UNIVERSITÉ BOURGOGNE EUROPE

école doctorale **sciences pour l'ingénieur et microtechniques** SPIM

Titre de la thèse/Thesis title : GAN-Based Cryptosystem for High Level Data Protection

Laboratoire d'accueil / Host Laboratory : ImViA Laboratory, CORES team, 21078, Dijon, France

Spécialité du doctorat préparé/Speciality : Instrumentation et informatique de l'image

Mots-clefs / Keywords : Cryptosystem, Generative Adversarial Networks (GANs), Deep-fakes, Images, FPGA, Python, C++.

Descriptif détaillé de la thèse / Job description

Abstract :

Detecting and safeguarding against malicious deep-fakes while ensuring means to protect private data through secure cryptographic algorithms have become very challenging tasks since the advent of AI in the field of cybersecurity. The aim of this doctoral thesis project is to propose relevant solutions to improve and strengthen the security of digital data, whether it be text, images, or videos by combining the fields of AI/deep learning, cryptography, cryptanalysis, chaotic systems, and FPGA programmable circuits. The approach proposed here is subdivided into two main steps:

1) Utilizing advanced artificial intelligence and machine learning techniques to detect deep-fakes in images or videos that may be manipulated using advanced techniques such as AI. Initially, the idea would be to generate datasets of fake images with high resolution. Then, we use FPGA devices to implement, accelerate, and ensure real-time processing.

2) Employing cryptography and cryptanalysis methods to enhance data protection. This work will involve designing attack techniques based on GANs (AI attacks) to potentially highlight security weaknesses in the existing systems. Finally, designing GAN countermeasures to make the security of the proposed systems robust against attacks. The thesis work will be oriented to FPGA-based design and implementation.

Project description:

The integration of AI technologies within cybersecurity frameworks has revolutionized the approach to safeguarding digital assets, enabling proactive threat detection, behavioral analysis, and predictive analytics to anticipate and counter potential attacks before they manifest.

However, while the integration of AI in cybersecurity has heralded significant advancements in threat detection and response capabilities, it has also engendered new challenges and vulnerabilities. One such challenge arises from the malicious exploitation of AI technologies by threat actors to orchestrate sophisticated cyber-attacks, circumvent traditional defense mechanisms, and perpetrate acts of cyber espionage, sabotage, and fraud [Chen 2019, Liao 2021]. The emergence of deep-fake technology exemplifies this trend, wherein adversaries employ AI algorithms to generate hyper-realistic counterfeit content, including forged audio recordings, images, and videos, for deceptive purposes such as disinformation campaigns, social engineering, and identity theft. In addition to the proliferation of deep-fakes, the convergence of AI and cryptography has introduced new dimensions of complexity and vulnerability to cybersecurity ecosystems [Zhu2020, Gomez 2018]. While AI-powered cryptographic solutions hold promise for enhancing data security and privacy, they also present new avenues for adversarial exploitation and cryptographic attacks [Pan 2023]. Adversaries have leveraged AI algorithms to enhance the efficiency and efficacy of cryptanalysis techniques, enabling them to circumvent encryption protocols, decipher sensitive information, and compromise encrypted communications channels. Generative Adversarial Networks (GANs) have emerged as particularly potent tools for cryptanalysis, demonstrating the capability to breach cryptographic defenses and extract confidential information from encrypted data streams [Liu 2021, Lin 2022]. To address the multifaceted challenges posed by the integration of AI in cybersecurity, researchers are exploring innovative approaches to bolster digital defenses and enhance the resilience of critical infrastructure against emerging cyber threats [Min 2024, P. Singh 2024, M. Singh]. One such approach involves

the utilization of Field-Programmable Gate Arrays (FPGAs) as hardware-accelerated platforms for implementing AI-driven cybersecurity solutions. FPGAs offer unparalleled flexibility, performance, and energy efficiency, making them well-suited for real-time threat detection, cryptographic operations, and data processing tasks. The integration of AI, cryptography, and FPGA technology represents a paradigm shift in the field of cybersecurity, offering a potent arsenal of tools and techniques for defending against emerging cyber threats and safeguarding the integrity, confidentiality, and availability of digital assets. The expected doctoral thesis work can be divided into 4 main tasks:

1) Design and train a GAN-based cryptosystem to cryptanalyses the standard cryptographic algorithms (AES, ZUC, Chaotic systems, etc.) to detect existing weaknesses facing the new IA-based cybersecurity attacks.

2) Design a GAN that can generate high-resolution deep-fake images to create a useful, dataset.

