Schéma de Tatouage basé sur la quantification dans le contexte du "Compressive Sensing"

Claude DELPHA, Rémy BOYER, Said HIJAZI

Laboratoire des Signaux et Systèmes (CNRS - Supelec - Univ. Paris-Sud)
3 Rue Joliot Curie, 91192 Gif sur Yvette, France
{Claude.Delpha, Remy.Boyer, Said.Hijazi}@lss.supelec.fr

Résumé – Nous présentons ici un schéma de dissimulation d'information basé sur la quantification et le "Compressive Sensing" avec la particularité de satisfaire à des contraintes d'invisibilité statistiques contrairement au bien connu Schéma Scalaire de Costa (SCS). Grâce à cette contrainte de transparence statistique, nous pouvons ainsi augmenter la probabilité de fausse alarme de l'attaquant : en présence d'un document contenant une information cachée, celui-ci doit penser, à tort, que le document ne l'est pas. On montre pour cela comment utiliser le "Compressive Sensing" dans le cadre du tatouage informé et ainsi améliorer la transparence statistique pour un schéma de tatouage informé sans utilisation de clé de cryptage. Dans notre approche, nous proposons en plus un schéma ou la complexité se retrouve essentiellement dans l'étape d'insertion de l'information contrairement aux approches proposées dans la littérature pour lesquelles des opérations de reconstruction de signaux parcimonieux sont nécessaires au décodage. Nous évaluons les performances du schéma de tatouage proposé et montrons, en s'appuyant sur le Lemme de Stein, qu'il permet d'assurer une probabilité de fausse alarme élevée pour l'attaquant. Les autres performances (robustesse et capacité) habituellement évaluées sont également étudiées et comparées à celles obtenues pour le SCS.

Abstract – In this paper, we present an informed data hiding scheme based on quantization and Compressive Sensing. The main benefit of such proposal compared to the famous Scalar Costa Scheme (SCS) is to satisfy statistical transparency constraint. Thanks to this statistical transparency constraint, we wonder to increase the false alarm probability for the attacker : in the presence of a document containing hidden information, it needs to think, wrongly, that the document is not watermarked. For this purpose, we show how to use Compressive Sensing (CS) in informed watermarking and thus improve statistical transparency for informed watermarking scheme without the use of encryption key. In our approach, the major complexity of the scheme is found in the embedding process unlike in the literature proposed schemes complex sparse signals reconstruction operations are required while decoding. We evaluate the performance of the proposed watermarking scheme and show that, based on Stein's lemma, it ensures a high false alarm probability for the attacker. Other performance usually evaluated like robustness and capacity are studied and compared to those obtained with the SCS.

1 Introduction

Les applications du tatouage numérique pour la sécurité multimédia deviennent de plus en plus courantes de nos jours. Aussi, il est important, pour ne pas éveiller les soupçons d'un utilisateur mal intentionné de s'assurer qu'on ne puisse faire de distinctions entre le signal hôte et le signal marqué. Dans ce cas, deux aspects rentrent en jeu : la transparence perceptuelle et la transparence statistique de l'information dissimulée. D'un point de vue perceptuel l'information insérée doit être parfaitement transparente. D'un point de vue statistique, il ne faut pas que les fonctions de densité de probabilité (PDF) des signaux marqués et non marqués se distinguent facilement. La transparence statistique dans le schéma de référence de tatouage informé (Schéma Scalaire de Costa, SCS [1]) est un problème récurrent qui a été abordé de plusieurs façons. On peut les regrouper en 3 groupes de méthodes distinctes.

– Le premier groupe consiste à utiliser une technique de quantification spécifique pour rompre avec la régularité du quantificateur scalaire. Des travaux proposant l'utilisation de la Quantification Codée en Treillis (TCQ) ou encore de la Quantification Fractale Flottante [2] ont été proposés mais ont mis en avant des faiblesses quant aux autres performances telles que la robustesse par exemple.
– Le second groupe de méthode concerne l'utilisation d'un domaine transformé pour effectuer l'insertion. L'utilisation de la transformée par étalement (ST) [3] ou encore l'insertion dans un domaine indépendant (ICA) [4] ont montré de bonnes performances pour atteindre une transparence statistique satisfaisante. Toutefois, elles présentent d'autres limitations comme par exemple une faible capacité en cas d'utilisation du ST.
– Le dernier groupe de méthode s'appuie essentiellement sur l'idée d'insertion de l'information dans un signal dont les statistiques ont été mises en forme. C'est, par exemple, la proposition que fait Guillon et al dans [5]. Il évoque pour son schéma de nombreuses complications techniques de mise en œuvre, notamment lors de l'utilisation d'images naturelles. Par ailleurs, les performances en termes de robustesse obtenues pour ce schéma sont assez faibles par rapport aux schémas de référence habituels comme le SCS.

