

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Tomáš Filler Tomáš Pevný
Scott Craver Andrew Ker (Eds.)

Information Hiding

13th International Conference, IH 2011
Prague, Czech Republic, May 18-20, 2011
Revised Selected Papers

 Springer

Volume Editors

Tomáš Filler
Digimarc Corporation
9405 Gemini Drive
Beaverton, OR, 97008, USA
E-mail: tomas.filler@digimarc.com

Tomáš Pevný
Czech Technical University
Faculty of Electrical Engineering, Department of Cybernetics
Karlovo namesti 13
121 35 Prague 2, Czech Republic
E-mail: pevnak@gmail.com

Scott Craver
SUNY Binghamton
T. J. Watson School, Department of Electrical and Computer Engineering
Binghamton, NY 13902, USA
E-mail: scraver@binghamton.edu

Andrew Ker
University of Oxford, Department of Computer Science
Wolfson Building, Parks Road
Oxford OX1 3QD, UK
E-mail: Andrew.Ker@comlab.ox.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-24177-2 e-ISBN 978-3-642-24178-9
DOI 10.1007/978-3-642-24178-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011936237

CR Subject Classification (1998): E.3, K.6.5, D.4.6, E.4, H.5.1, I.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The International Hiding Conference was founded 15 years ago, with the first conference held in Cambridge, UK, in 1996. Since then, the conference locations have alternated between Europe and North America. In 2011, during May 18–20, we had the pleasure of hosting the 13th Information Hiding Conference in Prague, Czech Republic. The 60 attendees had the opportunity to enjoy Prague in springtime as well as inspiring presentations and fruitful discussions with colleagues.

The International Hiding Conference has a tradition in attracting researchers from many closely related fields including digital watermarking, steganography and steganalysis, anonymity and privacy, covert and subliminal channels, fingerprinting and embedding codes, multimedia forensics and counter-forensics, as well as theoretical aspects of information hiding and detection. In 2011, the Program Committee reviewed 69 papers, using a double-blind system with at least 3 reviewers per paper. Then, each paper was carefully discussed until consensus was reached, leading to 23 accepted papers (33% acceptance rate), all published in these proceedings.

The invited speaker was Bernhard Schölkopf, who presented his thoughts on why kernel methods (and support vector machines in particular) are so popular and where they are heading. He also discussed some recent developments in two-sample and independence testing as well as applications in different domains.

At this point, we would like to thank everyone, who helped to organize the conference, namely, Jakub Havránek from the Mediaform agency and Bára Jeníková from CVUT in Prague. We also wish to thank the following companies and agencies for their contribution to the success of this conference: European Office of Aerospace Research and Development, Air Force Office of Scientific Research, United States Air Force Research Laboratory (www.london.af.mil), the Office of Naval Research Global (www.onr.navy.mil), Digimarc Corporation (www.digimarc.com), Technicolor (www.technicolor.com), and organizers of IH 2008 in Santa Barbara, CA, USA. Without their generous financial support, the organization would have been very difficult.

July 2011

Tomáš Filler
Tomáš Pevný
Scott Craver
Andrew Ker

Local Organization

Jakub Havránek
Barbora Jeníková

Mediaform, Czech Republic
Czech Technical University, Czech Republic

External Reviewer

Boris Škorić

Eindhoven University of Technology,
The Netherlands

Sponsoring Institutions

European Office of Aerospace Research and Development
Office of Naval Research
Digimarc Corporation, USA
Technicolor, France

Table of Contents

Fingerprinting

Asymptotic Fingerprinting Capacity for Non-binary Alphabets	1
<i>Dion Boesten and Boris Škorić</i>	
Asymptotically False-Positive-Maximizing Attack on Non-binary Tardos Codes	14
<i>Antonino Simone and Boris Škorić</i>	
Towards Joint Tardos Decoding: The ‘Don Quixote’ Algorithm	28
<i>Peter Meerwald and Teddy Furon</i>	
An Asymmetric Fingerprinting Scheme Based on Tardos Codes	43
<i>Ana Charpentier, Caroline Fontaine, Teddy Furon, and Ingemar Cox</i>	

Special Session on BOSS Contest

“Break Our Steganographic System” — The Ins and Outs of Organizing BOSS	59
<i>Patrick Bas, Tomáš Filler, and Tomáš Pevný</i>	
A New Methodology in Steganalysis : Breaking Highly Undetectable Steganography (HUGO)	71
<i>Gokhan Gul and Fatih Kurugollu</i>	
Breaking HUGO – The Process Discovery	85
<i>Jessica Fridrich, Jan Kodovský, Vojtěch Holub, and Miroslav Goljan</i>	
Steganalysis of Content-Adaptive Steganography in Spatial Domain	102
<i>Jessica Fridrich, Jan Kodovský, Vojtěch Holub, and Miroslav Goljan</i>	

Anonymity and Privacy

I Have a DREAM! (DiffeRentially privatE smArt Metering)	118
<i>Gergely Ács and Claude Castelluccia</i>	
Anonymity Attacks on Mix Systems: A Formal Analysis	133
<i>Sami Zhioua</i>	
Differentially Private Billing with Rebates	148
<i>George Danezis, Markulf Kohlweiss, and Alfredo Rial</i>	

Steganography and Steganalysis

Statistical Decision Methods in Hidden Information Detection	163
<i>Cathel Zitzmann, Rémi Cogramne, Florent Retraint, Igor Nikiforov, Lionel Fillatre, and Philippe Cornu</i>	
A Cover Image Model for Reliable Steganalysis	178
<i>Rémi Cogramne, Cathel Zitzmann, Lionel Fillatre, Florent Retraint, Igor Nikiforov, and Philippe Cornu</i>	
Video Steganography with Perturbed Motion Estimation	193
<i>Yun Cao, Xianfeng Zhao, Dengguo Feng, and Rennong Sheng</i>	

Watermarking

Soft-SCS: Improving the Security and Robustness of the Scalar-Costa-Scheme by Optimal Distribution Matching	208
<i>Patrick Bas</i>	
Improving Tonality Measures for Audio Watermarking	223
<i>Michael Arnold, Xiao-Ming Chen, Peter G. Baum, and Gwenaël Doërr</i>	
Watermarking as a Means to Enhance Biometric Systems: A Critical Survey	238
<i>Jutta Hämmerle-Uhl, Karl Raab, and Andreas Uhl</i>	
Capacity-Approaching Codes for Reversible Data Hiding	255
<i>Weiming Zhang, Biao Chen, and Nenghai Yu</i>	

Digital Rights Management and Digital Forensics

Code Obfuscation against Static and Dynamic Reverse Engineering	270
<i>Sebastian Schrittwieser and Stefan Katzenbeisser</i>	
Countering Counter-Forensics: The Case of JPEG Compression	285
<i>ShiYue Lai and Rainer Böhme</i>	

Data Hiding in Unusual Content

Stegobot: A Covert Social Network Botnet	299
<i>Shishir Nagaraja, Amir Houmansadr, Pratch Piyawongwisal, Vijit Singh, Pragma Agarwal, and Nikita Borisov</i>	

CoCo: Coding-Based Covert Timing Channels for Network Flows	314
<i>Amir Houmansadr and Nikita Borisov</i>	
LinL: Lost in n-best List	329
<i>Peng Meng, Yun-Qing Shi, Liusheng Huang, Zhili Chen, Wei Yang, and Abdelrahman Desoky</i>	
Author Index	343