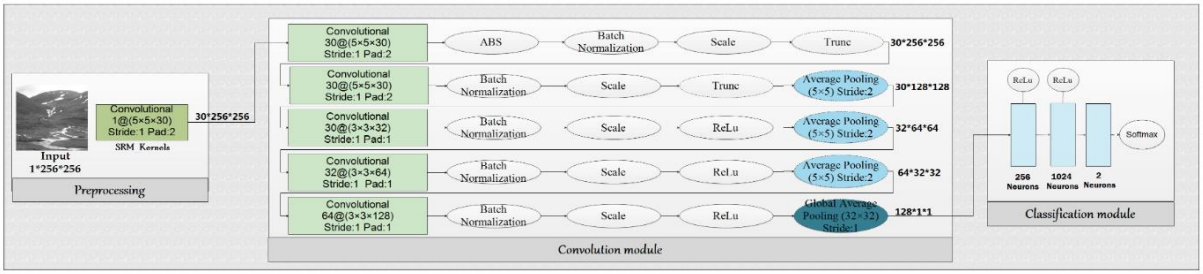
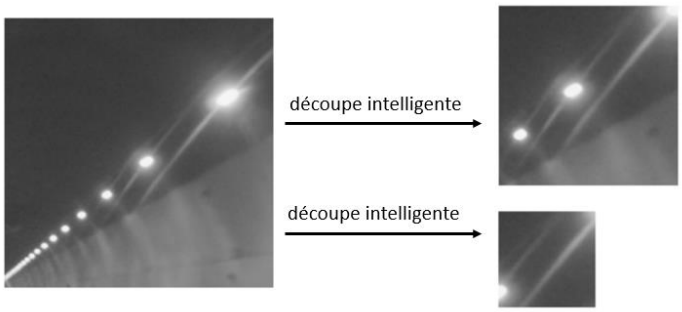
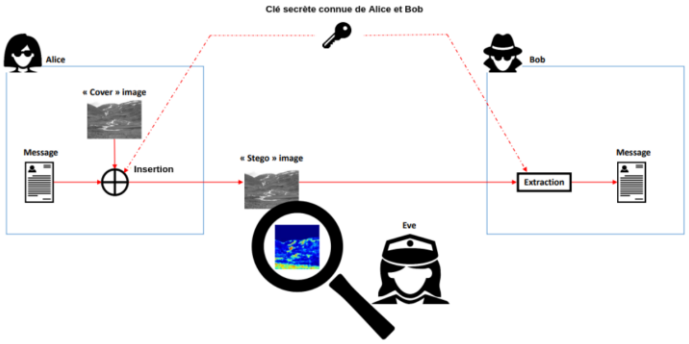


Base NNID (pseudo – gigognes)





Stage : " Vers une invariance en performance de la stéganalyse d'images de dimensions quelconques par deep learning "

Marc CHAUMONT, Fréderic COMBY, Kevin PLANOLLES
LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier)
Equipe ICAR, 161 rue Ada, 34392 Montpellier cedex 5 - France
Tel : +33 4.67.14.97.59, Marc.Chaumont@lirmm.fr

Mots clefs : Traitement d'images, Stéganographie, Stéganalyse, Machine Learning, Deep Learning.

La stéganographie / stéganalyse peut être expliquée comme un jeu à trois participants. Les stéganographes classiquement appelés Alice et Bob, souhaitent envoyer un message, en le dissimulant dans un support « anodin » (cela sera une image pour ce qui nous concerne). La stéganalyste, généralement appelé Eve, observe les échanges qui ont lieu entre Alice et Bob et cherche à déterminer si Alice et Bob communiquent [Simmons83]. La stéganographie est donc l'art de dissimuler un message dans un support pour le transmettre de manière secrète, et la stéganalyse est l'art de déceler la présence de ce message. Cette discipline dans sa version moderne, c'est-à-dire numérique, a débuté au début des années 2000.

