Problèmes d'optimisation en Stéganographie adaptative

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

Mots clefs : Modélisation probabiliste, Algorithmes, Stéganographie, Sécurité, Théorie des jeux.

Contexte :

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 utilisés pour cacher des informations (le message secret) dans une image, mais 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]. Lorsque les valeurs de *détectabilité* sont dans un intervalle réel, les algorithmes sont appelés *adaptatifs* [HUGO_2010], [Filler_MOD2011], [Kouider2012_ASO]. La stéganograhie *adaptative* est reconnu comme un problème intéressant de la stéganographie récente. 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 modèle de stéganographie adaptative est intéressant car l'insertion est effectuée en cherchant à optimiser une fonction de coût (la détectabilité) [Filler2011_STC]. Par contre, dans cette approche (cette stratégie), l'insertion ne prend pas en compte la stratégie retenue par le stéganographe pour effectuer sa stéganalyse. La stratégie de chacun des participants peut être modélisée par la *théorie des jeux*, qui est une méthode de modélisation idéale lorsqu'il faut prendre en compte deux (voire plusieurs) opposants qui doivent adapter leurs stratégies en fonction d'hypothèses sur le comportement des participants du jeu. De manière générale, les participants veulent maximiser leur gain ou minimiser leurs pertes dans cette compétition, et *l'équilibre de Nash* [vanDamme1991_Nash] permet d'obtenir une stabilité stratégique, i.e., aucun des participants au jeu ne peut changer sa stratégie sans affaiblir sa position personnelle. Dans un contexte de stéganographie/stéganalyse, les différents participants au jeu sont Nature, la stéganographe Eve, le Juge, et la stéganalyste Alice [Ettinger1998_SGE]. Dans [Schottle_GTA_2012], les auteurs développent la première méthode rigoureuse basée sur la théorie des jeux pour adapter l'insertion dans un contexte de sténographie adaptative. Une stratégie optimale de jeu est ainsi développée avec de fortes hypothèses sur le modèle : utilisation d'un modèle LSB (Least Significant Bit), utilisation d'une image à deux pixels, insertion d'un et d'un seul bit, etc.

Thèmes :
Les thèmes abordés dans ce travail de thèse incluent la modélisation probabiliste, la théorie des jeux, la stéganograhie/stéganalyse.

Travail demandé :
Le sujet de cette thèse consiste à travailler sur les problèmes d'optimalité en stéganographie adaptative. Dans ce sujet, l'étudiant devra analyser les différents liens entre la carte de détectabilité (et sa fonction de cût) et les stratégies en théorie des jeux. Il s'agira donc de proposer sur différents modèles de stéganographie, des stratégies, fonctions des valeurs de détectabilité et basées sur la Théorie des jeux. Ces stratégies devront également être évaluées et couvrir entre autres : des modèles plus ou moins hétérogènes, des cas d'insertions de bits en mode +-1, des insertions de plus de 1 bit, etc.

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.

[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.

[Ettinger1998_SGE] Ettinger, J. Mark , « Steganalysis and Game Equilibria », In : PetitColas, F.A.P.(ed) LNCS, vol.1525, pp319- 328. Springer, Heidelberg (1998).

[Schottle2012_GTA] P. Schöttle and R. Böhme, "A Game-Theoretic Approach to Content-Adaptive Steganography," in Information Hiding, Berkeley, California, **May 15-18, 2012**, vol. 6958 of Lecture Notes in Computer Science, IH'2012, Springer.

[vanDamme1991_Nash] Eric Van Damme « Stability and Perfection of Nash Equilibria, » Springer-Verlag, 1991 - 339 pages

[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