La stéganographie moderne : l'art de communication secrète

Marc Chaumont & William Puech
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
William.Puech@lirmm.fr

Mots clefs : stéganographie dans des images jpeg, codes détecteurs et correcteurs d'erreurs, codes BCH et Reed-Solomon.

L'idée du *codage matriciel* (en anglais : « Matrix encoding ») a été introduite en stéganographie par Cranddall [Crandall 1998] en 1998. La première implémentation a ensuite été proposée par Westfeld avec l'algorithme de stéganographie F5 [Westfeld 2001]. L'objectif est de transmettre un message au sein d'une image via la modification de l'image, mais avec la contrainte de minimiser le nombre de coefficients de l'image modifiés. Plus précisément, le *codage matriciel* consiste à détourner l'utilisation classique des codes détecteurs et correcteurs d'erreur en bloc. L'idée consiste du côté décodeur (c'est-à-dire à la réception de l'image) à calculer les syndromes de chaque bloc de coefficients à partir de la matrice de contrôle du code correcteur. Le syndrome correspond au message qui est contenu dans l'image. Toute l'astuce consiste donc, du côté codeur (c'est-à-dire à l'émission de l'image), à modifier l'image de sorte que les syndromes calculés au décodeur représentent le message et également de sorte que l'image soit le moins modifiée.

Pour aller un peu plus loin que la méthode appelée Modified Matrix Encoding : MME [Kim et al. 2007], qui est apparu après F5 et est plus performante, nous étudierons la stéganographie basée sur le code correcteur BCH : FastBCH [Zhang et al. 2009], [Sachnev et al. 2009]. S'il reste du temps, nous étudierons le codage RS : Reed-Solomon [Fontaine and Galand 2009] et le codage ZZW [Zhang et al. 2008]. Les codes BCH et RS possèdent une efficacité d'insertion $e = \frac{\textit{nombre de bits du message}}{\textit{nombre de coefficients modifiés}}$ meilleure que celle du code de Hamming utilisé dans F5, pour un même nombre de bits insérés. Pour avoir une première idée sur la sécurité des méthodes, nous évaluerons la sécurité en comparant F5 et/ou MME et/ou PQe+PQt [Fridrich et al. 2007] et FastBCH (et s'il reste du temps RS et ZZW) avec le « classifieur » de l'état de l'art de Pevny et Fridrich [Pevny and Fridrich 2007] ou bien en utilisant la méthode proposée dans [Pevny and Fridrich 2008]. Nous regarderons également la sécurité de telles approches aux méthodes de détection comme celle de [Pevny et al. 2009] ou bien de détection ciblées.

[Crandall 1998] R. Crandall: Some notes on steganography, Posted on Steganography Mailing List (1998), http://os.inf.tu-dresden.de/~westfeld/crandall.pdf.

[Westfeld 2001] A. Westfeld: "High capacity despite better steganalysis (F5 – a steganographic algorithm)". In: Moskowitz, I.S. (ed.) IH 2001. LNCS, vol. 2137, pp. 289–302. Springer, Heidelberg (2001).

[Kim et al. 2007] 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. Springer, Heidelberg (2007).

[Zhang et al. 2009] 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.

[Sachnev et al. 2009] 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.

[Zhang et al. 2008] W. Zhang, X. Zhang, and S. Wang. "Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes". In K. Solanki, K. Sullivan, and U. Madhow, editors, *Information Hiding, 10th International Workshop*, Lecture Notes in Computer Science, pages 60–71, Santa Barbara, CA, June 19–21, 2008. Springer-Verlag, New York.

[Fridrich et al. 2007] Fridrich, Pevny, T., Kodovsky, J.: Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities. In: Dittmann, J., Fridrich, J. (eds.) Proceedings of the 9th ACM Multimedia & Security Workshop, Dallas, TX, September 20–21, pp. 3–14 (2007).

[Pevny and Fridrich 2007] Pevny, T., Fridrich, J.: Merging Markov and DCT features for multi-class JPEG steganalysis. In: Delp, E.J., Wong, P.W. (eds.) Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, January 29 – February 1, vol. 6505, pp. 3-1–3-14 (2007).

[Pevny and Fridrich 2008] Pevny, T., Fridrich, J.: Benchmarking for Steganography In : K. Solanki, K. Sullivan, and U. Madhow (Eds.): Proceeding International Hiding IH'2008, LNCS 5284, pp. 251–267, Springer-Verlag Berlin Heidelberg 2008.

[Fontaine and Galand 2009] 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 et al. 2009] T. Pevny, P. Bas and J. Fridrich, Steganalysis by Subtractive Pixel Adjacency Matrix, Proc. ACM Multimedia and Security Workshop, Princeton, NJ, September 7–8, pp. 75–84, 2009.