June 27–28, 2022
Santa Barbara, CA, USA

1947 2022
Association for
Computing Machinery

IH-MMSec ’22

Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security

Sponsored by:

ACM SIGMM

General Chair:

B.S. Manjunath, University of California, Santa Barbara, USA

Technical Program Chairs:

Jan Butora, University of Lille, France
Benedetta Tondi, University of Siena, Italy
Claus Vielhauer, Brandenburg University of Applied Sciences, Germany

acm Association for Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, NY 10019-7434

ISBN: 978-1-4503-9355-3

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)
+1-212-626-0500 (Global)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org
Hours of Operation: 8:30 am – 4:30 pm ET

Printed in the USA

Preface

Welcome to the 2022 ACM Workshop on Information Hiding and Multimedia Security - IH&MMSec ‘22. The meeting is held at the beautiful University of California, Santa Barbara Campus, with a return to an in-person meeting after 2 years of virtual meetings.

In these challenging times, security and forensics are topics of significant global interest. We would like to thank all the authors who contributed to making this event possible. The meeting was advertised as in-person when the call for papers went out, and we received a total of 38 submissions. After a careful review of the submissions, 18 papers were accepted for presentation, 10 as full length papers and 8 as short papers. The papers cover a broad spectrum of topics ranging from security of multimedia data and machine learning models, data hiding to image/video forensics.

We would like to thank the IH&MMSec advisory board, especially Professor Jessica Fridrich, for her advice and guidance in getting this year’s workshop organized.

Our sincere thanks to UC Santa Barbara’s Marine Science Institute for the use of their auditorium and space for hosting the reception - spectacular balcony location overlooking the ocean and the mountains, and to our ACM SIGMM sponsor.

Sincerely

General Chair	*Technical Program Chairs*
B.S. Manjunath	**Jan Butora** **Benedetta Tondi** **Claus Vielhauer**

IH&MMSec 2022 Program Chairs' Welcome

It is our great pleasure to welcome you to the *10th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC 2022).* This year's workshop continues its tradition of being the premier events for presentation of research results and experience reports on multimedia security and attracts researchers from all over the world.

The workshop focuses on information hiding topics, such as digital watermarking, steganography, steganalysis, anonymity, hard-to-intercept communications, forensics, and covert/subliminal channels. It also covers a variety of multimedia security topics including multimedia identification and authentication, signal forensics, and biometrics.

The mission of the workshop is to share novel solutions that fulfil the needs of heterogeneous security applications and identify new directions for future research and development. IH&MMSEC gives researchers and practitioners a unique opportunity to share their perspectives with others interested in the various aspects of multimedia security.

The call for papers attracted submissions from Asia, Europe, and the United States. We are proud to announce that this year both the quality and number of submissions was extremely high.

As a consequence, the TPC chairs and general chairs worked very hard to compile a program, consisting of outstanding papers, based on a very strict selection of 18 accepted papers out of 38 submitted (acceptance rate: 47%).

Track	*Reviewed*	*Accepted*	
Full/ShortTechnical Papers	38	18	47%

We also encourage attendees to attend the keynote and invited talk presentations. These valuable and insightful talks can and will guide us to a better understanding of the future:

- *Towards Generalization in Deepfake Detection,* Luisa Verdoliva (University Federico II of Naples, Italy)
- *Looking for Signals: A Systems Security Perspective,* Christopher Kruegel (VMware, USA)
- *Intellectual Property (IP) Protection for Deep Learning and Federated Learning Models,* Farinaz Koushanfar (University of California San Diego, USA)

We hope that you will find this program interesting and thought-provoking and that the symposium will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.

IH&MMSEC 2022 Technical Program Chairs

Jan Butora
University of Lille, France

Benedetta Tondi
University of Siena, Italy

Claus Vielhauer
Brandenburg University of Applied Sciences, Germany

Table of Contents

10th Workshop on Information Hiding and Multimedia Security 2022 Organization vii

Keynote Talks

Session Chair: B.S. Manjunath *(UC Santa Barbara)*

- **Towards Generalization in Deepfake Detection** 1
  Luisa Verdoliva *(University Federico II of Naples)*
- **Looking for Signals: A Systems Security Perspective** 3
  Christopher Kruegel *(University of California, Santa Barbara)*
- **Intellectual Property (IP) Protection for Deep Learning and Federated Learning Models** 5
  Farinaz Koushanfar *(University of California, San Diego)*

