

**Lecture Notes in Computer Science**  
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

**2578**

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Fabien A.P. Petitcolas (Ed.)

# Information Hiding

5th International Workshop, IH 2002  
Noordwijkerhout, The Netherlands, October 7-9, 2002  
Revised Papers



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Fabien A. P. Petitcolas  
Microsoft Research Ltd.  
7 J. J. Thomson Avenue, Cambridge, CB3 0FB, UK  
E-mail: fabienpe@microsoft.com

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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

ISSN 0302-9743

ISBN 3-540-00421-1 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein  
Printed on acid-free paper SPIN: 10872352 06/3142 5 4 3 2 1 0

## Preface

These post-proceedings contain 27 papers that were accepted for presentation at the Fifth International Workshop on Information Hiding, held 7–9 October 2002, in Noordwijkerhout, The Netherlands. The papers were selected from 78 submissions on the basis of their scientific excellence and novelty by the program committee. We tried to have a balanced program covering several aspects of information hiding.

The program committee was composed of Ross J. Anderson (University of Cambridge, UK), Jan Camenisch (IBM Zurich Research Laboratory, Switzerland), Ingemar J. Cox (NEC Research Institute, USA), John McHugh (SEI/CERT, USA), Ira S. Moskowitz (Naval Research Laboratory, USA), Job Oostveen (Philips Research, The Netherlands), Andreas Pfitzmann (Dresden University of Technology, Germany), Mike Reiter (Carnegie Mellon University, USA), and me. We all wish to thank all the authors of submissions for offering their papers for consideration.

This year, contrary to the four previous workshops, the call for papers requested anonymous submissions. However, anonymity was not compulsory and we did accept some papers in which the identity of the authors was clear. Each submission was assigned to three members of the program committee. Papers submitted by program committee members were assigned to four reviewers. The program committee relied on the advice of outside colleagues. We also insisted that 12 of the 27 accepted papers should be revised according to the comments of the reviewers.

The reviewers were Javier-Francisco Aprea (Philips Digital Systems Labs, The Netherlands), Rene Barto (Philips Research, The Netherlands), Oliver Benedens (Freelance Researcher, Germany), Oliver Berthold (Freie Universität Berlin, Germany), Fons Bruekers (Philips Research, The Netherlands), LiWu Chang (Naval Research Laboratory, USA), Fred Cohen (Sandia National Laboratories, USA), Christian Collberg (University of Arizona, USA), Jana Dittmann (Leipzig University, Germany), Gwenaél Doërr (Institut Eurécom, France), Jean-Luc Dugelay (Institut Eurécom, France), Elke Franz (Dresden University of Technology, Germany), Jessica Fridrich (SUNY Binghamton, USA), Emmanuel Garcia (Institut Eurécom, France), Dieter Gollmann (Microsoft Research, UK), Kelly Heffner, Neil Johnson (Booz Allen Hamilton, USA), Ton Kalker (Philips Research, The Netherlands), Darko Kirovski (Microsoft Research, USA), Herbert Klimant (Dresden University of Technology, Germany), Thomas Kriegelstein (Dresden University of Technology, Germany), Heinrich Langos (Freie Universität Berlin, Germany), Aweke Lemma (Philips Digital Systems Labs, The Netherlands), Kivanç Mihçak (Microsoft Research, USA), Pierre Moulin (University of Illinois at Urbana-Champaign, USA), Ginger Myles, Richard Newman (University of Florida, USA), Adrian Perrig (Berkeley University, USA), Jonathan Poritz (IBM Research, Zurich Research Laboratory, Switzerland),

James Riordan (IBM Research, Zurich Research Laboratory, Switzerland), Keith Roberts (Philips Research, The Netherlands), Ahmad-Reza Sadeghi (Saarland University, Germany), Tomas Sander (HP Labs, USA), Dagmar Schönfeld (Dresden University of Technology, Germany), Marius Staring (Philips Research, The Netherlands), Sandra Steinbrecher (Dresden University of Technology, Germany), Martin Steinebach (Fraunhofer-IPSI Darmstadt, Germany), Joop Talstra (Philips Research, The Netherlands), Michiel van der Veen (Philips Research, The Netherlands), Arno van Leest (Philips Research, The Netherlands), Sviatoslav Voloshynovskiy (CUI, University of Geneva, Switzerland), Peter Wayner, Andreas Westfeld (Dresden University of Technology, Germany), and Francis Zane (Bell Labs, Lucent Technologies, USA). Thanks to all program committee members and reviewers who between them contributed over 230 reviews.

Paper and review submissions, dispatching of the reviews, and notifications to authors was greatly simplified by the use of the Microsoft Conference Management Tool. Thanks to Tim Olson and Jonathan Simon from Microsoft for their support.

Like last year we split the chairpersonship into the positions of ‘general’ chair and ‘program’ chair. Job Oostveen was the general chair. Together with his staff he did a terrific job with the local arrangements, printing the pre-proceedings and organizing the registration. He also organized a superb cruise dinner in Amsterdam. I thank Job very much for his efforts.

We hope that you will enjoy reading these proceedings and that they will be helpful for your future research on information hiding.

