Open PhD position on
the investigation of AI-based authentication detector for physical object security

Keywords:

Similarity metric learning, anomaly detection, copy detection pattern, physical object authentication

Context of the study

Due to the development and the broad availability of high-quality printing and scanning devices, the number of forged or counterfeited products and documents is dramatically increasing. One of the most promising and cheap solutions to prevent it is the use of Copy Detection Patterns (CDP) [1]. A CDP is a maximum entropy image, generated using a secret key or password, that takes full advantage of information loss principle during Printing-and-Digitalization (PD) process.

CDP based anti-counterfeiting solutions are successfully commercialized by several leading French and Swiss companies. However, recent work [2,8] have shown the vulnerability of such anti-counterfeiting solutions to deep learning-based attacks. These attacks helped to identify the drawbacks in the current authentication systems and raised up the following challenges:

1) the current falsification detectors are very sensitive to the digitization process, requiring high-resolution cameras or a flat-bed scanner to work accurately.
2) the large variability of manufacturing chains (variability of printer technologies, paper substrates, etc.), and the variability of fake techniques make the authentication detector less reliable: as we need to find a trade-off between the acceptance of a few fakes as authentic copies and the rejection of originals acquired with lower resolution.

Thus, it becomes necessary to develop authentication metrics that provides a better trade-off between both the false-negative and the false-positive rates in future detectors.

This PhD thesis is a part of ANR project *TRUSTIT: Theoretical and practical study of physical object security in real world use cases* that aims to construct a **robust authentication detector** using a smartphone camera for **physical object security.**

Hypothesis and approach of the PhD project

The security of CDP is based on the difficulty to reverse operation of PD process (i.e., to estimate the original code from its printed version). Nevertheless, the advances of deep learning techniques have made possible to reverse the PD process [2,3,4].

That is why, it is urgent to develop novel metrics [7] or machine learning models able to differentiate the estimated codes from the original unclonable codes. It was shown that in the case of supervised classification (when all possible fakes are known in the moment of training), the classical machine learning techniques can easily detect all the fakes. Nevertheless, when the fakes are unknown during the training stage or while the fakes are printed using the same device as the authentic samples, the current detectors are incapable of separating the originals from fakes. The recent work [8] presents the first tentative to consider the PD process and to detect the anomalies in the printable unclonable code. However, the current model cannot perfectly imitate the PD process and thus the anomalies were searched only in the pixels that are correctly imitated by the PD model (41-43% of code). In addition, current anomaly detectors are dependent to the training dataset (i.e., on the printer and acquisition device used). The work in [5] tried to address the modeling of printing and digitization process using image processing and the physics of specific production systems. Nevertheless, due to the stochastic nature of PD process, these models are individual for each pair of printing and digitization devices.

This PhD project aims to develop a robust AI-based authentication detector for CDP by studying similarity metric learning approaches [6] and forensic techniques. The PhD student will investigate how to combine forensic features with recent deep neural networks and train them to be robust against estimation attacks [2,3,4]. The student will be also encouraged to follow the best practices of reproducible research to share his/her advances with the research community.

Required profile:

- The candidate must get M.S. degree or Engineer diploma (that corresponds to Bac+5 in France) in Computer Science.
- Programming languages: Python.
- Libraries for image analysis and processing: OpenCV, scikit-image (Python).
- Machine learning frameworks: scikit-learn, Pytorch.
- Scientific knowledge: image and signal processing, machine learning and deep learning. Knowledge in multimedia security will be considered a plus.
- Languages: French or English.

Place:

The PhD thesis will be held in LIRIS (Laboratoire d’Informatique en Image et Systèmes d’information) laboratory, campus of Université Lumière Lyon 2, Bron.

Contact information:

E-mail: iuliia.tkachenko@liris.cnrs.fr, carlos.crispim-junior@liris.cnrs.fr and bertrand.kerautret@liris.cnrs.fr

Please provide your CV, the motivation letter, and the transcripts with your marks for the last two years of studies.

References

[1] J. Picard, “Digital authentication with copy-detection patterns”, Electronic Imaging 2004, pages 176–183, International Society for Optics and Photonics, 2004.

[2] R. Yadav, I. Tkachenko, A. Trémeau, T. Fournel, “Copy Sensitive Graphical Code Estimation: Physical vs Numerical Resolution”, IEEE WIFS 2019, December 2019, Delft, Netherlands.

[3] R. Chaban, O. Taran, J. Tutt, T. Holotyak, S. Bonev, and S. Voloshynovskiy, “Machine learning attack on copy detection patterns: are 1x1 patterns cloneable?”, IEEE WIFS, December 2021, Montpellier, France.

[4] E. Khermaza, I. Tkachenko, J. Picard, “Can Copy Detection Patterns be copied? Evaluating the performance of attacks and highlighting the role of the detector”, IEEE WIFS 2021, December 2021, Montpellier, France.

[5] Y. Belousov, B. Pulfer, R. Chaban, J. Tutt, O. Taran, T. Holotyak, S. Voloshynovskiy, “Digital twins of physical printing-imaging channel”, IEEE WIFS 2022.

[6] S. Duffner et al., “Similarity Metric Learning”, Multi-faceted Deep Learning – Models and Data, 2021.

[7] H. Zeghidi, C. Crispim-Junior, I. Tkachenko, “CDP-Sim: Similarity metric learning to identify the fake Copy Detection Patterns”, IEEE WIFS 2023, December 2023, Nuremberg, Germany.

[8] B. Pulfer, Y. Belousov, J. Tutt, R. Chaban, O. Taran, T. Holotyak, S. Voloshynovskiy, “Anomaly localization for copy detection patterns through print estimations”, IEEE WIFS 2022.