

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Mauro Barni Jordi Herrera-Joancomartí
Stefan Katzenbeisser
Fernando Pérez-González (Eds.)

Information Hiding

7th International Workshop, IH 2005
Barcelona, Spain, June 6-8, 2005
Revised Selected Papers



Springer

Volume Editors

Mauro Barni
Università di Siena
Dipartimento di Ingegneria dell'Informazione
Siena, Italy
E-mail: barni@dii.unisi.it

Jordi Herrera-Joancomartí
Universitat Oberta de Catalunya
Estudis d'Informàtica i Multimèdia
Barcelona, Spain
E-mail: jherrera@uoc.edu

Stefan Katzenbeisser
Technische Universität München
Institut für Informatik
München, Germany
E-mail: katzenbe@in.tum.de

Fernando Pérez-González
Universidad de Vigo
Signal Processing in Communications Group
Vigo, Spain
E-mail: fperez@tsc.uvigo.es

Library of Congress Control Number: 2005936733

CR Subject Classification (1998): E.3, K.6.5, K.4.1, K.5.1, D.4.6, E.4, C.2, H.4.3, H.3, H.5.1

ISSN	0302-9743
ISBN-10	3-540-29039-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-29039-1 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11558859 06/3142 5 4 3 2 1 0

Preface

It is our pleasure to present in this volume the proceedings of the 7th International Workshop on Information Hiding (IH 2005), held in Barcelona, Catalonia, Spain, during June 6–8, 2005. The workshop was organized by the Department of Computer Science and Multimedia, Universitat Oberta de Catalunya (UOC).

Continuing the tradition of previous workshops, we sought a balanced program, containing talks on various aspects of data hiding, anonymous communication, steganalysis, and watermarking. Although the protection of digital intellectual property has up to now motivated most of our research, there are many other upcoming fields of application. We were delighted to see that this year's workshop presented numerous new and unconventional approaches to information hiding.

The selection of the program was a very challenging task. In total, we received 90 submissions from 21 countries. At this point we want to thank all authors who submitted their latest work to IH 2005—and thus assured that the Information Hiding Workshop continues to be the top forum of our community. Each submission was refereed by three reviewers. Due to the space limitations of a single-track workshop, we could only accept 28 papers, keeping the high quality of previous workshops. We would like to thank all members of the Program Committee and all external reviewers for the enormous efforts they put into the review process. In addition to the regular presentations, an invited lecture entitled “On Joint Coding for Watermarking and Encryption” was given by Neri Merhav. Furthermore, to open the floor to additional ideas, we arranged a rump session.

Finally, we want to thank the Organizing Committee for handling all local organizational issues and the European Office of Aerospace Research and Development for their financial support.

We hope that you will enjoy reading these proceedings and that they will inspire your own research in the area of information hiding.

July 2005

Mauro Barni
Jordi Herrera Joancomartí
Stefan Katzenbeisser
Fernando Pérez-González

7th International Workshop on Information Hiding

June 6–8, 2005, Barcelona (Spain)

General Chairs

Jordi Herrera-Joancomartí, Universitat Oberta de Catalunya, Spain
Fernando Pérez-González, University of Vigo, Spain

Program Chairs

Mauro Barni, Università di Siena, Italy
Stefan Katzenbeisser, Technische Universität München, Germany

Program Committee

Ross J. Anderson, University of Cambridge, UK
Mauro Barni, Università di Siena, Italy
Jan Camenisch, IBM Zurich Research Laboratory, Switzerland
Christian Collberg, University of Arizona, USA
Ingemar J. Cox, University College London, UK
Jessica Fridrich, SUNY Binghamton, USA
Jordi Herrera-Joancomartí, Universitat Oberta de Catalunya, Spain
John McHugh, SEI/CERT, USA
Ira Moskowitz, Naval Research Laboratory, USA
Stefan Katzenbeisser, Technische Universität München, Germany
Darko Kirovski, Microsoft Research, USA
Richard C. Owens, University of Toronto, Canada
Fernando Pérez-González, University of Vigo, Spain
Andreas Pfitzmann, Dresden University of Technology, Germany
Michiel van der Veen, Philips Research, Netherlands

Local Organization

Joan Arnedo, Universitat Oberta de Catalunya, Spain
David Megías, Universitat Oberta de Catalunya, Spain
Julià Minguillón, Universitat Oberta de Catalunya, Spain
Emma Pedrol, Universitat Oberta de Catalunya, Spain
Jordi Serra, Universitat Oberta de Catalunya, Spain
Michael Tautschnig, Technische Universität München, Germany

External Reviewers

Michael A. Colón
Andre Adelsbach
Farid Ahmed
Felix Balado
Richard Bergmair
Mike Bergmann
Rainer Böhme
Roberto Caldelli
Mehmet Celik
R. Chandramouli
Sebastian Clauss
Pedro Comesaña Alfaro
Scott Craver
George Danezis
Alessia De Rosa
Josep Domingo-Ferrer
Sorina Dumitrescu
Hany Farid
Elke Franz
Shan He
Peter Hon Wah Wong
Mark Horgan
Neil Hurley