L'approche que l'on propose de développer s'appuie en grande partie sur l'idée développée pour ce dernier groupe de méthode : il s'agit de s'appuyer sur la mise en forme statistique du signal hôte avant d'effectuer la quantification pour la création de la marque à insérer. L'idée est alors d'utiliser les propriétés du "compressive sensing" [6], de rendre le signal hôte parcimonieux avant l'insertion de la marque qui doit aussi avoir les bonnes propriétés puis reconstruire le signal marqué dans le domaine original. L'extraction doit elle aussi dans ce cas s'effectuer sur les signaux parcimonieux, après l'opération de mise en forme statistique. Par rapport à d'autres travaux utilisant le "Compressive Sensing" pour des besoins en tatouage d'image [7], l'originalité de notre approche réside dans le fait que nous proposons de travailler avec une approche de tatouage informé et que la complexité de l'algorithme proposé se retrouve essentiellement dans la phase d'insertion.

Dans ce travail, nous montrons comment utiliser le CS dans le cadre de ce schéma informé pour une insertion et extraction efficace de la marque. Nous évaluons les performances du schéma de tatouage proposé et nous montrons, en s'appuyant sur le Lemme de Stein [8], qu'il permet d'assurer une probabilité de fausse alarme élevée pour l'attaquant. Nous montrons également que les autres performances de robustesse et capacité habituellement évaluées sont au moins équivalentes à celles existantes pour le schéma de référence tel que le SCS.

2 Le schéma proposé : Compressive Sensing Scalar Costa's Scheme (CS-SCS)

2.1 Description du schéma proposé

Dans notre proposition, le signal hôte X est compressé [1] pour obtenir un signal parcimonieux $\tilde{X}$. La marque à insérer $\tilde{W}$ sera obtenue en calculant l'erreur de quantification pondérée du signal parcimonieux $\tilde{X}$ tel que $(\tilde{W} = \alpha\tilde{q})$ pour les bits d_n à considérer du message m. Ansi pour une quantification scalaire $Q_\Delta\{.\}$ de pas Δ et un alphabet D binaire ($D = 2$) on calcule $\tilde{q} = Q_\Delta\{\tilde{X} - \Delta(\frac{d_n}{D})\} - \{\tilde{X} - \Delta(\frac{d_n}{D})\}$ et le facteur de pondération α qui correspond au paramètre d'optimisation de la robustesse défini par Costa [1]. Il faut noter que la quantification de $\tilde{X}$ sera effectuée uniquement pour les coefficients non nuls de $\tilde{X}$. La marque $\tilde{W}$ obtenue est ensuite ajoutée à $\tilde{X}$ pour obtenir un signal marqué parcimonieux $\tilde{S}$ (voir Figure 1).

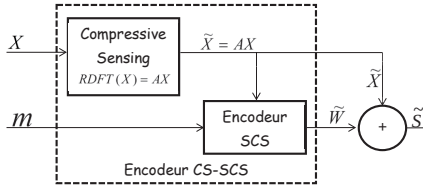

FIGURE 1 – Insertion de la marque pour le CS-SCS

1. Dans ce document, le symbole ˜ sera utilisé pour désigner les signaux parcimonieux

L'opération de "Compressive Sensing" inverse est ensuite effectuée pour reconstruire le signal marqué dans son domaine original non compressé S. Ce signal sera alors transmis dans un canal de communication dans lequel un observateur mal intentionné peut effectuer des opérations se traduisant par l'introduction d'une distortion à modéliser comme un bruit V sur le signal qui sera transmis au niveau du récepteur (voir Figure 2). Le signal reçu est alors $R = S + V$. Pour extraire l'information marquée, R est d'abord compressé pour en obtenir une représentation parcimonieuse $\tilde{R}$. Ensuite le décodage de l'information pour l'estimation du message $\hat{m}$ peut alors s'effectuer en déterminant l'erreur de quantification du signal $\tilde{R}$. On obtient alors $y_n = Q_\Delta\{\tilde{R}\} - \{\tilde{R}\}$ et on en déduit les éléments $\hat{d}_n$ de $\hat{m}$ tels que $\hat{d}_n = 0$ si $|y_n| \leq \frac{\Delta}{2}$ et $\hat{d}_n = 1$ si y_n est proche de $\pm\frac{\Delta}{2}$ (voir Figure 3).