Session 1: Forensics

Session Chair: Rainer Böhme *(University of Innsbruck)*

- **FMFCC-V: An Asian Large-Scale Challenging Dataset for DeepFake Detection** 7
  Gen Li *(Institute of Information Engineering, Chinese Academy of Sciences)*,
  Xianfeng Zhao *(Institute of Information Engineering, Chinese Academy of Sciences)*,
  Yun Cao *(Institute of Information Engineering, Chinese Academy of Sciences)*,
  Pengfei Pei *(Institute of Information Engineering, Chinese Academy of Sciences)*,
  Jinchuan Li *(Institute of Information Engineering, Chinese Academy of Sciences)*,
  Zeyu Zhang *(Institute of Information Engineering, Chinese Academy of Sciences)*
- **Know Your Library: How the libjpeg Version Influences Compression and Decompression Results** 19
  Martin Beneš *(University of Innsbruck)*, Nora Hofer *(University of Innsbruck)*,
  Rainer Böhme *(University of Innsbruck)*
- **Identity-Referenced Deepfake Detection with Contrastive Learning** 27
  Dongyao Shen *(Tsinghua University)*, Youjian Zhao *(Tsinghua University)*,
  Chengbin Quan *(Tsinghua University)*

Session 2: Security of Machine Learning

Session Chair: Yassine Yousfi *(Machine Learning Engineer)*

- **Sparse Trigger Pattern Guided Deep Learning Model Watermarking** 33
  Chun-Shien Lu *(Institute of Information Science, Academia Sinica)*,
- **BlindSpot: Watermarking Through Fairness** 39
  Sofiane Lounici *(SAP Security Research)*, Melek Önen *(EURECOM)*,
  Orhan Ermis *(Luxembourg Institute of Science and Technology (LIST))*,
  Slim Trabelsi *(SAP Security Research)*
- **Hiding Needles in a Haystack: Towards Constructing Neural Networks that Evade Verification** 51
  Árpád Berta *(University of Szeged)*, Gábor Danner *(University of Szeged)*,
  István Hegedűs *(University of Szeged)*,
  Márk Jelasity *(University of Szeged & ELKH SZTE Research Group on Artificial Intelligence)*

Session 3: Security & Privacy I

Session Chair: B.S. Manjunath *(UC Santa Barbara)*

- **Covert Communications through Imperfect Cancellation** 63
  Daniel Chew *(Johns Hopkins University)*, Christine Nguyen *(Johns Hopkins University)*,
  Samuel Berhanu *(Johns Hopkins University)*, Chris Baumgart *(Johns Hopkins University)*,
  A. Brinton Cooper *(Johns Hopkins University)*

- **Covert Channels in Network Time Security** 69
  Kevin Lamshöft *(Otto-von-Guericke University Magdeburg)*,
  Jana Dittmann *(Otto-von-Guericke University Magdeburg)*

- **Collusion-resistant Fingerprinting of Parallel Content Channels** 81
  Basheer Joudeh *(Eindhoven University of Technology)*, Boris Skoric *(Eindhoven University of Technology)*

Session 4: Steganography I

Session Chair: Jessica Fridrich *(SUNY Binghamton)*

- **Domain Adaptational Text Steganalysis Based on Transductive Learning** 91
  Yiming Xue *(China Agricultural University)*, Boya Yang *(China Agricultural University)*,
  Yaqian Deng *(China Agricultural University)*, Wanli Peng *(China Agricultural University)*,
  Juan Wen *(China Agricultural University)*

- **Few-shot Text Steganalysis Based on Attentional Meta-learner** 97
  Juan Wen *(China Agricutural University)*, Ziwei Zhang *(China Agricutural University)*,
  Yu Yang *(China Agricutural University)*, Yiming Xue *(China Agricutural University)*

- **Hidden in Plain Sight - Persistent Alternative Mass Storage Data Streams as a Means for Data Hiding With the Help of UEFI NVRAM and Implications for IT Forensics** 107
  Stefan Kiltz *(Otto-von-Guericke University)*, Robert Altschaffel *(Otto-von-Guericke University)*,
  Jana Dittmann *(Otto-von-Guericke University)*

- **Fighting the Reverse JPEG Compatibility Attack: Pick your Side** 113
  Jan Butora *(University Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL)*,
  Patrick Bas *(University Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL)*

