Stage : " Etude de l'invariance à la dimension / résolution des images lors de la stéganalyse par deep learning "

Marc CHAUMONT, Frederic COMBY, Mohamed BENKHETTOU
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 publiques 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/résolution des images utilisées par Alice et Bob. Peu de propositions ont été faites pour rendre invariant un reseau réseaux de neurones profonds (deep learning) dans le cadre de la stéganalyse :

- Le réseau siamois ***SiaSteg*** [You et al. 2020 - SiaStegNet] utilisant la notion de « *contrastive loss* ».

- Le réseau ***SID*** (Size Independant Detector) [Fuji-Tsang and Fridrich 2018 – SID] dont l'esprit est aujourd'hui assez classique. Il utilise le principe de « *global average pooling* » et de calcul de moments statistiques.

- Le réseau ***ZhuNet*** [Zhang et al. 2020 – ZhuNet] utilisant un « *spatial pyramid pooling layer* » en fin de réseau, et qui est un des successeurs du réseau Yedroudj-Net [Yedroudj et al. 2018 - Yedroudj-Net] que nous avons développé au sein de l'équipe, et qui lui aussi avait une structure lui permettant de manipuler des images de différentes résolution. Récement des améliorations ont été proposé pour ce réseau comme dans [Ahn et al. 2020]

On pourra éventuellement ré-implémenter tous ou une partie des réseaux mentionnées ci-dessus, en utilisant le réseau **EfficientNet** [Tan and Le 2019 – EfficientNet] avec de légères modifications. Ce réseau a été utilisé avec succès lors de la compétition Kaggle de l'été 2020 [Cogranne et al. 2020 – Alaska2], [Yousfi et al. 2020 – Alaka2], [Chubachi et al. 2020 – Alaksa2], et a donné de très bonnes performances.

Une étude de l'état de l'art provenant de la communauté deep learning est également à faire [Noord and Postma 2017 – Scale], [Jansson and Lindeberg 2020 – UnseenScale], etc. On note en particulier que dans le récent papier de [Jansson and Lindeberg 2020 – UnseenScale], les auteurs essayent d'aller plus loin qu'un apprentissage capable de faire face à des dimensions/résolutions observées lors de l'apprentissage, et cherchent a proposer une solution permettant de traiter des images dont les dimensions/résolutions n'ont pas été observées lors de l'apprentissage.

Une étude préliminaire, réalisée via l'encadrement d'un stage de M2R, a permis de mieux cerner le sujet et également de construire une base de données d'images multi-dimension où les images les plus grandes sont découpées (i.e. « crop ») plusieurs fois à différentes dimensions (2042x2042, 1024x1024, 512x512, 256x256). Pour une grande image, on obtient un tuple d'images à plusieurs dimensions (2042x2042, 1024x1024, 512x512, 256x256) et l'on impose une « sécurité empirique » similaire pour ce tuple d'images. Cette construction est à rapprocher d'études comme [Giboulot and Fridrich 2019] qui cherchent à conserver la distribution des coefficients de détectabilité (= coût) entre les dimensions. Par ailleurs, nous imposons d'insérer un nombre de bit fonction de la dimension [Kodovsky et al. 2008] afin d'observer plus facilement le phénomène d'invariance à la dimension.

L'objectif du stage consiste donc à étudier/analyser, en pratique (évaluation, modification, et proposition), l'existence ou non d'une invariance dans le cas d'une base multi-dimension, mais aussi d'une base multi-résolution, mais aussi de proposer une solution s'il n'y a pas d'invariance.

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), Frederic COMBY (Enseignant Chercheur), Mohamed BENKHETTOU (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 2022 à juin-juillet 2022 (5-6 mois).

Gratification de stage : plus de 550€ mois.

Bibliographie:

[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

[Ahn et al. 2020] W. Ahn, H. Jang, S. Nam, I. Yu and H. Lee, "Local-Source Enhanced Residual Network for Steganalysis of Digital Images," in *IEEE Access*, vol. 8, pp. 137789-137798, 2020, doi: 10.1109/ACCESS.2020.3011752. https://ieeexplore.ieee.org/abstract/document/9146867 **Date of Publication:** 24 July 2020

[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.

[Cogranne et al. 2020 – Alaska2] R. Cogranne, Q. Giboulot, and P. Bas, “Challenge Academic Research on Steganalysis with Realistic Images,” in Proceedings of the IEEE International Workshop on Information Forensics and Security,
WIFS’2020, Virtual Conference due to covid (Formerly New-York, NY, USA), Dec. 2020.

[Yousfi et al. 2020 – Alaka2] Y. Yousfi, J. Butora, E. Khvedchenya, and J. Fridrich, “ImageNet Pretrained CNNs for JPEG Steganalysis,” in Proceedings of the IEEE International Workshop on Information Forensics and Security, WIFS’2020, Virtual Conference due to covid (Formerly New-York, NY, USA), Dec. 2020.

[Chubachi et al. 2020 – Alaksa2] K. Chubachi, “An Ensemble Model using CNNs on Different Domains for ALASKA2 Image Steganalysis,” in Proceedings of the IEEE International Workshop on Information Forensics and Security, WIFS’2020, Virtual Conference due to covid (Formerly New-York, NY, USA), Dec.2020

[Tan and Le 2019 – EfficientNet] M. Tan and Q. Le, “EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks,” in *Proceedings of the 36th International Conference on Machine Learning, PMLR’2019*, vol. 97, Long Beach, California, USA, Jun. 2019, pp. 6105–6114. http://proceedings.mlr.press/v97/tan19a/tan19a.pdf

[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.

[Kodovsky et al. 2008] Jan Kodovsky Andrew D. Ker Tomas Pevny et Jessica Fridrich. « The Square Root Law of Steganographic Capacity ». In : Proc. 10th Workshop on Multimedia and Security pp.107-116 (2008).

[Giboulot and Fridrich 2019] Payload Scaling for Adaptive Steganography: An Empirical Study, Q. Giboulot and J. Fridrich, IEEE SPL 26(9), 1339–1343 July 2019. http://www.ws.binghamton.edu/fridrich/Research/SPL_SRL-07.21.pdf