sur la théorie de l'information utilisent le signal x pour encoder m. La marque w correspond alors à l'erreur de quantification pondérée de x. Les données s ainsi obtenues sont ensuite envoyées à travers un canal de communication où elles peuvent subir différentes attaques généralement modélisées par un bruit blanc Gaussien additif (AWGN) v. Le signal $r = s + v$ est finalement reçu par le destinataire qui extrait la marque et estime le message $\tilde{m}$ à partir des données bruitées reçues r.

2.1 Rappels : Schéma Scalaire de Costa (SCS)

Nous rappelons dans cette section les grandes lignes décrivant le fonctionnement du schéma scalaire de Costa (SCS) [4]. Dans le schéma de Costa, un dictionnaire contenant la règle de quantification est partagée entre l'encodeur et le décodeur. Ce dictionnaire, U^{L_x}, dont la longueur est donnée par L_x, est composé de sous-dictionnaires de dimension 1, notés U^1. On note dans la suite Δ_{scs} le pas de quantification, α_{scs} le paramètre d'optimisation de la capacité (et indirectement de la robustesse) et d un élément de m appartenant à un alphabet de longueur D. U^1 est alors choisi pour représenter une quantification scalaire uniforme de x de pas $\alpha_{scs}\Delta_{scs}/D$ de sorte que :

$$U^1 = \{u = l\alpha_{scs}\Delta_{scs} + \frac{d}{D}\alpha_{scs}\Delta_{scs} \mid d \in D, l \in \mathbb{Z}\}. \quad (1)$$

Le $d^{\text{ième}}$ sous dictionnaire est noté :

$$U_d^1 = \{u = l\alpha_{scs}\Delta_{scs} + \frac{d}{D}\alpha_{scs}\Delta_{scs} \mid l \in \mathbb{Z}\} \quad (2)$$

L'erreur de quantification q_n vérifie alors

$$q_n = Q_{\Delta_{scs}}\{x_n - \Delta_{scs}(\frac{d_n}{D})\} - \{x_n - \Delta_{scs}(\frac{d_n}{D})\} \quad (3)$$

où $Q_{\Delta_{scs}}\{.\}$ est une quantification scalaire uniforme de pas Δ_{scs}. La marque est alors donnée par $w = q\alpha_{scs}$ et on obtient :

$$s = x + w = x + q\alpha_{scs} \quad (4)$$

Au décodeur, on utilise un quantificateur scalaire uniforme qui quantifie le signal reçu $r = s+v$ au mot de code le plus proche, en utilisant le sous dictionnaire U^1 . On extrait alors y du signal reçu en prenant :

$$y_n = Q_{\Delta_{scs}}\{r_n\} - \{r_n\} \quad (5)$$

Si $|y_n|$ est proche de 0 on choisi $d_n = 0$ et si $|y_n|$ est proche de $\Delta_{scs}/2$, on estime d_n à 1.
Ce schéma est robuste aux attaques additives extérieures de type bruit blanc gaussien mais la distribution de probabilités de s est éloignée de celle de x (pas de transparence statistique de l'information cachée, Cf. Figure 1-a).
Pour résoudre cet dilemme, on introduit une autre méthode de tatouage, qui s'appuie sur l'approche proposée par P. Bas [10] dans un schéma de tatouage substitutif.

2.2 Schéma de Quantification à Structure Fractale Amélioré (IFFQ)

Ce quantificateur a été introduit dans sa forme initiale par P. Bas dans [10] pour améliorer la robustesse contre les attaques non linéaires avec une solution de tatouage par substitution. Nous le noterons FFQ. Dans nos travaux nous proposons dans un premier temps une amélioration de ce quantificateur pour une robustesse face aux attaques additives d'abords dans un contexte de tatouage substitutif (IFFQ) puis nous verrons comment l'utiliser dans un schéma de tatouage additif.
Les performances de ce type de quantificateur sont principalement dues à sa nature non uniforme. En effet, le pas de quantification, noté Δ_f, dépend des valeurs prises par le signal hôte x, et plus particulièrement des valeurs prises au voisinage d'un échantillon donné. Ainsi, si on veut coder le i-ème échantillon x_i, on regarde les valeurs prises par x_{i-1} et x_{i+1}, et après les avoir rangés par ordre croissant, on définit Δ_f par :

$$\Delta_f = \frac{r}{2^{(N_1+1)}} \text{ si } N > 0 \qquad \text{et} \qquad \Delta_f = \Delta \text{ si } N = 0 \quad (6)$$

où r est la distance entre la plus grande valeur prise par x, x_{max} et la plus petite x_{min}, Δ étant un pas de quantification fixé. En ce qui concerne les entiers N_1 et N ils sont définis grâce à la partie entière $\varepsilon_+()$, en prenant :

