

2024 IEEE International Workshop on Information Forensics and Security (WIFS 2024)

**Rome, Italy
2-5 December 2024**



**IEEE Catalog Number: CFP24WIF-POD
ISBN: 979-8-3503-6443-9**

**Copyright © 2024 by the Institute of Electrical and Electronics Engineers, Inc.
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:	CFP24WIF-POD
ISBN (Print-On-Demand):	979-8-3503-6443-9
ISBN (Online):	979-8-3503-6442-2
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

CURRAN ASSOCIATES INC.
proceedings
.com

2024 16th IEEE INTERNATIONAL WORKSHOP ON INFORMATION FORENSICS AND SECURITY (WIFS) 2024

TABLE OF CONTENTS

ORAL SESSION 1 – BIOMETRICS I

- **Explainable Presentation Attack Detection of Digital Fingerprints (Paper ID 60)...1**
Augustin Diers (GREYC), Christophe Rosenberger (ENSICAEN)
- **Effectiveness of learning-based image codecs on fingerprint storage (Paper ID 85)...7**
Daniele Mari (Università di Padova), Saverio Cavašin (Università di Padova), Simone Milani (Università di Padova), Mauro Conti (Università di Padova)
- **TempCharBERT: Keystroke Dynamics for Continuous Access Control Based on Pre-trained Language Models (Paper ID 102)...13**
Matheus Simão Caixeta, Fabiano Oliveira Costa Prado (UNESP), Omar Abdul Wahab (Polytechnique Montréal), Anderson R. Avila (INRS-EMT)
- **Synthetic Ethnicity Alteration for Diversifying Face Datasets – Investigating Recognition and Quality (Paper ID 13)...19**
Praveen Kumar Chandaliya (Sardar Vallabhbhai National Institute of Technology), Kiran Raja (NTNU), Haoyu Zhang (NTNU), Raghavendra Ramachandra (NTNU), Christoph Busch (NTNU)

ORAL SESSION 2 – MULTIMEDIA FORENSICS I

- **Assessing shadows and reflections consistency in AI-generated images (Paper ID 9)...25**
Massimo Iuliani (Amped Software), Stefano Bianchi (Amped Software), Andrea Paghera (European Forensic Institute), Marco Fontani (Amped Software), Martino Jerian (Amped Software)
- **Assessing the Viability of Synthetic Physical Copy Detection Patterns on Different Imaging Systems (Paper ID 45)...31**
Roman Chaban (University of Geneva), Brian Pulfer (University of Geneva), Slava Voloshynovskiy (University of Geneva)
- **A Taxonomy of Miscompressions: Preparing Image Forensics for Neural Compression (Paper ID 59)...37**
Nora Hofer (University of Innsbruck), Rainer Böhme (University of Innsbruck)

- **Spectrogram-Based Detection of Auto-Tuned Vocals in Music Recordings (Paper ID 86)...43**

Mahyar Gohari (University of Brescia), Paolo Bestagini (Politecnico di Milano), Sergio Benini (University of Brescia), Nicola Adami (University of Brescia)

- **PLUS Temporal Image Forensics Dataset (Paper ID 97)...49**

Robert Jöchl (University of Salzburg), Andreas Uhl (University of Salzburg)

- **Interactive Event Sifting using Bayesian Graph Neural Networks (Paper ID 104)...55**

José Nascimento (University of Campinas), Nathan Jacobs (Washington University in St. Louis), Anderson Rocha (University of Campinas)

ORAL SESSION 3 – BIOMETRICS II

- **Fixed-length Dense Descriptor for Efficient Fingerprint Matching (Paper ID 5)...60**

Zhiyu Pan (Tsinghua University), Yongjie Duan (Tsinghua University, China), Jianjiang Feng (Tsinghua University), Jie Zhou (Tsinghua University)

- **Strengthened Fuzzy Extractors using Turbo-codes: Case Study on Finger Vein Authentication (Paper ID 27)...66**

Enrique Argones Rua (KU Leuven), Emanuele Maiorana (Roma Tre University), Patrizio Campisi (Roma Tre University)

