Théorie du transport appliquée au tatouage sûr d'images naturelles

Benjamin Mathon, Patrick Bas, François Cayre, Benoît Macq

Théorie du transport appliquée au tatouage sûr d'images naturelles

Benjamin MATHON[1,3], Patrick BAS[2], François CAYRE[1] et Benoît MACQ[3]

[1]Grenoble Images Parole Signal Automatique Laboratoire
961 rue de la Houille Blanche, BP 46, 38402 Grenoble Cedex, France

[2]Laboratoire d'Automatique, Génie Informatique et Signal
Avenue Paul Langevin, BP 48, 59651 Villeneuve d'Ascq Cedex, France

[3]Laboratoire de Télécommunications et Télédétection
Place du Levant 2, Bâtiment Stévin, 1348 Louvain-la-Neuve, Belgique

{benjamin.mathon,francois.cayre}@grenoble-inp.fr,
patrick.bas@ec-lille.fr, benoit.macq@uclouvain.be

Résumé – Cet article présente une nouvelle méthode de tatouage sûre par étalement de spectre dans le cadre WOA (*Watermarked Only Attack*), un adversaire a accès à plusieurs contenus tatoués et tente d'estimer la clé secrète d'insertion, la sécurité du schéma de tatouage utilisé étant liée à la répartition des contenus tatoués. La question qui se pose alors pour le distributeur de contenus est : comment calculer la fonction d'insertion qui permettra d'obtenir une distribution tatouée donnée tout en minimisant la distorsion d'insertion ? Notre méthode utilise les résultats de la théorie du transport (initialisée par Gaspard Monge [9]) pour une affectation optimale entre deux distributions gaussiennes (en terme de distance euclidienne au carré) permettant d'atteindre la sous-espace sécurité en étalement de spectre. Cette méthode, appelée Tatouage Naturel Transporté (TNT), diminue la distorsion d'insertion (en espérance) sans modifier la robustesse ni la sécurité du Tatouage Naturel (TN) original. Nous utilisons un schéma de tatouage d'images naturelles agissant dans le domaine des ondelettes dans lequel nous comparons les méthodes TN et TNT en terme de sécurité (distributions), robustesse (ajout de bruit gaussien) et imperceptibilité. Pour cette dernière contrainte, le gain en PSNR moyen obtenu par notre nouvelle méthode est de $3.46\ dB$.

Abstract – This article presents a new technique for secure spread-spectrum watermarking in the WOA (Watermarked Only Attack) framework: an adversary owns several marked contents and try to estimate the secret key used for embedding. The security of the watermarking scheme being linked with the distribution of the marked contents, the embedding function will be computed in order to match a host distribution with a marked distribution while minimizing the embedding distortion. We use results of transportation theory (initialized by Gaspard Monge [9]) to derive an optimal mapping between two Gaussian distributions (considering the square Euclidean distance) which achieves the subspace-security in spread-spectrum. This method, called Transportation Natural Watermarking (TNW), is able to decrease the embedding distortion with no modification of the robustness and the security of the classical Natural Watermarking (NW). We use an image watermarking scheme which acts on wavelet domain and we compare the modulations TNW and NW from security (distributions), robustness (AWGN) and distortion point of view. For this last constraint, the PSNR on average is increased by $3.46\ dB$.

1 Introduction

Le passage de l'analogique au numérique a permis une meilleure gestion de la plupart des documents multimédia (musiques, films, images). En effet, le stockage des données est plus facile et l'indexation moins coûteuse. Cependant, son principal inconvénient réside dans le fait qu'on ne puisse pas distinguer une copie d'un original. L'évolution d'Internet et de réseaux d'échanges de données a accéléré la piraterie sur la propriété intellectuelle. Les œuvres soumises au droit d'auteur peuvent être partagées illégalement via téléchargement direct (*Megaupload*, *Rapidshare*), réseau pair à pair (*eMule*, *Torrent*), compression de DVD loués ou prêtés sous forme de fichiers *DIVX*.

