# Post-doctoral position on the investigation of AI-based authentication for physical object security in the real-world scenario


## Keywords:

Anomaly detection, diffusion model, smartphone acquisition device, 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 dependent to the acquisition device used.

2) The datasets collected in laboratories lack from realism [4, 5] (i.e. the collected images are not captured in a non-controlled setup by smartphones).

Thus, this post-doctoral research will be dedicated to the design and development of novel AI-based authentication detectors usable in real-world use case. This research 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 post-doctoral research project

The smartphone camera is a mainstream device nowadays. Therefore, it is natural to consider it for physical object authentication. Nevertheless, the current authentication systems are sensitive to acquisition setup conditions and require sometimes additional equipment as magnifying glass. Therefore, the use of smartphone camera for authentication is still an open question to the academic and industrial communities.

In this post-doctoral research, we want to consider the real-world use cases for CDP authentication. For this we will: 1) construct a public dataset of real-world samples using smartphone camera, 2) improve the image quality of real-world samples and 3) design and develop an AI-based anomaly detector that consider the conditions of real-world use case.

The printable unclonable codes captured using smartphone camera will differ a lot from those digitized using flat-bad scanners [5]. Therefore, we need to identify the pre-processing operations or design the AI-based systems that will consider the real-world use case for physical object authentication.

The focus of the research will be on designing and developing an anomaly detector, that outperform the recently proposed CDP detectors [6,7] in the real-world use case. We plan to explore the possibility to improve the anomaly detector by considering the collected real-

world images or by using the techniques of random data-augmentation [3]. The main goal is to make a novel anomaly detector less sensitive to capturing process impacts.

## Required profile:

- The candidate must get PhD degree 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 and duration:

This position is open for 18 months research period. The post-doctoral researcher will be affected to LIRIS (Laboratoire d'Informatique en Image et Systèmes d'information) laboratory in campus of Université Lumière Lyon 2, Bron.

## Contact information:

E-mail: iuliia.tkachenko@liris.cnrs.fr and Carlos.Crispim-Junior@liris.cnrs.fr
Please provide your CV, the motivation letter, and 2 recommendation letters.

## 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] Y. Lu et al., "A novel framework for assessment of learning-based detectors in realistic conditions with application to deepfake detection", arXiv:2203.11797..
[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] R. Chaban, B. Pulfer, and S. Voloshynovskiy. "Assessing the Viability of Synthetic Physical Copy Detection Patterns on Different Imaging Systems", IEEE WIFS 2024.
[6] B. Atoki, I. Tkachenko, B. Kerautret, C. Crispim-Junior, "Diffusion-Based Authentication of Copy Detection Patterns: A Multimodal Framework with Printer Signature Conditioning", WACV 2026, March 2026, Tucson, USA.
[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.