- **Ternary Neural Networks for Gait Identification in Wearable Devices (Paper ID 31)...72**

Giacomo Agnetti (Politecnico di Torino), Andrea Migliorati (Politecnico di Torino), Daniele Mari (Università di Padova), Tiziano Bianchi (Politecnico di Torino), Simone Milani (Università di Padova), Enrico Magli (Politecnico di Torino)

- **Vision through distortions: Atmospheric Turbulence- and Clothing-invariant long-range recognition (Paper ID 34)...78**

Gabriel Capiteli Bertocco (University of Campinas), Fernanda Andaló (University of Campinas), Terrance E Boulton (University of Colorado Colorado Springs), Anderson Rocha (University of Campinas)

- **MONOT: High-Quality Privacy-compliant Morphed Synthetic Images for Everyone (Paper ID 48)...84**

Guido Borghi (University of Modena and Reggio Emilia), Nicolò Di Domenico (University of Bologna), Matteo Ferrara (University of Bologna), Annalisa Franco (University of Bologna), Uzma Latif (University of Bologna), Davide Maltoni (University of Bologna)

ORAL SESSION 4 – CYBERSECURITY

- **Smart Contract Kill Switch for Security in a Private Blockchain-based Software Transaction System (Paper ID 16)...92**

Soonhong Kwon (Sejong University), Wooyoung Son (Sejong University), Jong-Hyoun Lee (Sejong University)

- **GUARD: Graph-based Unknown Attack Recognition and Detection (Paper ID 21)...98**

Shane R Dirksen (UC Santa Barbara), John Korah (Cal Poly Pomona)

- **Efficient Audio Deepfake Detection using WavLM with Early Exiting (Paper ID 93)...104**

Arthur S Pimentel (INRS), Yi Zhu (INRS), Heitor R Guimarães (INRS), Tiago H Falk (INRS-EMT)

- **Collective Threshold Multiparty Private Set Intersection Protocols for Cyber Threat Intelligence (Paper ID 100)...110**

Chelsea Guan (Delft University of Technology), Jorrit van Assen (Delft University of Technology), Zekeriya Erkin (TU Delft)

ORAL SESSION 5 – MULTIMEDIA FORENSICS II

- **Now ForReal: Towards Practical Forensic Room Identification with Real-World Audio Data (Paper ID 107)...116**

Denise Moussa (Friedrich-Alexander-University Erlangen-Nuremberg/Federal Criminal Police Office of Germany), Leon Huber (Friedrich-Alexander University Erlangen-Nuremberg), Germans Hirsch (Friedrich-Alexander University Erlangen-Nuremberg), Christian Riess (Friedrich-Alexander University Erlangen-Nuremberg)

- **Tiny autoencoders are effective few-shot generative model detectors (Paper ID 108)...122**

Luca Bindini (University of Florence), Giulia Bertazzini (University of Florence), Daniele Baracchi (University of Florence), Dasara Shullani (University of Florence), Paolo Frasconi (University of Florence), Alessandro Piva (University of Florence)

- **Beyond the Brush: Fully-automated Crafting of Realistic Inpainted Images (Paper ID 109)...128**

Giulia Bertazzini (University of Florence), Chiara Albisani (University of Florence), Daniele Baracchi (University of Florence), Dasara Shullani (University of Florence), Alessandro Piva (University of Florence)

- **SWIFT: Semantic Watermarking for Image Forgery Thwarting (Paper ID 64)...134**

Gautier Evennou (IRISA/IMATAG), Vivien Chappelier (IMATAG), Ewa Kijak (IRISA), Teddy Furon (INRIA)

ORAL SESSION 6 – DATA HIDING

- **Transferable Watermarking to Self-supervised Pre-trained Graph Encoders by Trigger Embeddings (Paper ID 19)...140**

Hanzhou Wu (Shanghai University)

- **Steganalysis in Directional JPEG Images (Paper ID 40)...146**

Benedikt Lorch (University of Innsbruck), Rainer Böhme (University of Innsbruck)

