Internship Proposal : Implementation of Deep-Learning Based Restoration and Interpretation Methods for Electro-Magnetic Intercepted Images

Supervisors :

- Florian Lemarchand, PhD Student
- Maxime Pelcat, Associate Professor HDR

Keywords : Deep Learning, Image Processing, Image Restoration

Context

All electronic devices produce electro-magnetic (EM) emanations that not only interfere with radio devices but also compromise the data handled by the information system. A third party may perform a side-channel analysis and recover the original information, hence compromising the system privacy. Such attack performed on the screen of an information system allow an attacker to reconstruct the displayed signal from tens of meters (see Figure 1). For information systems processing sensitive data, it is important to audit the risk of compromising. The work conducted on these attacks in our team aims to enhance these audits.

When retrieving visual information from an EM signal, an important part of the original information is lost through the leakage and interception

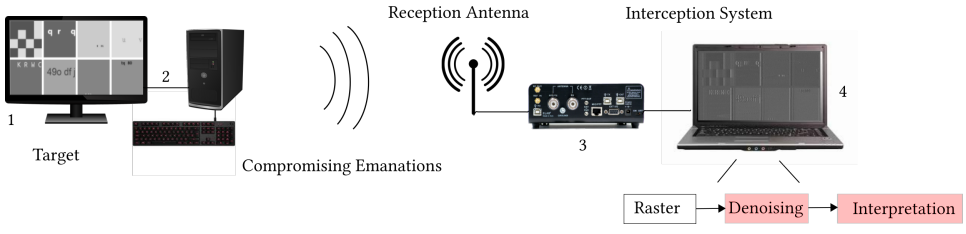

Figure 1: Interception system setup: the attacked system includes a screen (1) displaying sensitive information. It is connected to an information system (2). An interception chain (3) sends samples to a host computer (4) that implements signal processing to reconstruct and interpret the information.

(a)

(b)

Figure 2: A reference image given to the semantic segmantation and classification framework Mask-RCNN (a). The han is detected as bird and relatively well segmented. The intercepted counterpart of the reference image (b). Nothing is detected by the Mask-RCNN instance.

process. This loss leads to a drop of the signal to noise ratio (SNR) and a deterioration of spatial coherence into the reconstructed images, making it difficult to interpret (See example of Figure 2).

Deep learning algorithms have recently revolutionized most signal processing problems. These algorithms build from data have an extreme ability to fit complex problems. Different trained models exist that solve image denoising and restoration problems. These models are mainly designed for well-behaved known noise models like additive white Gaussian noise (AWGN). Thus, they do not adapt well to other noise models like the one generated by the EM interception.

The VAADER team from IETR (Institut d'Electronique et de Télécommunications de Rennes) holds an expertise in image processing and embedded low energy processing. This internship will act as a support for the PhD thesis of Florian Lemarchand on image restoration in a context of images intercepted from side channel signals. The objectives of the internship are thus closely related to research objectives and will aim at obtaining novel image restoration methods.

The candidate will be provided the chance to follow the seminars and scientific animations of the VAADER team to discover state of the art works in signal processing and embedded systems.

Task

The objective of the internship is to study novel methods to improve image restoration and interpretation in the context of intercepted data. The missions will include:

- constructing a representative database of intercepted images,
- modeling the interception noise,
- developing denoising deep learning algorithm to restore and interpret images,
- evaluating and benchmarking the different solutions with respect to the state of the art.

Requirement

The candidate is expected to be a master student with background in image processing and deep learning.

Python language and previous experiences with learning frameworks like PyTorch or Tensorflow are required, C++ is a plus.

Employment Details

- Application Procedure : Resume and motivation letter addressed to the undermentioned contact
- Start : February - August 2021
- Duration : 6 months
- Location : IETR CNRS 6164, VAADER Team, INSA Rennes, 20 avenue des buttes de Coësmes, 35700 Rennes
- Salary : About 550 € per month
- Contacts : florian.lemarchand[at]insa-rennes.fr