

Sujet d'impact :

Apprentissage de Modèles de Markov Cachés, estimation de clés secrètes en stéganalyse

La stéganographie est l'art de cacher de l'information dans des contenus quelconques (images, sons, vidéos, ...), la stéganalyse est l'art de détecter l'information cachée. Les méthodes de stéganographie réputées comme étant indétectables [1,2] utilisent une méthode de codage faisant appel à des modèles de Markov cachés (HMM pour "Hidden Markov Model") afin de maximiser la capacité d'insertion. Ces méthodes partent du principe que les paramètres de ce HMM sont secrets, ce qui signifie que si un adversaire arrive à estimer ces paramètres, il est alors capable d'avoir accès au message inséré.

L'objectif de cet impact sera d'utiliser les algorithmes de la littérature permettant d'apprendre le HMM à partir d'une ou de plusieurs observations (ici des images stéganographiées). L'étudiant devra dans un premier temps étudier l'algorithme de Baum-Welch [3] puis dans un second temps l'adapter à l'insertion proposée dans [2] qui présente des matrices de transitions périodiques. En fonction des paramètres du HMM, il cherchera notamment à calculer la quantité d'information minimale afin de pouvoir accéder de manière précise au secret.

Références:

- [1] : T. Pevny, T. Filler, and P. Bas. Using high-dimensional image models to perform highly undetectable steganography. In Information Hiding 2010, 2010.
- [2] : T. Filler, J. Judas, and J. Fridrich. Minimizing additive distortion in steganography using syndrome-trellis codes. Information Forensics and Security, IEEE Transactions on, 6(3) :920–935, 2011.
- [3] : http://en.wikipedia.org/wiki/Baum-Welch_algorithm

Contact:

Patrick Bas

Chercheur CNRS au LAGIS

patrick.bas@ec-lille.fr