17th IEEE International Workshop on Information Forensics & Security

Perth, WA, Australia

December 1st – 4th, 2025

IEEE WIFS 2025

17th IEEE INTERNATIONAL WORKSHOP ON INFORMATION FORENSICS & SECURITY

PERTH, WA, AUSTRALIA · 1st - 4th DECEMBER 2025

ECU EDITH COWAN UNIVERSITY

IEEE Signal Processing Society

WESTERN AUSTRALIA WALKING ON A DREAM | BUSINESS EVENTS PERTH

IEEE ComSoc IEEE Communications Society

IEEE Advancing Technology for Humanity

Table of Contents

Message from the Chairs




Greetings and a hearty welcome to the 17th IEEE International Workshop on Information Forensics & Security (IEEE WIFS) 2025, hosted at ECU, Perth, WA, Australia!

IEEE WIFS 2025 will be the 17th edition of the major annual event organised by the IEEE Information Forensics and Security Technical Committee (IFS-TC) of the IEEE Signal Processing Society (SPS). The major goal of WIFS is to bring together researchers working in the different areas of information forensics and security to discuss challenges, exchange ideas, and share state-of-the-art results and technical expertise, with the aim of building a community capable of providing adequate tools and solutions to face the challenges of tomorrow.

Ensuring the high quality and the full engagement of all the attendees, we will feature 3 distinguished keynote talks, 3 tutorials, 32 technical paper presentations, and 1 demonstration & poster session. This accomplishment is a testament to the dedication of the Steering Committee, Technical Program Committee, and, most importantly, the SPS IFS-TC community. This year, we are also celebrating the coming of IEEE WIFS to the Southern Hemisphere with a welcome drink at Joondalup Resort and a special gala dinner at Hillarys Yacht Club.

We express our heartfelt gratitude to the individuals who have contributed to the success of IEEE WIFS 2025. Special acknowledgment goes to the administrative staff and student volunteers from Edith Cowan University (ECU) for their ongoing support in ensuring the smooth operation of the conference.

Although we have a very packed and exciting program, we hope you also find time to enjoy the beautiful beaches and numerous tourist attractions in the beautiful city of Perth, the sunniest city in Australia, during your visit.

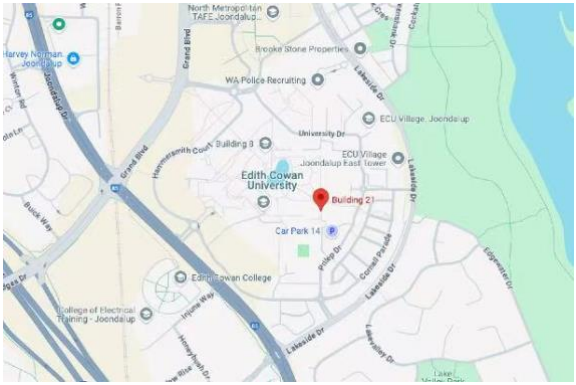
We look forward to a conference filled with enriching discussions, shared insights, and memorable experiences at IEEE WIFS 2025.

Best Regards,

Helge Janicke, Shihao Yan, Mauro Barni, and Jiande Sun

Workshop Venue

The conference will be hosted in Room 202 of Building 21 at the Joondalup Campus, Edith Cowan University (ECU).



- The campus is close to train/bus stations (walking distance about 10-15 mins).
- The centre is within walking distance to Joondalup shopping centre, where multiple restaurants and food courts are available for lunch.
- There are many cafes open on campus during the conference dates.

Schedule

Day 1 - Main Conference
(Monday 1 December 2025)

Room 202 of Building 21 at the Joondalup Campus, Edith Cowan University (ECU), WA

TIME (AWST)	SESSION
8:30-9:00	**Registrations**
9:00-10:30	**Tutorial 1:** Ms Viola Negroni & Dr Sara Mandelli **Topic:** Detecting Synthetic Speech: Pitfalls, Shortcuts and Generalisation
10:10-10:40	**Coffee Break**
11:00-12:30	**Tutorial 2:** Dr He (Henry) Chen **Topic:** RF Fingerprinting with Channel State Information: Principles, Methods, and Applications
12:30-14:00	**Lunch**
14:00-15:30	**Tutorial 3:** Dr. Elenore Ryser & Dr. Julian Broséus **Topic:** From isolated digital traces to investigative interpretation
17:00-19:00	**Welcome Reception** **Bus leaving at 4:30PM**

Day 2 - Main Conference

(Tuesday 2 December 2025)

Room 202 of Building 21 at the Joondalup Campus, Edith Cowan University (ECU), WA

TIME (AWST)	SESSION
8:30-9:00	**Registrations**
9:00-10:30	**Welcome by General Chair Prof. Helge Janicke** **Opening Speech:** **Prof. Kathryn Mcmahon, Associate Dean of Research, School of Science, ECU** **Keynote 1:** Dr Marthie Grobler **Topic:** Resilience Starts with People: Human-Centric Security for Critical Systems
10:10-10:40	**Coffee Break**
11:00-12:30	**Technical Session 1: Cyber Security Authentication.**
12:30-14:00	**Lunch**
14:00-15:30	**Technical Session 2: Physical Layer Security.**
15:30-16:00	**Coffee Break**
16:00-17:30	**Technical Session 3: Deepfake Detection**

Day 3 - Main Conference

(Wednesday 3 December 2025)

Room 202 of Building 21 at the Joondalup Campus, Edith Cowan University (ECU), WA

TIME (AWST)	SESSION
8:30-9:00	**Registrations**
9:00-10:30	**Announcements** **Keynote 2:** Prof. Stefano Tomasin **Topic:** Opportunities and challenges for physical layer security in wireless networks
10:10-10:40	**Coffee Break**
11:00-12:30	**Technical Session 4: Covert Communications.**
12:30-14:00	**Lunch Time**
14:00-15:30	**Technical Session 5: Multimedia Forensics.**
15:30-16:00	**Coffee Break**
15:30-17:00	**Demo** **Poster Session**
18:00-21:00	**Gala Dinner** **Bus leaving at 5:30PM**

Day 4 - Main Conference
(Thursday 4 December 2025)

Room 202 of Building 21 at the Joondalup Campus, Edith Cowan University (ECU), WA

TIME (AWST)	SESSION
8:30-9:10	**Registrations**
9:00-10:30	**Announcements** **Keynote 3:** Prof. Yao Zhao **Topic:** Generalised AI-Generated Image Detection: Challenges and Advances
10:10-10:40	**Coffee Break**
11:00-12:30	**Technical Session 6: Biometrics**
12:30-14:00	**Lunch**
14:00-15:30	**Technical Session 7: Information Hiding and Covert Communications**
15:30-16:00	**Coffee Break**
16:00-17:30	**Technical Session 8: AI Security and Privacy**

PLEASE NOTE: All time allocations are based on Time Zone: AWST (Australian Western Standard Time) UTC/GMT +8 hours.

Keynote Talks

E-Resilience Starts with People: Human-Centric Security for Critical Systems

Dr. Marthie Grobler
CSIRO, Australia

Abstract
As digital systems underpinning critical infrastructure grow in complexity and interdependence, ensuring their security and resilience demands more than technical robustness—it requires human-centred thinking. This talk explores how integrating behavioural insights, inclusive design, and socio-technical perspectives can enhance the trustworthiness of infrastructure systems. By framing cybersecurity as a human and societal challenge, we examine how human-centric security practices can reduce systemic risk, foster digital trust, and support resilience in the face of evolving threats. The discussion will highlight practical strategies for embedding human factors into security architectures.

Biography
Dr Marthie Grobler is a Principal Research Scientist at CSIRO's Data61, where she leads CSIRO's strategic portfolio on Critical Infrastructure Protection and Resilience. Her research focuses on strengthening the security and resilience of essential systems and services by addressing cybersecurity governance, risk mitigation, and the complex interdependencies across critical infrastructure sectors. With a strong emphasis on human factors and digital trust, Marthie's work enhances the usability and adoption of security solutions in real-world environments. She is actively involved in executive education and policy development, contributing to national efforts to build infrastructure resilience and public confidence in digital systems. Her work informs cyber policy and capability-building initiatives, helping ensure that Australia's critical infrastructure remains secure, adaptive, and interconnected in the face of evolving threats.

