Ingemar J. Cox
Ton Kalker
Heung-Kyu Lee (Eds.)

LNCS 3304

Digital Watermarking

Third International Workshop, IWDW 2004
Seoul, South Korea, October/ November 2004
Revised Selected Papers

Springer

Ingemar J. Cox Ton Kalker
Heung-Kyu Lee (Eds.)

Digital Watermarking

Third International Workshop, IWDW 2004
Seoul, South Korea, October 30 - November 1, 2004
Revised Selected Papers

Springer

Volume Editors

Ingemar J. Cox
University College London
Department of Computer Science &
Department of Electronic and Electrical Engineering, UK
E-mail: ingemar@ieee.org

Ton Kalker
Hewlett-Packard Lab.
Multimedia Communications & Networking Department
1501 Page Mill Road, Palo Alto, CA 94305, USA
E-mail: Ton.Kalker@hp.com

Heung-Kyu Lee
KAIST, Department of EECS
373-1 Gusong-Dong, Yusong-Gu, Daejon, South Korea, 305-701
E-mail: hklee@mmc.kaist.ac.kr

Library of Congress Control Number: 2005921087

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

ISSN 0302-9743
ISBN 3-540-24839-0 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11392385 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3304

Preface

We are happy to present to you the proceedings of the 3rd International Workshop on Digital Watermarking, IWDW 2004. Since its modern reappearance in the academic community in the early 1990s, great progress has been made in understanding both the capabilities and the weaknesses of digital watermarking.

On the theoretical side, we all are now well aware of the fact that digital watermarking is best viewed as a form of communication using side information. In the case of digital watermarking the side information in question is the document to be watermarked. This insight has led to a better understanding of the limits of the capacity and robustness of digital watermarking algorithms. It has also led to new and improved watermarking algorithms, both in terms of capacity and imperceptibility. Similarly, the role of human perception, and models thereof, has been greatly enhanced in the study and design of digital watermarking algorithms and systems.

On the practical side, applications of watermarking are not yet abundant. The original euphoria on the role of digital watermarking in copy protection and copyright protection has not resulted in widespread use in practical systems. With hindsight, a number of reasons can be given for this lack of practical applications.

We now know that watermark imperceptibility cannot be equated to watermark security. An information signal that cannot be perceived by the human sensory system is not necessarily undetectable to well-designed software and hardware systems. The existence of watermark readers bears proof of this observation. Designing watermarking methods that are robust to intentional and targeted attacks has turned out to be an extremely difficult task. Improved watermarking methods face more intelligent attacks. More intelligent attacks face improved watermarking methods. This cycle of improved attacks and counterattacks is still ongoing, and we do not foresee it ending soon.

It was the goal of IWDW 2004 to update the scientific and content-owner communities on the state of the art in digital watermarking. To that end, more than 60 submissions to IWDW 2004 were carefully reviewed, with at least three reviewers each. Emphasizing high quality and the state of the art, fewer than 50% of the submitted papers were selected for oral presentation. The topics that were addressed in the accepted papers cover all the relevant aspects of digital watermarking: theoreticals modeling, robustness, capacity, imperceptibility and the human perceptual system, security and attacks, steganography, methods, and watermarking systems. Every effort was made to give the authors the best possible podium to present their findings.

We hope that you enjoy the workshop proceedings and find it an inspiration for your future research.

October 2004

Ingemar J. Cox
Ton Kalker
Heung Kyu Lee

Organization

General Chair

P.J. Lee (POSTECH, South Korea)

Program Committee Co-chairs

Ingemar J. Cox (UCL, UK)
Ton Kalker (Philips, The Netherlands)
Heung-Kyu Lee (KAIST, South Korea)

Program Committee

Mauro Barni (U. of Florence, Italy)
Jana Dittman (Otto-von-Guericke U., Germany)
Jean-Luc Dugelay (Eurecom, France)
Jessica Friedrich (SUNY Binghamton, USA)
Teddy Furon (UCL, UK)
Stefan Katzenbeiser (Vienna U. of Tech., Austria)
Inald Lagendijk (Delft U. of Tech., Netherlands)
Benoit Macq (UCL, UK)
Nasir Memon (Polytechnic U., NY, USA)
Matt Miller (NEC, USA)
Pierre Moulin (U. of Illinois, USA)
Fernando Perez (U. of Vigo, Spain)
Ioannis Pitas (U. of Thessaloniki, Greece)
Sviatoslav Voloshynovsky (U. of Geneva, Switzerland)
Min Wu (U. of Maryland, USA)
Jiwu Huang (Zhongshan U., China)
Mohan Kankanhalli (NUS, Singapore)
K. Sakurai (Kyushu U., Japan)
Yun-Qing Shi (New Jersey Inst. of Tech., USA)
Yong-Man Ro (ICU, South Korea)
Hyung-Joong Kim (KangWon National University, South Korea)
Kivanc Mihcak (Microsoft, USA)

Organizing Committee Chair

Choong-Hoon Lee (KAIST, South Korea)

Lecture Notes in Computer Science

For information about Vols. 1–3306

please contact your bookseller or Springer

Vol. 3418: U. Brandes, T. Erlebach (Eds.), Network Analysis. XII, 471 pages. 2005.