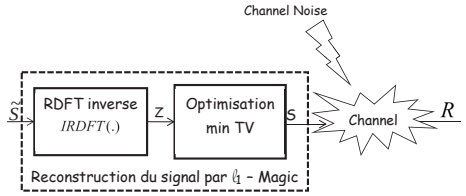

FIGURE 2 – Reconstruction du signal tatoué pour le CS-SCS

Dans la section qui va suivre nous présentons les détails des opérations de "Compressive Sensing" et de reconstructions des signaux ainsi que leurs spécificité pour le schéma de tatouage informé proposé.

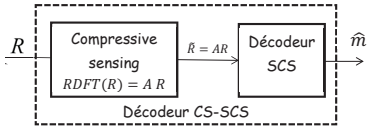

FIGURE 3 – Extraction de la marque pour le CS-SCS

2.2 Signal parcimonieux : génération et reconstruction. Cas du tatouage

Le "Compressive Sensing" (CS) peut être vu comme un paradigme d'échantillonnage qui permet d'aller en deçà des limites de Shannon en exploitant la structure parcimonieuse d'un signal, pour ainsi représenter le signal avec un taux d'échantillonnage bien inférieur à celui de Nyquist. Dans ce paradigme, l'étape de sous-échantillonnage est très rapide car elle utilise des projections linéaires non-adaptatives qui préservent la structure du signal. Le signal peut être reconstruit à partir de ces projections en considérant l'opération de décodage comme une opération inverse qui est traité comme problème d'optimization convexe de régularisation parcimonieuse. Ainsi, il est possible de reconstruire certains signaux et/ou images à partir de beaucoup moins d'observations que d'échantillons de données originaux N. Dans le cas du schéma proposé, en considérant X comme une image, on peut obtenir sa représentation parci-

monieuse $\tilde{X}$ en appliquant une transformation particulière telle que $\tilde{X} = A.X$ où A est la matrice de CS. Pour notre application au tatouage, nous avons choisi d'exploiter la Transformée de Fourier Discrète Restreinte (notée RDFT) avec RDFT$(X) = AX = \Psi\Phi X$ tel que Ψ est une base d'impulsion et Φ la base de Fourier. Il est possible de montrer que cette base est d'incohérence maximale [9]. De plus, il est décliné dans [10] les conditions permettant d'obtenir une reconstruction parfaite basée sur la connaissance d'un sous-ensemble des coefficients de Fourier. Comme mentionné préalablement, la marque $\tilde{W}$ est homogène à une erreur de quantification pondérée. Aussi il est possible de l'écrire sous la forme $\tilde{W} = \alpha(Q_\Delta\{\text{RDFT}(X) - \Delta(\frac{d_n}{D})\} - \{\text{RDFT}(X) - \Delta(\frac{d_n}{D})\})$. Après son insertion dans le signal $\tilde{X} = \text{RDFT}(X)$ tel que $\tilde{S} = \tilde{X} + \tilde{W}$, il est nécessaire de reconstruire le signal S dans le domaine original pour le transmettre dans le canal. En utilisant les propriétés de parcimonie du gradient des images naturelles, nous pouvons considérer la reconstruction comme un problème d'optimisation de Variation Totale (TV) tel que défini dans les références [10] et [11]. Le critère du min-TV est bien adapté au traitement d'images et plusieurs algorithmes ont été proposées pour le résoudre efficacement avec un faible coût de calcul [11]. Nous utilisons alors l'algorithme de $\ell_1 - Magic$ pour notre application. Ainsi, nous obtenons l'image tatouée S qui est alors reconstruite avec un PSNR (Peak Signal to Noise Ratio) entre S et X satisfaisant ($PSNR \geq 38.8dB$) ou encore un bon coefficient de similarité SSIM (Structural Similarity) $SSIM \geq 0.968$ confirmant ainsi la bonne transparence perceptuelle de l'information cachée dans le signal reconstruit S.

3 Résultats et Discussion

Nous avons appliqué notre algorithme noté CS-SCS à des images naturelles de taille 512×512 en niveau de gris et comparons ses performances à celles du SCS.

