Yun Qing Shi
Byeungwoo Jeon (Eds.)

LNCS 4283

Digital Watermarking

5th International Workshop, IWDW 2006
Jeju Island, Korea, November 2006
Proceedings

Springer

Yun Qing Shi Byeungwoo Jeon (Eds.)

Digital Watermarking

5th International Workshop, IWDW 2006
Jeju Island, Korea, November 8-10, 2006
Proceedings

Springer

Volume Editors

Yun Qing Shi
New Jersey Institute of Technology
Newark, New Jersey, USA
E-mail: shi@njit.edu

Byeungwoo Jeon
Sung Kyun Kwan University
300 Chunchun-dong
Jangan-gu, Suwon, Korea
E-mail: bjeon@yurim.skku.ac.kr

Library of Congress Control Number: 2006935426

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 3-540-48825-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-48825-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11922841 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4283

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

Welcome to the proceedings of the Fifth International Workshop on Digital Watermarking (IWDW). Since the first IWDW held in Seoul, Korea in 2002, it has been a focal point for meeting in person and disseminating valuable scientific and technological developments in watermarking. IWDW 2006 was held on Jeju, the dream island in Korea. The main theme of the workshop was "*Meet the Challenges in this Digital World!*" As we all know, digital watermarking and its related technologies have emerged as the key ingredients of this digital world. We report on new developments and discuss how to best utilize the watermarking and its related new technologies to cope with many challenging issues in this digital world.

This year, we accepted 34 papers out of 76 highly qualified submissions from 14 different countries. Each paper was reviewed by three reviewers. The acceptance ratio of 44% indicates IWDW's continuing commitment to ensuring the quality of the workshop. In addition, we had three invited lectures and one panel discussion that shed invaluable insights to the watermarking community on new developments and future directions. The technical program featured such topics as steganography and steganalysis, data forensics, digital right management, secure watermarking, and their applications. The 34 accepted papers, three invited lectures, and the panel discussion covered both theoretical and practical issues that all of us can benefit from. