

*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

*University of California, Los Angeles, CA, 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*

Yun Q. Shi (Ed.)

# Transactions on Data Hiding and Multimedia Security I



Springer

Volume Editor

Yun Q. Shi  
New Jersey Institute of Technology  
Department of Electrical and Computer Engineering  
323, M.L. King Blvd., Newark, NJ 07102, USA  
E-mail: shi@njit.edu

Library of Congress Control Number: 2006935869

CR Subject Classification (1998): K.4.1, K.6.5, H.5.1, D.4.6, E.3, E.4, F.2.2, H.3, I.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-49071-X Springer Berlin Heidelberg New York
ISBN-13	978-3-540-49071-5 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  
springer.com

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 11926214      06/3142      5 4 3 2 1 0

# Preface

It is our great pleasure to present in this volume the inaugural issue of the *LNCS Transactions on Data Hiding and Multimedia Security*. Since the mid-1990s, digital data hiding has been proposed as an enabling technology for solving security problems in multimedia distribution. Digital watermarks have now been used in applications including broadcast monitoring, movie fingerprinting, digital rights management, steganography, video indexing and retrieval, and image authentication, to name but a few. In some of these applications, data hiding and cryptographic techniques are combined to complement each other to achieve the goal. This combination resulted in a completely new research field, which now forms one important branch of multimedia security. It is expected that multimedia security will become more and more mature and will play a significant role in future commercial multimedia applications. Besides data hiding, the two related disciplines steganalysis and data forensics, which try, respectively, to detect steganographic transmission and to assert the integrity of media data, are increasingly attracting researchers. They have become another important branch of multimedia security. This new journal, *LNCS Transactions on Data Hiding and Multimedia Security*, aims to be a forum for all researchers in these important and new fields by publishing both original and archival research results.

This first issue contains five papers, divided into three groups. The first group consists of two papers dealing with watermarking. Dittmann et al. introduce a theoretical framework for robust digital audio watermarking algorithms, focusing on the triangle of robustness, transparency and capacity. The authors then compare selected audio watermarking algorithms in the newly developed model. In the second paper, Perez-Freire et al. provide a survey of watermarking security. Whereas watermark robustness has been generally identified with decoding error rate or resistance against intentional removal, watermark security is still a relatively fuzzy concept. This paper clarifies the concepts of watermark security and provides an exhaustive literature overview. It can serve as a starting point for newcomers interested in this important research topic.

The second group contains two papers. Adelsbach et al. discuss efficient implementations of zero-knowledge watermark detectors, which were recently proposed to overcome the drawbacks of symmetric watermarking schemes, i.e., the required disclosure of critical information (such as watermark and key) that jeopardizes the security of embedded watermark once the information is revealed. The authors propose efficient solutions for correlation-based detectors and more generally for watermarking schemes whose detection criteria can be expressed as a polynomial in the quantities required for detection. In the second paper, Koster et al. introduce the concept of personal entertainment domains (PED) in digital rights management (DRM) and outline the architecture of a complete PED-DRM scheme. In PEDs, content is bound to a person rather than to a device, thus providing a better user experience than in current DRM solutions.

The third group contains one paper dealing with steganalysis. Kharrazi et al. report on the use of fusion techniques to improve the detection accuracy of steganalysis. As various powerful steganalysis schemes have been reported in the literature in the past, in practice a steganalyst has to select one or more techniques which he or she applies on a suspected stego image. In the paper, the authors investigate methods that allow one to come to a conclusion if the decisions from these selected steganalytic techniques are contradictory.

We do hope that the inaugural issue of the *LNCS Transactions of Data Hiding and Multimedia Security* is of great interest to this research community and will trigger new research in this exciting field.

Finally, we sincerely thank all of the authors, reviewers and editors who have devoted their time to the success of the journal. Last but not the least special thanks go to Springer and Alfred Hofmann for their continuous support.