Opportunities And Challenges for Physical Layer Security in Wireless Networks

Prof. Stefano Tomasin
University of Padova, Italy

Abstract
As wireless communication evolves, it requires security mechanisms with diverse requirements to adequately cover an expanding attack surface. To this end, the wireless channel, which has a time-varying impulse response and random noise, can be used for security through mechanisms operating at the physical layer. Over the past decade, several solutions addressing confidentiality, authentication, and random key generation have been investigated. The time has come to assess the status of these approaches. While modern mechanisms have been shown to effectively provide security, several open research and innovation questions remain. This talk will provide an overview of the opportunities and challenges of physical-layer security and demonstrate the need to include it in future standards and devices to provide early-level protection at the lowest layer of communication networks.

Biography
Stefano Tomasin received his PhD from the University of Padua in Italy in 2003. He has been a full professor there since 2022. He was a visiting faculty member at Qualcomm in San Diego, California, in 2004; the Polytechnic University in Brooklyn, New York, in 2007; and the Mathematical and Algorithmic Sciences Laboratory of Huawei in Paris, France, in 2015. His research interests include physical layer security, the security of global navigation satellite systems, signal processing for wireless communications, synchronisation, and the scheduling of communication resources. He is a member of the IEEE and EURASIP and has been an associate editor for various journals of the two associations. He is currently an editor of the EURASIP Journal of Wireless Communications and Networking and deputy editor-in-chief of the IEEE Transactions on Information Forensics and Security.

Generalised AI-Generated Image Detection: Challenges and Advances

Prof. Yao Zhao
Beijing Jiaotong University, China

Abstract
The rapid advancements in generative AI have significantly impacted digital forensics and security, enabling the creation of highly realistic synthetic images that closely resemble authentic visuals. While these innovations present transformative opportunities for creative industries, they also introduce substantial challenges in detecting AI-generated content and preventing its misuse in misinformation campaigns and fraudulent activities. In this talk, we will highlight our recent efforts to advance AI-generated image detection, focusing on improving detection accuracy and enhancing generalisation across a range of generation methods. We will also explore the development of explainable AI-driven solutions, underscoring the urgent need for robust, scalable, and interpretable approaches to mitigate the growing threats posed by AI-generated content.

Biography
Dr Yao Zhao is a professor at Beijing Jiaotong University, the academic vice president of Taiyuan University of Science and Technology, a distinguished professor of the Yangtze River Scholar Program, a recipient of the National Science Fund for Distinguished Young Scholars, and an IEEE Fellow. He currently serves as the director of the "Science Fiction Audio and Video Intelligent Processing" Beijing Key Laboratory. His research areas include image/video compression, digital media content security, media content analysis and understanding, artificial intelligence, etc. He has presided over more than 30 projects, including the New Generation Artificial Intelligence Project and the 973 Program. He has published more than 300 papers in domestic and international journals and conferences. As the first contributor, he has won 5 provincial and ministerial awards and 1 Leading Technology Award at the World Internet Conference.

Tutorials

Detecting Synthetic Speech: Pitfalls, Shortcuts and Generalisation

Ms Viola Negroni, Dr Sara Mandelli
Politecnico di Milano

Abstract
We are witnessing a technological shift where AI is transforming not only how digital media is created, but also how people communicate, perceive authenticity, and build trust. One of the most striking advances is synthetic speech, where AI systems generate voice recordings that are almost indistinguishable from real human speech. These technologies are transforming accessibility and entertainment, from helping individuals with speech impairments to enhancing education and creative work. At the same time, while these technologies enable innovation, they also introduce serious risks. Audio deepfakes have already been used in financial fraud, identity theft, misinformation, and political manipulation, undermining trust and threatening both individuals and institutions. Nonconsensual voice cloning, in particular, presents serious risks to privacy, reputation, and personal safety. This tutorial will explore the rapidly expanding field of synthetic audio, with a particular emphasis on speech deepfake detection and the challenges it faces. We will begin by introducing the technical foundations of speech synthesis and detection, then focus on a key obstacle to reliable detection: the generalisation problem, where systems struggle to generalise beyond the datasets on which they were trained. A major, often underestimated, factor behind this issue is shortcut learning, where models depend on superficial patterns or dataset-specific artifacts instead of robust, meaningful task-related features. Through practical examples and demonstrations, we will explore the interplay between shortcut learning and generalisation in speech deepfake detection, illustrating common shortcuts exploited by detection models, discussing their impact and highlighting strategies to mitigate these issues to build more reliable systems. Attendees will gain a structured and comprehensive understanding of speech deepfake detection, including why models fail in real-world scenarios and how to design training and evaluation protocols that promote robustness and generalisation. We will also highlight the role of explainable detection methods, ensuring that synthetic audio technologies can foster innovation while minimising their potential for misuse.

Biography
Viola Negroni is a last-year PhD student at the Image and Sound Processing Laboratory (ISPL), Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milan, Italy. Her work focuses on audio forensics, with an emphasis on speech processing and deepfake detection. Her research aims to develop robust methods for identifying and countering synthetic speech, integrating signal processing and machine learning techniques. She has recently been a visiting researcher at Fraunhofer IDMT, working on a synthetic speech detection project, and will soon join the National Institute of Informatics (NII) in Tokyo for a research internship. Her work has been published at leading venues including WIFS,

ICASSP, INTERSPEECH and ICCV, reflecting her contributions to both the methodological and applied aspects of audio forensics.

Sara Mandelli received the PhD degree in information technology from the Politecnico di Milano, Milan, Italy, in 2020. She is currently an assistant professor with the Image and Sound Processing Laboratory (ISPL) at the Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano. Her research focuses on signal processing and deep learning for multimedia forensics, with emphasis on deepfake detection across image, audio, and video modalities. She is particularly interested in the interpretability of detection models and in designing robust approaches that can reliably generalise to unseen scenarios. Her work has appeared in leading conferences such as WIFS, ICIP and ICCV and top-tier journals like IEEE Transactions on Information Forensics and Security, IEEE Signal Processing Letters and IEEE Access.

RF Fingerprinting with Channel State Information: Principles, Methods, and Applications

Dr He (Henry) Chen

The Chinese University of Hong Kong

Abstract

This tutorial offers a comprehensive exploration of Channel State Information (CSI)-based RF fingerprinting, an emerging technique that leverages physical-layer signal characteristics for device authentication and security. The tutorial is structured to cover both theoretical foundations and practical applications, bridging the gap between signal processing, wireless communication, and information forensics. Attendees will first gain a deep understanding of CSI estimation in OFDM systems and how hardware-induced RF distortions become embedded in CSI measurements. We will then introduce two major design paradigms: intrinsic fingerprinting using micro-CSI and artificial fingerprint embedding via preamble modification. The tutorial will also present DeepCRF, a deep learning framework that significantly improves fingerprinting performance under noisy, dynamic channel conditions. Finally, we will discuss a novel orthogonal fingerprint embedding method that introduces artificial fingerprints directly into CSI through careful manipulation of the long training field (LTF) in Wi-Fi preambles. This approach enables robust, covert, and efficient PHY-layer authentication. The tutorial concludes with an outlook on future directions, including MIMO extensions, adversarial robustness, and applications in other wireless systems like 5G and beyond.

Biography

Dr Chen is currently an Assistant Professor in the Department of Information Engineering at The Chinese University of Hong Kong (CUHK). He received his PhD in Electrical and Information Engineering from the University of Sydney, Australia, in 2015. Before joining CUHK, he worked as a Postdoctoral Research Fellow at the University of Sydney from 2015 to 2019. His research interests include wireless physical-layer security, RF fingerprinting, wireless sensing, low-latency wireless communication, and their applications in robotics. Dr Chen has published several original works on CSI-based RF fingerprinting and PHY-layer authentication, including model-based and deep learning methods as well as artificial fingerprint embedding schemes. He has served on the editorial boards of IEEE Wireless Communications Letters, IEEE Transactions on Wireless Communications, and IEEE Transactions on Mobile Computing. He has delivered invited talks and tutorials on related topics at several academic institutions and international conferences.

