

# Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2137

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Ira S. Moskowitz (Ed.)

# Information Hiding

4th International Workshop, IH 2001  
Pittsburgh, PA, USA, April 25-27, 2001  
Proceedings



Springer

## Series Editors

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

## Volume Editor

Ira S. Moskowitz  
Naval Research Laboratory  
Washington, DC 20375, USA

## Cataloging-in-Publication Data applied for

### Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information hiding : 4th international workshop ; proceedings / IH 2001,  
Pittsburgh, PA, USA, April 25 - 27, 2001. Ira S. Moskowitz (ed.). - Berlin ;  
Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ;  
Tokyo : Springer, 2001  
(Lecture notes in computer science ; Vol. 2137)  
ISBN 3-540-42733-3

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 3-540-42733-3 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 2001  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein  
Printed on acid-free paper      SPIN 10840135      06/3142      5 4 3 2 1 0

# Preface

It is my pleasure and privilege to introduce the papers presented at the 4th International Information Hiding Workshop – IHW 2001. We held the first meeting, which was chaired by Ross Anderson, at the Newton Institute, Cambridge, UK almost five years ago. At that meeting, as Ross stated in his introduction to the first proceedings, we initiated public discussion and critical analysis of five different approaches to information hiding problems: watermarking; anonymous communications; covert channels; steganography; and unobtrusive communications, such as spread-spectrum and meteor scatter radio. Our efforts to bring together, in one meeting, these diverse strands of the information hiding community proved successful, as have our subsequent meetings in Portland, Oregon, USA, under the chairmanship of David Aucsmith, and in Dresden, Germany, which was chaired by Andreas Pfitzmann.

Since our first meeting, the necessity that governments and businesses confront issues related to information hiding has not decreased. Rather, due in large part to the growth of the Internet, such concerns have become ever more urgent. Recently, for example, the news media has exposed the use of embedded information transfers by “undesirable” groups and hidden file structures. On a commercial level, the recent litigation over Napster is unlikely to foil the threats faced by owners of digitally-communicable data to their intellectual property rights. However, as our community recognizes, legitimate privacy concerns must also be respected in order for information hiding techniques to be recognized as both lawful and ethical. These issues make the research presented at IHW 2001 even more pressing and timely.

As in previous years, researchers have approached issues related to the hiding of information from many different angles. For this workshop, we have made an effort to select papers which represent the gamut of interest to information hiders: watermarking and fingerprinting of digital audio, still image, and video; anonymous communications; steganography and subliminal channels; covert channels; database inference channels, etc. This year, several papers analyze problems related to chemistry and to natural language. On a more philosophical level, the papers also represent a mix of conjecture, theory, experimentation, and lessons learned.

We had many quality submissions this year. Unfortunately, due to the pressures of maintaining a balanced program and of providing each speaker with an adequate amount of time for presentation and discussion, we could accept only a small percentage of the submissions. In addition to the presented papers, we also had two discussion sessions. The difficult job of developing the program fell to the program committee which consisted of Ross Anderson (Cambridge University, UK), David Aucsmith (Intel Corp, USA), Jean-Paul Linnartz (Philips Research, The Netherlands), Steven Low (California Institute of Technology, USA), John McHugh (SEI/CERT, USA), Fabien Petitcolas (Microsoft Research, UK),

Andreas Pfitzmann (Dresden University of Technology, Germany), Jean-Jacques Quisquater (Université Catholique de Louvain, Belgium), Mike Reiter (Bell Labs, Lucent Technologies, USA) and Michael Waidner (IBM Zurich Research Lab, Switzerland), as well as myself. In addition, we are grateful for the assistance we received from Tuomas Aura, Oliver Berthold, LiWu Chang, Sebastian Clauß, Richard Clayton, George Danezis, Jean-François Delaigle, Cédric Fournet, Elke Franz, Teddy Furon, Ruth Heilizer, Markus Jakobsson, Anne-Marie Kermarrec, Darko Kirovski, Herbert Klimant, Stefan Köpsell, Garth Longdon, Henrique Malvar, Kai Rannenbergh, and Jianxin Yan.

This year we split the chairpersonship into the positions of “general” chair and “program” chair. John McHugh was the general chair for IHW 2001. Both he and his staff did a fantastic job with the local arrangements, putting together the preproceedings, and the registration process. In keeping with the nautical theme of the River Cam, the Columbia River, and the River Elbe, he arranged a wonderful dinner cruise for the workshop dinner. I thank John for the great job he has done!

If one looks through the past proceedings, in conjunction with IHW 2001, it is exciting to see how the field of information hiding is growing and maturing. We are all looking forward to the new research that will be presented at the next workshop.