September 2006

Yun Q. Shi  
Editor-in-Chief  
Hyoung-Joong Kim  
Vice Editor-in-Chief  
Stefan Katzenbeisser  
Vice Editor-in-Chief

# **LNCS Transactions on Data Hiding and Multimedia Security**

## **Editorial Board**

### **Editor-in-Chief**

Yun Q. Shi

New Jersey Institute of Technology, Newark, NJ, USA  
shi@njit.edu

### **Vice Editors-in-Chief**

Hyoung-Joong Kim

Korea University, Seoul, Korea  
khj-@korea.ac.kr

Stefan Katzenbeisser

Philips Research Europe, Eindhoven, Netherlands  
stefan.katzenbeisser@philips.com

### **Associate Editors**

Mauro Barni

University of Siena, Siena, Italy  
barni@dii.unisi.it

Jeffrey Bloom

Thomson, Princeton, NJ, USA  
Jeffrey.Bloom@thomson.net

Jana Dittmann

Otto-von-Guericke-University Magdeburg,  
Magdeburg, Germany  
jana.dittmann@iti.cs.uni-magdeburg.de

Jiwu Huang

Sun Yat-sen University, Guangzhou, China  
isshjw@mail.sysu.edu.cn

Mohan Kankanhalli

National University of Singapore, Singapore  
mohan@comp.nus.edu.sg

Darko Kirovski

Microsoft, Redmond, WA, USA  
darkok@microsoft.com

C. C. Jay Kuo

University of Southern California, Los Angeles, USA  
cckuo@sipi.usc.edu

Heung-Kyu Lee

Korea Advanced Institute of Science and Technology,  
Daejeon, Korea  
hklee@mmc.kaist.ac.kr

Benoit Macq

Catholic University of Louvain, Belgium  
macq@tele.ucl.ac.be

Nasir Memon

Polytechnic University, Brooklyn, NY, USA  
memon@poly.edu

Kivanc Mihcak

Bogazici University, Istanbul, Turkey  
kivanc.mihcak@boun.edu.tr

Hideki Noda	Kyushu Institute of Technology, Iizuka, Japan noda@mip.ces.kyutech.ac.jp
Jeng-Shyang Pan	National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan jspan@cc.kuas.edu.tw
Fernando Perez-Gonzalez	University of Vigo, Vigo, Spain fperez@gts.tsc.uvigo.es
Andreas Pfitzmann	Dresden University of Technology, Germany pfitza@inf.tu-dresden.de
Alessandro Piva	University of Florence, Florence, Italy piva@lci.det.unifi.it
Yong-Man Ro	Information and Communications University, Daejeon, Korea yro@icu.ac.kr
Ahmad-Reza Sadeghi	Ruhr-University, Bochum, Germany sadeghi@crypto.rub.de
Kouichi Sakurai	Kyushu University, Fukuoka, Japan sakurai@csce.kyushu-u.ac.jp
Qibin Sun	Institute of Infocomm Research, Singapore qibin@i2r.a-satr.edu.sg
Edward Wong	Polytechnic University, Brooklyn, NY, USA wong@poly.edu

## Advisory Board

Pil Joong Lee	Pohang University of Science and Technology, Pohang, Korea pjl@postech.ac.kr
Bede Liu	Princeton University, Princeton, NJ, USA liu@ee.princeton.edu

# Table of Contents

Theoretical Framework for a Practical Evaluation and Comparison of Audio Watermarking Schemes in the Triangle of Robustness, Transparency and Capacity .....	1
<i>Jana Dittmann, David Megías, Andreas Lang, Jordi Herrera-Joancomartí</i>	
Watermarking Security: A Survey .....	41
<i>Luis Pérez-Freire, Pedro Comesaña, Juan Ramón Troncoso-Pastoriza, Fernando Pérez-González</i>	
Efficient Implementation of Zero-Knowledge Proofs for Watermark Detection in Multimedia Data .....	73
<i>André Adelsbach, Markus Rohe, Ahmad-Reza Sadeghi</i>	
Identity-Based DRM: Personal Entertainment Domain .....	104
<i>Paul Koster, Frank Kamperman, Peter Lenoir, Koen Vrieling</i>	
Improving Steganalysis by Fusion Techniques: A Case Study with Image Steganography .....	123
<i>Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon</i>	
<b>Author Index</b> .....	139