- **Evaluation of Security of ML-based Watermarking: Copy and Removal Attacks (Paper ID 46)...152**
Vitaliy Kinakh (University of Geneva), Brian Pulfer (University of Geneva), Yury Belousov (University of Geneva), Pierre Fernandez (INRIA), Teddy Furon (INRIA), Slava Voloshynovskiy (University of Geneva)
- **Errorless Robust JPEG Steganography for Pixel Images (Paper ID 76)...158**
Jan Butora (CNRS), Patrick Bas (CNRS), Etienne Levecque (CNRS)
- **How to Form Bags in Batch Steganography (Paper ID 81)...164**
Eli Dworetzky (Binghamton University), Jessica Fridrich (SUNY, Binghamton)
- **Kerckhoffs in Prison: A Study of the Steganalyst's Knowledge (Paper ID 99)...170**
Martin Beneš (University of Innsbruck), Rainer Böhme (University of Innsbruck)

SPECIAL SESSION – SYNERGIES BETWEEN BIOMETRICS AND FORENSICS

- **AgeDiff: Latent Diffusion-based Face Age Editing with Dual Cross-Attention (Paper ID 47)...176**
Marcel Grimmer (NTNU), Christoph Busch (NTNU)
- **SynChildFace: Fine-tuning Face Recognition for Children with Synthetic Data (Paper ID 79)...182**
Franck V. Souop Kouam (Hochschule Darmstadt), Christian Rathgeb (Hochschule Darmstadt), Mathias Ibsen (Hochschule Darmstadt), Christoph Busch (Hochschule Darmstadt)
- **Combined CNN and ViT features off-the-shelf: Another astounding baseline for recognition (Paper ID 112)...188**
Fernando Alonso-Fernandez (Halmstad University), Kevin Hernandez-Diaz (Halmstad University), Prayag Tiwari (Halmstad University), Josef Bigun (Halmstad University, Sweden)

SPECIAL SESSION – SYNTHETIC MEDIA DETECTION IN MULTI-MEDIA FORENSICS I

- **Explainable Artifacts for Synthetic Western Blot Source Attribution (Paper ID 38)...194**
João Phillipe Cardenuto (University of Campinas), Sara Mandelli (Politecnico di Milano), Daniel Moreira (Loyola University Chicago), Paolo Bestagini (Politecnico di Milano), Edward Delp (Purdue University), Anderson Rocha (University of Campinas)
- **On the use of mixup augmentation for synthetic image attribution in the wild (Paper ID 52)...200**
Jun Wang (University of Siena), Benedetta Tondi (University of Siena), Mauro Barni (University of Siena)
- **When Synthetic Traces Hide Real Content: Analysis of Stable Diffusion Image Laundering (Paper ID 74)...206**
Sara Mandelli (Politecnico di Milano), Paolo Bestagini (Politecnico di Milano), Stefano Tubaro (Politecnico di Milano)

- **Localization of Synthetic Manipulations in Western Blot Images (Paper ID 75)...212**

Anmol Manjunath (Politecnico di Milano), Viola Negroni (Politecnico di Milano), Sara Mandelli (Politecnico di Milano), Daniel Moreira (Loyola University Chicago), Paolo Bestagini (Politecnico di Milano)

ORAL SESSION 7 – COMMUNICATION AND INFORMATION THEORETIC SECURITY

- **Randomized Distributed Function Computation with Semantic Communications: Applications to Privacy (Paper ID 15)...218**

Onur Günlü (Linköping University)

- **Provable Performance Guarantees of Copy Detection Patterns (Paper ID 29)...224**

Joakim Tutt (University of Geneva), Slava Voloshynovskiy (University of Geneva)

- **PUF Authentication for a Modular Coding Scheme (Paper ID 49)...230**

Johannes Voichtleitner (Technical University of Munich), Christoph Frisch (Technical University of Munich), Ullrich Mönich (Technical University of Munich), Michael Pehl (Technical University of Munich), Luis Torres-Figueroa (Technical University of Munich), Moritz Wiese (Technical University of Munich)

- **Detecting 5G Narrowband Jammers with CNN, k-nearest Neighbors, and Support Vector Machines (Paper ID 67)...236**

