

2025 IEEE International Workshop on Information Forensics and Security (WIFS 2025)

**Perth, Australia
1-4 December 2025**

IEEE Catalog Number:
ISBN:

CFP25WIF-POD
979-8-3315-7629-5



Copyright © 2025, IEEE

All Rights Reserved

Copyright and Reprint Permissions:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

*** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.

IEEE Catalog Number:	CFP25WIF-POD
ISBN (Print-On-Demand):	979-8-3315-7629-5
ISBN (Online):	979-8-3315-7628-8
ISSN:	2157-4766

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA

Phone:	(845) 758-0400
Fax:	(845) 758-2633
E-mail:	curran@proceedings.com
Web:	www.proceedings.com

TABLE OF CONTENTS

Physical/Machine-Learning Attacks Resilient Multi-Factor Authentication Employing Handwritten Challenge into Touch-Sensor PUF	1
<i>Ruochen Wang, Kosuke Kawamura, Jun Shiomi, Yoshihiro Midoh, Yuichi Tanaka, Minoru Kuribayashi Noriyuki Miura</i>	
Seeing Malware Differently: A Novel Signal-Based Graph and Image Approach to Detection	7
<i>Riccardo Bragaglia, Riccardo Lazzeretti</i>	
α -Forest: Proxy-Cloud Enabled Efficient and Secure Community Search over Encrypted Bipartite Graphs	13
<i>Xiaoxian Liu, Chen Chen, Xueqiao Liu, Xiaoyang Wang</i>	
GLFE: Video Frame Interpolation Forensics via Multi-Scale Global and Local Feature Exploitation	19
<i>Xiaowan Huang, Tongzhen Si, Xiaohui Yang</i>	
Physical Layer Authentication with Likelihood Test Using Machine Learning with Artificial Dataset	25
<i>Francesco Ardizzone, Stefano Tomasin</i>	
Security Analysis of RIS-Assisted Physical-Layer Authentication Over Multipath Channels	31
<i>Linda Senigaglia, Anna V. Guglielmi, Marco Baldi, Stefano Tomasin</i>	
Drone Detection on Wi-Fi Channels Using Radio Frequency Signal Power Variation Properties	37
<i>Yuchen Wang, Shihao Yan, Derek Tighe, Peng Chen, Ying He</i>	
STAR-RIS Aided Covert Communication with Symbiotic Backscatter	43
<i>Rong Chen, Jinsong Hu, Shihao Yan, Ruiquan Lin, Jun Wang, Hai Pei</i>	
Attention-based Mixture of Experts for Robust Speech Deepfake Detection	49
<i>Viola Negroni, Davide Salvi, Alessandro Ilic Mezza, Paolo Bestagini, Stefano Tubaro</i>	
CLIP Feature Selection Mechanism via Sparse Autoencoder for Generalized Deepfake Detection	55
<i>Lorenzo Berlincioni, Andrea Ciamarra, Pietro Pala, Roberto Caldelli, Alberto Del Bimbo</i>	
ADD: An Automated Neural Architecture Search Baseline for Deepfake Detection	61
<i>Ping Liu, Yuewei Lin, Jingen Liu, Yunchao Wei, Joey Tianyi Zhou</i>	
Deepfake Image Forger Detection	67
<i>Bin Deng, Yuanfang Guo, Wenqi Zhuo, Weina Xu, Junfu Wang, Liang Yang, Yunhong Wang</i>	
6D Movable Antenna Enhanced Covert Communication with Flexible Position and Rotation	73
<i>Longfa Luo, Jinsong Hu, Youjia Chen, Peng Kang, Jun Wang, Ruiquan Lin</i>	
Covert Waveform Design for Integrated Sensing and Communication System in Clutter Environment	79
<i>Xuyang Zhao, Jiangtao Wang, Xinyu Zhang</i>	
A Two-Phase Integrated Sensing and Communication-Assisted Covert D2D Communication Framework	85
<i>Bingbing Han, Jia Zhang, Shihao Yan, Ke Liu, Jiande Sun</i>	
Multiple Distributed Wardens with Amplify-and-Forward Fusing Strategy in Covert Communications	91
<i>Zhilin Chen, Jia Zhang, Xiaobo Zhou, Jiande Sun, Shihao Yan</i>	