$$N(r_{mid}) = \varepsilon_+(\log_2(\frac{r_{mid}}{\alpha\Delta})) \qquad N_1(r) = \varepsilon_+(\log_2(\frac{r}{\alpha\Delta})) \quad (7)$$

avec $r_{mid} = x_{mid} - x_{min}$ (où x_{mid} est la valeur médiane de x), $N(r_{mid})$ correspond à l'indice du quantificateur choisi.
L'objectif avec une telle definition pour $N(r_{mid})$ est de réduire l'influence néfaste des distortions additives lors du décodage. En effet, il s'agira alors de prendre en considération la valeur de l'échantillon médian x_{mid} et ainsi réduire l'effet d'une distortion additive (par exemple de type bruit additif Gaussien AWGN). Ainsi contrairement a l'approche donnée dans [10] tous les échantillons du triplet sont pris en compte dans les calculs liés au processus de codage et de décodage et pas seulement les extremes comme proposé par P. Bas [10].

$N_1(r)$ est utilisé pour calculer Δ_f. On choisit alors les valeurs possibles de Δ_f grâce à la relation $\alpha_1\Delta \leq \Delta_f \leq \alpha_2\Delta$, où α_1 et α_2 sont inférieurs à $\frac{1}{2}$. Dans la suite, on prendra $\alpha_1 = \frac{1}{4}$ et $\alpha_2 = \frac{1}{2}$ pour éviter tout recouvrement entre les cellules de quantification.
Pour la procédure d'encodage utilisée il faut d'abord choisir un triplet $\{x_i, x_j, x_k\}$ puis réarranger le triplet sous la forme $\{x_{min}, x_{mid}, x_{max}\}$ et calculer $r_{mid} = x_{mid} - x_{min}$, $r = x_{max} - x_{min}$, Δ_f, N_1 et N à l'aide des équations (6) et (7). Ensuite, si $Q_i \neq Q_0$, on effectue la quantification de r_{mid} (x_{mid}) avec Q_i et le bit de valeur b. Lorsque $Q_i = Q_0$, on est dans un cas particulier ; aussi si $b = 0$ on prend r_{mid} et r égaux à 0 et si $b = 1$ on pose r_{mid} et r à Δ. On poursuit alors la procédure de quantification en choisissant un autre triplet et en insérant un nouveau bit.
En ce qui concerne le processus de décodage on choisi d'abord le triplet à considérer $\{x_i, x_j, x_k\}$ et on calcule r_{mid}, r, Δ_f, N_1 et N. Si $N = 0$, il y a deux possibilités : si $r_{mid} \approx 0$ on estime 0, sinon on estime 1. Lorsque $N \neq 0$, on trouve le voisin le plus proche de x_{mid} et on estime le bit correspondant.
Cette approche qui peut être utilisée comme un schéma de tatouage substitutif à détection aveugle est notée IFFQ. Avec sa structure fractale flottante, elle pourra alors être la base de la quantification fractale à mettre en oeuvre dans un schéma de Costa et ainsi permettre de réduire la régularité des quantificateur pour assurer la transparence statistique recherchée.

2.3 Schéma de Costa à structure fractale (FCS) proposé

Le principe du schéma proposé repose sur la combinaison des deux techniques précédemment décrites : SCS et IFFQ. Le schéma de tatouage obtenu consiste à s'appuyer sur un schéma de tatouage additif à information adjacente du même type que le schéma de Costa tout en utilisant la quantification fractale flottante définie dans 2.2. Le dictionnaire choisi est U^{L_x} qui s'écrit comme un produit de L_x sous dictionnaires U^i, où $i \in \{1, \ldots, L_x\}$, tel que chaque U^i représente un quantificateur flottant de pas $\alpha_{scs}\Delta_{f_i}/D$, qui est défini par :

$$U^i = \{u = l\alpha_{scs}\Delta_{f_i} + \frac{d}{D}\alpha_{scs}\Delta_{f_i} \mid d \in D, l \in Z\} \quad (8)$$

Pour notre étude, α_{scs} est fixé à 1, autrement dit on n'optimise pas la capacité (et indirectement la robustesse) par rapport au canal. Après quantification, on ajoute à x_{mid} la valeur de $d\frac{\Delta_{f_i}}{2}$. Puis on procède de la même manière que pour le SCS classique, en utilisant les équations (1), (2) et (3).
Au décodeur on reçoit un signal $y = s + v$ duquel on veut extraire le message caché. Pour cela on quantifie y sur trois niveaux en utilisant les règles suivantes :

1. On choisit le triplet $\{y_i, y_j, y_k\}$ puis on calcule $r_{mid} = y_j - y_i$, r, Δ_f, N_1 et N.
2. Si $N = 0$, on utilise le quantificateur Q_0 pour décoder. Par contre, si $N \neq 0$, on utilise les trois quantificateurs $[Q_{N-1},\ Q_N,\ Q_{N+1}]$ pour quantifier r_{mid} à la cellule la plus proche.
3. On calcule $|r_{mid} - Q_{\Delta_f}(r_{mid})|$, et on estime d : $d = 1$ s'il est proche de $\frac{\Delta_f}{2}$ et $d = 0$ s'il est proche de 0.

