Codes correcteurs et stéganographie adaptative

sujet M2R pour 2012-2013

Eleonora Guerrini, Anne Elisabeth Baert, Marc Chaumont
LIRMM (Laboratoire d'Informatique, de Robotique et Microélectronique de Montpellier)
Equipes DALI (ECO), MAORE, ICAR
161 rue Ada, 34392 Montpellier cedex 5 - France
Tel : +33 4.67.14.97.59
Contacts : Eleonora.Guerrini@lirmm.fr, Anne-elisabeth.Baert@lirmm.fr, Marc.Chaumont@lirmm.fr

Mots clefs : Codes correcteurs, Stéganographie, Image.

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.

Les codes correcteurs sont des outils importants pour la conception d'algorithmes pour la sténographie. Ils sont utilisés pour cacher des informations (le message secret) dans une image et également pour extraire l'information cachée à partir de l'image modifiée (F5-Hamming [Westfeld2001_F5], Modified Matrix Encoding : MME [Kim2007_MME], FastBCH [Zhang2009_BCH], [Sachnev2009_BCH], Reed-Solomon (RS) [Fontaine2009_BCH], …). Par ailleurs, depuis peu, on admet que certains endroits de l'image sont plus sujets à détection, c'est à dire plus « sensible », que d'autres [Fridrich2007_Embedding]. On modélise donc cette « sensibilité », par une valeur de *détectabilité* attribuée à chaque pixel. L'insertion du message, à travers l'utilisation d'un code [Filler2011_STC], est alors effectuée avec la contrainte de minimisation de la somme des valeurs de *détectabilité* des pixels que l'on a modifiés. Ces valeurs peuvent être binaires, comme pour les algorithmes basés sur les *wet-paper codes* [Fridrich2005], ou bien dans un intervalle réel [Pevny_HUGO_2010], [Filler_MOD2011], [Kouider2012_ASO].

Dans ce stage, on s'intéresse au cas plus réaliste où les valeurs de *détectabilité* sont dans un intervalle réel. On appelle un algorithme qui prend en compte une telle contrainte un algorithme *adaptatif* et l'on parle de stéganographie *adaptative* [HUGO_2010], [Filler_MOD2011], [Kouider2012_ASO]. Le problème d'insertion adaptative est reconnu comme un problème intéressant de la stéganographie récente. Par ailleurs, le seul code existant pour le moment est le code de [Filler2011_STC]. Les propositions récentes [Pevny_HUGO_2010], [Filler_MOD2011], [Kouider2012_ASO], s'attachent, quant à elle, à la définition des valeurs de *détectabilités* plutôt qu'à l'aspect code correcteur.

Le stage se décomposera en deux parties: une première partie de compréhension du contexte de la stéganographie et de la steganalyse, ainsi que l'analyse des codes correcteurs d'erreurs utilisés dans les algorithmes **non**-adaptatifs (F5-Hamming [Westfeld2001_F5], Modified Matrix Encoding : MME [Kim et al. 2007], FastBCH [Zhang et al. 2009], [Sachnev et al. 2009], Reed-Solomon (RS) [Fontaine and Galand 2009], …). La deuxième partie sera consacrée à l'analyse du code de [Filler2011_STC], utilisé dans les algorithmes adaptatifs, et à l'analyse de faisabilité d'adapter les codes correcteur utilisé dans les approches **non**-adaptatives pour les passer dans un mode adaptatif (éventuellement en choisissant un nouveau type de code correcteur).

Thèmes :
Les thèmes abordés dans ce travail incluent l'analyse d'algorithmes, les codes correcteurs, la stéganograhie/stéganalyse.

Objectif(s) du stage : Le but du stage est de concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, de les analyser et de les évaluer pour des problèmes de stéganographie/stéganalyse.

Travail demandé :
Le stage se développera en plusieurs parties :
1- Comprendre le contexte de la stéganographie et de la steganalyse,
2- Etudier et classer les codes correcteurs utilisés dans les approches non-adaptatives,
3- Etudier et analyser le code de [Filler2011_STC] ainsi que son exploitation dans [Pevny_HUGO_2010].
4- Adapter ou/et transformer les codes des versions non-adaptatives pour produire des algorithmes adaptatifs. Analyser et étudier leurs performances.

Références :

[Westfeld2001_F5] Westfeld, A.: F5–A Steganographic Algorithm: High Capacity Despite Better Ste-ganalysis. In: Information Hiding - 4th International Workshop. vol. 2137, pp. 289–302. Springer-Verlag, New York, Pittsburgh, PA (April 25-27 2001)

[Kim2007_MME] Y. Kim, Z. Duric, D. Richards: "Modified matrix encoding technique for minimal distortion steganography". In: Camenisch, J.L., Collberg, C.S., Johnson, N.F., Sallee, P. (eds.) IH 2006. LNCS, vol. 4437, pp. 314–327 (2007).

[Zhang2009_BCH] R. Zhang, V. Sanchev, H. J. Kim: "Fast BCH Syndrome Coding for Steganography". In: Katzenbeisser, S. and Sadeghi, A.-R (Ed.) Information Hiding 2009, IH'2009, LNCS 5806, pp. 48-58, 2009, Springer-Verlag Berlin Heidelberg 2009.

[Sachnev2009_BCH] V. Sachnev, H.J. Kim and R. Zhang: "Security Less Detectable JPEG Steganography Method Based on Heuristic Optimization and BCH Syndrome Coding", The 11th ACM Workshop on Multimedia and Security, MM&Sec'09, September 7–8, 2009, Princeton, New Jersey, USA.

[Fontaine_2009_RS] C. Fontaine and F. Galand: "How Reed-Solomon Codes Can Improve Steganographic Schemes", Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2009, Article ID 274845, 10 pages doi:10.1155/2009/274845.

[Pevny_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/.*

[Filler_MOD2011] T. Filler and J. Fridrich, "Design of Adaptive Steganographic Schemes for Digital Images," in Media Watermarking, Security, and Forensics XIII, part of IS&T SPIE Electronic Imaging Symposium, San Francisco, CA, January 23-26 2011, vol. 7880, paper. 13, pp. F 1–14.

[Fridrich2005] J. Fridrich, M. Goljan, and D. Soukal. "Efficient wet paper codes". In M. Barni, editor, Proceedings, Information Hiding, 7th International Workshop, IH 2005, Barcelona, Spain, June 6–8, 2005, LNCS. Springer, Berlin, 2006.

[Fridrich2007_Embedding] Jessica J. Fridrich and Tomas Filler, "Practical Methods for Minimizing Embedding Impact in Steganography," in Security, Steganography, and Watermarking of Multimedia Contents IX, part of IS&T SPIE Electronic Imaging Symposium, San Jose, CA, January 29-February 1 2007, vol. 6505, pp. 02–03.
Principle of minimizing the embedding impact was proposed in 2007 [Fridrich2007]. It is based on the adaptivity of the embedding operation by the use of a detectability map.

[Filler2011_STC] T. Filler, J. Judas, and J. Fridrich, "Minimizing Additive Distortion in Steganography using Syndrome-Trellis Codes" *IEEE Trans. on Info. Forensics and Security*, vol. 6(1), pp. 920–935, 2011.

[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