Sujet stage M2R : “steganographie robuste”

Marc CHAUMONT, Lionel PIBRE (?), Dino IENCO (?), ...
LIRMM (Laboratoire d’Informatique, de Robotique et de Microélectronique de Montpellier)

Mots clef: Informatique, Technologies de l'information, Traitement des images, Sécurité multimédia, Codes, Stéganographie/Stéganalyse.

Le modèle de stéganographie couramment utilisé est celui proposé par Simmons en 1983 [Simmons 83]. Ce modèle considère que deux prisonniers enfermés dans des cellules séparées ont l’autorisation d’échanger des lettres sous la surveillance d’un gardien. Le gardien (la stéganalyste) essaye de déterminer si les prisonniers planifient une évasion. Le gardien peut analyser les lettres, modifier les lettres, falsifier frauduleusement les lettres. Les prisonniers (les stéganalyseurs) vont essayer de transmettre un message secret, à travers l’échange des lettres. Ce modèle présente trois types de comportements de la part du gardien : le comportement passif où le gardien ne modifie pas le support de communication, le comportement actif où le support est altéré, et le comportement malicieux où le gardien réussit à communiquer sur le canal secret.

Actuellement, la majeure partie des algorithmes de stéganographie par modification du support de couverture considèrent uniquement le scénario d’un gardien passif. Ainsi, un gardien prévoyant (un gardien actif) peut, dans la majeure partie des cas, empêcher que la communication secrète ait lieu, simplement en modifiant légèrement le support anodin échangé entre les deux prisonniers. Si le support de couverture est une image et que l’algorithme stéganographique est un algorithme par modification du support alors le gardien peut, par exemple, changer le format de compression et également réencoder l’image avec un facteur de quantification légèrement plus grand. Dans ce scénario, aucun algorithme de stéganographie ne pourra assurer de communication secrète.

Actuellement, le modèle de gardien actif est définis, mais il y a très peu de travaux sur le sujet. La stéganographie à gardien actif - appelé stéganographie robuste - se rapproche des problématiques du tatouage robuste puisque le message doit résister à une dégradation du support. Par exemple, certains schémas de tatouage comme le natural watermarking [Bas et al. 06] essayent de préserver un modèle de distribution. Le modèle de distribution est bien entendu trop simpliste pour résister à la stéganalyse actuelle, mais l’idée de préserver, ou aller vers un modèle, tout en utilisant des codes différents de ce que l’on utilise en stéganographie à gardien passif est prometteuse. Il est possible que cet axe de recherche puisse faire se rejoindre la discipline du tatouage et celle de la stéganographie.

Bibliographie:

[Simmons83] G. J. Simmons, “The prisoners problem and the subliminal channel,” in Advances in Cryptography, CRYPTO, Aug. 1983, pp. 51–67.