Avec le schéma proposé, nous avons pour principal objectif de réduire la régularité de la quantification qui était présente dans l'approche scalaire. Ici avec l'utilisation d'un pas de quantification Δ_f qui change en fonction des échantillons considérés nous atteignons cet objectif.
Nous allons donc vérifier dans la section suivante que les fonctions de densité de probabilité (PDF) des signaux marqués ne font pas apparaître de distortions significatives de la présence de la marque. Nous vérifierons également expérimentalement que les performances de robustesse sont satisfaisantes.

3 Résultats et Discussions

Pour évaluer les performances de l'algorithme proposé, nous avons étudié l'évolution du taux d'erreur binaire (BER) pour des attaques par ajout de bruit additif Gaussien (Robustesse), ainsi que l'indétectabilité de l'information insérée (transparence statistique) en s'assurant de sa transparence perceptuelle. Dans le cas de la transparence statistique nous comparons les PDF des signaux originaux et marqués et évaluons leur divergence en utilisant la Distance de Kullback-Leibler (KLD).
Toutes ces performances ont été évaluées en utilisant une base de 140 images de taille 512×512. Les résultats sont présentés sous la forme d'une moyenne de ceux obtenus pour ces images.

3.1 Transparence statistique

Nous avons évalué la transparence statistique tout en s'assurant d'une bonne transparence perceptuelle de l'information insérée dans le cas des schémas proposés FCS, et IFFQ. Nous

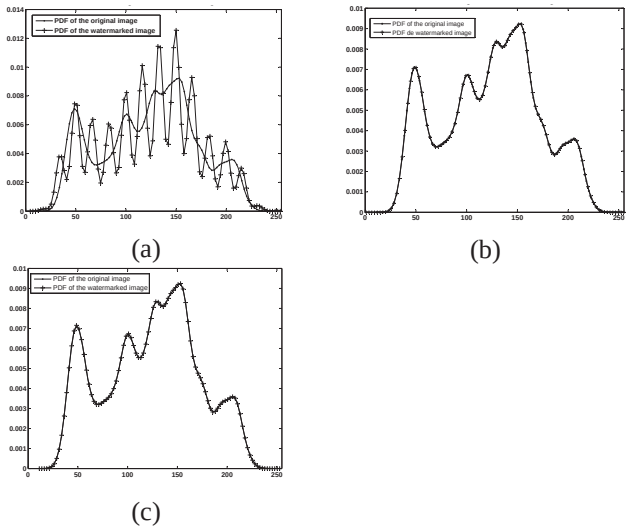

FIG. 1 – PDF des signaux originaux et marqués pour (a) SCS, (b) FCS et (c) IFFQ

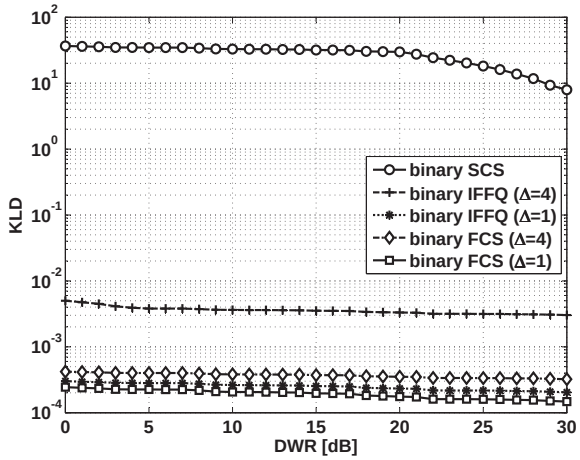

FIG. 2 – KLD en fonction du DWR pour les schémas proposés. Comparaison avec le SCS.

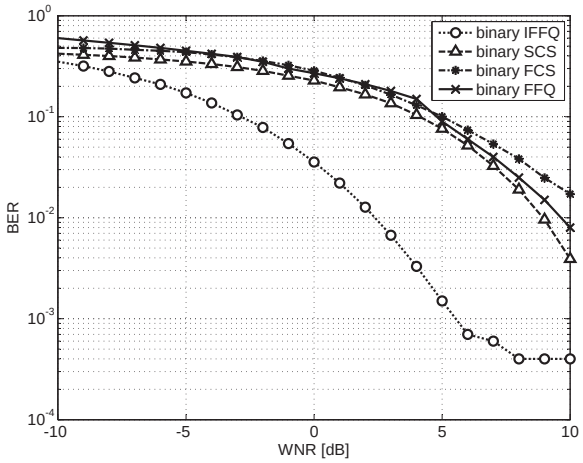

FIG. 3 – BER pour des attaques par ajout de bruit AWGN pour les schémas proposés FCS et IFFQ. Comparaison avec le FFQ proposé dans [10] et le SCS