From Isolated Digital Traces to Investigative Interpretation

Dr. Elenore Ryser, Dr. Julian Broséus
University of Technology Sydney

Abstract
The proposed workshop aims to bridge the gap between fragmented digital traces and the reasoning processes that might lead to investigative information. The interpretation of the information extracted from a digital device is inseparable from the context in which the trace originated, evolved, and was eventually captured. The interpretation of a digital trace depends not only on its technical properties but also on the circumstances of its creation, acquisition, and integration within an investigative process. Factors such as the acquisition method, the investigative stage, and the practitioner's prior knowledge or assumptions can influence how the extracted information is understood and presented. This workshop aims to: 1. Explore the role of context in interpreting digital traces, emphasising the uncertainties that arise when contextual information is partial or missing. 2. Examine interpretative divergence, showing how isolated artifacts (files, logs) can yield different or even contradictory interpretations depending on practitioner background and available context. 3. Discuss communication of interpretations, how analytical reasoning and uncertainty can be communicated in judicial and investigative settings.

Biography
Elenore joined the UTS Centre for Forensic Science in October 2025 as Lecturer in Digital Forensic Science. Elenore graduated from the School of Criminal Justice of the University of Lausanne (Switzerland), where she completed a BSc and an MSc in Forensic Science, specialising in chemical criminalistics. While conducting research for the Unit of Forensic Toxicology and Chemistry at the Romand University Centre of Legal Medicine (CURML), she worked for five years as a graduate assistant at the University of Lausanne, during which time she chose to change her focus towards digital forensic science. In 2020, in collaboration with the Neuchâtel Police State, she conducted the first phase of her doctoral research, examining the operationalisation of digital forensic science within a police agency. Following this, she joined Cranfield University as a lecturer, where she continued to investigate the exploitation of digital traces in judicial settings. She completed her PhD in 2024, earning a Faculty award, focusing on the presence, management and communication of uncertainty factors in digital forensic science. Her research centres on the evaluation of information extracted from digital traces, decision-making processes in forensic investigations, and the effective communication of forensic results to stakeholders. Elenore is more broadly interested in how emerging technologies influence and transform investigative processes, and how their integration affects forensic practices. She is an advocate for considering forensic science as a discipline of its own.

Julian joined the UTS Centre for Forensic Science in October 2025 as Senior Lecturer in Digital Forensic Science following eight years with the World Anti-Doping Agency (WADA), where he conducted worldwide investigations into the highest levels of sport doping and corruption, uncovered systemic data manipulation and delivered expert testimony in high-stakes regulatory settings. Julian founded and led the organisation's Data Analytics Unit, developing data strategies that enhanced operational performance and transformed complex datasets into actionable intelligence for informed decision-making. He completed his PhD at the École des Sciences Criminelles (ESC) of the University of Lausanne (Switzerland) in 2013, where his research on drug profiling and machine learning earned the Faculty Award. With academic experience across Europe and Canada, Julian brings deep expertise in forensic intelligence, data analytics, illicit markets, and digital forensic case reconstruction. His research interests include interdisciplinary approaches to understanding illicit markets and trafficking dynamics, the role of emerging tools and technologies to solve forensic science questions, and the continuity of evidence and reconstruction of activity in highly manipulated digital forensic cases.

Technical Sessions

S No	Technical Sessions	Name
01	**Cyber Security-Authentication** Day 2 11:00 – 12:30	Physical/Machine-Learning Attacks Resilient Multi-Factor Authentication Employing Handwritten Challenge into Touch-Sensor PUF
		Seeing Malware Differently: A Novel Signal-Based Graph and Image Approach to Detection
		α-Forest: Proxy-Cloud Enabled Efficient and Secure Community Search over Encrypted Bipartite Graphs
		GLFE: Video Frame Interpolation Forensics via Multi-Scale Global and Local Feature Exploitation
02	**Physical Layer Security** Day 2 14:00-15:30	Physical Layer Authentication with Likelihood Test Using Machine Learning with Artificial Dataset
		Security Analysis of RIS-Assisted Physical-Layer Authentication Over Multipath Channels
		Drone Detection on Wi-Fi Channels Using Radio Frequency Signal Power Variation Properties
		STAR-RIS Aided Covert Communication with Symbiotic Backscatter
03	**Deepfake Detection** Day 2 16:00-17:30	Attention-based Mixture of Experts for Robust Speech Deepfake Detection
		CLIP Feature Selection Mechanism via Sparse Autoencoder for Generalised Deepfake Detection
		ADD: An Automated Neural Architecture Search Baseline for Deepfake Detection
		Deepfake Image Forger Detection
04	**Covert Communications** Day 3 11:00-12:30	6D Movable Antenna Enhanced Covert Communication with Flexible Position and Rotation
		Covert Waveform Design for Integrated Sensing and Communication System in Clutter Environment
		A Two-Phase Integrated Sensing and Communication-Assisted Covert D2D Communication Framework
		Multiple Distributed Wardens with Amplify-and-Forward Fusing Strategy in Covert Communications

S No	Technical Sessions	Name
05	**Multimedia Forensics** Day 3 14:00-15:30	Disentangling Moiré and Texture: Towards Robust Display-Recapture Detection for Document Images
		Vision-Text Interactive Hybrid Granularity Proxy Representation Learning for AI-Generated Image Detection
		Towards Practical Audio Phylogeny: Multi-Transformation Detection in Incomplete Trees
		Training-free Source Attribution of AI-generated Images via Resynthesis
06	**Biometrics** Day 4 11:00-12:30	DPF: A Dual Perturbation Framework for Face Privacy Protection with Authorised Recognition
		Finger Vein Sample Compression using Recent AI-Based Still Image Compression Schemes
		Domain-Informed Eye Movement Biometrics with Practical Evaluation for VR/AR User Authentication
		Finger Vein Spoof GANs: Are they really useful to enhance PAD training?
07	**Information Hiding & Covert Communications** Day 4 14:00-15:30	Covert Communication in Sanitised Online Social Networks
		Beam Split Aided Multi-User Near-Field Covert Communication under Wardens Collusion
		PSyDUCK: Hiding Information in the Denoising Process of Latent Diffusion Models
		Hierarchical Multihospital Management based on Progressive Secret Sharing and Reversible Data Hiding
08	**AI Security & Privacy** Day 4 16:00-17:30	A Nearly Optimal Attack against Certifiably Robust Smoothed Classifiers
		Trust-Based Framework for Securing Decentralised Federated Learning against Malicious Clients
		Privacy-Preserving State Estimation with Crowd Sensors: An Information-Theoretic Respective
		GAFIN: Gradient Direction-Agnostic Differential Privacy Control for Federated Learning via Nussbaum-Enhanced PID Tracking

Technical Sessions

Technical Session 1: Cyber Security-Authentication

Physical/Machine-Learning Attacks Resilient Multi-Factor Authentication Employing Handwritten Challenge into Touch-Sensor PUF

Ruochen Wang (The University of Osaka); Kosuke Kawamura (The University of Osaka); Jun Shiomi (The University of Osaka); Yoshihiro Midoh (The University of Osaka); Yuichi Tanaka (The University of Osaka); Minoru Kuribayashi (Tohoku University); Noriyuki Miura (The University of Osaka)

Abstract—This paper presents a user-device Multi-Factor Authentication (MFA) framework which leverages handwriting as the input of a Physically Unclonable Function (PUF) that identifies variations embedded in the touch sensor (panel). This enables simultaneous authentication both for the user and device. The framework addresses vulnerabilities inherited in classical digital encryption at the analog interface. It enhances resilience to physical-layer attacks by identifying individual sensors within the existing touch sensor infrastructure prior to Analog-to-Digital Conversion (ADC). At its core, the PUF captures intrinsic variations in panel's capacitor distribution. These variations are dynamically interrogated by user handwriting, which prevents reconstruction attacks, even under partial key exposure. The measurement results demonstrate high-entropy key generation that fuses device-intrinsic randomness with user-specific behaviour without additional hardware cost. Cross-user evaluations show strong resiliency against Machine Learning (ML)-based simulated attacks. The proposed PUF achieves 97.8% reliability and 47.6% uniqueness in the worst case, maintains a low 3.07% attack success rate even when 1015 Challenge-Response Pairs (CRPs) are leaked, and only increases to 26.73% when 50% (~1030) of the total CRPs are compromised. The proposed MFA reduces attacker success rates by over 31× compared to traditional methods. Compatible with advanced measures (e.g. security token), this MFA delivers a model-independent, high-accuracy solution scalable to various attack surfaces, including invasive and learning-based spoofing.

