

# **2019 IEEE International Workshop on Information Forensics and Security (WIFS 2019)**

**Delft, Netherlands  
9 – 12 December 2019**



**IEEE Catalog Number: CFP19WIF-POD  
ISBN: 978-1-7281-3218-1**

**Copyright © 2019 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:	CFP19WIF-POD
ISBN (Print-On-Demand):	978-1-7281-3218-1
ISBN (Online):	978-1-7281-3217-4
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# TABLE OF CONTENTS

<b>DETECTION OF CYBER GROOMING IN ONLINE CONVERSATION</b> .....	1
<i>P. Bours, H. Kulsrud</i>	
<b>SIAMESE NETWORKS FOR STATIC KEYSTROKE DYNAMICS AUTHENTICATION</b> .....	7
<i>R. Giot, A. Rocha</i>	
<b>PHYSICAL LAYER PRIVACY IN BROADCAST CHANNELS</b> .....	13
<i>P. Lin, C. Kuhn, T. Strufe, E. Jorswieck</i>	
<b>POOLED STEGANALYSIS IN JPEG: HOW TO DEAL WITH THE SPREADING STRATEGY?</b> .....	19
<i>A. Zakaria, M. Chaumont, G. Subsol</i>	
<b>BLIND PHYSICAL LAYER AUTHENTICATION OVER FADING WIRELESS CHANNELS THROUGH MACHINE LEARNING</b> .....	25
<i>L. Senigagliesi, L. Cintoni, M. Baldi, E. Gambi</i>	
<b>TEMPLATE PROTECTION BASED ON HOMOMORPHIC ENCRYPTION: COMPUTATIONALLY EFFICIENT APPLICATION TO IRIS-BIOMETRIC VERIFICATION AND IDENTIFICATION</b> .....	31
<i>J. Kolberg, P. Bausipieß, M. Gomez-Barrero, C. Rathgeb, M. Durmuth, C. Busch</i>	
<b>BLIND VOCODER SPEECH RECONSTRUCTION USING GENERATIVE ADVERSARIAL NETWORKS</b> .....	37
<i>Y. Blum, D. Burshtein</i>	
<b>BIOMETRIC TEMPLATE PROTECTION IN THE IMAGE DOMAIN USING NON-INVERTIBLE GREY-SCALE TRANSFORMS</b> .....	43
<i>L. Debiasi, S. Kirchgasser, B. Prommegger, A. Uhl, A. Grudzien, M. Kowalski</i>	
<b>ENHANCING JPEG STEGANOGRAPHY USING ITERATIVE ADVERSARIAL EXAMPLES</b> .....	49
<i>H. Mo, T. Song, B. Chen, W. Luo, J. Huang</i>	
<b>GROUP MEMBERSHIP VERIFICATION WITH PRIVACY: SPARSE OR DENSE?</b> .....	55
<i>M. Gheisari, T. Furon, L. Amsaleg</i>	
<b>ON THE PRECISE PHASE RECOVERY FOR PHYSICAL-LAYER AUTHENTICATION IN DYNAMIC CHANNELS</b> .....	62
<i>H. Vogt, C. Li, A. Sezgin, C. Zenger</i>	
<b>FILE FRAGMENTATION IN THE WILD: A PRIVACY-FRIENDLY APPROACH</b> .....	68
<i>V. Meer, H. Jonker, G. Dols, H. Beek, J. Bos, M. Eekelen</i>	
<b>A VERSION SPACE PERSPECTIVE ON DIFFERENTIALLY PRIVATE POOL-BASED ACTIVE LEARNING</b> .....	74
<i>S. Rane, A. Brito</i>	
<b>DEBIASING OF SRAM PUFs: SELECTION AND BALANCING</b> .....	80
<i>L. Kusters, F. Willems</i>	
<b>ON THE ROBUSTNESS TO ADVERSARIAL EXAMPLES OF NEURAL ODE IMAGE CLASSIFIERS</b> .....	86
<i>F. Carrara, R. Caldelli, F. Falchi, G. Amato</i>	
<b>ADVERSARIAL CNN TRAINING UNDER JPEG LAUNDERING ATTACKS: A GAME-THEORETIC APPROACH</b> .....	92
<i>M. Barni, D. Huang, B. Li, B. Tondi</i>	
<b>COPY SENSITIVE GRAPHICAL CODE ESTIMATION: PHYSICAL VS NUMERICAL RESOLUTION</b> .....	98
<i>R. Yadav, I. Tkachenko, A. Tremeau, T. Fournel</i>	
<b>VISUAL FEATURE SPACE ANALYSES OF FACE MORPHING DETECTORS</b> .....	104
<i>C. Seibold, A. Hilsmann, A. Makrushin, C. Kraetzer, P. Eisert</i>	
<b>EFFICIENT BOUND FOR CONDITIONAL MIN-ENTROPY OF PHYSICAL UNCLONABLE FUNCTIONS BEYOND IID</b> .....	110
<i>F. Wilde, C. Frisch, M. Pehl</i>	
<b>SPN-CNN: BOOSTING SENSOR-BASED SOURCE CAMERA ATTRIBUTION WITH DEEP LEARNING</b> .....	116
<i>M. Kirchmer, C. Johnson</i>	
<b>SINGLE-COMPONENT PRIVACY GUARANTEES IN HELPER DATA SYSTEMS AND SPARSE CODING WITH AMBIGUATION</b> .....	122
<i>B. Razeghi, T. Stanko, B. Skoric, S. Voloshynovskiy</i>	

