

Présentation publique de Marc Chaumont (équipe ICAR - <http://www.lirmm.fr/~chaumont/>)
"Stéganographie par Deep Learning"
Le lundi 9/03/2020 à 14h dans la salle des séminaires.

Cette présentation s'effectue dans le cadre des réunions du CIEL et est ouverte à tous les membres du laboratoire.

Titre : **Stéganographie par Deep Learning**

Résumé :

Depuis plus de 2000 ans, la stéganographie est utilisée pour communiquer secrètement. Deux protagonistes souhaitant se transmettre des informations, sans éveiller les soupçons, vont dissimuler un message dans un support/objet qu'ils vont s'échanger. La stéganographie est donc l'art de d'intégrer un message de manière imperceptible dans un support/objet pour le transmettre de manière secrète alors que la stéganalyse est l'art de déceler la présence ou l'absence de ce message dans le support/objet.

La stéganographie/stéganalyse peut donc être modélisée comme un jeu à trois participants. Les stéganographes, classiquement appelés Alice (l'émetteur) et Bob (le récepteur), souhaitent envoyer un message, dont l'existence même n'est connue que d'eux seul. La stéganalyste, généralement appelé Eve, observe les échanges des supports/objets qui ont lieu entre Alice et Bob et cherche à déterminer si Alice et Bob communiquent.

Cette discipline dans sa version moderne, c'est-à-dire numérique, a débuté au début des années 2000. Entre les années 2000 et 2015, la stéganographie est passée par une phase de recherche sur les codes (théorie des codes correcteurs), puis sur la proposition d'algorithmes « adaptatifs », permettant la dissimulation de messages avec la prise en compte la nature statistique du « support » numérique. La stéganalyse a, quant à elle, évolué vers des approches utilisant le Machine Learning. A noter que cette discipline est également souvent abordée d'un point de vue traitement du signal, modélisation statistique, test d'hypothèses et théorie du jeu. Bref, on peut faire du très théorique ou du très pratique. Depuis 2015, l'arrivée du Deep Learning a permis d'aller vers des scénarios de stéganographie et de stéganalyse plus complexes et plus réalistes.

Dans cette présentation, nous rappellerons le contexte lié à cette discipline, nous définirons la problématique dans le cas où le support est une image numérique puis nous présenterons quatre familles de stéganographie par Deep Learning. Enfin, nous présenterons une approche récente mettant en compétition trois réseaux Deep Learning (extension de la notion de GAN) simulant un jeu à trois joueurs et dont l'objectif est d'obtenir en même temps un réseau utilisable pour l'insertion efficace (c.à.d. non perceptible) d'un message dans une image et un réseau utilisable pour l'extraction de ce même message.