Preface

The mid-1990s saw an exciting convergence of a number of different information protection technologies, whose theme was the hiding (as opposed to encryption) of information. Copyright marking schemes are about hiding either copyright notices or individual serial numbers imperceptibly in digital audio and video, as a component in intellectual property protection systems; anonymous communication is another area of rapid growth, with people designing systems for electronic cash, digital elections, and privacy in mobile communications; security researchers are also interested in ‘stray’ communication channels, such as those which arise via shared resources in operating systems or the physical leakage of information through radio frequency emissions; and finally, many workers in these fields drew inspiration from ‘classical’ hidden communication methods such as steganography and spread-spectrum radio.

The first international workshop on this new emergent discipline of information hiding was organised by Ross Anderson and held at the Isaac Newton Institute, Cambridge, from the 30th May to the 1st June 1996, and was judged by attendees to be a successful and significant event. In addition to a number of research papers, we had invited talks from David Kahn on the history of steganography and from Gus Simmons on the history of subliminal channels. We also had a number of discussion sessions, culminating in a series of votes on common terms and definitions. These papers and talks, together with minutes of the discussion, can be found in the proceedings, which are published in this series as Volume 1174.

Delegates were unanimous in their wish to have further conferences on this topic, and so the second workshop was held in Portland, Oregon, in April 1998 under my chairmanship. I was well supported by a program committee consisting of Ross Anderson (Cambridge), Steve Low (Melbourne), Ira Moskowitz (US Navy Labs), Andreas Pfitzmann (Dresden), Jean-Jacques Quisquater (Louvain), and Michael Waidner (IBM), who helped select 25 papers from 41 submissions. The standard was extremely high.

These papers cover a wider range of topics than was the case in 1996, and show how this young field is growing. Papers describe the application of copyright marks to protect banknotes, software, and circuit designs, as well as new ways of hiding data in images; how to provide anonymity in applications from file systems to biometrics; how to hide information in everything from audio and video conferencing traffic to the stray RF emanations from personal computers; some significant improvements in the art of image marking; the use for the first time of techniques such as game theory in analysing systems; and a number of practical papers showing how existing marking and hiding systems can be attacked.
The papers in this volume must stand for themselves. However, we can see three directions of growth, all of them encouraging. Firstly, the range of applications in which information hiding techniques are being used is increasing. Secondly, we are starting to understand some of the earliest applications (such as hiding copyright marks in digital images) more deeply. And thirdly, as people find interesting new ways to break some of the first-generation schemes, we are starting to see the rapid coevolution of attack and defence, which has pushed forward the state of the art in such fields as cryptography, computer security, and electronic warfare.

The future of information hiding looks extremely promising.

Finally, I would like to thank Fabien Petitcolas of Cambridge for his invaluable assistance in helping me edit these proceedings, Gary Graunke at Intel for handling the administrative arrangements for the conference, and Intel Corporation for its sponsorship of this event.

October 1998

David Aucsmith
Program Chair
Intel Architecture Labs
Portland, Oregon
# Table of Contents

## Steganography

Information Hiding to Foil the Casual Counterfeiter .......................... 1  
*Daniel Gruhl, Walter Bender (Massachusetts Institute of Technology)*

Fingerprinting Digital Circuits on Programmable Hardware ................. 16  
*John Lach, William H. Mangione-Smith, Miodrag Potkonjak  
  (University of California, Los Angeles)*

Steganography in a Video Conferencing System ................................. 32  
*Andreas Westfeld, Gritta Wolf (Technische Universität Dresden)*

Reliable Blind Information Hiding for Images ................................. 48  
*Lisa Marvel (U.S. Army Research Laboratory), Charles Boncelet  
  (University of Delaware), Charles Retter (U.S. Army Research  
  Laboratory)*

Cerebral Cryptography ...................................................................... 62  
*Shuang Hou, Yvo Desmedt (University of Wisconsin), Jean-Jacques  
  Quisquater (Université Catholique de Louvain)*

## Other Applications

The Steganographic File System ...................................................... 73  
*Ross J. Anderson (University of Cambridge), Roger M. Needham  
  (Microsoft Research), Adi Shamir (Weizmann Institute)*

Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System 83  
*Dogan Kesdogan, Jan Egner, Roland Büschkes (Aachen University of  
  Technology)*

Biometric yet Privacy Protecting Person Authentication ..................... 99  
*Gerrit Bleumer (AT&T Labs)*

On Software Protection via Function Hiding ..................................... 111  
*Tomas Sander, Christian Tscheudin (International Computer Science  
  Institute, Berkeley)*

Soft Tempest: Hidden Data Transmission Using Electromagnetic  
Emanations .................................................................................. 124  
*Markus G. Kuhn, Ross J. Anderson (University of Cambridge)*
Copyright Marking

Robust Digital Watermarking Based on Key-Dependent Basis Functions . . 143

Jiri Fridrich (Center for Intelligent Systems SUNY Binghamton), 2 Lt
Arnold C. Baldoza, Richard J. Simard (Air Force Research Laboratory)

Intellectual Property Protection Systems and Digital Watermarking . . . . 158

Jack Lacy, Schuyler Quackenbush, Amy Reibman, James Snyder (AT&T
Labs)

Secure Copyright Protection Techniques for Digital Images ................. 169

Alexander Herrigel (r³ Security Engineering), Joseph Ó Ruanaidh
(Université de Genève), Holger Petersen (r³ Security Engineering),
Shelby Pereira, Thierry Pun (Université de Genève)

Shedding More Light on Image Watermarks ....................................... 191

Juan Ramón Hernández, Fernando Pérez-González (Universidad de
Vigo)

Continuous Steganographic Data Transmission Using
Uncompressed Audio ................................................................. 208

Chr. Neubauer, J. Herre, K. Brandenburg (Fraunhofer Institut für
Integrierte Schaltungen)

Attacks

Attacks on Copyright Marking Systems .............................................. 218

Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn (University
of Cambridge)

Testing Digital Watermark Resistance to Destruction ....................... 239

Sabrina Sowers, Abdou Youssef (George Washington University)

Analysis of the Sensitivity Attack against Electronic Watermarks
in Images ......................................................................................... 258

Jean-Paul Linnartz, Marten van Dijk (Philips Research Laboratories)

Steganalysis of Images Created Using Current Steganography Software ... 273

Neil F. Johnson, Sushil Jajodia (George Mason University)

Twin Peaks: The Histogram Attack on Fixed Depth Image Watermarks . . 290

Maurice Maes (Philips Research Laboratories)
Theory

An Information-Theoretic Model for Steganography .................... 306
Christian Cachin (Massachusetts Institute of Technology)

Steganalysis and Game Equilibria ........................................... 319
J. Mark Ettinger (Los Alamos National Laboratory)

Modeling the False Alarm and Missed Detection Rate for Electronic
Watermarks ........................................................................... 329
Jean-Paul Linnartz, Ton Kalker, Geert Depovere (Philips Research
Laboratories)

Modelling the Security of Steganographic Systems .................... 344
J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke,
A. Westfeld, G. Wicke, G. Wolf (Technische Universität Dresden)

On Public-Key Steganography in the Presence of an Active Warden ... 355
Scott Craver (Intel Corporation)

Author Index ........................................................................... 369