Tatouage sûr

Encadrant : Marc Chaumont
Co-encadrant : William Puech
marc.chaumont@lirmm.fr
Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier

Depuis 2005, la sécurité des schémas de tatouage numérique [Cayre et al. 2005] est bien mieux comprise qu'à la naissance (années 1990) de la discipline du tatouage [Cox et al. 2001]. La distinction entre la notion de robustesse et celle de sécurité est maintenant bien plus nette. Une **attaque à la robustesse** consiste à faire disparaître le signal de tatouage alors qu'une **attaque à la sécurité** [Bas et Doërr 2007], [Mathon et al. 2007] consiste surtout à déterminer un secret (comme par exemple des porteuses ou des clefs secrètes) et ensuite de faire disparaître de manière chirurgicale le signal de tatouage, d'accéder aux informations confidentielles, ou de tatouer un document en usurpant une identité.

L'objectif de cette thèse est d'**étudier et de proposer des nouveaux schémas de tatouage à faible et forte capacité qui soient robustes et également sûrs**. Les schémas de tatouage 0-bit (i.e à capacité nulle) trouvent une excellente illustration avec le très récent algorithme de Broken Arrows [Furon et Bas 2008] utilisé dans la compétition BOWS-2 [BOWS-2 2008]. Ce type de schéma n'a pas encore été complètement évalué en termes de sécurité. Les schémas de tatouage multi-bits à forte capacité sont quant à eux encore moins avancés, pour ce qui concerne la sécurité, sur les plans théoriques et pratiques. Par exemple, que cela soit pour les schémas basés quantification [Eggers et al. 2003] , treillis [M.L Miller et al. 2004], tatouage naturel [Bas et Cayre 2006], tatouage circulaire [Mathon et al. 2007] etc., le compromis théorique dégradation/taux-d'erreur-sécurité n'est pas clairement établi. Les évaluations pratiques du niveau de sécurité ne sont pas non plus aussi poussées qu'avec une compétition comme BOWS-2.

Lors de la compétition BOWS-1 achevée le 15 juin 2006, l'un des algorithmes les plus performants pour le tatouage robuste à haute capacité [M.L Miller et al. 2004] a été utilisé. L'algorithme a été attaqué (le message n'était plus récupérable) avec de très faibles dégradations du support tatoué. Plusieurs conclusions pratiques pour renforcer la robustesse et la sécurité ont alors été dressées pour rendre plus difficile les attaques (éviter la super-robustesse, être plus proche du signal via l'insertion multiplicative, proposer une insertion plus robuste, proposer un réel algorithme zéro-bit, utiliser l'espace ondelette…). Ces conclusions ont été largement utilisées pour le schéma (zéro-bit) utilisé lors de la compétition BOWS-2 (algorithme de Broken Arrows) ; compétition qui s'est achevée le 17 avril 2008 et dont certains résultats sont déjà publiés [Westfeld 2008].

Encore une fois, il apparaît (voir les résultats sur http://bows2.gipsa-lab.inpg.fr/) que le schéma zéro-bit « Broken Arrows » peut être attaqué avec une dégradation faible (attaque à 50 dB dans le cas d'une attaque par oracle et de 42 dB dans le cas d'une attaque par collusion). Les schémas de tatouage complètements sûrs ne sont donc pas encore finalisés par la communauté du tatouage. La thèse a donc pour objectif :

1. de comprendre les mécanismes d'attaques et faire un état de l'art de ces mécanismes. Pour le moment ces méthodes sont peu décrites par la littérature du fait de l'intérêt très récent

pour la sécurité (2005). On regardera avec attention les attaques à la sensitivité [Cox et al. 2001], celles issus de BOWS-1 [Comesaña et Pérez-González 2007], [Earl 2007], celles utilisées pour les systèmes de tatouage multi-bits [Pérez-Freire et al. 2006], [Pérez- Freire et Pérez- González 2007], [Mathon et al. 2007], [Bas et Doërr 2007], mais aussi les travaux plus théoriques comme ceux de Moulin [Choubassi et Moulin 2007] et bien entendu ceux concernant l'attaque de Broken Arrows.

2. de proposer des contre-attaques aux attaques actuellement connues. Ces contres-attaques impliquent donc la proposition de nouveaux schémas de tatouage rendant plus difficiles ou inopérantes les attaques. Parmi ces contres-attaques, on peut penser entre autre à rendre le signal tatoué statistiquement proche du signal hôte (comme en stéganographie), tatouer sur des nouveaux espaces d'insertion sécurisés (exemple des transformations ondelettes de deuxième génération), rendre l'espace secret dépendant d'informations adjacentes, utiliser de nouvelles méthodes de détection et d'insertion (logique floue), rendre robustes les schémas aux désynchronisations (décodage universel), insérer des leurres, utiliser un cocktail de tatouages, … Bien sûr, parmi ces possibilités, certaines s'ajouteront au cours de la thèse et d'autres seront à écarter.

L'intérêt d'un tel sujet de thèse est de mettre à plat l'existant en termes d'attaque et de contre-attaque et de proposer de nouvelles approches de tatouage. De nombreuses études ont montré que la stéganographie ou le tatouage étaient utilisés à des fins terroristes comme canal de communication secret. Il est donc nécessaire de poursuivre l'effort de recherche sur de tels sujets. L'intérêt industriel est également clair puisque le tatouage robuste et sûr permet de dissimuler de manière cachée et sécurisée des informations comme l'identifiant d'un acheteur ce qui permet d'effectuer le suivi d'une transaction. Enfin, le caractère novateur est à chercher dans la connaissance et la compréhension la plus récente des techniques de tatouage mais aussi dans la création de nouveaux schémas. Comme en cryptographie, toute la sécurité repose sur l'avance technique du tatoueur par rapport à l'attaquant à un instant donné.