Vol. 3416: M. Böhlen, J. Gamper, W. Polasek, M.A. Wimmer (Eds.), E-Government: Towards Electronic Democracy. XIII, 311 pages. 2005. (Subseries LNAI).

Vol. 3412: X. Franch, D. Port (Eds.), COTS-Based Software Systems. XVI, 312 pages. 2005.

Vol. 3410: C.A. Coello Coello, A. Hernández Aguirre, E. Zitzler (Eds.), Evolutionary Multi-Criterion Optimization. XVI, 912 pages. 2005.

Vol. 3409: N. Guelfi, G. Reggio, A. Romanovsky (Eds.), Scientific Engineering of Distributed Java Applications. X, 127 pages. 2005.

Vol. 3406: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 829 pages. 2005.

Vol. 3404: V. Diekert, B. Durand (Eds.), STACS 2005. XVI, 706 pages. 2005.

Vol. 3403: B. Ganter, R. Godin (Eds.), Formal Concept Analysis. XI, 419 pages. 2005. (Subseries LNAI).

Vol. 3401: Z. Li, L. Vulkov, J. Waśniewski (Eds.), Numerical Analysis and Its Applications. XIII, 630 pages. 2005.

Vol. 3398: D.-K. Baik (Ed.), Systems Modeling and Simulation: Theory and Applications. XIV, 733 pages. 2005. (Subseries LNAI).

Vol. 3397: T.G. Kim (Ed.), Artificial Intelligence and Simulation. XV, 711 pages. 2005. (Subseries LNAI).

Vol. 3396: R.M. van Eijk, M.-P. Huget, F. Dignum (Eds.), Advances in Agent Communication. X, 261 pages. 2005. (Subseries LNAI).

Vol. 3393: H.-J. Kreowski, U. Montanari, F. Orejas, G. Rozenberg, G. Taentzer (Eds.), Formal Methods in Software and Systems Modeling. XXVII, 413 pages. 2005.

Vol. 3391: C. Kim (Ed.), Information Networking. XVII, 936 pages. 2005.

Vol. 3388: J. Lagergren (Ed.), Comparative Genomics. VIII, 133 pages. 2005. (Subseries LNBI).

Vol. 3387: J. Cardoso, A. Sheth (Eds.), Semantic Web Services and Web Process Composition. VIII, 147 pages. 2005.

Vol. 3386: S. Vaudenay (Ed.), Public Key Cryptography - PKC 2005. IX, 436 pages. 2005.

Vol. 3385: R. Cousot (Ed.), Verification, Model Checking, and Abstract Interpretation. XII, 483 pages. 2005.

Vol. 3383: J. Pach (Ed.), Graph Drawing. XII, 536 pages. 2005.

Vol. 3382: J. Odell, P. Giorgini, J.P. Müller (Eds.), Agent-Oriented Software Engineering V. X, 239 pages. 2005.

Vol. 3381: P. Vojtáš, M. Bieliková, B. Charron-Bost, O. Sýkora (Eds.), SOFSEM 2005: Theory and Practice of Computer Science. XV, 448 pages. 2005.

Vol. 3379: M. Hemmje, C. Niederee, T. Risse (Eds.), From Integrated Publication and Information Systems to Information and Knowledge Environments. XXIV, 321 pages. 2005.

Vol. 3378: J. Kilian (Ed.), Theory of Cryptography. XII, 621 pages. 2005.

Vol. 3376: A. Menezes (Ed.), Topics in Cryptology – CT-RSA 2005. X, 385 pages. 2004.

Vol. 3375: M.A. Marsan, G. Bianchi, M. Listanti, M. Meo (Eds.), Quality of Service in Multiservice IP Networks. XIII, 656 pages. 2005.

Vol. 3374: D. Weyns, H.V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems. X, 279 pages. 2005. (Subseries LNAI).

Vol. 3372: C. Bussler, V. Tannen, I. Fundulaki (Eds.), Semantic Web and Databases. X, 227 pages. 2005.

Vol. 3368: L. Paletta, J.K. Tsotsos, E. Rome, G.W. Humphreys (Eds.), Attention and Performance in Computational Vision. VIII, 231 pages. 2005.

Vol. 3366: I. Rahwan, P. Moraitis, C. Reed (Eds.), Argumentation in Multi-Agent Systems. XII, 263 pages. 2005. (Subseries LNAI).

Vol. 3363: T. Eiter, L. Libkin (Eds.), Database Theory - ICDT 2005. XI, 413 pages. 2004.

Vol. 3362: G. Barthe, L. Burdy, M. Huisman, J.-L. Lanet, T. Muntean (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 257 pages. 2005.

Vol. 3361: S. Bengio, H. Bourlard (Eds.), Machine Learning for Multimodal Interaction. XII, 362 pages. 2005.

Vol. 3360: S. Spaccapietra, E. Bertino, S. Jajodia, R. King, D. McLeod, M.E. Orlowska, L. Strous (Eds.), Journal on Data Semantics II. XI, 223 pages. 2005.

Vol. 3359: G. Grieser, Y. Tanaka (Eds.), Intuitive Human Interfaces for Organizing and Accessing Intellectual Assets. XIV, 257 pages. 2005. (Subseries LNAI).

Vol. 3358: J. Cao, L.T. Yang, M. Guo, F. Lau (Eds.), Parallel and Distributed Processing and Applications. XXIV, 1058 pages. 2004.

Vol. 3357: H. Handschuh, M.A. Hasan (Eds.), Selected Areas in Cryptography. XI, 354 pages. 2004.

Vol. 3356: G. Das, V.P. Gulati (Eds.), Intelligent Information Technology. XII, 428 pages. 2004.

Vol. 3355: R. Murray-Smith, R. Shorten (Eds.), Switching and Learning in Feedback Systems. X, 343 pages. 2005.

Vol. 3353: J. Hromkovič, M. Nagl, B. Westfechtel (Eds.), Graph-Theoretic Concepts in Computer Science. XI, 404 pages. 2004.

Vol. 3352: C. Blundo, S. Cimato (Eds.), Security in Communication Networks. XI, 381 pages. 2005.

Vol. 3350: M. Hermenegildo, D. Cabeza (Eds.), Practical Aspects of Declarative Languages. VIII, 269 pages. 2005.

Vol. 3349: B.M. Chapman (Ed.), Shared Memory Parallel Programming with Open MP. X, 149 pages. 2005.

Vol. 3348: A. Canteaut, K. Viswanathan (Eds.), Progress in Cryptology - INDOCRYPT 2004. XIV, 431 pages. 2004.

Vol. 3347: R.K. Ghosh, H. Mohanty (Eds.), Distributed Computing and Internet Technology. XX, 472 pages. 2004.

Vol. 3346: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 249 pages. 2005. (Subseries LNAI).

Vol. 3345: Y. Cai (Ed.), Ambient Intelligence for Scientific Discovery. XII, 311 pages. 2005. (Subseries LNAI).

Vol. 3344: J. Malenfant, B.M. Østvold (Eds.), Object-Oriented Technology. ECOOP 2004 Workshop Reader. VIII, 215 pages. 2005.

Vol. 3342: E. Şahin, W.M. Spears (Eds.), Swarm Robotics. IX, 175 pages. 2005.

Vol. 3341: R. Fleischer, G. Trippen (Eds.), Algorithms and Computation. XVII, 935 pages. 2004.

Vol. 3340: C.S. Calude, E. Calude, M.J. Dinneen (Eds.), Developments in Language Theory. XI, 431 pages. 2004.

Vol. 3339: G.I. Webb, X. Yu (Eds.), AI 2004: Advances in Artificial Intelligence. XXII, 1272 pages. 2004. (Subseries LNAI).

Vol. 3338: S.Z. Li, J. Lai, T. Tan, G. Feng, Y. Wang (Eds.), Advances in Biometric Person Authentication. XVIII, 699 pages. 2004.

Vol. 3337: J.M. Barreiro, F. Martin-Sanchez, V. Maojo, F. Sanz (Eds.), Biological and Medical Data Analysis. XI, 508 pages. 2004.

Vol. 3336: D. Karagiannis, U. Reimer (Eds.), Practical Aspects of Knowledge Management. X, 523 pages. 2004. (Subseries LNAI).

Vol. 3335: M. Malek, M. Reitenspieß, J. Kaiser (Eds.), Service Availability. X, 213 pages. 2005.

Vol. 3334: Z. Chen, H. Chen, Q. Miao, Y. Fu, E. Fox, E.-p. Lim (Eds.), Digital Libraries: International Collaboration and Cross-Fertilization. XX, 690 pages. 2004.

