Stégananalyse d'algorithmes +-1 embedding par classification

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, Support Vector Machine.

La compétition BOSS [BOSS 2010] se déroule du 9 septembre au 15 décembre 2010 et consiste à déterminer parmi 1000 images lesquelles contiennent un message (ce sont les images « stégo » [HUGO 2010]) et lesquelles ne contiennent pas de message (ce sont les images « cover »). Le 1 novembre, au moins une équipe a réussi à obtenir une précision dans la classification de 75%.

L'objectif du stage n'est pas de participer à la compétition (puisqu'elle sera terminée lors du stage) mais plutôt d'étudier les toutes récentes approches d'analyse (stéganalyse, attaque) permettant de classer les images en « stego / non-stego » pour les algorithmes stéganographiques de type LSB matching (+-1 embeding). Pour le moment, la classification des algorithmes stéganographiques est effectuée par analyse statistique. Un vecteur caractérisant est extrait pour chaque image et ensuite un algorithme de classification (qui a préalablement appris) classe l'image en « stego / non-stego ».

Pour ce stage, il faudra dans un premier temps prendre en main les techniques listées ci-dessous [COM 2005], [WAM 2006], [ALE 2008], [SPAM 2009], [CDF 2010] (et même d'autres), les mixer pour obtenir un vecteur encore plus caractérisant mais également proposer des nouveaux vecteurs caractérisant. D'autre part, il est nécessaire de prendre en main un « bon classifieur ». Actuellement au sein de la communauté de la stéganographie le « Support Vector Machine » est reconnu comme l'un des plus performants. Il sera peut-être nécessaire d'adapter la phase d'apprentissage du SVM pour que celui-ci puisse gérer les apprentissages sur des vecteurs caractérisant de grande dimension et sur de très grandes bases d'images. Un autre angle d'attaque est de réduire la dimension par ACP ou toute autre méthode supportant les grandes dimensions [OPAST 2000]. On pourra également transférer les algorithmes sur des super-calculateurs du centre de calcul de haute performance HPC Montpellier (http://www.hpc-project.com/) et ainsi manier plus facilement les algorithmes complexes en coût de calcul. On pourra se servir des outils de visualisation scientifique. Enfin, on pourra également envisager de tester la résistance sur d'autres algorithmes que l'algorithme Hugo [HUGO 2010] comme par exemple l'algorithme adaptive ternary LSB matching [WAM 2006] ou MPSteg [MPSteg 2006].

Références :

[BOSS 2010] Break Our Steganography System, 2010, http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/.

[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/.

[COM 2005] Center Of Mass of the adjacency histogram, "Steganalysis of LSB matching in grayscale images", A. D. Ker, IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441–444, June 2005.
Résumé: On calcule le ratio entre le centre de gravité calculé de l'histogramme d'adjacence 2D et le centre de gravité de l'histogramme de l'image sous échantillonnée. L'algorithme est référencé par l'acronyme ***2D-HCFC*** *dans [ALE 2008].*
Code source : http://www.cs.ucl.ac.uk/staff/I.Cox/Content/Downloads.html

[WAM 2006] Wavelet Absolute Moment, « New blind steganalysis and its implications". M. Goljan, J. Frodroch, T. Holotyak, In: Proceedings SPIE, EI, Security, Steganography, and Watermarking of Multimedia Contents VIII. Vol. 6072, pp. 1-13. San Jose, CA, 2006.
Résumé : Le bruit stego est estimé dans le domaine ondelette en utilisant un débruitage basé sur l'approche de Wiener. 9 moments sont calculés par sous-bande. Le vecteur caractéristique est de taille 27.

[ALE 2008] Amplitude of Local Extrema, "Detection of ±1 LSB Steganography Based on the Amplitude of Histogram Local Extrema", G. Cancelli, G. Doërr, M. Barni and I. J. Cox, in Proceedings of the IEEE International Conference on Image Processing, pp. 1288-1291, 2008.

Résumé : Le LSB matching a tendance à effectuer un filtre passe bas sur l'histogramme. Le vecteur caractéristique est donc construit par sommation des amplitudes des extremas locaux d'un histogramme 2D d'adjacence. Le vecteur caractéristique est de taille 10.
Code source : http://www.cs.ucl.ac.uk/staff/I.Cox/Content/Downloads.html

[SPAM 2009] "Steganalysis by Subtractive Pixel Adjacency Matrix" Tomáš Pevný and Patrick Bas and Jessica Fridrich, Proceeding of the 11th ACM Multimedia & Security Workshop. Pp 75-84. Princeton, NJ (September 7-8 2009.
Résumé : Des triplets de différences sont calculés. Seules les valeurs de différences comprises entre –T et T sont considérées. Classiquement T=3 et les probabilités markoviennes d'ordre 2 sont calculées. Le vecteur caractéristique est de taille 2 x 343 = 686.
Code source : http://dde.binghamton.edu/download/

[CDF 2010] Cross Domain Feature, "Modern steganalysis can detect YASS", J. Kodovský, T. Pevný, J. Fridrich, In proceedings SPIE, Electronic Imaging, Media Forensics and Security XII. San Jose, CA, 2010.
Résumé : Le vecteur caractéristique est composé des caractéristiques SPAM et de caractéristiques basées DCT.
Code source : http://dde.binghamton.edu/download/ccmerged/

[MPSteg 2006] "MPsteg: Hiding a message in the matching pursuit domain", G. Cancelli, M. Barni, G. Menegaz, In proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII. Vol.6072, p. 60720P. San Jose, CA (2006).

[OPAST 2000] Orthogonal Projection Approximation Subspace Tracking; "Fast orthogonal past algorithm ", K. Abed-Meraim, A. Chkeif, and Y. Hua. IEEE Signal Processing Letters, 7(3), March 2000.