Le tatouage numérique (*digital watermarking*) est une technique permettant de résoudre certains problèmes liés aux droits d'auteur, elle consiste à insérer un message dans un contenu numérique respectant trois contraintes : imperceptibilité (le tatouage ne doit pas détériorer l'usage principal du contenu), robustesse (la marque doit résister aux modifications que subit le contenu : compression, transformations géométriques, etc.) ainsi que sécurité. Cette dernière contrainte a pris de plus en plus d'importance au sein de la communauté des tatoueurs [5, 10]. Un schéma de tatouage respecte généralement le principe de Kerckhoffs [6] : l'algorithme et les paramètres du schéma de tatouage sont publics. Une clé secrète permettant l'insertion d'un message et de son décodage est l'unique paramètre inconnu d'un adversaire. Une attaque de sécurité consiste alors en une estimation de la clé secrète par ce dernier. Selon le degré d'estimation, ce dernier pourra alors modifier le message inséré, le supprimer ou le copier sur un contenu vierge.

Nous nous intéressons au cadre WOA (*Watermarked Only*

Attack) [4], un adversaire a accès a plusieurs contenus tatoués et tente d'estimer la clé secrète d'insertion. Le Tatouage Naturel (TN) [2] est une technique de tatouage par étalement de spectre permettant d'atteindre la sous-espace-sécurité [1]. Nous proposons dans cet article une amélioration du TN basée sur la théorie du transport. La sécurité étant liée à la distribution de contenus avant et après tatouage, nous appliquons une affectation optimale entre distributions de façon à minimiser la distorsion provoquée par l'ajout de tatouage. Nos expériences sont réalisées dans le cadre d'un schéma de tatouage d'images agissant dans le domaine des ondelettes.

2 Le tatouage naturel par étalement de spectre

Nous considérons un message binaire $\mathbf{m} \in \mathbb{F}_2^{N_c}$ que l'on souhaite cacher dans un signal hôte $\mathbf{x} \in \mathbb{R}^{N_v}$. La clé secrète utilisée est formée de N_c porteuses $\mathbf{u}_i \in \mathbb{R}^{N_v}$ construites à l'aide d'un générateur de nombres pseudo-aléatoires (initialisé par une graine $K \in \mathbb{N}$) puis orthogonalisées et enfin réduites. Le signal tatoué $\mathbf{y}$ est obtenu en sommant le signal hôte et le signal de tatouage $\mathbf{w}$:

$$\mathbf{y} = \mathbf{x} + \mathbf{w} = \mathbf{x} + \sum_{i=0}^{N_c-1} \mathrm{s}\left(\mathbf{m}(i), \mathbf{x}\right) \mathbf{u}_i, \tag{1}$$

où $\mathrm{s} : \mathbb{F}_2 \times \mathbb{R}^{N_v} \to \mathbb{R}$ désigne une modulation.

Le décodage du message est assuré par le calcul du vecteur de corrélations $\mathbf{z_y}$ entre le signal $\mathbf{y}$ et les porteuses secrètes $\{\mathbf{u}_i\}_{i\in[N_c]}$:

$$\forall i \in [N_c],\ \mathbf{z_y}(i) = \frac{1}{N_v}\langle \mathbf{y}|\mathbf{u}_i\rangle. \tag{2}$$

Le Tatouage Naturel (TN) [2] est une technique de tatouage par étalement de spectre permettant de conserver la distribution originale des $\mathbf{z_x}(i)$ lorsque celle-ci est circulaire. La modulation TN est donnée par :

$$\mathrm{s}_{TN}(\mathbf{m}(i), \mathbf{x}) = \left((-1)^{\mathbf{m}(i)}\mathrm{signe}\left(\langle \mathbf{x}|\mathbf{u}_i\rangle\right) - 1\right) \frac{\langle \mathbf{x}|\mathbf{u}_i\rangle}{N_v}. \tag{3}$$

Lorsque le signal $\mathbf{x}$ est gaussien, le tatouage naturel appartient à la sous-espace-sécurité : dans le cadre WOA, quelque soit le nombre de contenus tatoués possédés par un adversaire, ce dernier n'a aucun moyen d'estimer correctement le sous-espace engendré par les porteuses secrètes [8].