3) Design and implement a new GANs-based cryptographic algorithm able to resist modern IA-based attacks by considering the results of steps 1 and 2.

4) Optimize and FPGA implement the proposed IA-based cryptosystem to achieve real-time requirements.

Références bibliographiques / Bibliography

- [Lin 2022] Lin Z, Shi Y, Xue Z. Idsgan: Generative adversarial networks for attack generation against intrusion detection. In Advances in Knowledge Discovery and Data Mining: 26th Pacific-Asia Conference, PAKDD 2022, Chengdu, China, May 16–19, 2022.
- [Liao 2021] Liao MH, Zheng SS, Pan SX, Lu DJ, He WQ et al. Deep-learning-based ciphertext-only attack on optical double random phase encryption. Opto-Electron Adv 4, 200016 (2021). doi: 10.29026/oea.2021.200016
- [Liu 2021] Xiaodong Liu, Tong Li, Runzi Zhang, Di Wu, Yongheng Liu, Zhen Yang, "A GAN and Feature Selection-Based Oversampling Technique for Intrusion Detection", Security and Communication Networks, vol. 2021, Article ID 9947059, 15 pages, 2021. https://doi.org/10.1155/2021/9947059
- [Zhu 2020] Zhu, J., Park, T., Isola, P., & Efros, A. A. (2017). Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks. ArXiv. /abs/1703.10593
- [Chen 2019] Chen He, Kan Ming, Yongwei Wang, Z. Jane Wang, A Deep Learning Based Attack for The Chaos-based Image Encryption, 2019, https://doi.org/10.48550/arXiv.1907.12245
- [Gomez 2018] Gomez, A. N., Huang, S., Zhang, I., Li, B. M., Osama, M., & Kaiser, L. (2018). Unsupervised Cipher Cracking Using Discrete GANs. ArXiv. /abs/1801.04883
- [Pan 2023] Ke Pan, Maoguo Gong, Yuan Gao, Privacy-enhanced generative adversarial network with adaptive noise allocation, Knowledge-Based Systems, Volume 272, 2023, 110576, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2023.110576.
- [Min 2024] Min Li. (2024). Application of GAN-Based Data Encryption Technology in Computer Communication System,Informatice, Vol 48, No 15 (2024). doi.org/10.31449/inf.v48i15.6390
- [P. Singh 2024] Singh P, Dutta S, Pranav P. Optimizing GANs for Cryptography: The Role and Impact of Activation Functions in Neural Layers Assessing the Cryptographic Strength. *Applied Sciences*. 2024; 14(6):2379. https://doi.org/10.3390/app14062379
- [M. Singh 2024] M. Singh, N. Baranwal, K. N. Singh and A. K. Singh, "Using GAN-Based Encryption to Secure Digital Images With Reconstruction Through Customized Super Resolution Network," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3977-3984, Feb. 2024, doi: 10.1109/TCE.2023.3285626.

Profil demandé / Applicant profile

Applicants must hold a Master's degree in Advanced Electronic Systems Engineering, Electrical engineering, Embedded systems, or Computer Science. We are looking for a highly motivated and enthusiastic student with good knowledge in the following fields: Deep Learning skills, Configurable architectures, FPGA; VHDL, C++, and Python programming.

The PhD thesis will be driven by the ImVia laboratory located in Dijon (France).

Preferred selection criteria:
- Academic Qualifications: A solid background in Cryptography, Deep Learning and Python programming
- Familiarity with GPUs & FPGAs
- References and Recommendations
- Written & oral communication Skills: The candidate should be capable of writing research papers and able to present their research clearly and effectively in English, whether in conferences, seminars, etc.

Personal characteristics:
- Independence and project management skills
- Motivation and Career Goals
- Teamwork and Collaboration
- Free from any other professional commitment during registration for the thesis until the defense

Financement : MESRI Etablissement

Application to be submitted by: Apply no later than May 15, 2025.

Contract start date: October 1, 2025
Gross monthly salary: € 2200 (from January 1, 2026: € 2300 gross)

Direction de la thèse:/ **Thesis Supervisor**
Supervisor : El-Bay Bourennane (Professor); ebourenn@ube.fr

Encadrement de la thèse : **co-directeur(s) et co-encadrant(s)**
Co-encadrant : Mahdi Madani (Docteur); mahdi.madani@ube.fr

Applicants are invited to submit their application to the PhD supervisors.
Application must contain the following documents:
- CV
- Cover letter
- At least 1 reference letter
- Master marks and ranking