Math-STIC Workshop - 28 June 2022
Biometrics and Visual Cryptography : Theory and Applications

Venue: Université Sorbonne Paris Nord, France

- **Hybrid mode**: **Amphi Fermat**, Institut Galilée, USPN

Technical program

08:45 - 09:00	**Welcome & Opening** – **A. Beghdadi**
	SESSION 1 – Amphi Fermat Chair : **Azeddine Beghdadi**
09:00 - 09:40	Visual content watermarking: between information theory and deep learning by **Mihai Mitrea**, Telecom Sud-Paris, France
09:40 - 10:20	Finite Field Elliptic Curve for Key Generation and Biometric Template Protection by **Kiran Raja**, NTNU, Norway
10:20 - 10: 50	Coffee Break
	SESSION 2 – Amphi Fermat Chair : **Mounir Kaaniche**
10: 50 - 11:30	Federated Adversarial Training with Transformers by **Wassim Hamidouche**, INSA, Rennes, France
11:30 - 12:10	Deep Facial Diagnosis: Sense Deeper toward Genotypes and Phenotypes by **Richard Jiang**, Lancaster University, UK
12:10 - 13:50	**Lunch (F003-F004)**

	SESSION 3 – Amphi Fermat Chair : **Farid Mokrane**
14:00 - 14:40	Nonlinear Fuzzy Commitments with Kerdock Codes By **Patrick Lacharme**, Laboratoire GREYC, Ensicaen, Caen, France
14:40 - 15:20	Bridging deep learning and classical profiled side-channel attacks By **Gabriel Zaid,** Thales ITSEF, Toulouse, France
15:20 - 15:35	Coffee Break
	SESSION 4 – Amphi Fermat Chair : **Farid Mokrane**
15 :35-16 :15	Privacy and security of shared data by **Ashref Aloui ,**LAGA Université Paris 8
16:15 - 16:55	Imaging for Forensics and Security: From Theory to Practice By Ahmed Bouridane, University of Sharjah, UAE,
16:55 -17:45	**Panel discussion : Moderators : M. Mihai & A. Beghdadi**

Abstracts

Mihai Mitrea
Title: Visual content watermarking: between information theory and deep learning
Abstract:

Image/video watermarking emerged some two decades ago as a cross-disciplinary research field, combining principles from information theory, image processing and human visual perception. This way, the mark to be inserted stands for a message to be transmitted through an abstract channel where the original content itself and the attacks represent the noise sources; the emitter power is drastically limited by the human visual system sensitivity. Hence, both theoretical and methodological attempts have been made to mathematically model the information sources and the encoding constraints set to watermarking applications. Recently, the applicative performances of deep learning-based solutions imposed themselves as an opportunity to reconsider this theoretical model.

The talk presents a succinct state-of-the-art survey on achievements related to both theoretical models and deep-learning usage for video watermarking. Rather than a confrontation, it tries to identify the synergy and the complementary among these two approaches and to identify the trends, as steamed for the needs none of these two approaches is ready to solve today.

Kiran Raja

Norwegian University of Science and Technology, Norway,

Title: Finite Field Elliptic Curve for Key Generation and Biometric Template Protection
Abstract:

The need to protect biometric data has been well advised according to various regulations and standards. The most popular Bloom Filter-based template protection schemes for iris recognition directly depend on the keys to avoid linkability challenges. This talk discusses existing approaches and a new approach for generating the keys directly from the iris biometric data using chaotic maps and elliptic curves over finite fields. The application of it will be discussed for template protection scheme that can directly exploit the generated keys to provide better security using a Quarter-Rounded template encoding which employs the inter-relation of bits in the neighborhood of the iriscode.

Richard Jiang
Lancaster University, UK

Title : Deep Facial Diagnosis: Sense Deeper toward Genotypes and Phenotypes
Abstract :

In this talk, we will review the recent advances on the study of the nexus between face and genetic/medical causes, and summarize the cross-disciplinary challenges and opportunities that can be worth of further efforts from the biometric communities.