3 La théorie du transport appliquée au tatouage naturel

Le problème du transport consiste à trouver la bijection (le transport) $\mathrm{T} : \mathcal{X} \subset \mathbb{R}^{N_c} \to \mathcal{Y} \subset \mathbb{R}^{N_c}$ entre un échantillon $\mathbf{z_x} \in \mathcal{X}$ de loi μ et un échantillon $\mathbf{z_y} \in \mathcal{Y}$ de loi ν. On considère une fonction de coût $\mathrm{h}(\mathbf{z_y} - \mathbf{z_x}) \geq 0$. Un transport est optimal s'il minimise le coût moyen entre les deux distributions. Pour $N_c = 1$, un plan de transport optimal T pour une fonction de coût convexe h est donné par [11] :

$$\mathrm{T} = \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu, \tag{4}$$

où P_δ désigne la fonction de répartition d'une mesure de probabilité δ. Plus généralement, pour tout N_c, nous avons le théorème suivant :

Théorème 1 ***Critère d'optimalité de Knott-Smith [7]*** *: si μ (respectivement ν) représente la distribution de $\mathcal{X}$ (resp. $\mathcal{Y}$), les conditions suffisantes pour que le plan de transport* T *minimise le problème du transport avec* $\mathrm{h} = \|.\|^2$ *sont :*

i) $\mathrm{T}(\mathcal{X})$ *a pour distribution ν,*

ii) la matrice jacobienne $\mathbf{J}_\mathrm{T}$ *de* T *est symétrique et semi-définie positive.*

Nous savons que la sécurité des schémas par étalement de spectre s'appuie sur la distribution des corrélations entre les signaux tatoués et les porteuses secrètes. Une des propriétés du TN est la préservation de la distribution des corrélations avant et après tatouage des signaux (supposés ici gaussiens). Nous avons :

$$\mathbf{z_x}(i) \sim \mathcal{N}\left(0, \frac{\sigma_\mathbf{x}^2}{N_v}\right) = \mu;\ \mathrm{P}_\mu(t) = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{t\sqrt{N_v}}{\sigma_\mathbf{x}\sqrt{2}}\right)\right). \tag{5}$$

Nous considérons tout d'abord l'insertion du message de N_c bits $(0, 0, \ldots, 0)$ pour chaque signal hôte. Nous obtenons alors :

$$\mathbf{z_y}(i) \sim \mathcal{N}^+\left(0, \frac{\sigma_\mathbf{x}^2}{N_v}\right) = \nu;\ \mathrm{P}_\nu^{-1}(t) = \frac{\sigma_\mathbf{x}\sqrt{2}}{\sqrt{N_v}}\mathrm{erf}^{-1}\left(t\right), \tag{6}$$

où $\mathcal{N}^+$ désigne une distribution gaussienne tronquée dans la région $\mathbb{R}^+$:

$$\mathrm{P}_\nu(t) = \begin{cases} 0 \text{ si } t < 0, \\ 2\mathrm{P}_\mu(t) - 1 \text{ si } t \geq 0. \end{cases} \tag{7}$$

La stratégie que nous adoptons ici est la suivante : nous construisons un plan de transport optimal pour chaque dimension du sous-espace privé de dimension N_c grâce à l'équation (4). Le calcul du plan de transport T_0 pour insérer le message $(0, \ldots, 0)$ est donné par :

$$\mathrm{T}_0\begin{pmatrix} \mathbf{z_x}(0) \\ \vdots \\ \mathbf{z_x}(N_c-1) \end{pmatrix} = \begin{pmatrix} \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu(\mathbf{z_x}(0)) \\ \vdots \\ \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu(\mathbf{z_x}(N_c-1)) \end{pmatrix}. \tag{8}$$

Le plan de transport T_0 ainsi construit respecte le théorème 1 (la preuve utilise la séparabilité d'une distribution multi-gaussienne) et est alors optimal pour la fonction de coût $\mathrm{h} = \|.\|^2$ (proportionnelle à la distorsion provoquée par l'ajout du tatouage).