3.1 Transparence statistique

L'évaluation de la transparence statistique a pour but d'étudier l'aptitude qu'aura un utilisateur à facilement distinguer un document marqué d'un document non marqué. Si on considère les 2 hypothèses suivantes $\mathcal{H}_0$: le signal n'est pas marqué, sa PDF est p_X et $\mathcal{H}_1$: le signal est marqué, sa PDF est p_S. Il s'agit de maximiser la probabilité de fausse alarme P_{fa} tel que $P_{fa} = Pr(\mathcal{H}_1|\mathcal{H}_0)$, *i.e.* maximiser la probabilité pour l'attaquant de considérer à tort qu'un document n'est pas marqué. En considérant le Lemme de Stein avec de telles hypothèses, on peut écrire que $D(p_X\|p_S) = \int_{-\infty}^{+\infty} p_X(z) \ln \frac{p_X(z)}{p_S(z)} dz \propto -lnP_{fa}$. Ainsi, maximiser la P_{fa} revient à minimiser la divergence de Kullback-Leibler ($KLD = D(p_X\|p_S)$) entre les PDF (p_S) et (p_X).

Pour le schéma de tatouage proposé, nous avons tracé les PDF des signaux marqués et non marqués (Figure 5) et pouvons les comparer à celles obtenues pour le SCS (Figure 4). Dans le cas du SCS, de nombreuses distortions sont visibles sur la PDF du signal marqué conduisant à une P_{fa} faible. Ces distortions dues à la régularité de la quantification sont très largement supprimées dans le cas du schéma CS-SCS proposé : il y a alors une transparence statistique très largement améliorée et ceci grâce aux opérations de CS utilisées (P_{fa} améliorée).

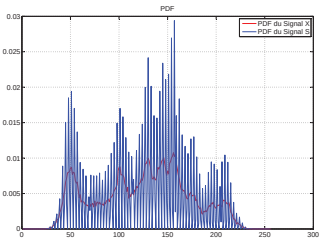

FIGURE 4 – PDF SCS

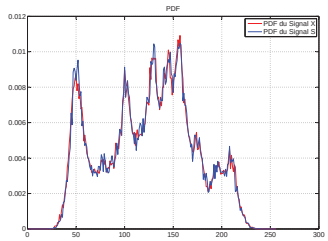

FIGURE 5 – PDF CS-SCS

Cette bonne transparence statistique est confirmée suite à l'étude de la KLD des 2 schémas (SCS et CS-SCS) en fonction du DWR (Document-to-Watermark-Ratio) présentée dans la Figure 6 : les valeurs obtenues pour notre schéma sont bien plus petites que celles obtenues pour le SCS ($\simeq 10^3$ fois plus petites).

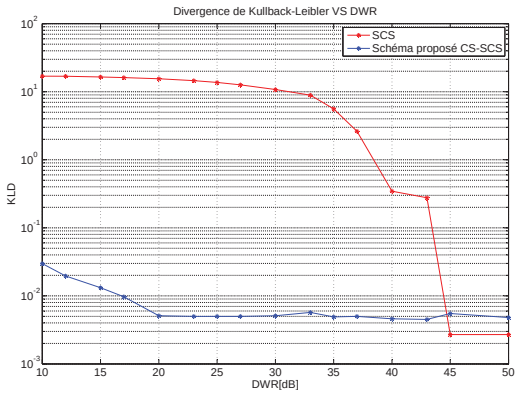

FIGURE 6 – KLD du SCS et CS-SCS

L'algorithme proposé permet bien de construire une image marquée avec une P_{fa} très élevée pour l'attaquant, le conduisant ainsi à conclure à tort à une image non-marquée.

3.2 Robustesse

Nous avons évalué la robustesse de l'information de tatouage (marque) à un bruit blanc additif Gaussien (AWGN) modélisant les distortions apportées par l'attaquant dans le canal. A partir de l'information extraite dans des conditions de bruits différentes (watermarking-to-noise ratio, WNR variable), nous calculons le taux d'erreurs binaire (BER) obtenu. Ainsi, nous présentons sur la figure 7 les résultats obtenus. Les performances obtenues pour le schéma proposé (CS-SCS) en termes de robustesse sont similaires à celles du SCS. C'est donc un schéma offrant de bonnes performances en termes de robustesse pour

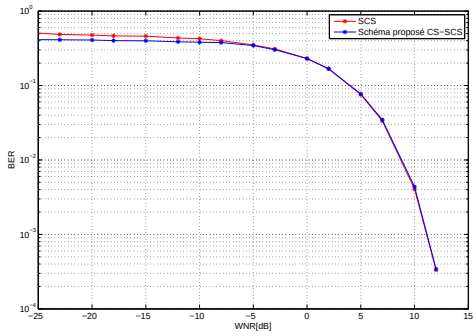

FIGURE 7 – BER pour le SCS et le schéma proposé

cette attaque.