Wassim Hamidouche
INSA Rennes, France
Title: Federated Adversarial Training with Transformers
Abstract

Federated learning (FL) has emerged to enable global model training over distributed clients' data while preserving its privacy. However, the global trained model is vulnerable to the evasion attacks especially, the adversarial examples (AEs), carefully crafted samples to yield false classification. Adversarial training (AT) is found to be the most promising approach against evasion attacks and it is widely studied for convolutional neural network (CNN). Recently, vision transformers have been found to be effective in many computer vision tasks. To the best of the authors' knowledge, there is no work that studied the feasibility of AT in a FL process for vision transformers.

In this talk such feasibility is explored with different federated model aggregation methods and different vision transformer models with different tokenization and classification head techniques.

Gabriel Zaid
Thales ITSEF, Toulouse, France
Titre : Bridging deep learning and classical profiled side-channel attacks

Abstract : Over the recent years, the cryptanalysis community leveraged the potential of research on Deep Learning to enhance attacks. In particular, several studies have recently highlighted the benefits of Deep Learning based Side-Channel Attacks (DLSCA) to target real-world cryptographic implementations. While this new research area on applied cryptography provides impressive result to recover a secret key even when countermeasures are implemented (e.g. desynchronization, masking schemes), the lack of theoretical results make the construction of appropriate models a notoriously hard problem. In this talk, we propose to investigate a new research axis in order to bridge Deep Learning and Side-Channel Attacks. In particular, we explain the similarities between the generative models and the classical profiled attack (i.e. template attacks, stochastic attacks), and we develop the first DLSCA model that can be fully explained from side-channel theoretical results. This model reduces the black-box property of DL and eases the architecture design for every real-world crypto-system. Finally, a discussion is provided to define the benefits and the limitations of this new solution and a new perspective is proposed for DLSCA models.

Ashref Aloui
LAGA Université Paris 8
Titre : Privacy and security of shared data

Abstract : Nowadays, many challenges arise in privacy due to the rapid increase in the volume of sensitive data, the need to extract it from the analyzer, and to identify it when sharing in distributed systems. Typically, the Big Data field was born to take up this kind of challenge in a context where the orders of magnitude are immense. IWe are particularly interested in anonymization and security when sharing sensitive and private data. Firstly, we present a new protocol (PPDS) to preserve confidentiality in a distributed system. We are mainly focused on providing solutions to the following specific issues at the node level (e.g., a bank, but it could be other structures like a hospital) that process sensitive data :

(a) How to aggregate the records recorded in the various branches of the Bank while protecting the confidentiality of clients without the intervention of a trusted third party in the process ;
(b) How to merge data stored in separate bank branches while maintaining customer privacy.

Secondly, we improve the performance of a model regarding anonymizing sensitive data making it very difficult to identify their private users. Adequate data anonymization is indeed essential for big data analysis while preserving user privacy. Thus a company willHave the capacity to exchange and communicate the data it collects through its divisions and its network of companies and partners. All data collected, as well as cross-references created in its aggregation, remain confidential. We apply our results in the specific context of NetFlow. The approach we offer consists of an analysis method that proposes classifying identifiers according to their degree of criticality. Concretely, we introduce a risk analysis phase concerning critical user identifiers to boost the anonymization model (K-anonymity) defined by Sweeny in 2002.

Patrick Lacharme
Laboratoire GREYC, Ensicaen, Caen, France
Title : Nonlinear Fuzzy Commitments with Kerdock Codes

Abstract:

The fuzzy commitment scheme is one of the most known biometric protection systems. This scheme uses error correcting codes for the protection of fixed-length biometric data, as iriscode. Fuzzy commitment schemes are known to be vulnerable to related records attacks if a linear code is used. This talk evaluates the resistance of nonlinear fuzzy commitments against these attacks with a special focus on Kerdock codes.

Ahmed Bouridane

Title : Imaging for Forensics and Security: From Theory to Practice

Abstract :

This talk provides a detailed analysis of new imaging and pattern recognition techniques for the understanding and deployment of biometrics and forensic techniques as practical solutions to increase security. It contains a collection of the recent advances in the technology ranging from theory, design, and implementation to performance evaluation of biometric and forensic systems. This book also contains new methods such as the multiscale approach, directional filter bank, and wavelet maxima for the development of practical solutions to biometric problems.