Session 5: Security & Privacy II

Session Chair: Daniel Chew *(Johns Hopkins Whiting School of Engineering)*

- **A Nearest Neighbor Under-sampling Strategy for Vertical Federated Learning in Financial Domain** 123
  Denghao Li *(Ping An Technology (Shenzhen) Co., Ltd.)*,
  Jianzong Wang *(Ping An Technology (Shenzhen) Co., Ltd.)*,
  Lingwei Kong *(Ping An Technology (Shenzhen) Co., Ltd.)*, Shijing Si *(Ping An Technology (Shenzhen) Co., Ltd.)*,
  Zhangcheng Huang *(Ping An Technology (Shenzhen) Co., Ltd.)*,
  Chenyu Huang *(Ping An Technology (Shenzhen) Co., Ltd.)*, Jing Xiao *(Ping An Technology (Shenzhen) Co., Ltd.)*

- **COLMADE: Collaborative Masking in Auditable Decryption for BFV-based Homomorphic Encryption** 129
  Alberto Ibarrondo *(IDEMIA & EURECOM)*, Hervé Chabanne *(IDEMIA & Telecom Paris)*,
  Vincent Despiegel *(IDEMIA)*, Melek Önen *(EURECOM)*

Session 6: Steganography II

Session Chair: Jan Butora *(University of Lille)*

- **AMR Steganalysis based on Adversarial Bi-GRU and Data Distillation** 141
  Zhijun Wu *(Civil Aviation University of China)*, Junjun Guo *(Civil Aviation University of China)*

- **Capacity Laws for Steganography in a Crowd** 147
  Andrew D. Ker *(University of Oxford)*

- **Detector-Informed Batch Steganography and Pooled Steganalysis** 157
  Yassine Yousfi *(Binghamton University)*, Eli Dworetzky *(Binghamton University)*,
  Jessica Fridrich *(Binghamton University)*

Author Index 169

10th Workshop on Information Hiding and Multimedia Security 2022 Organization

General Chair:	B.S. Manjunath *(UC Santa Barbara, California, USA)*
Technical Program Chairs:	Jan Butora *(University of Lille, France)*
	Benedetta Tondi *(University of Siena, Italy)*
	Claus Vielhauer *(Brandenburg University of Applied Sciences, Germany)*
Steering Committee:	Patrizio Campisi *(University of Roma TRE, Italy)*
	Jana Dittmann *(University of Magdeburg, Germany)*
	Jessica Fridrich *(SUNY Binghamton, New York, USA)*
	Stefan Katzenbeisser *(University of Passau, Germany)*
	Balakrishnan Prabhakaran (*University of Dallas, Texas, USA)*
ACM Liaison:	Jana Dittmann *(University of Magdeburg, Germany)*
Program Committee:	Irene Amerini *(Sapienza University of Rome, Italy)*
	Patrick Bas *(CNRS CRISTAL, Lille, France)*
	Roberto Caldelli *(CNIT, Florence, Italy)*
	Marc Chaumont *(University of Montpellier, LIRMM, France)*
	Remi Cogranne *(Université de Technologie de Troyes, France)*
	Pedro Comesaña-Alfaro *(University of Vigo, Spain)*
	Claude Delpha *(Université Paris Saclay - CNRS - CentraleSupelec, France)*
	Jana Dittman *(Otto-von-Guericke University Magdeburg, Germany)*
	Jessica Fridrich *(Binghamton University, USA)*
	Quentin Giboulot *(Université de Technologie de Troyes, France)*
	Stefan Katzenbeisser *(University of Passau, Germany)*
	Andrew Ker *(University of Oxford, UK)*
	Christian Kraetzer *(Otto-von-Guericke University Magdeburg, Germany)*
	Wojciech Mazurczyk *(Warsaw University of Technology, Poland)*
	Alessandro Piva *(University of Florence, Italy)*
	Balakrishnan Prabhakaran *(The University of Texas at Dallas, USA)*
	William Puech *(LIRMM - CNRS, France)*
	Christian Riess *(University of Erlangen-Nuremberg, Germany)*
	Pascal Schoettle *(Management Center Innsbruck, Austria)*
	Jiande Sun *(Shandong University, China)*
	Shunquan Tan *(Shenzen University, China)*

Program Committee (continued): Andreas Uhl *(University of Salzburg, Austria)*
Kai Wang *(GIPSA-lab, CNRS, University of Grenoble Alpes, France)*
Yassine Yousfi *(Binghamton University, USA)*
Xinpeng Zhang *(Fudan University, China)*

Sponsor: SIGMM