Lecture Notes in Computer Science 12617

Founding Editors

Gerhard Goos
Karlsruhe Institute of Technology, Karlsruhe, Germany
Juris Hartmanis
Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino
Purdue University, West Lafayette, IN, USA
Wen Gao
Peking University, Beijing, China
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Gerhard Woeginger
RWTH Aachen, Aachen, Germany
Moti Yung
Columbia University, New York, NY, USA

More information about this subseries at http://www.springer.com/series/7410

Xianfeng Zhao · Yun-Qing Shi ·
Alessandro Piva · Hyoung Joong Kim (Eds.)

Digital Forensics and Watermarking

19th International Workshop, IWDW 2020
Melbourne, VIC, Australia, November 25–27, 2020
Revised Selected Papers

Springer

Editors
Xianfeng Zhao
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Alessandro Piva
Department of Information Engineering
University of Florence
Florence, Italy

Yun-Qing Shi
Department of Electrical
and Computer Engineering
New Jersey Institute of Technology
Newark, NJ, USA

Hyoung Joong Kim
School of Cybersecurity
Korea University
Seoul, Korea (Republic of)

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-69448-7 ISBN 978-3-030-69449-4 (eBook)
https://doi.org/10.1007/978-3-030-69449-4

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The International Workshop on Digital-forensics and Watermarking (IWDW) is a premier forum for researchers and practitioners working on novel research, development and application of digital watermarking and forensics techniques for multimedia security. The 19th International Workshop on Digital-forensics and Watermarking (IWDW 2020) was organized by the Digital Research & Innovation Capability Platform at Swinburne University of Technology, Australia and the State Key Laboratory of Information Security at the Institute of Information Engineering, Chinese Academy of Sciences. It was held in Melbourne, Australia, during November 25–27, 2020. Although IWDW 2020 was held with the aid of an online conference system due to the persistent Covid-19 epidemic situation, it was very successful and as significant as the previous editions. More than 160 people attended the workshop online.

IWDW 2020 aimed at promoting research and development in both new and traditional areas of multimedia security. The organizers updated the topics of interest in the Call For Papers to reflect the new directions of emerging technologies such as AI-generated multimedia and detection of them, DeepFake videos and detection of them, convolutional neural networks and deep learning for multimedia security, and social media steganography. IWDW 2020 received 43 valid submissions. The decisions of the Technical Program Committee were made on a highly competitive basis. Only 20 submissions were accepted. The accepted papers cover many important topics in current research in multimedia security, and the presentations were organized into four sessions including "Steganography and Steganalysis", "Watermarking", "Multimedia Forensics" and "Security of AI-based Multimedia Applications". In addition, 3 invited keynotes including "Using the sensor noise model to design better steganographic schemes" by Dr. Patrick Bas, "DeepFake detection" by Dr. Wenbo Zhou, and "On the sharing-based model of steganography" by Prof. Xianfeng Zhao reported new advances.

We would like to thank all of the authors, committee members, reviewers, keynote speakers, volunteers and attendees. It is the participation of them all that made a wonderful and special IWDW again. And we appreciate the generous support from the organizers and sponsors. Finally, we hope that the readers will enjoy this volume and find it rewarding in providing inspirations and possibilities for future work.

December 2020

Xianfeng Zhao
Yun-Qing Shi
Alessandro Piva
Hyoung Joong Kim

Organization

General Chairs

Yun-Qing Shi	New Jersey Institute of Technology, USA
Yang Xiang	Swinburne University of Technology, Australia

Technical Program Chairs

Xianfeng Zhao	Chinese Academy of Sciences, China
Hyoung Joong Kim	Korea University, Korea
Alessandro Piva	University of Florence, Italy

Program Committee

Pradeep K. Atrey	University at Albany, USA
Mauro Barni	University of Siena, Italy
Patrick Bas	University of Lille, France
Marc Chaumont	University of Montpellier, France
Pedro Comesaña Alfaro	University of Vigo, Spain
Isao Echizen	National Institute of Informatics, Japan
Teddy Furon	Inria, France
Anthony T. S. Ho	University of Surrey, UK
Jiwu Huang	Shenzhen University, China
Yongfeng Huang	Tsinghua University, China
Xinghao Jiang	Shanghai Jiao Tong University, China
Xiangui Kang	Sun Yat-sen University, China
Sang-ug Kang	Sangmyung University, Korea
Stefan Katzenbeisser	University of Passau, Germany
Suah Kim	Korea University, Korea
Christian Kraetzer	Otto-von-Guericke University of Magdeburg, Germany
Minoru Kuribayashi	Okayama University, Japan
Bin Li	Shenzhen University, China
Xiaolong Li	Beijing Jiaotong University, China
Feng Liu	Chinese Academy of Sciences, China
Wojciech Mazurczyk	Warsaw University of Technology, Poland
Jiangqun Ni	Sun Yat-sen University, China
Akira Nishimura	Tokyo University of Information Sciences, Japan
Fernando Pérez-González	University of Vigo, Spain