Grâce à la propriété de symétrie des corrélations en étalement de spectre, pour insérer des messages qui diffèrent de $(0, \ldots, 0)$, des changements de signe doivent intervenir sur les coefficients $\mathbf{z_x}(i)$ au niveau des indices qui ont subi des symétries. Après insertion, des symétries inverses doivent être

effectuées pour pouvoir insérer le message correct $\mathbf{m}$. Nous construisons alors le plan de transport optimal $\mathrm{T}_{\mathbf{m}}$ pour tout message $\mathbf{m} \in \mathbb{F}_2^{N_c}$. Nous définissons une nouvelle technique de tatouage par étalement de spectre basée sur la théorie du transport, nommée **Tatouage Naturel Transporté (TNT)**, la modulation correspondante est donnée par :

$$s_{TNT}(\mathbf{m}(i), \mathbf{x}) = \mathrm{T}_{\mathbf{m}}(\mathbf{z}_{\mathbf{x}})(i) - \mathbf{z}_{\mathbf{x}}(i). \tag{9}$$

4 Expérimentations

Dans cette partie, nous implémentons les modulations par étalement de spectre TN et TNT sur des images codées en niveaux de gris (1 octet/pixel). Après une transformée en 4 niveaux d'ondelettes CDF 9/7, nous arrangeons les sous-bandes HL4 et LH4 de chaque image hôte originale projetées sur des signaux uniformes (afin d'obtenir une distribution gaussienne) dans un signal $\mathbf{x} \in \mathbb{R}^{256}$. Ce dernier est alors tatoué par étalement de spectre avec $N_c = 10$ bits. Les tests sont réalisés sur 2000 images naturelles de 512×512 pixels [3]. La figure 1 présente notre schéma de tatouage expérimental. La figure 2 montre une image hôte tatouée en utilisant d'une part la modulation TN, d'autre part la modulation TNT.

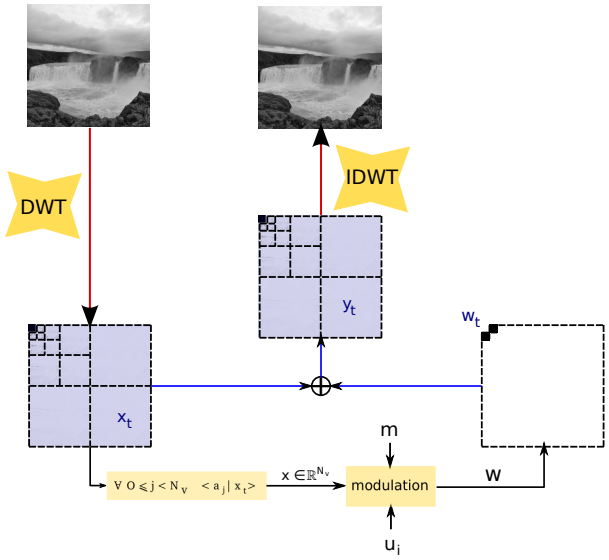
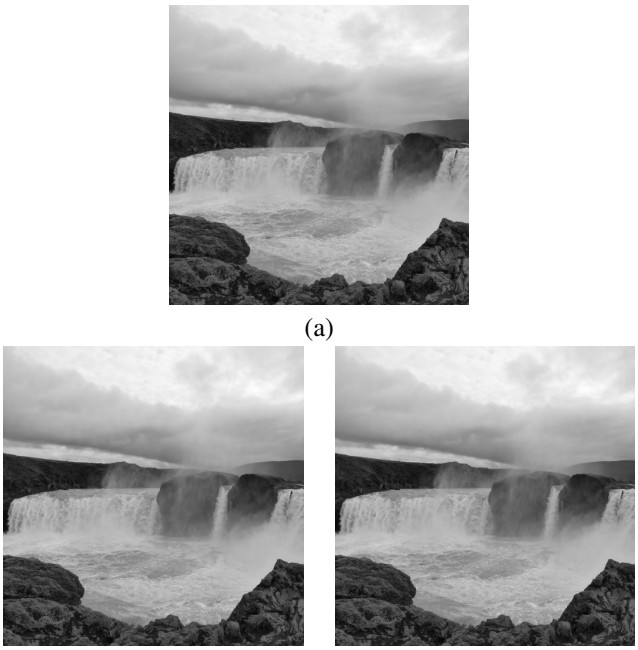


FIGURE 1 – Schéma de tatouage expérimental.

