Internship proposal

Diffusion models to create challenging graphical code counterfeits

Keywords: Diffusion model, image processing, printed graphical code

Context of the study

The nowadays challenges are the fast, reliable, and cheap detection of faked packaging and documents. Due to development and broad availability of high-quality printing and scanning devices, the number of forged or counterfeited products and documents is dramatically increasing. Therefore, different security elements have been designed to prevent this socio-economic plague. One of the most promising and cheap solutions 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-scanning process. Such an unpredictable pattern is highly sensitive to distortions occurring inevitably during production (printing), verification (scanning) and reproduction (duplication) processes. Counterfeiting a printed CDP requires scanning then re-printing that increases image degradations. Initially, the detection of counterfeited CDP was devoted to evaluating the level of information loss. However, the security of CDP based authentication system was shown to be vulnerable to neural network estimation attacks [3,4] which attempted to infer the CDP after scanning and before re-printing to fool the detector. During this internship we will work on construction of novel public dataset and on estimation attacks using stable diffusion: to study the limits of existing CDP detectors and to create the competitive counterfeits of CDP for further research.

This internship is a part of ANR project *TRUSTIT: Theoretical and practical study of physical object security in real world use cases* that aims to explore the potential offered by deep learning methods in the context of secure printing from the verifier's point of view.

Description of the subject

The existing public CDP datasets [3,4] contain the CDP images and its counterfeits created via some estimation attacks. These datasets were created in the laboratory conditions and do not reflect the real-world case of CDP use. Additionally, the estimation methods used do not consider the recent advances in the field of generative neural networks and probabilistic latent diffusion models [2]. During this internship we will work on construction of more challenging CDP dataset and estimation attacks to reverse the distortions added by Printing-and-Digitalization (PD) process to create a more challenging CDP counterfeits.

The main tasks of this internship are:

1) To create a challenging real-world CDP dataset using the set of pre-defined printers and scanners, as well as smartphones.
2) To create a counterfeited CDPs using SOTA methods [3,4].
3) To propose an estimation attack based on probabilistic diffusion model to create a more challenging CDP counterfeits.
4) To compare the proposed estimated samples with existing counterfeit samples [3,4].

5) To add estimated CDP (SOTA and challenging CDP counterfeits) for real-world CDP dataset and if possible, to publish the results in the international conference or scientific journal.

Required profile

- The candidate must currently be enrolled in a Master 1 or Master 2 program or in the final year of engineering school (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: signal processing, image analysis, machine learning and deep learning.
- Knowledge on multimedia security will be considered a plus.
- Languages: French or English.

Place and allowance of internship

The internship will be held in LIRIS (Laboratoire d'Informatique en Image et Systèmes d'information) laboratory, campus of Université Lumière Lyon 2, Bron. Internship allowance is 4.5 euros per hour.

Contact information

E-mail: iuliia.tkachenko@liris.cnrs.fr and Carlos.Crispim-Junior@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. In Electronic Imaging 2004, pages 176–183. International Society for Optics and Photonics, 2004.
[2] 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.
[3] 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.
[4] R. Chaban, O. Taran, J. Tutt, T. Holotyak, S. Bonev, S. Voloshynovskiy, "Machine learning attack on copy detection patterns: are 1x1 patterns cloneable?", WIFS 2021, December 2021, Montpellier, France.