Stégananalyse universelle
sans « source-cover mismatch »

sujet 2011-2012

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

Mots clefs : stéganographie, stéganalyse, classifieur.

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 steganographie/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 connait de l'environnement utilisé par le stéganographe.

Dans ce stage, nous allons nous intéresser au scénario que nous appelons « **stéganalyse universelle** ». Ce scénario considère que l'on ne connait pas l'algorithme de stéganographie utilisé, s'il y a insertion d'un message secret, que l'on ne connait pas le *payload* (quantité de bits insérée), mais par contre que l'on connait les « cover-source » c'est-à-dire que l'on a à disposition suffisamment d'images (sans message) du même « type » (on parle de distribution) que celles utilisées par un potentiel suspect.

Il n'y a pas pour le moment de solutions satisfaisantes pour ce scénario [Pevny2008, Pevny2011]. L'objectif du stage est d'étudier ce scénario pour être capable de gérer la nouveauté (algorithmes différents de ceux utilisés lors de l'apprentissage), ainsi que des longueurs de messages inconnus. Il faudra donc passer en version multi-classe le classifieur FLD [Kodovský2011], mettre en place le OC-NM [Pevný2008], prendre en main un ensemble d'algorithmes connus [Pevný2008] ainsi que les caractéristiques HOLMES [Fridrich2011], et mettre en place le protocole d'évaluation de la sécurité.

Références :

[Pevný2008] T. Pevný and J. Fridrich, « Novelty Detection in Blind Steganalysis », ACM Multimedia and Security Workshop, MM&Sec2008, Oxford, UK, September 22-23, pp. 167-176, 2008.

[Pevný2011] T. Pevný, « Detecting messages of unknown length », 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.

[Kodovský2011] J. Kodovský and J. Fridrich, "Steganalysis in high dimensions: fusing classifiers built on random subspaces", 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.

[Fridrich2011] 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, to appear in LNCS, Springer-Verlag.