Seeing Malware Differently: A Novel Signal-Based Graph and Image Approach to Detection

Riccardo Bragaglia (Sapienza University of Rome); Riccardo Lazzeretti

Abstract—Malware remains a primary threat in cybersecurity, used by cybercriminals to damage digital systems. In this work, we propose a novel malware classification pipeline that transforms raw executable files, even obfuscated ones, into structured data representations, namely graphs and grayscale images, suitable for deep learning models. Starting from real-world samples executed in a sandboxed environment, our method extracts opcodes from memory dumps and builds opcode transition graphs, which can be used directly or as the basis for image construction. With our prototype, we evaluate lightweight deep learning models on both representations, demonstrating that

even with simple architectures and a limited dataset, our approach achieves promising results, particularly high precision, highlighting its potential for early-stage, automated malware triage.

α-Forest: Proxy-Cloud Enabled Efficient and Secure Community Search over Encrypted Bipartite Graphs

Xiaoxian Liu (UNSW); Chen Chen (UOW); Xueqiao Liu (UOW); Xiaoyang Wang (UNSW)

Abstract—Bipartite graphs model critical relationships (e.g., user-item interactions), but privacy-preserving (α, β)-core queries face inefficiency and structural leakage. We propose an α-Forest framework featuring: A hierarchical index enabling direct (α, β)-community retrieval without iterative traversal; Secure protocols to hide query parameters, results, and graph topology; A practical proxy-cloud architecture avoiding two cloud reliance. Theoretical analysis proves IND-CPA security and minimal leakage. Experiments show 71ms query latency (vs. 2+ hours in baselines) and 99.3% fewer iterations, with sub-250ms latency on 16K-edge graphs.

GLFE: Video Frame Interpolation Forensics via Multi-Scale Global and Local Feature Exploitation

Xiaowan Huang (School of Information Science and Engineering, University of Jinan); Tongzhen Si (School of Information Science and Engineering, University of Jinan); Xiaohui Yang (School of Information Science and Engineering, University of Jinan)

Abstract—With the continuous development of video technology, video frame interpolation (VFI) has made significant advances. Frame interpolation can generate new frames from existing ones to increase the frame rate. At the same time, it poses a serious threat to information security. As the videos produced by frame generation technology become increasingly realistic, many of them can mislead the public. Therefore, an algorithm that is robust and highly accurate is needed to determine whether a video is authentic. In this paper, we construct a video frame interpolation forensic framework. On one hand, we propose a multi-scale framework that processes video features from coarse to fine. On the other hand, we combine a global information module and a local information module to enrich the extracted tampering features. Additionally, we place an efficient multi-scale attention (EMA) module at the end of our framework to fuse the results from the three scales. Extensive experiments demonstrate that our method achieves comparable performance to the current state-of-the-art detectors.

Technical Session 2: Physical Layer Security

Physical Layer Authentication with Likelihood Test Using Machine Learning with Artificial Dataset

Francesco Ardizzon (University of Padova); Stefano Tomasin (University of Padova)

Abstract—In physical layer authentication (PLA) mechanisms, a verifier applies a test to decide whether a received message has been transmitted by a legitimate user or an intruder, according to some measured channel features (CFs). When the legitimate CF statistics are known, a well-known good solution is the likelihood test (LT). When a dataset of legitimate CFs is available, machine learning (ML) models can be used to perform one-class classification (OCC). Still, currently, i) while a good understanding of how ML models make decisions is important to ensure security, these models are not explainable, and ii) statistics and ML-based solutions appear as distinct solutions. In this paper, we aim at bridging such a gap by obtaining ML PLA verifiers that operate as the LT via neural network (NN) and least-square support vector machine (SVM) models, trained as two-class classifiers on the single-class dataset and an artificial dataset for the negative class. The artificial dataset is obtained by generating CF vectors uniformly distributed over the domain of the legitimate class dataset. In turn, we show that autoencoder classifier generally does not provide the LT. Numerical results are obtained considering PLA on both wireless and underwater acoustic channels.

Security Analysis of RIS-Assisted Physical-Layer Authentication Over Multipath Channels

Anna Valeria Guglielmi (University of Padova); Linda Senigagliesi (Università Politecnica delle Marche); Marco Baldi (Università Politecnica delle Marche); Stefano Tomasin (University of Padova)

Abstract—In physical layer authentication, verification of a user's identity is based on the characteristics of the transmission channel through which signals are delivered to the authenticator (Bob). In this paper, we assume that the signals received by Bob pass through a reconfigurable intelligent surface (RIS) (controlled by Bob) and that the legitimate transmitter (Alice) is equipped with one antenna. Conversely, the attacker (Trudy) has multiple antennas and uses precoding to deceive Bob's verification. Assuming that Trudy knows all the channel matrices, we first derive her optimal attack strategy. Then, we analyse the conditions under which the channel estimated by Bob is indistinguishable when either Alice or Trudy is transmitting. When Trudy has a single antenna, we show that the indistinguishability condition cannot be met when the channels to the RIS are the result of propagation over multiple paths. For single-path line-of-sight (LOS) conditions, instead, Trudy can impersonate Alice, although transmitting from a different position. We verify these results numerically and assess the security of the considered scenario, even when the indistinguishability conditions cannot be met.

Drone Detection on Wi-Fi Channels Using Radio Frequency Signal Power Variation Properties

Yuchen Wang (Edith Cowan University); Shihao Yan (Edith Cowan University); Derek Tighe (Edith Cowan University); Peng Chen (Curtin University); Ying He (University of Technology Sydney)

Abstract—Passive radiofrequency (RF) sensing in the congested 2.4 GHz industrial, scientific and medical (ISM) band remains challenging due to bursty Wi-Fi traffic and the cost of training heavy models for real-time use. We present a lightweight, training-free detector for drone presence on standard Wi-Fi channels that exploits temporal stability of in-band power. For channels 1/6/11, the wideband in-phase and quadrature (I/Q) stream is windowed every 10ms, converted to power spectral density (PSD), averaged within each channel band, and evaluated with a sliding-window temporal max–min (MaxDiff) statistic (max–min of the band-mean power). Small MaxDiff indicates a stable, sustained link typical of drones; large values reflect Wi-Fi's carrier-sense multiple-access with collision avoidance (CSMA/CA) burstiness. We derive single-channel tests and a max-band aggregation (MBA) rule and adopt Neyman–Pearson thresholding. Using wideband captures with a Universal Software Radio Peripheral (USRP) X310 and a UBX-160 front-end at a sampling rate Fs = 200 MS/s in realistic ISM conditions, the area under the receiver operating characteristic (ROC) curve (AUC) rises rapidly with the window length and saturates: MBA and the low-band (Ch. 1) rule both achieve AUC $\geq$ 0.99 with sub0.2 s latency (0.14 s and 0.16 s, respectively), while the mid-band (Ch. 6) requires substantially longer integration. At false-alarm rate $\alpha = 0.05$, MBA attains $\approx$ 0.97 detection by 0.13 s. The approach is explainable, computationally negligible, and well-suited as a front-end stage before downstream identification or tracking; we discuss adaptive windowing/thresholding, extension to 5/6 GHz bands, and multi-antenna/site fusion as future directions.

STAR-RIS Aided Covert Communication with Symbiotic Backscatter

Rong Chen (Fuzhou University); Jinsong Hu (Fuzhou University); Shihao Yan (Edith Cowan University); Ruiquan Lin (Fuzhou University); Jun Wang (Fuzhou University); Hai Pei (Fuzhou University)

Abstract—This paper investigates a covert communication with symbiotic backscatter, based on a segmented simultaneously transmitting and reflecting reconfigurable intelligent surface (STAR-RIS), ensuring reliable communication between transmitter Alice and warden user Willie, while simultaneously enabling covert communication with user Bob. The structure of the STARRIS is segmented into a primary zone (P zone) and a covert zone (C zone), adopting the energy splitting (ES) and time switching (TS) protocols, respectively. Reliable transmission between Alice and Willie is maintained via the P zone. In contrast, the C zone conveys covert information to Bob by embedding the backscatter signal into the primary system signal during the transmission phase while further maintaining reliable communication with Willie during the reflection phase. By analysing the connection outage probability (COP), the allocation of time resources between the two phases of the C zone is studied. Furthermore, under the constraint of covertness, both the allocation of elements and transmission/reflection coefficients are adjusted to optimise and achieve the highest effective covert rate. The results of the simulation reveal a notable improvement in covert communication performance due to the proposed system.