La figure 3 montre la distribution des signaux tatoués par TN (a) et TNT (b) sur deux porteuses. Comme nous pouvons le constater, la distribution des corrélations après tatouage est la même pour les deux techniques. Conformément à l'approche théorique, l'utilisation de la théorie du transport permet d'obtenir la distribution souhaitée.

La figure 4 quantifie le gain en distorsion apporté par la méthode TNT. Pour un PSNR moyen de $46.69dB$ pour la méthode TN, nous obtenons un PSNR de $50.15dB$ pour la méthode TNT.



(a)

(b) (c)

FIGURE 2 – Image hôte (a) tatouée avec la modulation TN (b) (PSNR=48.65 dB) et TNT (c) (PSNR=52.35 dB) avec $N_c = 10$ bits insérés.

Nous avons de plus calculé le taux d'erreur binaire moyen en fonction de la variance de bruit gaussien $\mathbf{n}$ ajouté dans le domaine pixellique pour la modulation TN ainsi que son amélioration TNT (figure 5). Nous remarquons que la méthode TNT ne modifie pas la robustesse du schéma initial TN. Ceci est normal puisque les distributions des contenus tatoués sont identiques.

5 Conclusion

Dans cet article, nous avons développé une nouvelle méthode par étalement de spectre basée sur la théorie du transport, le Tatouage Naturel Transporté, permettant un tatouage sûr. De plus, nous avons montré que celle-ci pouvait être utilisable en pratique (tatouage d'images naturelles) et permet de minimiser la distorsion d'insertion (gain en PSNR de 3.46 dB) tout en gardant les même propriétés de robustesse et de sécurité que le Tatouage Naturel original.

Références

[1] P. Bas et F. Cayre. *Achieving Subspace or Key Security for WOA using Natural or Circular Watermarking*, *in* MM&Sec '06 : Proceedings of the 8th workshop on Multimedia and security, New York, NY, USA, 2006, ACM, p. 80–88.

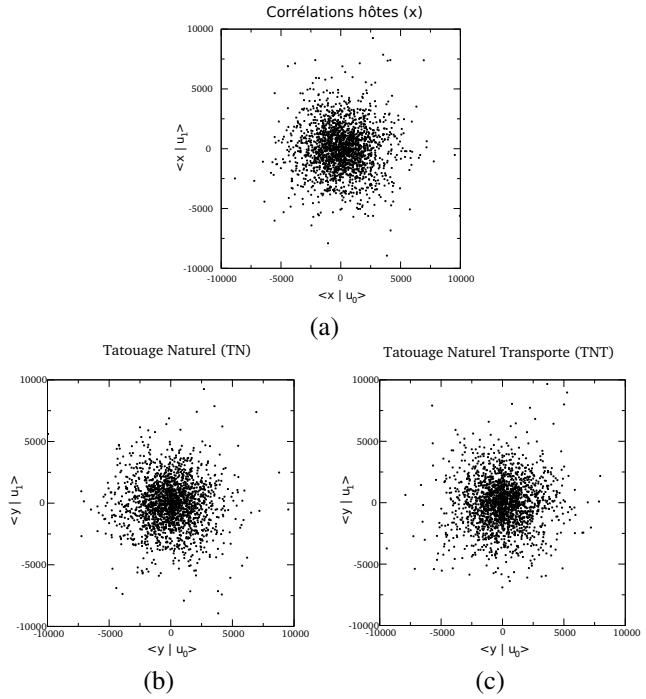


FIGURE 3 – Corrélations entre deux porteuses secrètes et signaux hôtes $\mathbf{x}$ (a) et tatoués $\mathbf{y}$ pour les modulations TN (b) et TNT (c).