Disentangling Moiré and Texture: Towards Robust Display-Recapture Detection for Document Images	96
<i>Peiquan Li, Changsheng Chen, Yulia Chernyshova, Dmitry Nikolaev, Shunquan Tan, Vladimir Arlazarov</i>	
Vision-Text Interactive Hybrid Granularity Proxy Representation Learning for AI-Generated Image Detection	102
<i>Feng Ding, Yue Zhang, Mengyao Xiao, Kangkang Wei, Zhangyi Shen, Hong Rao</i>	
Towards Practical Audio Phylogeny: Multi-Transformation Detection in Incomplete Trees	108
<i>Milica Gerhardt, Luca Cuccovillo, Patrick Aichroth</i>	
Training-free Source Attribution of AI-generated Images via Resynthesis	114
<i>Pietro Bongini, Valentina Molinari, Andrea Costanzo, Benedetta Tondi, Mauro Barni</i>	
DPF: A Dual Perturbation Framework for Face Privacy Protection with Authorized Recognition	120
<i>Ao Li, Ting Li, Huayue Sun, Rui Zhai, Rongrong Ni, Yao Zhao</i>	
Finger Vein Sample Compression using Recent AI-Based Still Image Compression Schemes	126
<i>Christof Kauba, Gerald Angerer, Andreas Uhl</i>	
Domain-Informed Eye Movement Biometrics with Practical Evaluation for VR/AR User Authentication	132
<i>Paul Sansah Gyreyiri, Diksha Shukla</i>	
Finger Vein Spoof GANs: Are they really useful to enhance PAD training?	138
<i>Tessnim Boulfoul, Valentin Pröpster, Andreas Vorderleitner, Andreas Uhl</i>	
Covert Communication in Sanitized Online Social Networks	144
<i>Zhiying Zhu, Zhongjie Ba, Guobiao Li, Zhenxing Qian, Xinpeng Zhang</i>	
Beam Split Aided Multi-User Near-Field Covert Communication under Wardens Collusion	150
<i>Duanrui Liao, Mingfeng Ji, Haojie Yin, Jinsong Hu, Youjia Chen, Jun Wang, Ruiquan Lin</i>	
PSyDUCK: Hiding Information in the Denoising Process of Latent Diffusion Models	156
<i>Aqib Mahfuz, Georgia Channing, Mark van der Wilk, Philip H.S. Torr, Fabio Pizzati Christian Schroeder de Witt</i>	
Hierarchical Multihospital Management based on Progressive Secret Sharing and Reversible Data Hiding	162
<i>Jing Li, Yannan Ren, Jiantao Wang, Xuquan Wang, Lingchen Gu, Jiande Sun, Wenbo Wan</i>	
A Targeted Attack against Certifiably Robust Smoothed Classifiers	168
<i>Kai Zeng, Mauro Barni, Benedetta Tondi</i>	
Trust-Based Framework for Securing Decentralized Federated Learning against Malicious Clients	174
<i>Imen Ben Said, Talal Halabi, Adel Abusitta, Mohammad Zulkernine</i>	
Privacy-Preserving State Estimation with Crowd Sensors: An Information-Theoretic Respective	180
<i>F. Farokhi</i>	
GAFIN: Gradient Direction-Agnostic Differential Privacy Control for Federated Learning via Nussbaum-Enhanced PID Tracking	186
<i>Chen Li, Xuelei Qi, Kai Wu, Xin Yuan, Wei Ni, Ren Ping Liu, Quan Z. Sheng</i>	