William Puech	University of Montpellier, France
Pascal Schöttle	Management Center Innsbruck, Austria
Yun-Qing Shi	New Jersey Institute of Technology, USA
Luisa Verdoliva	University of Naples Federico II, Italy
Hongxia Wang	Sichuan University, China
Kai Wang	Grenoble-INP GIPSA-Lab, France
Andreas Westfeld	University of Applied Sciences Dresden, Germany
Yang Xiang	Swinburne University of Technology, Australia
Wei Qi Yan	Auckland University of Technology, New Zealand
Dengpan Ye	Wuhan University, China
Xinpeng Zhang	Fudan University, China
Weiming Zhang	University of Science and Technology of China, China
Yao Zhao	Beijing Jiaotong University, China
Guopu Zhu	Chinese Academy of Sciences, China

Organization Chairs

Yang Xiang	Swinburne University of Technology, Australia
Hong Zhang	Chinese Academy of Sciences, China

Organization Committee

Abby Xu	Insightek, Australia
Xiaolei He	Chinese Academy of Sciences, China
Yanfei Tong	Chinese Academy of Sciences, China

Additional Reviewers

Qi Chang
Rong Huang
Jian Li
Bo Ou
David Vázquez-Padín
Kai Zeng

Sponsors

Chinese Academy of Sciences

Swinburne University of Technology

New Jersey Institute of Technology

Springer

Contents

Steganography and Steganalysis

Multi-modal Steganography Based on Semantic Relevancy 3
Yuting Hu, Zhongliang Yang, Han Cao, and Yongfeng Huang

Variable Rate Syndrome-Trellis Codes for Steganography on Bursty Channels 15
Bingwen Feng, Zhiquan Liu, Kaimin Wei, Wei Lu, and Yuchun Lin

Steganographic Distortion Function for Enhanced Images 31
Zichi Wang, Guorui Feng, and Xinpeng Zhang

Improving Text-Image Matching with Adversarial Learning and Circle Loss for Multi-modal Steganography 41
Yuting Hu, Han Cao, Zhongliang Yang, and Yongfeng Huang

Constructing Immune Cover for Secure Steganography Based on an Artificial Immune System Approach 53
Hongxia Wang, Zhilong Chen, and Peisong He

Generating JPEG Steganographic Adversarial Example via Segmented Adversarial Embedding 68
Sai Ma and Xianfeng Zhao

High-Performance Linguistic Steganalysis, Capacity Estimation and Steganographic Positioning 80
Jiajun Zou, Zhongliang Yang, Siyu Zhang, Sadaqat ur Rehman, and Yongfeng Huang

On the Sharing-Based Model of Steganography 94
Xianfeng Zhao, Chunfang Yang, and Fenlin Liu

Watermarking

Towards Informed Watermarking of Personal Health Sensor Data for Data Leakage Detection 109
Sebastian Gruber, Bernd Neumayr, Christoph Fabianek, Eduard Gringinger, Christoph Georg Schuetz, and Michael Schrefl

Complete Quality Preserving Data Hiding in Animated GIF with Reversibility and Scalable Capacity Functionalities 125
KokSheik Wong, Mohamed N. M. Nazeeb, and Jean-Luc Dugelay

Visible Reversible Watermarking for 3D Models Based on Mesh Subdivision 136
Fei Peng, Wenjie Qian, and Min Long

Multimedia Forensics

Defocused Image Splicing Localization by Distinguishing Multiple Cues between Raw Naturally Blur and Artificial Blur 153
Xiaoyu Zhao, Yakun Niu, Rongrong Ni, and Yao Zhao

Deepfake Video Detection Using Audio-Visual Consistency 168
Yewei Gu, Xianfeng Zhao, Chen Gong, and Xiaowei Yi

A Machine Learning Approach to Approximate the Age of a Digital Image 181
Robert Jöchl and Andreas Uhl

Facing Image Source Attribution on iPhone X 196
Daniele Baracchi, Massimo Iuliani, Andrea G. Nencini, and Alessandro Piva

Data-Dependent Scaling of CNN's First Layer for Improved Image Manipulation Detection 208
Ivan Castillo Camacho and Kai Wang

ISO Setting Estimation Based on Convolutional Neural Network and its Application in Image Forensics 224
Hui Zeng, Kang Deng, and Anjie Peng

A Hybrid Loss Network for Localization of Image Manipulation 237
Qilin Yin, Jinwei Wang, and Xiangyang Luo

Security of AI-based Multimedia Applications

Efficient Generation of Speech Adversarial Examples with Generative Model 251
Donghua Wang, Rangding Wang, Li Dong, Diqun Yan, and Yiming Ren

Lightweight DCT-Like Domain Forensics Model for Adversarial Example . . . 265
Junjie Zhao and Jinwei Wang

Author Index 281