Vol. 3333: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part III. XXXV, 785 pages. 2004.

Vol. 3332: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part II. XXXVI, 1051 pages. 2004.

Vol. 3331: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part I. XXXVI, 667 pages. 2004.

Vol. 3330: J. Akiyama, E.T. Baskoro, M. Kano (Eds.), Combinatorial Geometry and Graph Theory. VIII, 227 pages. 2005.

Vol. 3329: P.J. Lee (Ed.), Advances in Cryptology - ASIACRYPT 2004. XVI, 546 pages. 2004.

Vol. 3328: K. Lodaya, M. Mahajan (Eds.), FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science. XVI, 532 pages. 2004.

Vol. 3327: Y. Shi, W. Xu, Z. Chen (Eds.), Data Mining and Knowledge Management. XIII, 263 pages. 2005. (Subseries LNAI).

Vol. 3326: A. Sen, N. Das, S.K. Das, B.P. Sinha (Eds.), Distributed Computing - IWDC 2004. XIX, 546 pages. 2004.

Vol. 3325: C.H. Lim, M. Yung (Eds.), Information Security Applications. XI, 472 pages. 2005.

Vol. 3323: G. Antoniou, H. Boley (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 215 pages. 2004.

Vol. 3322: R. Klette, J. Žunić (Eds.), Combinatorial Image Analysis. XII, 760 pages. 2004.

Vol. 3321: M.J. Maher (Ed.), Advances in Computer Science - ASIAN 2004. Higher-Level Decision Making. XII, 510 pages. 2004.

Vol. 3320: K.-M. Liew, H. Shen, S. See, W. Cai (Eds.), Parallel and Distributed Computing: Applications and Technologies. XXIV, 891 pages. 2004.

Vol. 3319: D. Amyot, A.W. Williams (Eds.), System Analysis and Modeling. XII, 301 pages. 2005.

Vol. 3318: E. Eskin, C. Workman (Eds.), Regulatory Genomics. VIII, 115 pages. 2005. (Subseries LNBI).

Vol. 3317: M. Domaratzki, A. Okhotin, K. Salomaa, S. Yu (Eds.), Implementation and Application of Automata. XII, 336 pages. 2005.

Vol. 3316: N.R. Pal, N.K. Kasabov, R.K. Mudi, S. Pal, S.K. Parui (Eds.), Neural Information Processing. XXX, 1368 pages. 2004.

Vol. 3315: C. Lemaître, C.A. Reyes, J.A. González (Eds.), Advances in Artificial Intelligence – IBERAMIA 2004. XX, 987 pages. 2004. (Subseries LNAI).

Vol. 3314: J. Zhang, J.-H. He, Y. Fu (Eds.), Computational and Information Science. XXIV, 1259 pages. 2004.

Vol. 3313: C. Castelluccia, H. Hartenstein, C. Paar, D. Westhoff (Eds.), Security in Ad-hoc and Sensor Networks. VIII, 231 pages. 2005.

Vol. 3312: A.J. Hu, A.K. Martin (Eds.), Formal Methods in Computer-Aided Design. XI, 445 pages. 2004.

Vol. 3311: V. Roca, F. Rousseau (Eds.), Interactive Multimedia and Next Generation Networks. XIII, 287 pages. 2004.

Vol. 3310: U.K. Wiil (Ed.), Computer Music Modeling and Retrieval. XI, 371 pages. 2005.

Vol. 3309: C.-H. Chi, K.-Y. Lam (Eds.), Content Computing. XII, 510 pages. 2004.

Vol. 3308: J. Davies, W. Schulte, M. Barnett (Eds.), Formal Methods and Software Engineering. XIII, 500 pages. 2004.

Vol. 3307: C. Bussler, S.-k. Hong, W. Jun, R. Kaschek, D.. Kinshuk, S. Krishnaswamy, S.W. Loke, D. Oberle, D. Richards, A. Sharma, Y. Sure, B. Thalheim (Eds.), Web Information Systems – WISE 2004 Workshops. XV, 277 pages. 2004.

Table of Contents

Invited Lecture

Reversible Data Hiding
Yun Q. Shi 1

Fingerprinting Curves
Hongmei Gou, Min Wu 13

Informed Detection Revisited
Jeffrey A. Bloom, Matt L. Miller 29

Session I: Systems

A Counter-Geometric Distortions Data Hiding Scheme Using Double Channels in Color Images
Gang Xue, Peizhong Lu, Jinlian Wang 42

A Secure Internet-Based Personal Identity Verification System Using Lossless Watermarking and Fingerprint Recognition
Guorong Xuan, Junxiang Zheng, Chengyun Yang, Yun Q. Shi, Dekun Zou, Liu Liansheng, Bai Weichao 55

Better Use of Human Visual Model in Watermarking Based on Linear Prediction Synthesis Filter
Xinshan Zhu, Yangsheng Wang 66

Watermarking System for QoS Aware Content Adaptation
Tae Meon Bae, Seok Jun Kang, Yong Man Ro 77

Session II: Theory

Weighted Segmented Digital Watermarking
Glen E. Wheeler, Reihaneh Safavi-Naini, Nicholas Paul Sheppard 89

Robust Estimation of Amplitude Modification for Scalar Costa Scheme Based Audio Watermark Detection
Siho Kim, Keunsung Bae 101

Reversible Data Hiding Using Integer Wavelet Transform and Companding Technique
Guorong Xuan, Chengyun Yang, Yizhan Zhen, Yun Q. Shi, Zhicheng Ni 115

Session III: Authentication and Stego

Alteration-Locating Authentication Watermarking for Binary Images
Hae Yong Kim, Ricardo Lopes de Queiroz 125

On Security Notions of Steganographic Systems
Kisik Chang, Robert H. Deng, Bao Feng, Sangjin Lee, Hyungjun Kim 137

A Multi-feature Based Invertible Authentication Watermarking for JPEG Images
Deng-Pan Ye, Yao-Bin Mao, Yue-Wei Dai, Zhi-Quan Wang 152

Steganographic Scheme Using a Block Cipher
Jeong Jae Yu, Chang-ho Jung, Seok-Koo Yoon, Sangjin Lee 163

Watermarking Attack: Security of WSS Techniques
François Cayre, Caroline Fontaine, Teddy Furon 171

Session IV: Cryptography

Flaws in Generic Watermarking Protocols Based on Zero-Knowledge Proofs
Raphael C.-W. Phan, Huo-Chong Ling 184

Cryptanalysis of a Wavelet Based Watermarking Scheme
Tanmoy Kanti Das, Jianying Zhou, Subhamoy Maitra 192

A Generalized Method for Constructing and Proving Zero-Knowledge Watermark Proof Systems
Xianfeng Zhao, Yingxia Dai, Dengguo Feng 204

Towards the Public but Noninvertible Watermarking
Xianfeng Zhao, Yingxia Dai, Dengguo Feng 218

A Generalization of an Anonymous Buyer-Seller Watermarking Protocol and Its Application to Mobile Communications
JaeGwi Choi, JiHwan Park 232

Session V: Methods

Robust Frequency Domain Audio Watermarking: A Tuning Analysis
David Megías, Jordi Herrera-Joancomartí, Julià Minguillón 244

Watermarking Technique for Authentication of 3-D Polygonal Meshes
Wan-Hyun Cho, Myung-Eun Lee, Hyun Lim, Soon-Young Park 259

Fidelity-Controlled Robustness Enhancement of Blind Watermarking Schemes Using Evolutionary Computational Techniques
Chun-Hsiang Huang, Chih-Hao Shen, Ja-Ling Wu 271

Robust Watermarking on Polygonal Meshes Using Distribution of Vertex Norms
Jae-Won Cho, Min-Su Kim, Remy Prost, Hyun-Yeol Chung, Ho-Youl Jung 283

A Video Watermarking Using the 3D Wavelet Transform and Two Perceptual Watermarks
Seung-Jin Kim, Suk-Hwan Lee, Tae-Su Kim, Ki-Ryong Kwon, Kuhn-Il Lee 294

Author Index 305

Reversible Data Hiding

Yun Q. Shi

Department of Electrical and Computer Engineering,
New Jersey Institute of Technology,
Newark, NJ 07102, USA
shi@njit.edu

Abstract. Reversible data hiding, in which the stago-media can be reversed to the original cover media exactly, has attracted increasing interests from the data hiding community. In this study, the existing reversible data hiding algorithms, including some newest schemes, have been classified into three categories: 1) Those developed for fragile authentication; 2) Those developed for achieving high data embedding capacity; 3) Those developed for semi-fragile authentication. In each category, some prominent representatives are selected. The principles, merits, drawbacks and applications of these algorithms are analyzed and addressed.

1 Introduction

Digital watermarking, often referred to as data hiding, has recently been proposed as a promising technique for information assurance. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as *lossy* data hiding. It can be shown that most of the data hiding algorithms reported in the literature are lossy. Here, let us examine three major classes of data hiding algorithm. With the most popularly utilized spread-spectrum watermarking techniques, either in DCT domain [1] or block 8x8 DCT domain [2], *round-off* error and/or *truncation* error may take place during data embedding. As a result, there is no way to reverse the stago-media back to the original without distortion. For the least significant bit-plane (LSB) embedding methods, the bits in the LSB are substituted by the data to be embedded and the bit-replacement is *not memorized.* Consequently, the LSB method is not reversible. With the third group of frequently used watermarking techniques, called quantization index modulation (QIM) [3], *quantization* error renders lossy data hiding.

