

Introduction au Tatouage d'Images

J.-L. Dugelay, C. Rey, S. Roche

Institut Eurécom, Multimedia Communications Dpt.
Sophia Antipolis
{ dugelay,rey,roche }@eurecom.fr
<http://www.eurecom.fr/~image>

1 Introduction

Le tatouage d'image est apparu au début des années 90 dans le but de résoudre les problèmes liés à la mise en circulation d'œuvres « copyrightées » via des médias dépourvus de mécanismes de sécurité. Aujourd'hui, le tatouage est devenu un domaine majeur en traitement d'image ; le nombre de publications, selon les sources *INSPEC*, est passé de deux en 1992 à plus d'une centaine en 1999 [1]. Le tatouage d'image consiste à insérer (généralement sous forme invisible) une information dans une image puis à tenter de la récupérer après que l'image ait éventuellement subi des manipulations de nature variée.

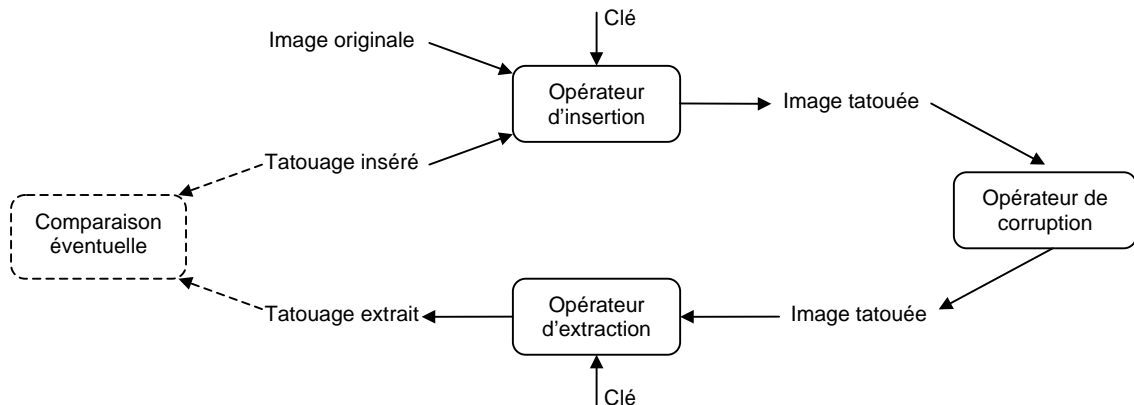


Figure 1 : Dispositif générique d'un système de tatouage.

Les algorithmes de tatouage se distinguent les uns des autres essentiellement par les quatre points clés suivants :

- la manière de sélectionner les points (ou blocs) dans le document hôte qui porteront l'information cachée,
- le choix d'un espace de travail pour réaliser l'opération d'enfouissement (dans le domaine spatial, ou transformé comme DCT, Ondelettes, Fourier-Melin),
- la stratégie utilisée pour mettre en forme l'information à cacher avant son enfouissement (redondance, codes correcteurs),
- la manière de mélanger intimement le message avec le signal hôte (modulation) ; l'idée de base consiste le plus souvent à imposer une relation binaire entre les bits du message et des caractéristiques choisies de l'image porteuse.

Actuellement, il existe deux grandes familles de méthodes : celles qui opèrent dans le domaine spatial et celles qui opèrent dans un domaine transformé ; plus quelques méthodes originales.

2 Choix des éléments de l'image recevant l'information de signature

2.1 Le domaine spatial

L'algorithme « Patchwork » a été proposé par Bender *et al.* en 1995 [2]. Cet algorithme opère directement dans le domaine spatial, c'est-à-dire au niveau même des pixels. Cette technique appartient à la famille des méthodes de tatouage à réponse binaire. Elle permet de répondre par oui ou par non à la question : une personne est-elle en possession de l'information secrète ayant permis de générer le tatouage ? Dans cette méthode on ne cherche en aucun cas à extraire le tatouage.

