



vers une « batch » steganographie

sujet M2R pour 2012-2013

Marc Chaumont

LIRMM (Laboratoire d'Informatique, de Robotique et Microélectronique de Montpellier)

Equipe ICAR

161 rue Ada, 34392 Montpellier cedex 5 - France

Tel : +33 4.67.14.97.59

Marc.Chaumont@lirmm.fr



Mots clefs : Traitement d'images, Sécurité multimédia, steganographie, stéganalyse, machine learning.

La stéganographie est l'art de dissimuler un message de manière secrète dans un support anodin. La stéganalyse est l'art de déceler la présence d'un message secret. L'étude de la stéganographie/stéganalyse moderne a réellement débuté au début des années 2000. Actuellement, lorsque l'on effectue une stéganalyse, on définit un « scénario », c'est-à-dire un certain nombre d'hypothèses sur ce que le stéganalyste connaît de l'environnement utilisé par le stéganographe.

En 2006, Andrew Ker [Ker2006] propose d'étendre le scénario classique de la stéganalyse d'une image à une approche où le message à dissimuler est découpé et dispatché dans plusieurs images. Pour extraire le message, il est donc nécessaire de disposer de l'ensemble des images utilisées lors de l'insertion. Ce scénario est appelé « batch » stéganographie et « pooled » stéganalyse. L'étude théorique de ce scénario a alors été poursuivie par Andrew Ker. Tout récemment, Tomas Pevny s'est associé à Andrew Ker, et ils ont proposé trois papiers abordant le problème de manière pratique [Ker2011_Clustering], [Ker2012_LOF], [Ker2012_RW].

Le sujet qui nous intéresse dans ce stage est indirectement lié à la « batch » stéganographie et « pooled » stéganalyse. Nous nous intéresserons à l'algorithme ASO [Kouider2012_ASO], [Kouider2012_ASOf]. Cet algorithme peut être envisagé pour effectuer de la « batch » stéganographie, mais pour le moment aucune démonstration ou expérimentation n'a montré qu'il permettrait d'obtenir un bon niveau de sécurité.

Dans un premier temps, nous nous intéresserons à rendre l'algorithme ASO plus simple. Nous simplifierons l'oracle (utilisé dans ASO) en remplaçant *l'ensemble classifier* par un algorithme trivial. Nous utiliserons les mêmes caractéristiques que pour ASO c'est-à-dire un sous-ensemble des caractéristiques HOLMES [Fridrich2011-HOLMES]. Nous évaluerons alors expérimentalement la sécurité de l'algorithme via l'utilisation de *l'ensemble classifier* de Kodovsky [Kodovsky2012_EC] en utilisant des vecteurs caractéristiques « Rich Model » [Fridrich2012_SRM_SRMQ1].

Dans un second temps, et s'il reste du temps, nous évaluerons l'approche dans le cadre de la « batch » stéganographie / « pooled » stéganalyse. Il sera alors nécessaire de trouver une grande base d'images non compressées pour laquelle les images sont toutes de même dimension, puis on lancera le calcul des vecteurs caractéristiques, et on reprendra la méthodologie de stéganalyse par acteur, par LOF, proposée dans [Ker2012_RW] [Ker2012_LOF].

Références :

[Ker2006] A. Ker "Batch Steganography and Pooled Steganalysis", J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 265–281, 2007. Springer-Verlag Berlin Heidelberg 2007.

[Ker2011_Clustering] A. D. Ker and T. Pevný, "A New Paradigm for Steganalysis via Clustering", Media Watermarking, Security, and Forensics III, Part of IS&T/SPIE 21th Annual Symposium on Electronic Imaging, SPIE'2011, Volume 7880, San Francisco, California, USA, Feb 2011.

[Ker2012_LOF] Andrew D. Ker and Tomas Pevny "Identifying a steganographer in realistic and heterogeneous data sets" Media Watermarking, Security, and Forensics, Part of IS&T/SPIE Annual Symposium on Electronic Imaging, SPIE'2012, Volume 8303, San Francisco, California, USA, January 22, 2012.

[Ker2012_RW] A. Ker and T. Pevny, "Batch Steganography in the Real World", ACM Multimedia and Security Workshop, MM&Sec2012, Coventry, UK, September 6-7, 2012.

[Kouider2012_ASO] S. Kouider and M. Chaumont and W. Puech, "Technical Points About Adaptive Steganography by Oracle (ASO)", EUSIPCO'2012, 20th European Signal Processing Conference 2012, Bucharest, Romania, August 27 - 31, 2012. <http://www.lirmm.fr/~chaumont/Publications.html>

[Kouider2012_ASOf] S. Kouider, M. Chaumont, et W. Puech, « Stéganographie Adaptative par Oracle (ASO) », CORESA'2012, COmpression et REprésentation des Signaux Audiovisuels, Lille, France, 24-25 mai, 2012, 6 pages. <http://www.lirmm.fr/~chaumont/Publications.html>

[Fridrich2011-HOLMES] J. Fridrich, J. Kodovský, V. Holub, and M. Goljan, "Steganalysis of Content-Adaptive Steganography in Spatial Domain", 13th Information Hiding Conference, IH'2011, Prague, Czech Republic, May 18–20, 2011, LNCS, Springer-Verlag. <http://ws2.binghamton.edu/fridrich/publications.html>

[Kodovsky2012_EC] Jan Kodovský, Jessica Fridrich, Member, IEEE, and Vojtěch Holub, "Ensemble Classifiers for Steganalysis of Digital Media", IEEE Transaction on Infor Forensics and Security, vol. 7(2), pp. 432-444, 2012. <http://ws2.binghamton.edu/fridrich/publications.html>

[Fridrich2012_SRM_SRMQ1] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images", IEEE Transactions on Information Forensics and Security, 2012. http://dde.binghamton.edu/download/feature_extractors/