Summer Research Internship position

On Mutual Information Neural Estimation (MINE) for information leakage estimation

Context and research statement

Mutual Information (MI) was the key information measures introduced by Shannon in 1948, in order to quaitify the quantity of information exchanged between two random processes (here termed operands). Subsequent applications of the mutual information between two random processes ranged from the dimensioning of communication rates on noisy channel links, to the performance assessment of lossy compression algorithms, the estimation of the information leakage in secure communications, the identification of coding and non-coding areas of DNA/RNA strings, the design of statistical learning algorithms through the information bottleneck problem, and many other disciplines which can hardly be summarized.

However, the evaluation of MI following the classical by-the-book formulation is untractable when one of the operands (random data) lies in a high-dimensional space as it requires an exponential number of operations (in the dimension of the data). This intractability is further amplified when one of the operands of the MI lies in a continuous space. Thus, except for a few cases of marginal interest, there exist no universal algorithm for mutual information evaluation with a reasonable complexity (non-exponential) for highly dimensional (possibly) continuous spaces.

To leverage this exponential complexity, many attempts were made in the litterature in order to find practical MI evaluation algorithms. The first approaches consisted in exploiting existing structures in the random processes to reduce the number of operations needed (markov chains [1], MAP-decoder approach [2]), however these solutions do not apply to any type of data. Another family of solutions consists in estimating lower bounds or upper bounds on the MI which do not require an exponential number of operations [3], however these remain mainly as approximation and would not be of interest in the case for instance of information leakage estimation. A third family of approaches consisted in a variational formulation of the MI which transforms the problem of MI evaluation into finding the optimum of a specific optimization problem. Based on the latter approach, the Mutual Information Neural Estimator (MINE) was introduced in [4] showing accurate estimates even in the case of arbitrary data. Many applications of MINE followed both in the traditional Machine Learning related problems (image classification, computed vision, natural language processing, ...) and as well in communication enginering.

In this project, we wish to investigate the application of MINE to a secure communication system, namely, the wiretap communication system, in order to evaluate the information leakage estimation at an undesired eavesdropper. The project will be organized as follows. First a comprehensive state of the art on neural network based MI estimation (MINE) will be conducted, then

a practical implementation of MINE on Tensorflow (Keras) will be developped on synthetic data. Finally, the resulting algorithm will be tested on a USRP-based practical bench for the wiretap channel, and compared to the team's previous contribution on MI estimation.

References

[1] D. Arnold, H.-A. Loeliger, P. Vontobel, A. Kavcic, and W. Zeng, "Simulation-based computation of information rates for channels with memory," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3498–3508, 2006.

[2] K. Taleb and M. Benammar, "On the information leakage of finite block-length wiretap polar codes," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 61–65.

[3] L. Paninski, "Estimation of entropy and mutual information," *Neural computation*, vol. 15, no. 6, pp. 1191–1253, 2003.

[4] M. I. Belghazi, A. Baratin, S. Rajeshwar, S. Ozair, Y. Bengio, A. Courville, and D. Hjelm, "Mutual information neural estimation," in *Proceedings of the 35th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, J. Dy and A. Krause, Eds., vol. 80. PMLR, 10–15 Jul 2018, pp. 531–540. [Online]. Available: https://proceedings.mlr.press/v80/belghazi18a.html

Candidate profile and application

Applicants should be last-year research master (or/and engineer) students. A strong background in applied mathmatics, probabilities and statistics, and machine learning is required. Good communication skills in English are necessary (written and oral), as well as good development skills (Python, Matlab). Applications from candidates familiar with digital communications, information theory or error correction coding are particularly encouraged.

Applications (CV, cover letter) are to be addressed to {`meryem.benammar`}`@isae-supaero.fr`

About

The internship will take place in the Communication and Information Theory (ComIT) team of the Department of Electronics Optronics and Signal processing (DEOS) of ISAE-SUPAERO. The physical layer security USRP bench on which the results will be implements is deployed in the Télécommunication lab (07.139).

- A gratification of around 540 eur/month
- Dates and duration: between June and September 2023 (2 months).
- **Application deadline: open until April 25th, 2023**.