Le principe du Patchwork est de sélectionner, à l'aide d'une clé secrète, une séquence S_a de n couples de pixels (A_i, B_i) , puis de modifier très légèrement l'image en augmentant d'une unité le niveau de gris des pixels de type A_i et en diminuant d'un niveau de gris les pixels de type B_i . Considérons la somme S des différences de luminance des couples de pixels sélectionnés. Une personne ne disposant pas de la clé sera incapable de régénérer la bonne séquence S_a et obtiendra $S = 0$. Seule la personne disposant de la clé sera en mesure d'obtenir « la bonne valeur » de S , c'est-à-dire $2 \times n$. Ces propos doivent être modérés par l'objection suivante : un individu malveillant peu tout à fait appliquer le même algorithme et ainsi créer une nouvelle image signée $S' = 2 \times n$ à partir d'une clé $K'_s \neq K_s$. On tombe ici sur un problème de multi-signatures qui dépasse largement le cadre de cet algorithme.

Cette méthode de base n'est bien-sûr pas très robuste ; cependant, différentes extensions de cet algorithme ont vu le jour [3, 4]. Elles permettent par exemple d'accroître la résistance du système à des opérations de filtrage sur l'image en considérant non plus des couples de pixels mais des couples de blocs. L'emploi de plusieurs séquences aléatoires orthogonales dans le but de dissimuler plusieurs bits (1 bit par séquence aléatoire) a également été proposé.

2.2 Le domaine DCT

De nombreuses méthodes ont été développées à partir des connaissances acquises auparavant en codage de source. Les auteurs de ces méthodes espèrent ainsi en travaillant dans le domaine DCT [5], anticiper et prévenir au moins les attaques liées à une compression Jpeg [6]. Ils espèrent également pouvoir travailler plus rapidement en couplant le tatouage d'images avec le codage de source. En d'autres termes, le tatouage est réalisé directement sur le flux compressé. Le dernier point opérant en faveur d'un tatouage dans le domaine DCT est qu'il est possible de bénéficier, au moins en partie, des études psychovisuelles déjà menées en codage de source pour gérer les problèmes de visibilité.

2.3 L'espace engendré par la transformée de Fourier-Mellin

Des transformations géométriques de l'image tatouée conduisent fréquemment à l'impossibilité d'extraire le tatouage pour de nombreux algorithmes. Ce constat a conduit à envisager l'implantation du tatouage dans un espace transformé présentant une invariance aux opérations géométriques usuelles de l'image. Dans l'article [7], Ó Ruanaidh *et al.* préconisent l'usage de la transformée de Fourier-Mellin pour assurer la restitution du tatouage après que l'image ait subi une translation et/ou une rotation et/ou un changement d'échelle. L'espace invariant est obtenu ; d'une part grâce à la propriété de la transformée de Fourier qui répercute une translation de l'image exclusivement sur la phase et laisse invariant l'amplitude ; et d'autre part, par un changement de repère, de cartésien vers logarithmique-polaire, qui ramène les opérations de rotation et de changement d'échelle à une translation.

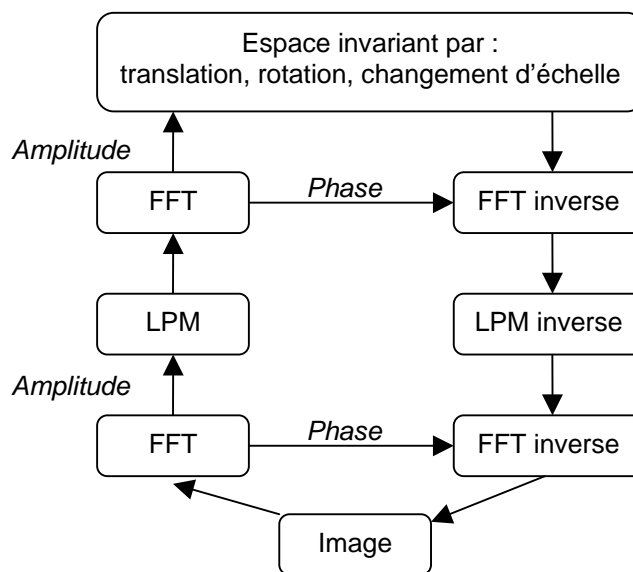


Figure 2 : Construction d'un espace invariant par translation, rotation et changement d'échelle

