Attaque de systèmes de tatouage

M. Chaumont
LIRMM (Laboratoire d'Informatique, de Robotique et Microélectronique de Montpellier)
Equipe ICAR
161 rue Ada, 34392 Montpellier cedex 5 - France
Tel : +33 4.67.41.85.14
Fax : +33 4.67.41.85.00
Marc.Chaumont@lirmm.fr

Le tatouage est l'art d'altérer un média (une image, un son, une vidéo...) de sorte qu'il contienne un message le plus souvent en rapport avec le média et le plus souvent de manière imperceptible. Dans le cas de tatouage d'image, le message sera « mélangé » aux pixels sans altérations visibles de l'image. Une attaque à la sécurité d'un système de tatouage consiste à récupérer une information secrète du système (comme une clef ou bien des porteuses) pour ensuite effectuer (cas multi-bit) :

- une copie non-autorisée du signal de tatouage issu d'une ou plusieurs images tatouées avec le même message,
- une lecture non-autorisée d'un message,
- une modification non-autorisée du signal de tatouage de sorte que le message extrait soit erroné,
- une écriture non-autorisée permettant de substituer le message présent par un autre message.

Plusieurs points gravitant autour de la sécurité pourront être envisagées :

- L'**attaque du système de tatouage basé treillis** (Dirty Paper Trellis Code [Miller et al. 2004]). 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, de mener une attaque « Watermak Only Attack (WOA)». Cependant, pour l'attaquant, il reste encore à régler le problème de « randomisation » des coefficients pour pouvoir attaquer le schéma original. On abordera ce problème, entre autre, en s'aidant 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].

- L'**attaque du système zéro-bit de BOWS-2** [BOWS-2 2008] : Broken Arrows [Furon et Bas 2008]. On reprendra les travaux basés sur l'attaque par oracle [Comesaña et Pérez-González 2006], sur l'attaque par régression [Westfeld 2008] et sur la séparation de sources illustrée dans [Bas et Cayre 2006] et [Mathon et al. 2007]. On doit pouvoir obtenir une version attaquée de faible PSNR. Cette version pourrait être utilisée comme base pour une attaque de type WOA ou même « Kown-Original Attack (KOA) ».

- L'**analyse des techniques récentes en vue de la proposition de schémas sûrs**. De nombreuses attaques on été étudiés (attaques à la sensibilité [Cox et al. 2001], [Comesaña et Pérez-González 2007], [Earl 2007], attaques des systèmes de tatouage multi-bits [Pérez-Freire et al. 2006], [Pérez-Freire et Pérez- González 2007], [Mathon et al. 2007], [Bas et Doërr 2007]), et montrent quelles sont les failles des systèmes actuels. Certaines contres-attaques sont connues et utilisées dans « Broken Arrows » [Furon et Bas 2008] (espace d'insertion sécurisé, frontières de détection non régulières et aléatoires (leurres) …). On étudiera donc la sécurité des approches asymétriques [Furon 2001], BPSK [Mathon et al. 2007] et de [Venturini 2005] vis à vis de l'attaque par oracle [Comesaña et Pérez-González 2007] et l'on proposera des solutions ou pistes pour renforcer la sécurité.

Références :

[M.L Miller, G. J. Doerr and J. Cox 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.

[P. Bas, G. Doerr 2007] « Practical Security Analysis of Dirty Paper Trellis Watermarking », Information Hiding 2007

[Bas et Doërr 2008] « Evaluation of an Optimal Watermark Tampering Attack Against Dirty Paper Trellis Schemes », Patrick Bas, Gwenaël Doërr, Multimedia & Security ACM Workshop MMSEC2008, Oxford, United Kingdom, 22-23 September 2008.

[Comesaña et Pérez-González 2006] Pedro Comesaña, Luis Pérez-Freire, and Fernando Pérez-González. Blind Newton Sensitivity Attack. IEE Proceedings on Information Security, 153(3):115-125, September 2006

[Comesaña et Pérez-González 2007] Pedro Comesaña and Fernando Pérez-González. Breaking the BOWS Watermarking System: Key Guessing and Sensitivity Attacks. EURASIP Journal on Information Security, 2007. Vol 2007, Article ID 25308, 8 pages.

[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.

[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.

[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.

[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.*

[T.Furon, I Venturini, P Duhamel 2001] An unified approach of asymmetric watermarking schemes. SPIE 2001

[Ilaria Venturini 2005] « Oracle attacks and covert channels », Fourth International Workshop on Digital Watermarking, Sept 2005.