In applications, such as in law enforcement, medical image systems, it is desired to be bale to reverse the stego-media back to the original cover media for legal consideration. In remote sensing and military imaging, high accuracy is required. In some scientific research, experimental data are expensive to be achieved. Under these circumstances, the reversibility of the original media is desired. The data hiding schemes satisfying this requirement can be referred to as *lossless*. The terms of *reversible*, or *invertible* also used frequently. We choose to use reversible in this paper.

I.J. Cox et al. (Eds.): IWDW 2004, LNCS 3304, pp. 1 – 12, 2005.

In Section 2, we classify the reversible data hiding techniques that have appeared in the literature over the past several years into three different categories. In each category, the most prominent representatives are selected and the principles, merits, drawbacks and applications of these algorithms are analyzed in Sections 3, 4, and 5, respectively. Conclusions are drawn in Section 6.

2 Classification of Reversible Data Hiding Algorithms

The following list contains, to our knowledge, most of reversible data hiding algorithms published in the literature. The list is not expected to be completed as the research in this area continues to make vigorous progress. These algorithms can be classified into three categories: 1st, those for fragile authentication, 2nd, those for high embedding capacity, and 3rd, those for semi-fragile authentication. Among each category, one or two prominent algorithms are selected as representative. Their fundamental idea and scheme to achieve reversibility, and their performance are discussed in the following sections.

1. Barton's U.S. Patent 5,646,997 (97) (1st)
2. Honsinger et al.'s US Patent 6,278,791 B1 (01) (1st)
3. Fridrich et al.'s method (SPIE01) (1st)
4. de Vleeschouwer et al.'s method (MMSP01) (3rd)
5. Goljan et al.'s method (IHW01) (2nd)
6. Xuan et al.'s method (MMSP02) (2nd)
7. Ni et al.'s method (ISCAS03) (2nd)
8. Celik et al.'s method (ICIP02) (2nd)
9. Tian's method (CSVT03) (2nd)
10. Yang et al.'s method (SPIE04) (2nd)
11. Thodi & Rodríguez's method (SWSIAI04) (2nd)
12. Ni et al.'s method (ICME04) (3rd)
13. Zou et al.'s method (MMSP04) (3rd)
14. Xuan et al.'s method (MMSP04) (2nd)
15. Xuan et al.'s method (IWDW04) (2nd)

3 Those for Fragile Authentication

The first several reversible data hiding algorithms developed at the early stage belong to this category. Since fragile authentication does not need much data to be embedded in a cover medium, the embedding capacity in this category is not large, normally between 1k to 2k bits. For a typical 512×512 gray scale image, this capacity is equivalent to a data hiding rate from 0.0038 bits per pixel (bpp) to 0.0076 bpp.

In this category, we choose Honsinger et al.'s patent in 2001 [5] as its representative. It describes in detail a reversible data hiding technique used for fragile authentication. Their method is carried out in the image spatial domain by using modulo-256 addition. In the embedding, $Iw = (I + W) \bmod 256$, where Iw denotes the marked image, I an original image, W is the payload derived from the hash function of the original image. In the authentication side, the payload W can be extracted from the marked image by subtracting the payload from the marked image, thus reversibly recovering the original image. By using modulo-256 addition, the issue of over/underflow is avoided. Here, by over/underflow, it is meant that grayscale values either exceeding its upper bound (*overflow*) or its lower bound (*underflow*). For instance, for an 8-bit gray image, its gray scale ranges from 0 to 255. The overflow refers to grayscale exceeds 255, while the underflow refers to below 0. It is clear that either case will destroy reversibility. Therefore this issue is often a critical issue in reversible data hiding. Using modulo-256 addition can avoid over/underflow on the one hand. On the other hand, however, the stego-image may suffer from the salt-and-pepper noise during possible grayscale flipping over between 0 and 255 in either direction due to the operation of modulo-256 addition. The effect caused by salt-and-pepper noise will become clear when we discuss an algorithm also using modulo-256 addition in the third category.