Matteo Varotto (Hochschule Darmstadt), Florian Heinrichs (Hochschule Darmstadt), Timo Schuerg (Hochschule Darmstadt), Stefano Tomasin (Università di Padova), Stefan Valentin (Hochschule Darmstadt)

- **DPGEM: Differentially Private Generative Model with Exponential Mechanism (Paper ID 103)...242**

Usman Hassan (University of Kentucky), Jiangyue Zhu (University of Kentucky), Dongjie Chen (University of California, Davis), Sen-Ching Samson Cheung (University of Kentucky)

- **Vulnerabilities in Machine Learning-Based Voice Disorder Detection Systems (Paper ID 88)...248**

Gianpaolo Perelli (University of Cagliari), Andrea Panzino (University of Cagliari), Roberto Casula (University of Cagliari), Marco Micheletto (University of Cagliari), Giulia Orrù (University of Cagliari), Gian Luca Marcialis (University of Cagliari)

SPECIAL SESSION 3 – SYNTHETIC MEDIA DETECTION IN MULTI-MEDIA FORENSICS II

- **Spotting fully-synthetic facial images via local camera surface frames (Paper ID 77)...254**

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

- **TGIF: Text-Guided Inpainting Forgery Dataset (Paper ID 91)...260**

Hannes Mareen (Ghent University), Dimitrios Karageorgiou (Information Technologies Institute – Centre for Research and Technology Hellas), Glenn Van Wallendael (Ghent University), Peter Lambert

(Ghent University), Symeon Papadopoulos (Information Technologies Institute – Centre for Research and Technology Hellas)

- **Exploring the Adversarial Robustness of CLIP for AI-generated Image Detection (Paper ID 96)...266**
Vincenzo De Rosa (University Federico II of Naples), Fabrizio Guillaro (University Federico II of Naples), Giovanni Poggi (University Federico II of Naples), Davide Cozzolino (University Federico II of Naples), Luisa Verdoliva (University Federico II of Naples)
- **Attribution of Diffusion Based Deepfake Speech Generators (Paper ID 105)...272**
Kratika Bhagtani (Purdue University), Amit Kumar Singh Yadav (Purdue University), Paolo Bestagini (Politecnico di Milano), Edward Delp (Purdue University)

POSTER SESSION

- **Take It Easy: Label-Adaptive Self-Rationalization for Fact Verification and Explanation Generation (Paper ID 26)...278**
Jing Yang (University of Campinas), Anderson Rocha (University of Campinas)
- **Privacy Preserving Protest Dynamics (Paper ID 51)...284**
Cohen G Archbold (University of Kentucky), Usman Hassan (University of Kentucky), Nazmus Sakib (University of Kentucky), Sen-ching Samoson Cheung (Mialab), Abdullah Al Zubaer Imran (University of Kentucky)
- **When does gradient estimation improve black-box adversarial attacks? (Paper ID 63)...290**
Enoal Gesny (INRIA), Eva Giboulot (INRIA), Teddy Furon (INRIA)
- **Privacy-aware Berrut Approximated Coded Computing applied to Federated Learning (Paper ID 14)...296**
Xavier Martínez-Luaña (GRADIANT), Manuel Fernández Veiga (University of Vigo), Rebeca Díaz-Redondo (University of Vigo)

DEMO SESSION

- **MedTech Chain: Decentralised, Secure and Privacy-preserving Platform for Medical Device Data Research (Paper ID 114)...302**
Alin Petru-Rosu (TU Delft), Tamara Tataru (TU Delft), Jegor Zelenjak (TU Delft), Roland Kromes (TU Delft), Zekeriya Erkin (TU Delft)
- **MedGuard: Securing Medical iot with compiler polymorphism (Paper ID 115)...305**
Dimitris Santorinaios (Zortenet), Akis Kourtis (Zortenet), George Oikonomakis (Zortenet)
- **Unmasking the Unseen: CryptojackingTrap, the Most Resilient Evasion-Proof Cryptojacking Malware Detection Algorithm (Paper ID 113)...308**
Atefeh Zareh Chahoki (University of Trento), Hamid Reza Shahriari (Amirkabir University of Technology), Marco Roveri (University of Trento)