2.4 Décomposition de l'image en canaux perceptifs

L'évaluation de la qualité des images est une préoccupation constante des systèmes de traitements d'image. Les modèles psychovisuels introduits pour évaluer cette qualité considèrent généralement le système visuel humain comme un ensemble de canaux [12, 13, 14] par lesquels sont transmis différents types d'information au cerveau. Les techniques de tatouage, dans le but d'améliorer l'invisibilité de la signature dans l'image, ont cherché à utiliser ces travaux et en particulier les effets de masquage [15]. Delaigle *et al.* [16, 17] ont développé un modèle perceptif permettant d'évaluer analytiquement la visibilité ou l'invisibilité d'une marque afin de pouvoir éventuellement rétroagir sur l'algorithme de tatouage. L'algorithme proposé réalise une décomposition de l'image originale en canaux. La détermination de chaque canal est faite sur la base de caractéristiques fréquentielles (module et phase) ainsi que de la localisation dans le champ de vision. Toute la difficulté consiste à identifier des canaux

en adéquation avec les critères perceptifs humains. L'hypothèse sous-jacente consiste à admettre que deux signaux à l'intérieur d'un même canal ne pourront être distingués par l'oeil humain.

Le domaine ondelette : les transformées en ondelettes qui tout comme la transformée DCT fait l'objet de nombreuses études dans le contexte du codage ont également trouvé un écho dans la communauté du tatouage d'image [8,9,10,11]. Cet intérêt repose d'une part sur les analyses en termes psychovisuels menées afin d'optimiser les tables de quantifications des codeurs, d'autre part sur l'aspect multi-échelle de telles transformées propice à une répartition plus robuste du tatouage. Ce gain en robustesse apporté par l'usage d'une transformée ondelette est particulièrement significatif si l'on considère les algorithmes de compression de type EZW (Embedded Zero-tree Wavelet) qui seront vraisemblablement intégrés dans la nouvelle norme de compression JPEG-2000.

3 Ajout de redondance à la signature

La taille des signatures nécessaires à l'identification sans ambiguïté un individu sont de l'ordre de quelques octets, or une image constitue un volume d'information binaire bien supérieur. Il est donc légitime d'ajouter de la redondance à la signature originale afin d'accroître la robustesse du tatouage face à des manipulations de l'image.

3.1 Étalement de spectre

Les techniques d'étalement de spectre ont été introduites pour résoudre des problèmes de communications sur des canaux bruités entre plusieurs utilisateurs [18]. En complément du gain en robustesse que procurent ces techniques vis à vis des imperfections du canal de transmission, elles permettent d'assurer la confidentialité entre les différentes communications via un même canal de transmission.

Étalement par séquence directe : cette technique réalise l'étalement directement dans le domaine temporel (ou spatial). Un signal à bande étroite S peut être étalé spectralement par modulation à l'aide d'un signal à large spectre PN (s'apparentant à un bruit blanc). Cette modulation confère au signal résultant S_e les caractéristiques spectrales de PN . Si le signal de transmission présente un évanouissement dans la bande étroite où se situe le signal à transmettre S , la technique d'étalement permettra d'assurer une bonne transmission de ce signal. La connaissance du signal PN permet de démoduler le signal S_e et de reconstruire le signal S .

3.2 Codes correcteurs

De nombreux articles [17, 19, 20, 21] font référence à une utilisation potentielle de codes correcteurs d'erreurs afin d'augmenter les performances en termes de robustesse des algorithmes de tatouage. L'emploi de tels codes apparaît en effet naturel si l'on examine le problème de la robustesse du tatouage sous l'angle de la communication d'un signal sur un canal bruité. Les travaux actuellement publiés proposent par exemple l'utilisation de codes BCH et Reed-Muller.

L'usage des codes correcteurs dans le cadre du tatouage d'image reste un problème ouvert, requérant la conception de codes compacts capables de prendre en compte la diversité des attaques.