Technical Session 3: Deepfake Detection

Attention-based Mixture of Experts for Robust Speech Deepfake Detection

Viola Negroni (Politecnico di Milano); Davide Salvi (Politecnico di Milano); Alessandro Ilic Mezza (Politecnico di Milano); Paolo Bestagini (Politecnico di Milano); Stefano Tubaro (Politecnico di Milano)

Abstract—AI-generated speech is becoming increasingly used in everyday life, powering virtual assistants, accessibility tools, and other applications. However, it is also being exploited for malicious purposes such as impersonation, misinformation, and biometric spoofing. As speech deepfakes become nearly indistinguishable from real human speech, the need for robust detection methods and effective countermeasures has become critically urgent. In this paper, we present the ISPL's submission to the SAFE challenge at IH & MMSec 2025, where our system ranked first across all tasks. Our solution introduces a novel approach to audio deepfake detection based on a Mixture of Experts architecture. The proposed system leverages multiple state-of-the-art detectors, combining their outputs through an attention-based gating network that dynamically weights each expert based on the input speech signal. In this design, each expert develops a specialised understanding of the shared training data by learning to capture different complementary aspects of the same input through inductive biases. Experimental results indicate that our method outperforms existing approaches across multiple datasets. We further evaluate and analyse the performance of our system in the SAFE challenge.

CLIP Feature Selection Mechanism via Sparse Autoencoder for Generalised Deepfake Detection

Lorenzo Berlincioni (University of Florence); Andrea Ciamarra (CNIT, National Interuniversity Consortium for Telecommunications); Pietro Pala (University of Florence); Roberto Caldelli (CNIT, National Interuniversity Consortium for Telecommunications and Universitas Mercatorum); Alberto Del Bimbo (University of Florence)

Abstract—Generating multimedia contents, particularly images, by using AI-based tools is becoming an everyday practice, generally just for fair applications but always more for malevolent aims such as disinformation, defamation and blaming. Reliably detecting synthetically generated pictures is becoming crucial. However, new generative models are emerging at a much faster pace than the development of accurate deepfake detectors. According to this, it is fundamental to improve generalisation capabilities in order to preserve performance in front of content created by unknown and new emerging generation methods. This paper investigates in this direction, proposing the idea to select a reduced set of CLIP-based features by resorting to a sparse autoencoder (SAE); such a set should ideally be termed the features of fake and could provide an improved generalisation capacity. Experimental results carried out on extended datasets highlight this notable behaviour, and diversely designed detectors, based on this approach, achieve state-of-the-art performances.

ADD: An Automated Neural Architecture Search Baseline for Deepfake Detection

Ping Liu (University of Nevada, Reno); Yuewei Lin (Brookhaven National Laboratory); Jingen Liu (JD AI Research); Yunchao Wei (Beijing Jiaotong University); Joey Tianyi Zhou (CFAR)

Abstract—This paper presents an effective baseline for deepfake detection based on Automated Machine Learning (AutoML) techniques. An adaptive neural architecture search strategy is introduced, specifically tailored for deepfake detection tasks. By exploring a carefully designed search space, the proposed method establishes a strong baseline that performs competitively with manually designed architectures of comparable complexity. To further enhance robustness and generalisation, we adopt a simple yet effective strategy that jointly predicts potential manipulation regions and real/fake labels. Unlike traditional manually designed approaches, our method streamlines architecture construction, reducing labour-intensive tuning and the reliance on prior knowledge of manipulation techniques or regions. Extensive experiments on two benchmark datasets validate the effectiveness of our method and highlight its potential as a solid starting point for future research on AutoML-based deepfake detection.

Deepfake Image Forger Detection

Bin Deng (Beihang University); Yuanfang Guo (Beihang University); Weina Xu (Beihang University); Wenqi Zhuo (Beihang University); Junfu Wang (Beihang University); Liang Yang (Hebei University of Technology); Yunhong Wang (Beihang University)

Abstract—The proliferation of deepfake technology has led to the widespread dissemination of manipulated images featuring counterfeit faces on the internet. In recent years, researchers have devoted themselves to developing deepfake image detection techniques, which focus solely on identifying the integrity of images, without considering the malicious users who created and posted these deepfake images. In this paper, we propose a new detection task, i.e., identifying the malicious users who hide among the normal users and publish deepfake images (referred to as 'image forgers'), named deepfake image forger detection. To accomplish this task, we firstly construct a new dataset based on existing deepfake datasets and social network data from the internet. Based on this dataset, we propose a novel graph neural network-based detection method, named Deepfake Image Forger Detection (DIFD), by exploiting the similarities among the images posted by the same user and leveraging user relationships in social networks. Experiments demonstrate the effectiveness of our proposed work.

Technical Session 4: Covert Communications

6D Movable Antenna Enhanced Covert Communication with Flexible Position and Rotation

Longfa Luo (Fuzhou University); Jinsong Hu (Fuzhou University); Youjia Chen (Fuzhou University); Peng Kang (Fuzhou University); Jun Wang (Fuzhou University); Ruiquan Lin (Fuzhou University)

Abstract—This work proposes a six-dimensional movable antenna (6DMA) enhanced covert communication scheme, enabling flexible adjustments of both positions and rotations of 6DMA surfaces to improve covert performance. We first formulate an optimisation problem to maximise effective throughput by jointly designing the positions, rotations, and transmit beamforming of the 6DMAs, subject to a covert constraint, a total power constraint, and the antenna spatial feasibility constraints. To address the non-convex optimisation challenge, we employ an alternating optimisation framework combined with semidefinite relaxation (SDR) method. Results show that the proposed scheme achieves higher effective throughput than fixed or partially adjustable antennas, demonstrating its effectiveness in enhancing covert communication through flexible adjustments.

Covert Waveform Design for Integrated Sensing and Communication System in Clutter Environment

Xuyang Zhao (Xidian University); Jiangtao Wang (Xidian University); Xinyu Zhang (Aalto University)

Abstract—This paper proposes an integrated sensing and communication (ISAC) system covert waveform design method for complex clutter environments, with the core objective of maximising the signal-to-clutter-plus-noise ratio (SCNR). The design achieves efficient clutter suppression while meeting the covertness requirement through joint optimisation of the transmit waveform and receive filter, enabling cooperative radar detection and wireless communication. This study presents key innovations that explicitly address target Doppler shift uncertainty, significantly enhancing system robustness against Doppler effects. To ensure communication reliability, the method incorporates phase difference constraints between communication signal elements in the waveform design, along with energy constraint, covert constraint, and peak-to-average power ratio (PAPR) constraint. The original non-convex optimisation problem is transformed into a tractable convex optimisation form through convex optimisation technique. Simulation results demonstrate that the optimised waveform not only satisfies the covertness requirement in complex clutter environment but also achieves superior target detection performance. It also ensures reliable communication and confirms the effectiveness of proposed method.

A Two-Phase Integrated Sensing and Communication-Assisted Covert D2D Communication Framework

Bingbing Han (Shandong Normal University); Jia Zhang (Shandong Normal University); Shihao Yan (Edith Cowan University); Ke Liu (Shandong Normal University); Jiande Sun (Shandong Normal University)

Abstract—This paper investigates a covert device-to-device (D2D) communication system assisted by an integrated sensing and communication (ISAC) base station. In the proposed two-phase framework, the ISAC-enabled base station simultaneously performs downlink communication and environmental sensing in the first phase to detect the presence of a passive warden. Based on the sensing outcome, a D2D transmitter determines whether to initiate covert transmission to its receiver in the second phase. To enhance covert transmission performance, we formulate a covert rate maximisation problem subject to both quality-of-service (QoS) and ISAC detection constraints. The resulting non-convex problem is addressed via an alternating optimisation approach. Simulation results show that the achievable D2D covert rate declines under stricter detection probability constraints and is significantly more sensitive to the QoS requirement of the second phase cellular user than that of the first. Furthermore, increasing the D2D transmit power or relaxing the detection constraint yields notable gains in covert throughput. These findings reveal the fundamental trade-offs among sensing accuracy, covertness, and communication quality in our proposed ISAC-assisted covert D2D communication framework.