<b>SECRET KEY GENERATION FROM A TWO COMPONENT COMPOUND SOURCE WITH RATE CONSTRAINED ONE WAY COMMUNICATION: PERFECT SECRECY</b> .....	128
<i>S. Baur, N. Cai, M. Wiese, H. Boche</i>	
<b>A POWER CONTROL GAME INVOLVING JAMMING AND EAVESDROPPING DEFENSE</b> .....	134
<i>A. Garnaev, W. Trappe</i>	
<b>IMAGE SEMANTIC REPRESENTATION FOR EVENT UNDERSTANDING</b> .....	140
<i>C. Rodrigues, L. Pereira, A. Rocha, Z. Dias</i>	
<b>RANKING-BASED ATTACKS TO IN-REGION LOCATION VERIFICATION SYSTEMS</b> .....	146
<i>A. Brighente, F. Formaggio, G. Ruvoletto, S. Tomasin</i>	
<b>RESOURCE ALLOCATION FOR SECURE COMMUNICATION SYSTEMS: ALGORITHMIC SOLVABILITY</b> .....	152
<i>H. Boche, R. Schaefer, H. Poor</i>	
<b>INCREMENTAL LEARNING FOR THE DETECTION AND CLASSIFICATION OF GAN-GENERATED IMAGES</b> .....	158
<i>F. Marra, C. Saltori, G. Boato, L. Verdoliva</i>	
<b>DETECTING AND SIMULATING ARTIFACTS IN GAN FAKE IMAGES</b> .....	164
<i>X. Zhang, S. Karaman, S. Chang</i>	
<b>AUTOMATIC RELIABILITY ESTIMATION FOR SPEECH AUDIO SURVEILLANCE RECORDINGS</b> .....	170
<i>C. Borrelli, P. Bestagini, F. Antonacci, A. Sarti, S. Tubaro</i>	
<b>PRIVACY-AWARE LOCATION SHARING WITH DEEP REINFORCEMENT LEARNING</b> .....	176
<i>E. Erdemir, P. Dragotti, D. Gunduz</i>	
<b>INFORMATION SECURITY MEETS ADVERSARIAL EXAMPLES</b> .....	182
<i>M. Kirchmer, C. Pasquini, I. Shumailov</i>	
<b>Author Index</b>	