November 2002

Fabien A.P. Petitcolas

# Table of Contents

## Session 1 – Information Hiding and Networking

Session chair: Neil Johnson (Booz Allen Hamilton)

Hiding Intrusions: From the Abnormal to the Normal and Beyond .....	1
<i>Kymie Tan, John McHugh, and Kevin Killourhy</i>	
Eliminating Steganography in Internet Traffic with Active Wardens .....	18
<i>Gina Fisk, Mike Fisk, Christos Papadopoulos, and Joshua Neil</i>	

## Session 2 – Anonymity

Session chair: Andreas Pfitzmann (Dresden University of Technology)

From a Trickle to a Flood: Active Attacks on Several Mix Types .....	36
<i>Andrei Serjantov, Roger Dingledine, and Paul Syverson</i>	
Limits of Anonymity in Open Environments .....	53
<i>Dogan Kedogan, Dakshi Agrawal, and Stefan Penz</i>	
Chaffinch: Confidentiality in the Face of Legal Threats .....	70
<i>Richard Clayton and George Danezis</i>	

## Session 3 – Watermarking Fundamentals

Session chair: Job Oostveen (Philips Research)

Nothing But a Kiss:	
A Novel and Accurate Approach to Assessing the Performance of Multidimensional Distortion-Compensated Dither Modulation .....	87
<i>Fernando Pérez-González and Félix Balado</i>	
Robustness and Efficiency of Non-linear Side-Informed Watermarking .....	106
<i>Guénolé C.M. Silvestre, Neil J. Hurley, and Teddy Furon</i>	
Security of Public Watermarking Schemes for Binary Sequences .....	119
<i>Qiming Li and Ee-Chien Chang</i>	

## Session 4 – Watermarking Algorithms I

Session chair: Hyoung Joong Kim (Kangwon National University)

Direct Embedding and Detection of RST Invariant Watermarks .....	129
<i>Peter A. Fletcher and Kieran G. Larkin</i>	

## VIII Table of Contents

Robust Image Watermark Using Radon Transform and Bispectrum Invariants .....	145
<i>Hyung-Shin Kim, Yunju Baek, Heung-Kyu Lee, and Young-Ho Suh</i>	
Audio Watermark Robustness to Desynchronization via Beat Detection ...	160
<i>Darko Kirovski and Hagai Attias</i>	

### Session 5 – Watermarking Algorithms II

Session chair: Ton Kalker (Philips Research)

Robust Watermarking and Affine Registration of 3D Meshes .....	177
<i>Oliver Benedens</i>	
Natural Language Watermarking and Tamperproofing .....	196
<i>Mikhail J. Atallah, Victor Raskin, Christian F. Hempelmann, Mercan Karahan, Radu Sion, Umut Topkara, and Katrina E. Triezenberg</i>	

### Session 6 – Attacks on Watermarking Algorithms

Session chair: Fabien A. P. Petitcolas (Microsoft Research)

Cryptanalysis of UCLA Watermarking Schemes for Intellectual Property Protection .....	213
<i>Tri Van Le and Yvo Desmedt</i>	
Cryptanalysis of Discrete-Sequence Spread Spectrum Watermarks .....	226
<i>M. Kvanç Mhçak, Ramarathnam Venkatesan, and Mustafa Kesal</i>	
Detectors for Echo Hiding Systems .....	247
<i>Scott Craver, Bede Liu, and Wayne Wolf</i>	

### Session 7 – Steganography Algorithms

Session chair: Jessica Fridrich (SUNY Binghamton)

A Steganographic Embedding Undetectable by JPEG Compatibility Steganalysis .....	258
<i>Richard E. Newman, Ira S. Moskowitz, LiWu Chang, and Murali M. Brahmadesam</i>	
Steganography Preserving Statistical Properties .....	278
<i>Elke Franz</i>	
Bit-Plane Decomposition Steganography Combined with JPEG2000 Compression .....	295
<i>Hideki Noda, Jeremiah Spaulding, Mahdad N. Shirazi, Michiharu Niimi, and Eiji Kawaguchi</i>	



**Session 8 – Steganalysis I**

Session chair: Richard Clayton (University of Cambridge)

Steganalysis of JPEG Images: Breaking the F5 Algorithm .....	310
<i>Jessica Fridrich, Miroslav Goljan, and Dorin Hoge</i>	
Detecting Low Embedding Rates .....	324
<i>Andreas Westfeld</i>	

**Session 9 – Steganalysis II**

Session chair: John McHugh (SEI/CERT)

Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines .....	340
<i>Siwei Lyu and Hany Farid</i>	
Detection of LSB Steganography via Sample Pair Analysis .....	355
<i>Sorina Dumitrescu, Xiaolin Wu, and Zhe Wang</i>	

**Session 10 – Hiding Information in Unusual Content I**

Session chair: Christian S. Collberg (University of Arizona)

Hiding Data in DNA .....	373
<i>Boris Shimanovsky, Jessica Feng, and Miodrag Potkonjak</i>	
Tracing the Source of a Shredded Document .....	387
<i>Jack Brassil</i>	

**Session 11 – Hiding Information in Unusual Content II**

Session chair: Caroline Fontaine (Université des Sciences et Technologies de Lille)

Oblivious Hashing: A Stealthy Software Integrity Verification Primitive ...	400
<i>Yuqun Chen, Ramarathnam Venkatesan, Matthew Cary, Ruoming Pang, Saurabh Sinha, and Mariusz H. Jakubowski</i>	
Practical Oblivious Transfer Protocols .....	415
<i>Christian Tobias</i>	

<b>Author Index</b> .....	427
---------------------------	-----