Multiple Distributed Wardens with Amplify-and-Forward Fusing Strategy in Covert Communications

Zhilin Chen (Shandong Normal University); Jia Zhang (Shandong Normal University); Xiaobo Zhou (Anhui Agriculture University); Jiande Sun (Shandong Normal University); Shihao Yan (Edith Cowan University)

Abstract—This paper investigates covert wireless communication in the presence of multiple distributed wardens. In the proposed system model, a transmitter (Alice) aims to covertly send information to a legitimate receiver (Bob) with the aid of a friendly jammer, while multiple adversarial wardens (Willies) monitor the channel and forward their observations to a centralised fusion centre (FC). The FC then performs a global decision to detect potential transmissions. To assess the covert performance of the system, we first derive the optimal decision threshold and the corresponding minimum decision error probability at the FC. We then propose an optimal amplification coefficient (OAC) scheme that maximises detection uncertainty at the FC. Numerical results show that the OAC scheme achieves the lowest detection error probability, and its performance advantage becomes more prominent with an increasing number of wardens. Furthermore, both analytical and simulation results reveal a fundamental trade-off between covertness and transmission reliability, emphasising the need for careful system-level design in multi-warden environments.

Technical Session 5: Multimedia Forensics

Disentangling Moiré and Texture: Towards Robust Display-Recapture Detection for Document Images

Peiquan Li (ShenZhen University); Changsheng Chen (Shenzhen MSU-BIT University); Yulia Chernyshova (Smart Engines Service LLC); Dmitry Nikolaev (Smart Engines Service LLC); Shunquan Tan (Shenzhen MSU-BIT University); Vladimir Arlazarov (Smart Engines Service LLC)

Abstract—Display-recapture attacks pose a critical threat to the integrity and authenticity of digital document images, particularly by concealing tampering traces through rephotographing displayed content. Existing document presentation attack detection (DPAD) methods often struggle to distinguish forensic artifacts (e.g., chromatic distortions and moiré patterns) from the natural textures inherent in documents with complex backgrounds. To address this texture confusion challenge, we propose a dual-stream LC&DF framework that integrates Local Chromaticity (LC) features with a Masked Attention mechanism and a Discriminative Frequency (DF) branch enhanced via a Frequency-domain Moiré-Aware Adapter (FMA-Ada). This architecture jointly models local chromatic distortions and global frequency cues to robustly isolate recapture-induced artifacts from genuine document content. Extensive evaluations on cross-domain and in-the-wild datasets demonstrate that our LC&DF method significantly outperforms existing state-of-the-art approaches, achieving an AUC of 0.9105 and reducing the Equal Error Rate by up to 15.72 percentage points on challenging document benchmarks. Visualisations of challenging samples further confirm that our claims on distinguishing the forensic artifacts from the document textures. The source code of this work will be available upon acceptance.

Vision-Text Interactive Hybrid Granularity Proxy Representation Learning for AI-Generated Image Detection

Feng Ding (NanChang University); Yue Zhang (NanChang University); Mengyao Xiao (NanChang University); Kangkang Wei (NanChang University); Zhangyi Shen (Hangzhou Dianzi University); Hong Rao (NanChang University)

Abstract—With the significant success of Generative Adversarial Networks and Diffusion Models in visual synthesis, the risk of disinformation has also increased. Despite many researchers dedicated to solving this issue, they still rely on limited visual features when dealing with complex generated images. In this work, we propose vision-text interactive hybrid granularity proxy representation learning, which overcomes the limitations of previous methods that solely rely on visual information by incorporating cross-modal textual information. First, we design a cross-modal interactive reconstruction framework that uses a reconstruction mechanism to understand and learn information from different modalities, thereby preliminarily establishing semantic relationships between image-text pairs. Based on this, the hybrid granularity proxy representation learning method is introduced, which utilises fine-grained proxy points within the same modality and coarse-grained proxy points

across modalities to reduce the feature space distance between the two modalities. This method not only helps mitigate the interference of label noise on representation learning but also enhances the discrimination of the feature representations through text-guided cross-modal indirect alignment. We have carried out extensive experimental verification on multiple datasets, and the experimental results show that our method shows significant performance improvement in accuracy and generalisation.

Towards Practical Audio Phylogeny: Multi-Transformation Detection in Incomplete Trees

Milica Gerhardt (Fraunhofer IDMT); Luca Cuccovillo (Fraunhofer IDMT); Patrick Aichroth (Fraunhofer IDMT)

Abstract—Audio phylogeny aims to reconstruct the transformation history of near-duplicate audio files by identifying parent-child relationships and tracing their modification paths. A key challenge is accurately estimating the transformations between file pairs, particularly when sequences of edits (e.g., compression, trimming, fading) or missing intermediate files are involved. We propose a deep learning-based method that formulates transformation detection as a multi-label classification task, enabling the identification of multiple transformations per audio pair. Unlike existing approaches limited to detecting one or two transformations, our method achieves notable improvements in accuracy when reconstructing sparse and incomplete trees. To address the variability of real-world scenarios—including both full and sparse trees—we further introduce a hybrid strategy that combines our model with the current state-of-the-art, balancing precision in dense trees with robustness in sparse conditions.

Training-free Source Attribution of AI-generated Images via Resynthesis

Pietro Bongini (University of Siena); Valentina Molinari (University of Siena); Andrea Costanzo (University of Siena); Benedetta Tondi (University of Siena); Mauro Barni (University of Siena)

Abstract—Synthetic image source attribution is a challenging task, especially in data scarcity conditions requiring few-shot or zero-shot classification capabilities. We present a new training-free one-shot attribution method based on image resynthesis. A prompt describing the image under analysis is generated, then it is used to resynthesize the image with all the candidate sources. The image is attributed to the model which produced the resynthesis closest to the original image in a proper feature space. We also introduce a new dataset for synthetic image attribution consisting of face images from commercial and open-source text-to-image generators. The dataset provides a challenging attribution framework, useful for developing new attribution models and testing their capabilities on different generative architectures. The dataset structure allows to test approaches based on resynthesis and to compare them to few-shot methods. Results from state-of-the-art few-shot approaches and other baselines show that the proposed resynthesis method outperforms existing techniques when only a few samples are available for training or fine-tuning. The experiments also demonstrate that the new dataset is a challenging one and represents a valuable benchmark for developing and evaluating future few-shot and zero-shot methods.

Technical Session 6: Biometrics

DPF: A Dual Perturbation Framework for Face Privacy Protection with Authorised Recognition

Ao Li (Beijing Jiaotong University); Ting Li (Beijing Jiaotong University); Huayue Sun (Beijing Jiaotong University); Rui Zhai (Beijing Jiaotong University); Rongrong Ni (Beijing Jiaotong University); Yao Zhao (Beijing Jiaotong University)

Abstract—Existing face privacy protection methods employ adversarial perturbations to disrupt unauthorised face recognition systems. However, these perturbations often introduce irreversible distortions that degrade image recognizability and hinder identity authentication in authorised contexts. In our work, we introduce DPF, a Dual Perturbation Framework for Face Privacy Protection with Authorised Recognition. First, we carefully design Identity Adversarial Perturbation Algorithm (IAPA) against malicious identity recognition. Second, we design an Anti-Purification Perturbation Generator (APPG) that generates purification-resistant adversarial perturbations to interfere with unauthorised purification models. The added dual perturbation, consisting of identity adversarial perturbation and purification adversarial perturbation, ensures the prevention of unauthorised recognition while protecting facial identity privacy. Furthermore, we design a Perturbation Erase Network (PENet) to eliminate dual perturbation, enabling successful authorised face recognition.