4 Fusion des données : image et signature

4.1 Techniques de modulation

Modulation de phase

La transformée de Fourier d'une image réelle est généralement de nature complexe ; elle possède donc un module et une phase. Des études expérimentales ont montré que l'information contenue dans la phase était prépondérante sur celle contenue dans l'amplitude dans la représentation de l'image. Cette constatation conduit les auteurs à introduire le tatouage au niveau de la phase pour, d'une part s'assurer qu'une tentative de suppression du tatouage engendrera inévitablement des dégradations importantes de l'image ; d'autre part les techniques de modulation de phase sont reconnues comme étant plus robuste au bruit que les techniques de modulation d'amplitude. Un tel système privilégie a priori l'aspect robustesse sur l'aspect visibilité.

Modulation d'amplitude

Dans l'article [22], il est proposé de réaliser l'insertion de la signature par une modulation d'amplitude de la composante bleue d'une image couleur (RGB). Ce choix de la composante bleue est motivé selon les auteurs par une moindre sensibilité de l'oeil humain dans les longueurs d'onde proches du bleu.

4.2 Ajout du tatouage par quantification des coefficients DCT

Modification de la fonction d'arrondi

Dans l'une de leurs méthodes, Matsui et Tanaka [23] proposent d'introduire la signature binaire lors de l'étape de quantification des coefficients DCT. Plus précisément, ils modifient la fonction d'arrondi. Par rapport à la fonction classiquement utilisée dans un codeur Jpeg, on ne considère plus l'entier le plus proche mais l'entier pair (respectivement impair) le plus proche lorsque l'on désire introduire un bit de signature à 1 (respectivement 0). L'erreur de quantification ainsi créée est donc directement corrélée avec la signature. Les auteurs admettent que la dégradation engendrée par cette erreur est suffisamment faible pour ne pas entraîner de gêne visuelle. Si tel n'est pas le cas, il est possible de réduire le pas de quantification des tables de coefficients DCT pour se positionner à un niveau de dégradation acceptable. Malheureusement, cette opération entraîne une moindre résistance du tatouage. Le pas de quantification fournit donc un paramètre de réglage du compromis robustesse vs. visibilité.

Définition d'une relation de N-uplet de coefficients

La technique exposée précédemment introduit un bit de tatouage au niveau de chaque coefficient DCT en ne tenant pas compte des coefficients voisins. Koch et Zhao [24, 25] ont cherché à rétablir une notion de voisinage en proposant une modulation différentielle des coefficients DCT.

Superposition des coefficients DCT de l'image et du tatouage

Cette technique inspirée des méthodes stéganographiques [26, 27] est particulièrement indiquée lorsque le tatouage est de même nature que les données à tatouer. Autrement dit, dans le cadre des images, si le tatouage est lui même une image (par exemple un logo).

4.3 Ajout du tatouage par substitution de blocs : codage fractal

La plupart des méthodes de tatouage introduisent la signature dans l'image par le biais d'une perturbation de la quantification de certaines grandeurs caractéristiques de l'image. Dans le cadre par exemple des méthodes basées sur la quantification de certains coefficients DCT, les effets visuels résultant de cette manipulation sont parfois difficilement maîtrisables. Le laboratoire de Traitement des Signaux de l'EPFL propose une nouvelle approche reposant sur le codage fractal [28]. Le codage fractal est basé sur la définition d'une association entre différentes régions de l'image. Cette association est réalisée selon un critère d'auto-similarité fondé sur la minimisation de l'erreur quadratique entre les blocs cibles et les blocs sources transformés. Pour un bloc cible donné, la recherche du bloc source associé s'effectue dans deux fenêtres de recherche centrées sur le bloc cible, selon une certaine convention et de la valeur du bit à cacher.

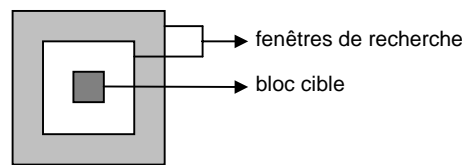


Figure 3 : Bloc cible et les deux sous fenêtres de recherche associées.

