

2023 IEEE International Workshop on Information Forensics and Security (WIFS 2023)

**Nurnberg, Germany
4 – 7 December 2023**



**IEEE Catalog Number: CFP23WIF-POD
ISBN: 979-8-3503-2492-1**

**Copyright © 2023 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:	CFP23WIF-POD
ISBN (Print-On-Demand):	979-8-3503-2492-1
ISBN (Online):	979-8-3503-2491-4
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

TABLE OF CONTENTS

Robust Retraining-Free GAN Fingerprinting via Personalized Normalization	1
<i>Jianwei Fei, Zhihua Xia, Benedetta Tondi, Mauro Barni</i>	
JPEG Steganalysis using Leaked Cover Thumbnails	7
<i>Martin Beneš, Benedikt Lorch, Rainer Böhme</i>	
An Explainable Model-Agnostic Algorithm for CNN-Based Biometrics Verification.....	13
<i>Fernando Alonso-Fernandez, Kevin Hernandez-Diaz, José M. Buades, Prayag Tiwari, Josef Bigun</i>	
A First Look at Shill Looping in NFT Ecosystem	19
<i>Ankit Gangwal, Apoorva Thirupathi, Alessandro Brighente, Mauro Conti</i>	
The Automotive BlackBox: Towards a Standardization of Automotive Digital Forensics.....	25
<i>Kim Strandberg, Ulf Arnljung, Tomas Olovsson</i>	
Observing Bag Gain in JPEG Batch Steganography	31
<i>Edgar Kaziakhmedov, Eli Dworetzky, Jessica Fridrich</i>	
One Standard to Rule Them All? Assessing the Disruptive Potential of Jamming Attacks on Matter Networks	37
<i>Felix Klement, Emily Vorderwülbeke, Stefan Katzenbeisser</i>	
Towards Traitor Tracing in Black-And-White-Box DNN Watermarking with Tardos-Based Codes	43
<i>Elena Rodríguez-Lois, Fernando Pérez-González</i>	
Advancing Audio Phylogeny: A Neural Network Approach for Transformation Detection.....	49
<i>Milica Gerhardt, Luca Cuccovillo, Patrick Aichroth</i>	
An Open Dataset of Synthetic Speech.....	55
<i>Artem Yaroshchuk, Christoforos Papastergiou, Luca Cuccovillo, Patrick Aichroth, Konstantinos Votis, Dimitrios Tzovaras</i>	
Are You Really Alone? Detecting the Use of Speech Separation Techniques on Audio Recordings	61
<i>Davide Salvi, Mirco Pezzoli, Sara Mandelli, Paolo Bestagini, Stefano Tubaro</i>	
Single and Multi-Speaker Cloned Voice Detection: From Perceptual to Learned Features	67
<i>Sarah Barrington, Romit Barua, Gautham Koorma, Hany Farid</i>	
Audio Spectrogram Transformer for Synthetic Speech Detection via Speech Formant Analysis	73
<i>Luca Cuccovillo, Milica Gerhardt, Patrick Aichroth</i>	
Stochastic Digital Twin for Copy Detection Patterns	79
<i>Yury Belousov, Olga Taran, Vitaliy Kinakh, Slava Voloshynovskiy</i>	
Leveraging Data Geometry to Mitigate CSM in Steganalysis.....	85
<i>Rony Abecidan, Vincent Itier, Jérémie Boulanger, Patrick Bas, Tomáš Pevný</i>	
Three Bricks to Consolidate Watermarks for Large Language Models.....	91
<i>Pierre Fernandez, Antoine Chaffin, Karim Tit, Vivien Chappelier, Teddy Furon</i>	
Recoverable Active Protection Framework for Neural Network Models	100
<i>Lin Huang, Gejian Zhao, Chuan Qin</i>	

Enhancement Strategies for Copy-Paste Generation & Localization in RGB Satellite Imagery.....	106
<i>Edoardo Daniele Cannas, Sriram Baireddy, Paolo Bestagini, Stefano Tubaro, Edward J. Delp</i>	
Distribution-Agnostic Database De-Anonymization Under Synchronization Errors.....	112
<i>Serhat Bakirtas, Elza Erkip</i>	
PRNU-Based Source Camera Statistical Certification.....	118
<i>Marina Gardella, Pablo Musé, Miguel Colom, Jean-Michel Morel, Denis Perraud</i>	
AlphaNet: Single Morphing Attack Detection using Multiple Contributors.....	124
<i>Juan Tapia, Christoph Busch</i>	
Protecting Voice-Controlled Devices Against LASER Injection Attacks.....	130
<i>Hashim Ali, Dhimant Khuttan, Rafi Ud Daula Refat, Hafiz Malik</i>	
Practical Wiretap Code Design by Concatenated Autoencoder and LDPC Codes.....	136
<i>Shangxuan Lyu, Ramprasad Raghunath, Luca Kunz, Karl-Ludwig Besser, Pin-Hsun Lin, Eduard A. Jorswieck</i>	
Optimizing Key-Selection for Face-Based One-Time Biometrics via Morphing.....	143
<i>Dailé Osorio-Roig, Mahdi Ghafourian, Christian Rathgeb, Ruben Vera-Rodriguez, Christoph Busch, Julian Fierrez</i>	
Reversing Deep Face Embeddings with Probable Privacy Protection.....	149
<i>Dailé Osorio-Roig, Paul A. Gerlitz, Christian Rathgeb, Christoph Busch</i>	
Private Variable-Length Coding with Non-Zero Leakage.....	155
<i>Amirreza Zamani, Tobias J. Oechtering, Mikael Skoglund</i>	
Private Variable-Length Coding with Zero Leakage.....	161
<i>Amirreza Zamani, Tobias J. Oechtering, Deniz Gündüz, Mikael Skoglund</i>	
MT-PRO: Multibiometric Template Protection Based on Homomorphic Transciphering.....	167
<i>Pia Bauspieß, Chiara-Marie Zok, Anamaria Costache, Christian Rathgeb, Jascha Kolberg, Christoph Busch</i>	
Securing Voice Biometrics: One-Shot Learning Approach for Audio Deepfake Detection.....	173
<i>Awais Khan, Khalid Mahmood Malik</i>	
On Exploring Audio Anomaly in Speech.....	179
<i>Tiago Roxo, Joana Cabral Costa, Pedro R. M. Inácio, Hugo Proença</i>	
CDP-Sim: Similarity Metric Learning to Identify the Fake Copy Detection Patterns.....	185
<i>Hédi Zeghidi, Carlos Crispim-Junior, Iuliia Tkachenko</i>	
Fully Homomorphic Encryption Operators for Score and Decision Fusion in Biometric Identification.....	191
<i>Tilak Sharma, Mahika Wason, Vishnu Boddeti, Arun Ross, Nalini Ratha</i>	
To Impute Or Not: Recommendations for Multibiometric Fusion.....	197
<i>Melissa R Dale, Elliot Singer, Bengt J. Borgström, Arun Ross</i>	

Author Index