Finger Vein Sample Compression using Recent AI-Based Still Image Compression Schemes

Christof Kauba (University of Salzburg); Andreas Uhl (University of Salzburg); Gerald Angerer (University of Salzburg)

Abstract—The compression of the sample files enables more efficient storage and transmission of biometric data. Four different recent still image compression techniques (JPEG2000, JPEG XL, JPEGAI and Compress AI) are applied to finger vein sample images in two different scenarios, first where the gallery is uncompressed and second where the gallery is JPEG2000 compressed (as it is the current ISO/IEC standard). The impact on the recognition accuracy is assessed on three different data sets using six finger vein recognition schemes to answer the question of which compression works best for the probe samples in each of the two scenarios. The results show that JPEG2000 is not competitive, but the more recent methods, especially JPEGAI, perform well up to a compression ratio of 200 (0.04 bpp).

Domain-Informed Eye Movement Biometrics with Practical Evaluation for VR/AR User Authentication

Paul Gyreyiri (University of Wyoming); Diksha Shukla (University of Wyoming)

Abstract—Eye movement biometrics (EMB) shows promise for VR/AR authentication; however, current state-of-the-art evaluations often overestimate real-world performance, relying on a limited number of positive samples and single-task protocols. We introduce Domain-Informed Eye Movement Biometrics (DIEMB), which models specialised feature extraction modules based on well-understood eye movement characteristics, including saccades, fixations, smooth pursuits, and scan paths. This approach aims to capture the various temporal patterns of eye movement. Additionally, we provide a comprehensive evaluation using 1-second subsequences across different tasks. DIEMB achieves comparable performance to the state-of-the-art Eye Know You Too (EKYT) (15.2% vs. 16.2% average EER when enrolled with all tasks and EER computed across all rounds and tasks but at the user level), while using 6% fewer parameters. Our analysis on the GazeBase dataset, a 37-month longitudinal study, shows a non-linear temporal degradation and highlights optimal task combinations for enrolment. Notably, our studies show that strategically selecting 2–3 structured tasks can match full-task performance while enabling better cross-task generalisation. These findings provide practical guidelines for the efficient deployment of EMB in VR/AR environments.

Finger Vein Spoof GANs: Are they really useful to enhance PAD training?

Tessnim Boulfoul (University of Salzburg); Valentin Pröpster (Univsersity of Salzburg); Andreas Vorderleitner (University of Salzburg); Andreas Uhl (University of Salzburg)

Abstract—Four traditional GAN-based I2I translation techniques have been employed for the synthesis of biometric finger vein presentation attack instrument (PAI) samples (three public presentation attack datasets have been considered). These synthetic samples have been used to train presentation attack detectors (PAD). This work considers a more realistic setting to augment PAD training sets with synthetic data, instead of entirely replacing real samples with synthetic samples, as done in earlier work. Our analysis reveals that uninformed usage of synthetic data in the considered context has to be avoided, as it can lead to dramatically high errors when trying to detect attack samples (high APCER). Instead, we recommend to use an augmentation of training data with synthetic samples only in case of too many false positive PA alarms (high BPCER values) when training with real data alone.

Technical Session 7: Information Hiding & Covert Communications

Covert Communication in Sanitised Online Social Networks

Zhiying Zhu (East China University of Science and Technology); Zhongjie Ba (Zhejiang University); Guobiao Li (Fudan University); Zhenxing Qian (Fudan University); Xinpeng Zhang (Fudan University)

Abstract—Robust steganography has made significant progress over the years, and it is now highly convenient to transmit secret messages through lossy channels such as Online Social Networks (OSNs). As a countermeasure, recent studies propose sanitising networks to indiscriminately process uploaded images on OSNs, which are effective in interrupting illegal covert communications. Unfortunately, these sanitising networks also corrupt the secret data of certain legitimate and justified needs. To this end, we present in this paper a novel scheme tailored for authorised users to conduct covert communication in OSNs deployed with sanitising networks. Specifically, we first joined the sanitising network with a decoder whose weights are generated according to a secret seed (i.e., key). Then, we iteratively optimise a cover image using the jointed network until the updated cover image (i.e., stego image) triggers the jointed network to generate the specific output corresponding to the secret. As such, only authorised receivers who possess the seed could rebuild the decoder to recover the secret data from the sanitised stego images. Various experiments have been conducted to demonstrate the advantage of our proposed method for covert communication in sanitised OSNs.

Beam Split Aided Multi-User Near-Field Covert Communication under Wardens Collusion

Duanrui Liao (Fuzhou University); Mingfeng Ji (Fuzhou University); Haojie Yin (Fuzhou University); Jinsong Hu (Fuzhou University); Youjia Chen (Fuzhou University); Jun Wang (Fuzhou University); Ruiquan Lin (Fuzhou University)

Abstract—The 6G mobile communication system leverages wideband extra-large multiple-input multiple-output (XLMIMO) to achieve ultra-high data rates, which also leads to new security vulnerabilities due to the near-field spherical wavefront characteristics. This work investigates the problem of near-field multi-user covert communication and proposes a joint location estimation (LE) and data transmission (DT) design based on the beam split effect. The proposed method employs a time delay phase shifters (TD-PS) precoding architecture to generate focusable beams at controllable locations across different subcarriers, enabling simultaneous localisation of multiple users. Subsequently, beam split is suppressed to support covert communication involving a legitimate user, Bob, and multiple wardens, Willies. In addition, an optimisation problem is formulated to maximise the effective covert rate (ECR) under both non-colluding and colluding detection strategies, and a two-stage optimisation approach is used to solve the non-convex problem. Numerical results show that the non-colluding detection strategy achieves a higher ECR compared to the colluding one and demonstrate the effectiveness of the proposed design in balancing covertness and transmission efficiency.

PSyDUCK: Hiding Information in the Denoising Process of Latent Diffusion Models

Aqib Mahfuz (Google); Georgia Channing (University of Oxford); Mark van der Wilk (University of Oxford); Philipp Torr (University of Oxford); Fabio Pizzati (University of Oxford); Christian Schroeder de Witt (University of Oxford)

Abstract—Recent advances demonstrate that information can be covertly embedded in the outputs of stochastic generative AI models, raising both opportunities for secure communication and risks of misuse. Existing latent diffusion steganography methods typically hide data in the entropy of the initial latent state, inherently limiting embedding capacity. In this work, we instead investigate information hiding within the entropy of the diffusion denoising process itself. We introduce PSyDUCK, a simple but efficient framework that leverages controlled divergence and local mixing during denoising to enable high-capacity message embedding while preserving visual fidelity. Our empirical evaluation shows PSyDUCK can hide substantial information in both image and video diffusion models. While our formal analysis indicates that the security guarantees of denoising-based embedding are limited, the existence of this channel nonetheless requires that steganalysis methods account for entropy throughout the entire denoising process - not just in the initial latent state.

Hierarchical Multihospital Management based on Progressive Secret Sharing and Reversible Data Hiding

Jing Li (Shandong Normal University); Yannan Ren (Shandong JiaoTong University); Jiantao Wang (Shandong Normal University); Xuquan Wang (Tongji University); Lingchen Gu (Shandong Normal University); Jiande Sun (Shandong Normal University); Wenbo Wan (Shandong Normal University)

Abstract—In multihospital healthcare management systems, the rapid growth of medical data and the increasing need for cross-institutional collaboration have underscored the critical importance of secure data sharing and privacy protection for patient information. This paper presents a Hierarchical Multihospital Management (HMM) framework that integrates Progressive Secret Sharing (PSS) and Reversible Data Hiding (RDH) to securely manage patient information, medical reports, and medical images. Specifically, patients' textual data—including personal details and diagnostic reports—are divided into multiple shares using PSS, while medical images are segmented into lesion and non-lesion regions for differentiated secret sharing. The textual data is subsequently embedded into the secret-shared segments of the medical images. Under this hierarchical model, attending physicians can reconstruct complete patient records and medical reports from the embedded images, whereas junior physicians are permitted to access only basic identity information, diagnostic results, and the images themselves. System administrators retain access solely to patient identity data, without authorisation to view sensitive medical information. This access control mechanism enforces hierarchical security in multi-institutional medical environments.