> *Remarque : Pour bien faire, le message doit être compressé (sans perte) puis chiffré. Il y a alors autant de 0 que de 1 (on a alors une entropie maximale), et ceux-ci sont considéré comme aléatoirement répartis. Le message en lui-même peut être tout et n'importe quoi. On peut donc envisager d'avoir du texte, de l'audio, de la vidéo, une image, du code (code d'un virus par exemple), etc. Alice et Bob peuvent être (souvent) des humains, mais cela peut également être des programmes.*

La stéganalyse dite « de laboratoire », « clairvoyante », ou « pire attaque », est effectuée le plus souvent en reprenant les principes de [Kerckhoffs 1883] utilisés en cryptographie. La stéganalyste a donc une connaissance de tous les paramètres publics ainsi qu'une bonne approximation de la distribution des supports « anodin » utilisés par Alice et Bob. Or, dans la "vrai vie", Eve, la stéganalyste, n'a pas accès à toutes ces informations, et en particulier a une connaissance très mauvaise de la distribution des supports « anodins » utilisés par Alice et Bob.

Dans le cadre de ce stage, nous souhaitons aborder cette stéganalyse dite "real life" / "real world" / "into the wild" [Ker et al. 2013 - Real World] et cela par deep learning [Chaumont 2020].

Plus exactement, nous souhaitons étudier le cas où Eve n'a pas de connaissance concernant la dimension des images utilisées par Alice et Bob. Peu de propositions ont été faites pour rendre invariant un réseau de neurones profonds (deep learning) dans le cadre de la stéganalyse. On peut distinguer deux familles (non-invariant, mais pouvant prendre en entrée des images de dimensions quelconques):

- La première famille est constituée des approches calculant une unique moyenne avant le bloc de classification. On trouve dans cette famille les réseaux utilisant le principe de « *global average pooling* » : ***Yedroudj-Net*** [Yedroudj et al. 2018 - Yedroudj-Net], ***GBRASNet*** [Tabares et al. 2021], ***CC-Net*** [Fu et al. 2022]. On trouve également ***ZhuNet*** [Zhang et al. 2020 – ZhuNet] utilisant un « *spatial pyramid pooling layer* » en fin de réseau. Enfin, on trouve des approches un peu plus exotiques comme ***Convolutional Vision Transformer*** [Luo et al. 2022] et ***EWNet*** [Su et al. 2021]

- La deuxième famille est constituée des approches calculant en plus de la moyenne, les moments statistiques suivants : minimum, maximum, et variance. On trouve dans cette famille le réseau ***SID*** (Size Independant Detector) [Fuji-Tsang and Fridrich 2018 – SID] et le réseau siamois ***SiaSteg*** [You et al. 2020 - SiaStegNet] qui utilise, en plus du réseau SID, la notion de « *contrastive loss* ».

Nous avons observé [Planolles et al. 2023] sur quelques architectures que l'invariance en performance n'était pas atteinte sur la base NNID, même en utilisant un apprentissage sur base mixe (utilisation de toutes les dimensions). L'objectif du stage consiste à poursuivre l'étudie et en particulier à proposer des modifications au sein des architectures de deep learning pour imposer plus d'invariance en performance. On pourra également évaluer le réseau sur des images non vues lors de l'apprentissage, tester des architectures non évaluées dans [Planolles et al. 2023], générer d'autres bases, proposer d'autres solutions s'inspirant de la littérature comme [Noord and Postma 2017 – Scale], [Jansson and Lindeberg 2020 – UnseenScale], etc.

Pour mener à bien ce sujet, il est préférable d'avoir certaines connaissances : en traitement des images, et/ou en classification/fouille de données, et/ou en architecture des machines/installation d'OS. Il est également intéressant d'avoir de bonnes bases en programmation et en math.

Profil recherché : Master (M2) ou Ecole d'Ingénieur (3ème année) ayant une bonne maitrise de la programmation (C++, Python…), des connaissances en fouille de données / indexation / classification, traitement des images, sécurité.

Encadrement : Marc CHAUMONT (Enseignant Chercheur), Fréderic COMBY (Enseignant Chercheur), Kevin PLANOLLES (doctorant).

Modalité de candidature : Envoyez un CV, une lettre de motivation ainsi que votre relevé de notes de M1 le plus tôt possible. Après pré-sélection des candidatures, des entretiens téléphoniques ou en personne seront planifiés.

Contacts : Marc Chaumont (*marc.chaumont@lirmm.fr*)

Lieu du stage : LIRMM, équipe ICAR.

Période du stage : févier-mars 2023 à juin-juillet 2023 (5-6 mois).
Gratification de stage : plus de 550€ mois.

Bibliographie:

[Planolles et al. 2023] Titre à préciser « INVARIANCE IN SECURITY… », en cours de soumission, Kevin Planolles, Marc Chaumont, Frédéric Comby.