Myong Kang
Andrew Ker
Dogan Kesdogan
Farinaz Koushanfar
Thomas Kriegelstein
Ginger M. Myles
John McDermott
Catherine Meadows
David Megías
Nasir Memon
Juliá Minguillón
Steven Murdoch
Aweke N. Lemma
Jasvir Nagra
Richard Newman
Luis Perez-Freire
Alessandro Piva
Miodrag Potkonjak
Gang Qu
Majid Rabbani
Victor Raskin
Ahmad-Reza Sadeghi
Phil Sallee

Elisa Sayrol
Dagmar Schönfeld
G.C.M. Silvestre
Sandra Steinbrecher
Kenneth Sullivan
Ashwin Swaminathan
Paul Syverson
Cuneyt Taskiran
Clark Thomborson
Roman Tzschoppe
José Emilio Vila-Forcén
Renato Villán
Changjie Wang
Ying Wang
Brent Waters
Andreas Westfeld
Kevin Whelan
Jennifer Wong
Min Wu
Li Wu Chang
Yacov Yacobi
Hong Zhao

Table of Contents

Invited Talk

On Joint Coding for Watermarking and Encryption <i>Neri Merhav</i>	1
---	---

Anonymity

Compulsion Resistant Anonymous Communications <i>George Danezis, Jolyon Clulow</i>	11
Provable Anonymity for Networks of Mixes <i>Marek Klonowski, Mirosław Kutylowski</i>	26
On Blending Attacks for Mixes with Memory <i>Luke O'Connor</i>	39
Pervasive Random Beacon in the Internet for Covert Coordination <i>Hui Huang Lee, Ee-Chien Chang, Mun Choon Chan</i>	53
Censorship Resistance Revisited <i>Ginger Perng, Michael K. Reiter, Chenxi Wang</i>	62

Watermarking

Optimal Embedding for Watermarking in Discrete Data Spaces <i>Stéphane Bounkong, Borémi Toch, David Saad</i>	77
A Spread Spectrum Watermarking Scheme Based on Periodic Clock Changes for Digital Images <i>Vincent Martin, Marie Chabert, Bernard Lacaze</i>	91
A Quantization Watermarking Technique Robust to Linear and Non-linear Valumetric Distortions Using a Fractal Set of Floating Quantizers <i>Patrick Bas</i>	106

Theory

Efficient Steganography with Provable Security Guarantees
Aggelos Kiayias, Yona Raekow, Alexander Russell 118

Information-Theoretic Analysis of Security in Side-Informed Data
Hiding
Luis Pérez-Freire, Pedro Comesaña, Fernando Pérez-González 131

Fundamentals of Data Hiding Security and Their Application to
Spread-Spectrum Analysis
Pedro Comesaña, Luis Pérez-Freire, Fernando Pérez-González 146

Watermark Attacks

How to Combat Block Replacement Attacks?
Gwenaël Doërr, Jean-Luc Dugelay 161

On the Intractability of Inverting Geometric Distortions
in Watermarking Schemes
Maciej Liśkiewicz, Ulrich Wölfel 176

Steganography

Pre-processing for Adding Noise Steganography
Elke Franz, Antje Schneidewind 189

Efficient Wet Paper Codes
Jessica Fridrich, Miroslav Goljan, David Soukal 204

Hiding in Unusual Content

Translation-Based Steganography
*Christian Grothoff, Krista Grothoff, Ludmila Alkhutova,
Ryan Stutsman, Mikhail Atallah* 219

ID Modulation: Embedding Sensor Data in an RFID Timeseries
*Joshua R. Smith, Bing Jiang, Sumit Roy, Matthai Philipose,
Kishore Sundara-Rajan, Alexander Mamishev* 234

Embedding Covert Channels into TCP/IP
Steven J. Murdoch, Stephen Lewis 247

Steganalysis

Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions <i>Guorong Xuan, Yun Q. Shi, Jianjiong Gao, Dekun Zou, Chengyun Yang, Zhenping Zhang, Peiqi Chai, Chunhua Chen, Wen Chen</i>	262
Assessment of Steganalytic Methods Using Multiple Regression Models <i>Rainer Böhme</i>	278
A General Framework for Structural Steganalysis of LSB Replacement <i>Andrew D. Ker</i>	296
New Steganalysis Methodology: LR Cube Analysis for the Detection of LSB Steganography <i>Kwangsoo Lee, Changho Jung, Sangjin Lee, Jongin Lim</i>	312
An Analysis of Empirical PMF Based Tests for Least Significant Bit Image Steganography <i>Stark Draper, Prakash Ishwar, David Molnar, Vinod Prabhakaran, Kannan Ramchandran, Daniel Schonberg, David Wagner</i>	327

Software Watermarking

Self-validating Branch-Based Software Watermarking <i>Ginger Myles, Hongxia Jin</i>	342
Data Hiding in Compiled Program Binaries for Enhancing Computer System Performance <i>Ashwin Swaminathan, Yinian Mao, Min Wu, Krishnan Kailas</i>	357
Dither Modulation Watermarking of Dynamic Memory Traces <i>Alan J. Larkin, Félix Balado, Neil J. Hurley, Guenolé C.M. Silvestre</i>	372

Fingerprinting

A Family of Collusion 2-Secure Codes <i>Josep Cotrina-Navau, Marcel Fernandez, Miguel Soriano</i>	387
--	-----

Best Security Index for Digital Fingerprinting
 Kozo Banno, Shingo Orihara, Takaaki Mizuki, Takao Nishizeki 398

Author Index 413