Dans un premier temps, l'étudiant étudiera le schéma Broken Arrows (zero-bit) [Furon et Bas 2008] et créera des attaques génériques et efficaces en s'inspirant des travaux sur la régression [Westfeld 2008], sur l'attaque à la sensibilité [Comesaña et Pérez-González 2007] ainsi que la séparation de source [Mathon et al. 2007]. Fort de cette expérience, l'étudiant devra alors être en mesure de proposer des schémas plus sûrs et/ou plus robustes.

Dans un second temps, l'étudiant abordera les schémas à forte capacité, adaptera ses précédents résultats, formalisera la notion d'attaque et proposera de nouvelle attaques, ou de nouveaux schémas. Par exemple les travaux menés par Bas et Doërr [P. Bas, G. Doërr 2007], [Bas et Doërr 2008] montrent qu'il est possible, en simplifiant le schéma de tatouage original basé treillis, de mener une attaque « Watermak Only Attack (WOA)». Cependant, pour l'attaquant, il reste encore à régler le problème de « randomisation » des coefficients. Ce problème pourra être abordé en s'inspirant de l'attaque à la sensibilité [Comesaña et Pérez-González 2006] et de l'estimation des porteuses par séparation de sources [Mathon et al. 2007].

Bibliographie :

[Cayre et al. 2005] « Watermarking Security: Theory and Practice », F. Cayre, C. Fontaine, T. Furon, IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3976—3987, 2005.

[Cox et al. 2001] « Digital Watermarking », I. Cox, M. Miller, and J. Bloom, Morgan Kaufmann Publisher, 2001.

[Bas et Doërr 2007] "Practical security analysis of dirty paper trellis watermarking," P. Bas and G. Doërr, in Information Hiding: 9th international workshop, T. Furon, F. Cayre, G. Doërr, and P. Bas, Eds., Saint-Malo, June 2007, vol. 4567 of Lecture Notes in Computer Science, Springer Verlag.

[Mathon et al. 2007] « Practical performance analysis of secure modulations for WOA spread-spectrum based image watermarking », B. Mathon, P. Bas, F. Cayre. ACM'2007, Multimedia and Security Workshop, 20-21 September 2007, Dallas, Texas, USA.

[BOWS-2 2008] « BOWS-2 : The second Break Our Watermarking System Contest », 17/07/2007 – 17/04/2008, Organised within the activity of the Watermarking Virtual Laboratory (Wavila) of the European Network of Excellence ECRYPT, http://bows2.gipsa-lab.inpg.fr/

[Furon et Bas 2008] « Broken Arrows » T. Furron and P. Bas, Article en cours de soumission 2008.

[Bas et Cayre 2006] « Natural Watermarking: a secure spread spectrum technique for WOA » Patrick Bas, and François Cayre, Information Hiding 2006, pp.1-14, 4437.

[M.L Miller et al. 2004] « Applying Informed Coding and Embedding to Design a Robust, High capacity Watermark », M.L Miller, G. J. Doerr and J. Cox, IEEE Trans. On Image Processing, 13, 6, 792-807, June 2004.

[Eggers et al. 2003] « Scalar Costa scheme for information embedding » J.J. Eggers, R. Bauml, R. Tzschoppe, B. Girod, IEEE Transactions on Signal Processing, IEEE Transactions on], Volume 51, Issue 4, Apr 2003 Page(s): 1003 – 1019.

[Westfeld 2008] « A Regression-Based Restoration Technique for Automated Watermark Removal », Andreas Westfeld, TU Dresden, Multimedia & Security ACM Workshop MMSEC2008, Oxford, United Kingdom, 22-23 September 2008.

[Comesaña et Pérez-González 2007] « Two different approaches for attacking BOWS » Pedro Comesaña and Fernando Pérez-González, Security, Steganography, and Watermarking of Multimedia Contents IX, edited by Edward J. Delp III, Ping Wah Wong, Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6505, 2007 SPIE-IS&T.

[Earl 2007] « Tangential sensitivity analysis of watermarks using prior Information », John W. Earl, Security, Steganography, and Watermarking of Multimedia Contents IX, edited by Edward J. Delp III, Ping Wah Wong, Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6505, 2007 SPIE-IS&T.

[Choubassi et Moulin 2007] « SENSITIVITY ANALYSIS ATTACKS AGAINST RANDOMIZED DETECTORS », *Maha El Choubassi and Pierre Moulin,* ICIP'2007, IEEE International Conference on Image Processing, San Antonio, Texas, USA, 16-19 September, 2007, 4 pages.

[Pérez-Freire et al. 2006] « Security of Lattice-Based Data Hiding Against the Known Message Attack », Luis Pérez-Freire, Fernando Pérez- González, Teddy Furon, Pedro Comesaña, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 2006.

[Pérez- Freire et Pérez- González 2007] « Exploiting security holes in lattice data hiding », L. Perez- Freire, F. Perez-Gonzalez. In Information Hiding, IH'07, Lecture Notes in Computer Science, Saint-Malo, France, 11-13 June 2007. Springer-Verlag.