



Évaluation de « stéganalyseurs » de faibles complexités

Sujet M2R pour 2012-2013

Marc Chaumont & Sandra Bringay

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

Equipe ICAR et TATOO

161 rue Ada, 34392 Montpellier cedex 5 - France

Tel : +33 4.67.14.97.59

Marc.Chaumont@lirmm.fr, Sandra.Bringay@lirmm.fr

Mots clefs : Traitement d'images, Sécurité multimédia, stéganographie, 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.

Dans ce stage, l'étudiant partira d'un classifieur extrêmement simple produit par Andrew Ker et Ivans Lubenko : *l'ensemble average perceptron* [Lubenko2012_Perceptron], [Lubenko2012_Mismatched]. Ce classifieur, s'il est utilisé sur des bases d'environ un million d'images, permet d'obtenir des résultats aussi bons, voir meilleurs que les autres classifieurs de l'état-de-l'art dans le cas difficile « cover-source mismatch ». Ce cas se réfère à un scénario où les images utilisées pour l'apprentissage par le stéganalyste ne viennent pas de la même source que les images utilisées pour tester le stéganalyste. La complexité de cet algorithme est bien plus faible que les autres approches. Nous étudierons donc les propriétés de ce classifieur. Nous comparerons ses performances avec les algorithmes classiques en fouille de données et présents dans le logiciel WEKA¹. Nous comparerons ses faiblesses et avantages vis-à-vis du classifieur par ensemble de Kodovsky [Kodovsky2012_EC]. Finalement, nous chercherons à proposer des améliorations.

Dans un premier temps, l'étudiant proposera des implémentations rapides et efficaces permettant d'améliorer les performances de classification. Il expérimentera la stéganalyse sur des images n'ayant pas subi de compression et dont l'insertion a été effectuée par l'algorithme HUGO [HUGO_2010]. Il sera nécessaire de trouver une grande base d'images non compressées dont les images sont toutes de même dimension, de lancer le calcul des vecteurs caractéristiques tels que ceux issus du « Rich Model » [Fridrich2012_SRM_SRMQ1], puis de reprendre la méthodologie de stéganalyse proposée dans [Lubenko2012_Mismatched]. Ce protocole expérimental diffère de celui retenu dans [Lubenko2012_Perceptron], [Lubenko2012_Mismatched] puisque les images étaient compressées en JPEG. Ce protocole permettra de vérifier si l'on obtient de bonnes performances dans un cas plus difficile (« plus » de *cover-source mismatch*).

Dans un second temps, et s'il reste du temps, on proposera des améliorations au classifieur par ensemble comme cela a déjà été proposé dans [Chaumont2012].

¹ <http://www.cs.waikato.ac.nz/ml/weka/>

Références :

[Lubenko2012_Perceptron] I. Lubenko and A. Ker, "Going from Small to Large Data in Steganalysis", 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

[Lubenko2012_Mismatched] I. Lubenko and A. Ker, "Steganalysis with Mismatched Covers: Do Simple Classifiers Help?" ACM Multimedia and Security Workshop, MM&Sec2012, Coventry, UK, September 6-7, 2012.

[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>

[HUGO_2010] "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography", T. Pevny, T. Filler and P. Bas, 12th Information Hiding Conference, June 28 - 30, 2010, Calgary, Alberta, Canada. *Code source : Break Our Steganography System, 2010*, <http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/>.

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

[Chaumont2012] M. Chaumont and S. Kouider, "Steganalysis by Ensemble Classifiers with Boosting by Regression, and Post-Selection of Features", ICIP'2012, IEEE International Conference on Image Processing, Lake Buena Vista (suburb of Orlando), Florida, USA, September 30 - October 3, 2012.