Technical Session 8: AI Security & Privacy

A Targeted Attack against Certifiably Robust Smoothed Classifiers

Kai Zeng (University of Siena); Mauro Barni (University of Siena); Benedetta Tondi (University of Siena)

Abstract—Randomised Smoothing (RS) has been proposed as a technique to develop deep learning classifiers with certified robustness. For these classifiers, a certain level of robustness can be theoretically guaranteed, and, for every input, a certified radius can be defined, such that no perturbation within this radius can change the network classification result. Many works have focused on extending the randomised smoothing theory in several directions and getting larger certified robust radii. However, the gap between the empirical certified radius derived from the theory and the practical robustness, assessed by attacking the RS classifiers with minimum distortion adversarial examples, is still unexplored. By focusing on binary classifiers, in this paper, we derive a targeted attack algorithm against RS classifiers. Experiments carried out on tasks from two different application domains, namely gender classification and synthetic image detection, reveal that the proposed attack outperforms existing attacks, contributing to closing the gap between theory and practical results. The proposed attack can be a useful tool to evaluate the real-world effectiveness and tightness of RS empirical certification bounds.

Trust-Based Framework for Securing Decentralised Federated Learning against Malicious Clients

Imen Ben Said (Laval University); Talal Halabi (Laval University); Adel Abusitta (Polytechnique Montréal, Université de Montréal); Mohammad Zulkernine (Queen's University)

Abstract—Decentralised federated learning (DFL) enables collaborative model training across distributed clients without relying on a central server. However, this paradigm is highly vulnerable to poisoning attacks, especially when a large proportion of participating clients behave maliciously. In this paper, we propose a robust defence framework that empowers each client to detect and mitigate the influence of malicious peers. Our approach combines local gradient-based anomaly detection using DBSCAN with an uncertainty-aware trust aggregation mechanism grounded in Dempster–Shafer theory. This enables clients to assign trust scores to their neighbours and dynamically perform trust-weighted model aggregation, integrating only reliable updates. Our experiments on two standard benchmark datasets, NSL-KDD and ToN IoT, show that our method maintains over 93% and 83% accuracy, respectively, even when 70% of clients are adversarial under coordinated label-flipping attacks. These results highlight the robustness and effectiveness of our framework in highly adversarial DFL environments, demonstrating its ability to maintain reliable performance even when the majority of clients behave maliciously.

Privacy-Preserving State Estimation with Crowd Sensors: An Information-Theoretic Respective

Farhad Farokhi (The University of Melbourne)

Abstract—Privacy-preserving state estimation for linear time-invariant dynamical systems with crowd sensors is considered. At any time step, the estimator has access to measurements from a randomly selected sensor from a pool of sensors with prespecified models and noise profiles. A Luenberger-like observer is used to fuse the measurements with the underlying model of the system to recursively generate the state estimates. An additive privacy-preserving noise is used to constrain information leakage. Information leakage is measured via mutual information between the identity of the sensors and the state estimate conditioned on the actual state of the system. This captures an omnipotent adversary that not only can access state estimates but can also gather direct high-quality state measurements. Any prescribed level of information leakage is shown to be achievable by appropriately selecting the variance of the privacy-preserving noise. Therefore, privacy-utility trade-off can be fine-tuned.

GAFIN: Gradient Direction-Agnostic Differential Privacy Control for Federated Learning via Nussbaum-Enhanced PID Tracking

Chen Li (University of Technology Sydney); Xuelei Qi (Northeastern University); Kai Wu (University of Technology Sydney); Xin Yuan (Commonwealth Scientific and Industrial Research Organisation (CSIRO)); Wei Ni (Commonwealth Scientific and Industrial Research Organisation (CSIRO)); Renping Liu (University of Technology Sydney); Quan Z. Sheng (Macquarie University)

Abstract—Handling uncertain gradient descent directions poses a critical challenge in privacy-preserving federated learning (FL) systems under Gaussian differential privacy (GDP). Classical Proportional-Integral-Derivative (PID) controllers, while effective in tracking target privacy budgets, may suffer from convergence failures when facing direction uncertainty caused by DP noise and heterogeneous client updates. To address this, we propose GAFIN, a novel gradient direction-agnostic control framework that integrates a Nussbaum-type function into a PID controller. The Nussbaum modulation dynamically adjusts the control gain to compensate for unknown or varying gradient directions, thereby enabling stable and robust tracking of the desired privacy budget. Extensive experiments across multiple benchmark datasets and privacy settings demonstrate that GAFIN preserves the fast convergence behaviour of PID control while consistently accelerating convergence by 20.9% to 80.0% across MLP and CNN models on MNIST, FEMNIST, and CIFAR10, effectively balancing privacy protection and communication efficiency in FL systems under varying initial privacy budgets.

Welcome Reception

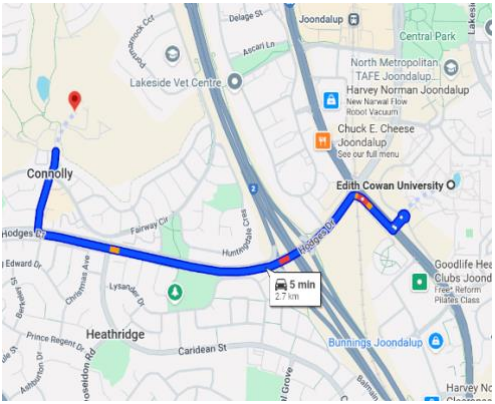
The welcome drink will be at Joondalup Resort, which is about a 5-minute drive from the conference venue.

Address: Joondalup Resort

Time: 5:00 PM-7:00 PM

How to get there: The conference committee has arranged 1 coach from ECU to Joondalup Resort with the departure time of 4:45 PM and return time of 7:00 PM.

Note: You are welcome to drive there, and there are plenty of parking spaces.



Gala Dinner

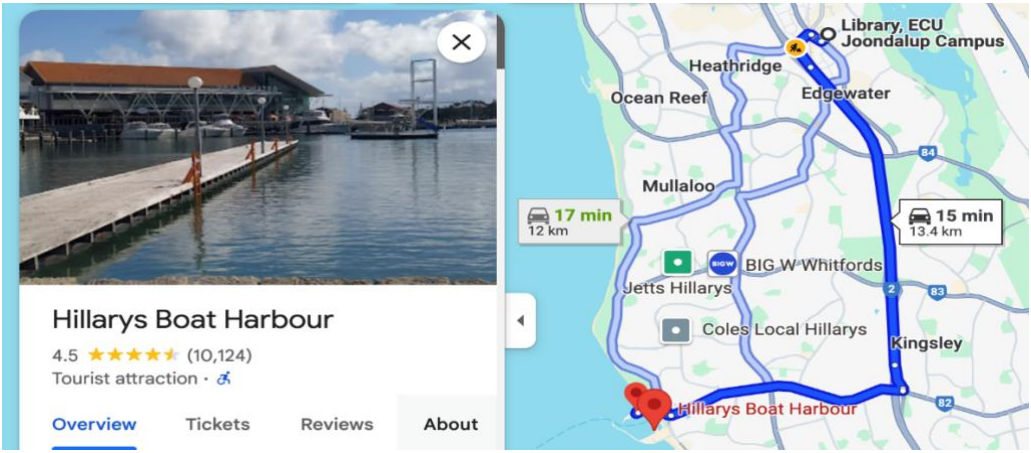
The social dinner will be at the Hillarys Yacht Club, which is about a 15-minute drive away from the conference venue.

Address: 65 Northside Dr, Hillarys, WA 6025.

Time: 6:00 PM-9:00 PM

How to get there: The conference committee has arranged 1 coach from ECU to Hillarys Yacht Club with the departure time of 5:30 PM and return time of 9:00 PM (passing a few train stations).

Note: You are welcome to drive there, and there are plenty of parking spaces.



Thanks to Our Committees

General Chair
Prof Helge Janicke

Program Chairs
A/Prof Shihao Yan
Prof Mauro Barni
Prof Jiande Sun

Publication Chairs
Dr Shams Islam
Dr Jia Zhang
Prof Benedetta Tondi

Keynotes & Tutorials
Prof Parastoo Sadeghi
A/Prof Jing Dong
Prof Yue Rong

Operations Chair
Prof Paul Haskell-Dowland

Sponsorship Chair
Mr Derek Tighe

Government Chair
Prof Andrew Woodward

Award Chair
Prof A. Lee Swindlehurst
Dr Mohiuddin Ahmed

Finance Chair
Dr Ahmad Mohsin

Local Arrangements Chairs
Dr Peng Chen

Student Volunteers
Maha Intakhab Alam
Zeynab Khodkar
Zihan Peng
Chris Wang