L'intérêt de cette approche est de mettre à profit certaines propriétés d'invariance propres aux fractales afin de pouvoir prévenir certaines attaques et récupérer la marque sans avoir recours à l'image originale.

5 Optimisation du détecteur

L'extraction de la signature est composée d'opérations duales de l'insertion, auxquelles il faut ajouter divers techniques propres à la phase d'extraction visant à accroître la robustesse du tatouage. Certains algorithmes [29] pratiquent un filtrage de l'image tatouée avant d'entreprendre la vérification du tatouage. D'autres algorithmes [30] confectionnent un tatouage comprenant des bits dont les valeurs sont prédéfinies afin de permettre une première estimation de l'attaque qu'a pu subir l'image. Ces derniers algorithmes sont propices à la mise en place de seuils de décisions adaptatifs. Enfin, les tests d'hypothèses font également partis des outils usuellement utilisés dans le cadre de problèmes où une prise de décision intervient. En tatouage d'images, ils trouvent particulièrement leur intérêt lorsque la signature est connue et qu'il s'agit de vérifier sa présence dans telle ou telle image, le plus souvent par corrélation.

6 Conclusion

Cet état de l'art nous a permis de dégager les grandes lignes conduisant à la conception d'un système de tatouage et a révélé la diversité des techniques mises en œuvre. Néanmoins, la robustesse du tatouage semble surtout vérifiée vis-à-vis des standards de compression, elle n'est pas assurée face à une combinaison d'attaques de nature différente. La plupart des efforts se sont portés vers une gestion appropriée du compromis robustesse vs. visibilité, le plus souvent au détriment d'autres aspects comme la capacité d'insertion ou le mode d'extraction. Les algorithmes les plus robustes réalisent rarement l'extraction en mode aveugle (i.e. on ne présume ni la connaissance de l'image originale et ni la connaissance du tatouage).

7 Références

- [1] S.Roche & J.-L. Dugelay. Image watermarking based on the fractal transform. *IEEE MultiMedia Signal Processing – MMSP (1998)*, L.A., CA, pp. 358-362, 1998.
- [2] W. Bender, D. Gruhl & N. Morimoto. Techniques for data hiding. *Proceedings of the SPIE*, 1995.
- [3] G.C. Langelaar, J.C.A. Van der Lubbe & R.L. Lagendijk. Robust labeling methods for copy protection of images. *Proceedings of the SPIE Electronic Imaging'97, Storage and Retrieval for Image and Video Databases*, San Jose, California, 1997.
- [4] I. Pitas & T.H. Kaskalis. Applying signatures on digital images. *IEEE Workshop on Nonlinear Signal and Image Processing*, pp. 460-463, Thessaloniki, Greece, 1995.
- [5] K.R. Rao & P. Yip. Discrete cosine transform: algorithms, advantages, applications. *Academic Press Inc.*, 1990.
- [6] W.B. Pennebaker & J.L. Mitchell. JPEG still image data compression standard. *Van Nostrand Reinhold Compagny*, 1992.
- [7] J.J.K Ó Ruanaidh & T. Pun. Rotation, translation and scale invariant digital image watermarking. *IEEE Signal Processing Society 1997 Int. Conf. on Image Processing (ICIP'97)*, vol. 1, pp. 536-539, Santa-Barbara, CA, Oct. 1997.
- [8] H.-J. Wang & C.-C Jay Kuo. Image protection via watermarking on perceptually significant wavelet coefficients. *Proc. of IEEE Multimedia Signal Processing Workshop (MMSP'98)*, pp. 279-284, Redondo Beach CA USA, Dec. 1998.
- [9] X.-G. Xia, C.G. Boncelet & G.R. Arce. Wavelet transform based watermark for digital images. *Optis Express*, 3(12) : 497-511, Dec. 1998.
- [10] D. Kundur & D. Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, vol. 6, pp. 2969-2972, 1998.
- [11] W. Zeng, B. Liu & S. Lei. Extraction of multiresolution watermark images for claiming rightful ownership. *Proc. of SPIE, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, vol. 3657, Jan. 1999.
- [12] S. Western, R. Lagendijk & J. Biermond. Perceptual image quality based on a multiple channel hvs model. *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'95)*, vol. 4, pp. 2351-2354, 1995.
- [13] S. Winkler A perceptual distortion metric for digital color images. *Proc. of the Int. Conf. on Image Processing (ICIP'98)*, vol. 1, pp. 399-403, Chicago, Illinois, US, Oct. 1998.
- [14] J.-F. Delaigle, C. De Vleeschouwer & B. Macq. Psychovisual approach for digital picture watermarking. *Journal of Electronic Imaging*, 7(3) : 319-336, May 1998.
- [15] F. Bartolini, M. Barni, V. Cappellini & A. Piva. Mask building for perceptually hiding frequency embedded watermarks. *Proc. of the Int. Conf. on Image Processing (ICIP'98)*, vol. 1, pp. 450-454, Chicago, Illinois, US, Oct. 1998.