Finally, I would like to thank my colleagues on the program committee, the people who assisted the program committee, the workshop participants, and especially every author who submitted a paper to IHW 2001. You all help make the workshop stronger and more interesting!

April 2001

Ira S. Moskowitz

# Table of Contents

Trustworthy Paper Documents .....	1
<i>Marshall Bern, Jeff Breidenbach, and David Goldberg</i>	
An Implementation of Key-Based Digital Signal Steganography .....	13
<i>Toby Sharp</i>	
Distortion-Free Data Embedding for Images .....	27
<i>Miroslav Goljan, Jessica J. Fridrich, and Rui Du</i>	
Information Hiding through Noisy Channels .....	42
<i>Valeri Korjik and Guillermo Morales-Luna</i>	
A Perceptual Audio Hashing Algorithm: A Tool for Robust Audio Identification and Information Hiding .....	51
<i>M. Kwanç Mihçak and Ramarathnam Venkatesan</i>	
Computational Forensic Techniques for Intellectual Property Protection ....	66
<i>Jennifer L. Wong, Darko Kirovski, and Miodrag Potkonjak</i>	
Intellectual Property Metering .....	81
<i>Farinaz Koushanfar, Gang Qu, and Miodrag Potkonjak</i>	
Keyless Public Watermarking for Intellectual Property Authentication .....	96
<i>Gang Qu</i>	
Efficiency Improvements of the Private Message Service .....	112
<i>Oliver Berthold, Sebastian Clauß, Stefan Köpsell, and Andreas Pfitzmann</i>	
A Reputation System to Increase MIX-Net Reliability .....	126
<i>Roger Dingledine, Michael J. Freedman, David Hopwood, and David Molnar</i>	
Neural Networks Functions for Public Key Watermarking .....	142
<i>Justin Picard and Arnaud Robert</i>	
A Graph Theoretic Approach to Software Watermarking .....	157
<i>Ramarathnam Venkatesan, Vijay Vazirani, and Saurabh Sinha</i>	
COiN-Video: A Model for the Dissemination of Copyrighted Video Streams over Open Networks .....	169
<i>Dimitris Thanos</i>	
Natural Language Watermarking: Design, Analysis, and a Proof-of-Concept Implementation .....	185
<i>Mikhail J. Atallah, Victor Raskin, Michael Crogan, Christian Hempelmann, Florian Kerschbaum, Dina Mohamed, and Sanket Naik</i>	
Digital Watermarking of Chemical Structure Sets .....	200
<i>Joachim J. Eggers, Wolf-Dietrich Ihlenfeldt, and Bernd Girod</i>	

## VIII Table of Contents

The Strong Eternity Service .....	215
<i>Tonda Beneš</i>	
Real World Patterns of Failure in Anonymity Systems .....	230
<i>Richard Clayton, George Danezis, and Markus G. Kuhn</i>	
Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems .....	245
<i>Adam Back, Ulf Möller, and Anton Stiglic</i>	
Automatic Detection of a Watermarked Document Using a Private Key ...	258
<i>Julien P. Stern and Jean-Pierre Tillich</i>	
Zero-Knowledge Watermark Detection and Proof of Ownership .....	273
<i>André Adelsbach and Ahmad-Reza Sadeghi</i>	
F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis .....	289
<i>Andreas Westfeld</i>	
A Collusion-Secure Fingerprinting Code Reduced by Chinese Remaindering and Its Random-Error Resilience .....	303
<i>Hirofumi Muratani</i>	
Practical Capacity of Digital Watermarks .....	316
<i>Ryo Sugihara</i>	
Blur/Deblur Attack against Document Protection Systems Based on Digital Watermarking .....	330
<i>Sviatoslav Voloshynovskiy, Alexander Herrigel, and Thierry Pun</i>	
Second Generation Benchmarking and Application Oriented Evaluation ...	340
<i>Shelby Pereira, Sviatoslav Voloshynovskiy, Maribel Madueno, Stéphan Marchand-Maillet, and Thierry Pun</i>	
Robust Covert Communication over a Public Audio Channel Using Spread Spectrum .....	354
<i>Darko Kirovski and Henrique Malvar</i>	
Hiding Association Rules by Using Confidence and Support .....	369
<i>Elena Dasseni, Vassilios S. Verykios, Ahmed K. Elmagarmid, and Elisa Bertino</i>	
How to Break a Semi-anonymous Fingerprinting Scheme .....	384
<i>Ahmad-Reza Sadeghi</i>	
An Analysis of One of the SDMI Candidates .....	395
<i>Julien Boeuf and Julien P. Stern</i>	
<b>Author Index .....</b>	<b>411</b>