avons observés que les PDF des signaux marqués et originaux pour ces deux schémas sont très proches et font apparaître vraiment peu de distortion dues au marquage (Cf. figure 1) pour les schémas proposés.
Aussi pour valider ces bons résultats, nous avons calculé la KLD pour les schémas FCS, IFFQ, et SCS et nous nous avons tracé son évolution en fonction du rapport signal à marque (DWR). Nous présentons sur la figure 2 les résultats obtenus.
Nous confirmons que les performances du FCS et du IFFQ en terme d'indétectabilité sont bien meilleures que celles du SCS et ce pour plusieurs valeurs du pas de quantification général Δ. Il faut tout de même souligné que la valeur de Δ aura un impact perceptuel important s'il est trop grand. Aussi nous préconisons d'utiliser la plus petite valeur possible de Δ, à savoir $\Delta = 1$.

3.2 Robustesse

Pour évaluer la robustesse de notre algorithme, nous avons tracé l'évolution du BER en fonction des valeurs du rapport marque-à-bruit (WNR). Nous présentons sur la figure 3 les résultats obtenus pour les 2 schémas proposés (FCS et IFFQ) et les comparons avec ceux obtenus pour les schémas existants dans la littérature : le SCS [4] et le FFQ [10].
Les résultats obtenus montrent que le FCS, le SCS et le FFQ ont des performances de robustesse très proches. On peut donner toutefois un très léger avantage aux SCS et FFQ de la littérature notamment dans le cas de niveaux de bruits très faibles (WNR élevés). Toutefois les performances obtenues pour le IFFQ sont largement meilleures : les valeurs du BER sont plus petites sur toute la gamme de WNR.
Les résultats obtenus nous prouvent que la structure de quantification fractale n'altère la robustesse du schéma de Costa que dans une moindre mesure.

4 Conclusion

Nous[1] avons proposé ici un schéma de tatouage basé sur un quantificateur flottant à structure fractale. Après avoir décrit ce quantificateur et son utilisation dans un schéma substitutif (IFFQ), nous montrons comment intégrer celui-ci dans un schéma de tatouage à informations adjacente basé sur la quantification (schéma de Costa), FCS.
Nous avons pu montrer que les performances d'invisibilité statistiques du FCS sont meilleures que pour le IFFQ et pour le SCS : la distribution du signal marqué est quasiment confondue avec celle du signal initial. De plus, nous obtenons aussi des résultats fiables et satisfaisants en termes de robustesse, puisqu'ils sont du même ordre de grandeur que pour le schéma de scalaire de Costa (SCS).

Références

[1] B. Chen and G. W. Wornell. Provably robust digital watermarking. In *SPIE : Multimedia Systems and Applications II*, volume 3845, pages 43–54, Boston, MA, USA, September 1999.

[2] M. L. Miller I. J. Cox and A. L. McKellips. Watermarking as communications with side information. In *IEEE Proc., Issue on Identification and Protection of Multimedia Information*, volume 87, pages 1127–1141, July 1999.

[3] M. H. M. Costa. Writing on dirty paper. *IEEE Trans. on Information Theory*, 29 :439–441, May 1983.

[4] J. J. Eggers, R. Bauml, R. Tzchoppe, and B. Girod. Scalar costa scheme for information embedding. *IEEE Trans. on Signal Processing*, 51 :1003–1019, 2003.

[5] T. Furon P. Guillon and P. Duhamel. Applied public-key steganography. In *SPIE*, San Jose, CA, USA, 2002.

[6] S. Braci, C. Delpha, R. Boyer, and G. Le Guelvouit. Informed stego-systems in active warden context : Statistical undetectability and capacity. In *IEEE MMSP*, Cairns, Australia, October 2008.

[7] E. Esen and A.A. Alatan. Data hiding using trellis coded quantization. In *ICIP*, Singapore, October 2004.

[8] S. Braci, R. Boyer, and C. Delpha. On the tradeoff between security and robustness of the trellis coded quantization scheme. In *IEEE ICASSP*, April 2008.

[9] I. Benkara Mostefa, S. Braci, C. Delpha, R. Boyer, and M. Khamadja. Quantized based image watermarking in an independent domain. *Elsevier Journal on Signal Processing : image communication*, 26(3) :194–204, March 2011.

[10] P. Bas. A quantization watermarking technique robust to linear and non-linear valumetric distortions using a fractal set of floatting quantizers. In *IH*, Barcelona, Spain, 2005.

[1] Les auteurs remercient le projet ANR MEDIEVALS pour son financement.