- [16] J.-F. Delaigle, C. De Vleeschouwer & B. Macq. Watermarking using a matching model based on the human visual system. Ecole thématique CNRS GDR-PRC ISIS : Information Signal Images Marly le Roi, Apr. 1997.
- [17] J.-F. Delaigle, C. De Vleeschouwer & B. Macq. Watermarking algorithm based on a human visual model. *Signal Processing*, 66(3) : 319-336, May 1998.
- [18] R.L. Pickholtz, D.L. Schilling & L.B. Millstein. Theory of spread spectrum communications – a tutorial. *IEEE Trans. On Communications*, pp. 855-884, 1982.
- [19] J.-F. Delaigle, J.-M. Boucqueau, J.-J. Quisquarter & B. Macq. Digital images protection techniques in a broadcast framework : overview. *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST'96)*, pp. 711-728, Louvain-la-Neuve, Belgium, May 1996.
- [20] V. Darmstaedter, J.-F. Delaigle, D. Nicholson & B. Macq. A block based watermarking technique for MPEG-2 signals : Optimization and Validation on real digital TV distribution links. *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST'98)*, May 1998.
- [21] J.R. Hernández, F. Pérez-González, J.M. Rodríguez & G. Nieto. The impact of channel coding on the performance of spatial watermarking for copyright protection. *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'98)*, vol. 5, pp. 2973-2976, 1998.
- [22] M. Kutter, F. Jordan & F. Bossen. Digital signature of color images using amplitude modulation. *Proc. of SPIE storage and retrieval for image and video databases*, pp 518-526, San Jose, USA, Feb. 1997.
- [23] K. Matsui & K. Tanaka. Video-steganography : how to secretly embed a signature in a picture. *Journal of the interactive Multimedia Association Intellectual Property Project*, 1 : 187-206, 1994.
- [24] E. Koch & J. Zhao. Towards robust and hidden image copyright labeling. *IEEE Workshop on Nonlinear Signal and Image Processing*, Thessaloniki, Greece, 1995.
- [25] J. Zhao. A WWW service to embed and prove digital copyright watermarks. *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST'96)*, 1996.
- [26] N.F. Johnson & S. Jajodia. Exploring steganography : seeing the unseen. *Computer*, 31(2) : 26-34, Feb. 1998.
- [27] N.F. Johnson & S. Jajodia. Steganalysis of images created using current steganography software. *Proc. Second Int. Workshop on Information Hiding*, pp 273-289, Apr. 1998.
- [28] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. *Proc. of SPIE Photonics East Symposium*, vol. 1, Boston, USA, Nov. 18-22 1996.
- [29] T. Kalker & J.-P. Linnartz. Improved watermark detection reliability using filtering before correlation. *Proc. IEEE int. Conf. on Image Processing*, 1998.
- [30] M. Kutter. Watermarking resisting to translation, rotation and scaling. *Proc. of SPIE*, vol. 3528, pp. 423-431, Boston USA, Nov. 1998.