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

[Kerckhoffs 1883] Kerckhoffs, A. (1883). La cryptographie militaire. Journal des sciences militaires, IX(3):5–83. Cité page 39.

[Ker et al. 2013 - Real World] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevny. Moving steganography and steganalysis from the laboratory into the real world. In Proc. 1st ACM workshop on Inf. hiding and multimedia security (IH&MMSec), Montpellier, France, pages 45–58, June 17-19, 2013.

[Chaumont 2020] Marc Chaumont, "Deep Learning in steganography and steganalysis", Elsevier Book chapter. Book title: "Digital Media Steganography 1st Edition: Principles, Algorithms, and Advances", Book Editor: M. Hassaballah. ISBN: 9780128194386. Chapter 14. pp. 321-349. Published Date: 1st July 2020. (ArXiv longer version ; 46 pages). Seen more than 296 times on ResearchGate the 23th of December 2019. https://arxiv.org/abs/1904.01444. Associated video talk.mp4. Slides seen more than 600 times on ResearchGate the 23th of December 2019.

[You et al. 2020 - SiaStegNet] W. You, H. Zhang and X. Zhao, "A Siamese CNN for Image Steganalysis," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 291-306, 2021, doi: 10.1109/TIFS.2020.3013204. https://ieeexplore.ieee.org/document/9153041

[Fuji-Tsang and Fridrich 2018 – SID] C. Fuji-Tsang and Jessica Fridrich « Steganalyzing Images of Arbitrary Size with CNNs », , Proc. IS&T, Electronic Imaging, Media Watermarking, Security, and Forensics 2018, San Francisco, CA, January 29–February 1, 2018. http://www.ws.binghamton.edu/fridrich/Research/Scale-1.12.16.pdf

[Zhang et al. 2020 – ZhuNet] R. Zhang, F. Zhu, J. Liu and G. Liu, "Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis » in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1138-1150, 2020, https://ieeexplore.ieee.org/document/8809687

[Yedroudj et al. 2018 - Yedroudj-Net] Mehdi Yedroudj, Frédéric Comby, and Marc Chaumont, " Yedrouj-Net: An efficient CNN for spatial steganalysis ", IEEE International Conference on Acoustics, Speech and Signal Processing, **ICASSP'2018**, 15–20 April 2018, Calgary, Alberta, Canada, 5 pages. pdf, poster. FAQ and parameters for Yedroudj-Net are given here: Yedroudj-Net.

[Noord and Postma 2017 – Scale] Nanne van Noord, Eric Postma, "Learning scale-variant and scale-invariant features for deep image classification", Pattern Recognition, Volume 61, 2017, Pages 583-592, ISSN 0031-3203, https://www.sciencedirect.com/science/article/pii/S0031320316301224

[Jansson and Lindeberg 2020 – UnseenScale] Jansson and Lindeberg, "Exploring the ability of CNNs to generalise to previously unseen scales over wide scale ranges", *Proc. International Conference on Pattern Recognition (ICPR 2020)*, to appear, preprint at arXiv:2004.01536.

[Tabares et al. 2021] Tabares-Soto Reinel, Arteaga-Arteaga Harold Brayan, BravoOrtiz Mario Alejandro, Mora-Rubio Alejandro, AriasGarzon Daniel, Alzate-Grisales Jesus Alejandro, Burbano-Jacome Alejandro Buenaventura, Orozco-Arias Simon, Isaza Gustavo, and Ramos-Pollan Raul, "Gbras-net: A convolutional neural network architecture for spatial image steganalysis," *IEEE Access*, vol. 9, pp. 14340–14350, 2021.

[Fu et al. 2022] Tong Fu, Liquan Chen, Zhangjie Fu, Kunliang Yu, and Yu Wang, "CCNet: CNN model with channel attention and convolutional pooling mechanism for spatial image steganalysis," *Journal of Visual Communication and Image Representation*, vol. 88, pp. 103633, 2022.

[Su et al. 2021] Ante Su, Xianfeng Zhao, and Xiaolei He, "Arbitrary-SizedJPEG Steganalysis Based on Fully Convolutional Network,"in *Proceedings of International Workshop on Digital-forensics and Watermarking, IWDW'2021*, Berlin, Heidelberg, Nov.2021, p. 197–211, Springer-Verlag.