4 Those for High Data Embedding Capacity

All the reversible data hiding techniques in the first category aim at fragile authentication, instead of hiding large amount data. As a result, the amount of hidden data is rather limited and may not be suitable for applications such as covert communications and medical data systems. Hence, Goljan et al. [10] presented a first reversible data hiding technique, referred to as R-S scheme, which is suitable for the purpose of having high data embedding capacity. Later, a difference expansion scheme was developed by Tian [15], which has greatly advanced the performance of reversible data hiding in terms of data embedding capacity versus PSNR of marked images with respect to original images. Recently, some integer wavelet transform based reversible data hiding schemes have been developed by Xuan et al. [16,17], which have demonstrated superior performance over that reported in [15]. These representative schemes are presented in this section.

4.1 R-S Scheme

The mechanism of this scheme is described as follows. The pixels in an image are grouped into non-overlapped blocks, each consisting of a number of adjacent pixels. For instance, it could be a horizontal block consisting of four consecutive pixels. A discrimination function that can capture the smoothness of the groups is established to classify the blocks into three different categories, Regular, Singular and Unusable. An invertible operation F can be applied to groups. That is, it can map a block from one category to another as $F(R)=S$, $F(S)=R$, and $F(U)=U$. It is invertible since applying it to a block twice produces the original block. This invertible operation is hence called *flipping F*. An example of the invertible operation F can be the permutation between 0 and 1, 2 and 3, 3 and 4, and so on. This is equivalent to flipping the least significant bit (LSB). Another example is the permutation between 0 and 2, 1 and 3, 4 and 6, and so on, i.e., flipping the second LSB. Apparently, the *strength* of the latter flipping is stronger than the former. The principle to achieve reversible data embedding lies in that there is a bias between the number of regular blocks and that of singular blocks for most of images. This is equivalent to say that there is a redundancy and some space can be created by lossless compression. Together with some proper bookkeeping scheme, one can achieve reversibility.

The proposed algorithm first scan a cover image block-by-block, resulting in a so-called RS-vector formed by representing, say, an R-block by binary 1 and an S-block by binary 0 with the U groups simply skipped. Then the algorithm losslessly compresses this RS-vector – as an overhead for bookkeeping usage in reconstruction of the original image late. By assigning binary 1 and 0 to R and S blocks, respectively, one bit can be embedded into each R or S block. If the bit to-be-embedded does match the type of a block under consideration, the flipping operation F is applied to the block to obtain a match. The actual embedded data consist of the overhead and the watermark signal (pure payload). In data extraction, the algorithm scans the marked image in the same manner as in the data embedding. From the resultant RS-vector, the embedded data can be extracted. The overhead portion will be used to reconstruct the original image, while the remaining portion is the payload.

While it is novel and successful in reversible data hiding with a large embedding capacity, the amount of data that can be hidden by this technique is still not large enough for some applications such as covert communications. From what is reported in [10], the estimated embedding capacity ranges from 0.022 bpp to 0.17 bpp when the embedding strength is six and the PSNR of the marked image versus the original image is about 36.06 dB. Note that the embedding strength six is rather high and there are some block artifacts in the marked image generated with this embedding strength. On the one hand, this embedding capacity is much higher than that in the first category discussed in the previous subsection. On the other hand, however, it may be not high enough for some applications. This limited embedding capacity is expected because each block can at most embed one bit, U blocks cannot accommodate data, and the overhead is necessary for reconstruction of the original image. Another problem with this method is that when the embedding strength increases, the embedding capacity will increase, at the same time the visual quality will drop. Often, block artifacts will take place at this circumstance, thus causing visual quality of marked image to decrease.

4.2 Difference Expansion Scheme

Tian presented a promising high capacity reversible data embedding algorithm in [15]. In the algorithm, two techniques are employed, i.e., difference expansion and generalized least significant bit embedding, to achieve a very high embedding capacity, while keep the distortion low. The main idea of this technique is described below. For a pair of pixel values x and y , the algorithm first computes the integer average l

and difference h of x and y, where $h = x - y$. Then h is shifted to the left-hand size by one bit and the to-be-embedded bit b is appended into the LSB. This is equivalent to $h' = 2 \times h + b$, where h' denotes the expanded difference, which explains the term of Difference Expansion. Finally the new x and y, denoted by x' and y', respectively, are calculated based on the new difference values h' and the original integer average value l. In this way, the stego-image is obtained. To avoid over/underflow, the algorithm only embeds data into the pixel pairs that shall not lead to over/underflow. Therefore, a two-dimensional binary bookkeeping image is losslessly compressed and embedded as overhead.

Note that the above-mentioned relationship between the pair of integers x and y versus the pair of integers l and h is implemented in the following manner.

$$l = \lfloor 0.5 \times (x + y) \rfloor \qquad x = l + \lfloor 0.5 \times (h + 1) \rfloor$$
$$h = x - y \qquad y = l - \lfloor 0.5 \times h \rfloor \tag{1}$$

where the floor operation is utilized. According to integer Haar transform, it is reversible between these two integer pairs. Apparently, the reversible transformation between integers avoids round-off error. This together with the bookkeeping data mentioned above guaranteed reversibility.