3.3 Capacité

La capacité est définie comme la quantité maximale d'information que l'on peut insérer et extraire sans erreur dans un médium pour un niveau de distortions données dans le canal de communication [12]. Elle est donnée en bits par échantillons. Pour notre étude, nous avons évalué la capacité pour le SCS et le schéma proposé pour plusieurs valeurs du WNR. Les résultats sont tracés sur la figure 8. Comme le prouvent les résultats

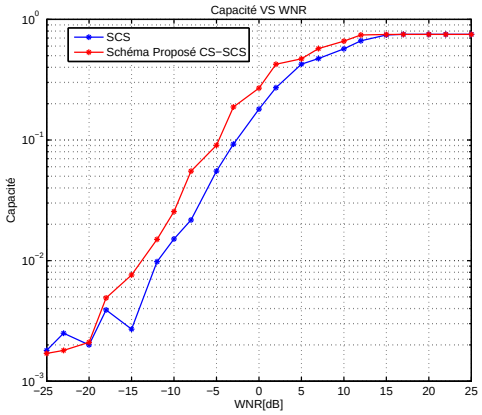

FIGURE 8 – Capacité pour le SCS et le schéma proposé

obtenus sur la figure 8, le schéma proposé (CS-SCS) offre une capacité légèrement meilleure que celle du SCS. En effet même si les valeurs des deux schéma sont globalement proches, on a dans une zone critique du $WNR = [-15dB; 10dB]$ des valeurs meilleures pour notre schéma.

4 Conclusion

Nous proposons un schéma de dissimulation d'information informé basé sur la quantification et le Compressive Sensing avec une faible complexité à l'extraction du message. Ce schéma proposé permet à un attaquant de supposer à tort qu'un signal (ici une image) n'est pas tatoué avec une probabilité de fausse alarme élevée. Nous obtenons grâce à notre approche un schéma de tatouage avec lequel nous sommes capable d'atteindre une bonne transparence statistique comparée au schéma de référence : Schéma Scalaire de Costa. Appliqué aux images naturelles, nous montrons qu'avec des performances de transparence perceptuelles correctes, que les autres performances (en terme de robustesse et de capacité) sont satisfaisantes : la robustesse du schéma que nous proposons est équivalente au SCS et la capacité est très légèrement meilleure que celle du SCS pour les niveaux de bruit élevés (WNR faibles).

Références

[1] J. J. Eggers, R. Bauml, R. Tzchoppe, and B. Girod. Scalar costa scheme for information embedding. *IEEE Trans. on Signal Processing*, April 2003.

[2] A. Komaty, C. Delpha, and A. Fraysse. Floating costa scheme with fractal structure for information embedding. In *IEEE Int. Conf. on Telecommunications*, Lebanon, April 2012.

[3] S. Braci, C. Delpha, and R. Boyer. How quantization based schemes can be used in image steganographic context. *Elsevier Journal on Signal Processing : image communication*, 26(8-9) :567–576, October 2011.

[4] 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.

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

[6] J.-L. Starck, F. Murtagh, and J.M. Fadili. *Sparse Image and Signal Processing : Wavelets, Curvelets, Morphological Diversity*. Cambridge University Press, 2010.

[7] X. Zhang, Z. Qian, Y. Ren, and G. Feng. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. *IEEE Transactions On Information Forensics And Security*, 6(4) :1223–1232, December 2011.

[8] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley, 1991.

[9] E. J. Candes and J. Romberg. Sparsity and incoherence in compressive sampling. *Inverse Problems*, 23 :969–985, 2006.

[10] E. J. Candes, J. Romberg, and T. Tao. Robust uncertainty principles : Exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions On Information Theory*, 52(2) :489–509, February 2006.

[11] E. Candes and J. Romberg. ℓ_1-magic : Recovery of sparse signals via convex programming, October 2005.

[12] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker. *Digital watermarking and steganography*. Morgan Kaufmann, second edition, 2008.