PhD Position at Institut Polytechnique de Paris (October 1st, 2021)

Neural Network Watermarking for Mobile Multi-Media Applications

Supervisors

Mihai Mitrea (mihai.mitrea@telecom-sudparis.eu), Marco Cagnazzo (marco.cagnazzo@telecom-paris.fr), Attilio Fiandrotti (attilio.fiandrotti@telecom-paris.fr)

Topic

The goal of this PhD thesis is to propose a methodological framework for NN watermarking via regulation. To this end, the PhD student will incrementally fulfill the following main steps: (1) in-depth study the state of the art references, (2) elaborate the information theory model for the problem, (3) express the generic watermarking transparency and robustness properties as applicative constraints, (4) design and implement a watermarking procedure for the NN considered for video encoding; (5) carry out an experimental study in terms of robustness (Pmd and Pfa), transparency (impact in the encoded video quality) and data payload (length in bits of the information which can be inserted/extracted). The results are expected to contribute to international standardization activities (MPEG, MPAI).

Study of the state-of-the-art references

The PhD student will gather in-depth knowledge in the fields of watermarking and neural networks for video coding applications; he/she will also become a general informed reader on topics related to energy efficiency and hardware implementation

Elaborate the information theory model for the problem

The watermarking applications are modeled as a side-information noisy channel, where the watermark is a sample from the information source, the original content a Gaussian noise source known at the encoder and the attacks an unknown (potentially Gaussian) noise source. Yet, for the case of the NN watermarking, modeling the two noise sources becomes very abstract and requires a fine statistical investigation of the ergodicity/stationarity behavior of these noise sources.

Express the generic watermarking transparency and robustness properties as applicative constraints

This step will provide some formal representation (in the form of some constraint functions) for the property the watermarking application should feature, and namely transparency (imperceptibility) and robustness (the ability to identify modified NN structures).

Design and implement a watermarking procedure for the NN considered for video encoding

The work here will consider the joint optimization between the NN simplification (e.g. pruning) and watermarking insertion. The starting point is given by the NN simplification algorithm and an additional block will be added for guiding the mark insertion according to the above-obtained transparency and robustness constraint functions. The energy effectiveness will be also considered here as a constraint function.

Carry out an experimental study in terms of robustness, transparency and data payload

The experimental study will be carried out at two levels: (1) laboratory conditions and (2) industrial conditions cross-checking. These two levels of experimental work will be carried out in a real testbed based on FPGA+ ARM processors.

Hosting team

The thesis will be conducted at Institut Polytechnique de Paris (France), at the ARTEMIS (Telecom SudParis) and LTCI (Telecom Paris) departments.

The PhD student will visit (3-6 months) the EIDOS team of Università di Torino (Italy).

A tight industrial partnership is already established with ATEME (France) and SISVEL (Italy).

Candidate profile

Theoretical: information theory, random processes, video coding (concepts, basic tools, standards), neural network principles

Programming: C/C++/C#, Python

Languages: English (professional usage) and French (basic notions)