It has been reported in [15] that the embedding capacity achieved by the difference expansion method is much higher than that achieved by [10]. This does not come with surprise since intuitively each pair of pixels can possibly embed one bit, while only each block of pixels can possibly embed one bit.

4.3 Integer Wavelet Transform Based Schemes

Xuan et al. proposed three high capacity reversible data hiding algorithms based on integer wavelet transform (IWT) [11, 16, 18]. These three algorithms have three features in common. The first is that they are all implemented in the IWT domain. Consideration is as follows. IWT as a WT is known to be able to decorrelate signal well in the transformation domain. Its feature consists with that of our human vision system (HVS). WT can be implemented efficiently by using lifting scheme. IWT can further ensure the reversible forward wavelet transform and inverse wavelet transform. For these reasons, IWT have been used in JPEG2000 for lossless compression. It is shown in Xuan et al.'s algorithms that IWT plays an important role in reversible data hiding. The second feature is that these algorithms all contain a preprocessing stage, histogram modification, in order to prevent overflow and underflow. That is, an efficient scheme has been developed to shrink the histogram towards the center, leaving two ends empty. Consequently, the perturbation caused by modification of selected IWT coefficients will not cause overflow and underflow. For reversibility, the histogram modification parameters need to be embedded as overhead. Because of the efficiency of the modification scheme [12], the overhead is not heavy. The third feature is that all of three algorithms embed data in IWT coefficients of high frequency subbands. This is because the modification of coefficients in these subbands will be imperceptible if the magnitude of the modification is not large.

The first algorithm [11, 12] losslessly compresses some selected middle bit-planes of IWT coefficients in high frequency subbands to create space to hide data. Since the bias between binary 1 and 0 in the bit-planes of IWT high frequency coefficients becomes much larger than that in the spatial domain, this method achieves rather higher embedding capacity than [7], that is the counterpart of this algorithm in spatial domain.

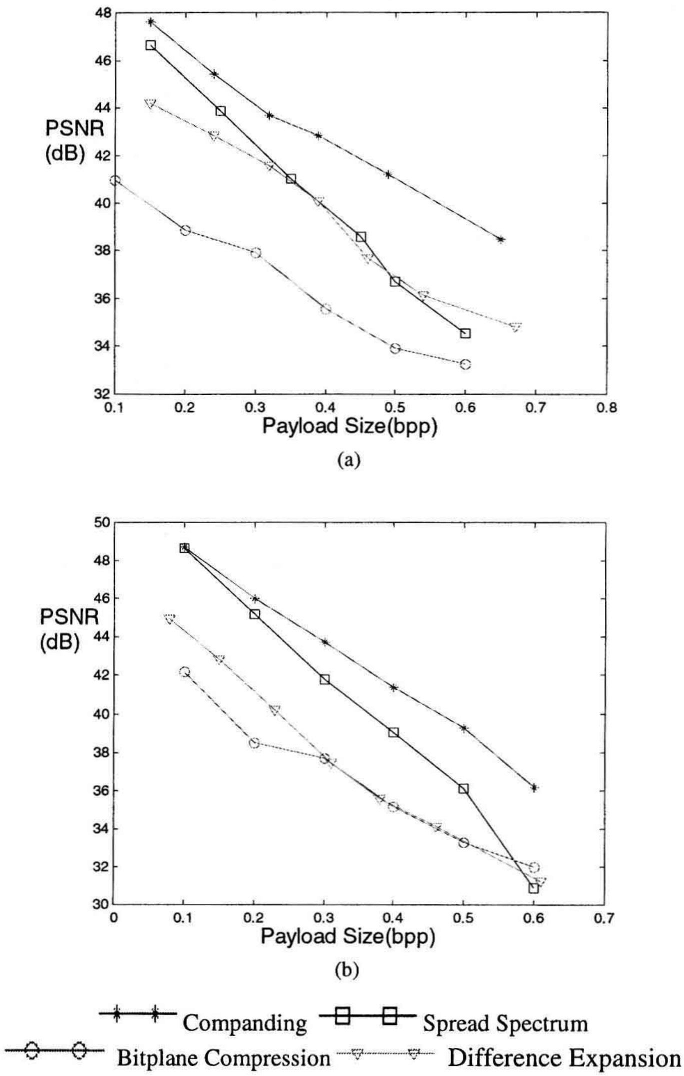

Fig. 1. Comparison results on Lena (left) and Barbara (right) images