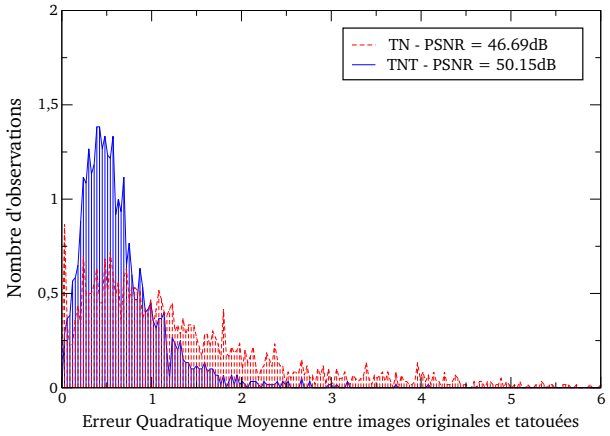


FIGURE 4 – Histogrammes des erreurs quadratiques moyennes entre images originales et tatouées pour les méthodes TN et TNT (cette dernière méthode étant appliquée avec la même distribution de corrélations entre signaux tatoués et porteuses secrètes que la méthode classique TN). Pour la méthode TN nous obtenons $\mathbb{E}(\mathrm{EQM}) = 1.39,\ \mathrm{std}(\mathrm{EQM}) = 1.38$; pour la méthode TNT nous obtenons $\mathbb{E}(\mathrm{EQM}) = 0.63,\ \mathrm{std}(\mathrm{EQM}) = 0.451$. Nous remarquons que l'utilisation de la méthode TNT permet un gain de $3.46dB$ en PSNR moyen. De plus cette méthode réduit considérablement la variance des distorsions.

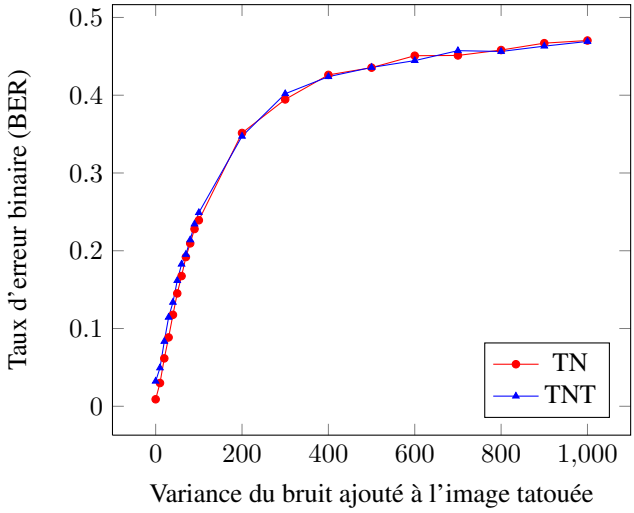


FIGURE 5 – Taux d'erreur binaire moyen en fonction de la variance du bruit $\mathbf{n}$ ajouté dans le domaine pixellique pour la modulation TN ainsi que son amélioration TNT. Nous remarquons que la méthode basée sur modèle ne modifie pas la robustesse du schéma initial.

[2] P. Bas et F. Cayre. *Natural Watermarking : A Secure Spread Spectrum Technique for WOA*, *in* Information Hiding, vol. 4437 de Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2007, p. 1–14.

[3] P. Bas et T. Furon. *Break Our Watermarking System 2nd edition*, 2007. `http://bows2.gipsa-lab.inpg.fr`.

[4] F. Cayre, C. Fontaine et T. Furon. *Watermarking Security : Theory and Practice*, Signal Processing, IEEE Transactions on, 53 (2005), p. 3976–3987.

[5] T. Kalker. *C*onsiderations on watermarking security, *in* Multimedia Signal Processing, 2001 IEEE Fourth Workshop on, 2001, p. 201–206.

[6] A. Kerckhoffs. *La Cryptographie militaire*, Journal des Sciences militaires, IX (1883), p. 5–38.

[7] M. Knott et C. S. Smith. *O*n the optimal mapping of distributions, Journal of Optimization Theory and Applications, 43 (1984), p. 39–49.

[8] B. Mathon, P. Bas, F. Cayre et B. Macq. *Comparison of Secure Spread-Spectrum Modulations Applied to Still Image Watermarking*, Annals of Telecommunications, 64 (2009), p. 801–813.

[9] G. Monge. *M*émoire sur la théorie des déblais et des remblais, Histoire de l'Académie Royale des Sciences de Paris, avec les Mémoires de Mathématique et de Physique pour la même année, (1781), p. 666–704.

[10] L. Pérez-Freire et F. Pérez-González. *Spread-Spectrum Watermarking Security*, Information Forensics and Security, IEEE Transactions on, 4 (2009), p. 2–24.

[11] C. Villani. *Topics in optimal transportation*, Amer Mathematical Society, 2003.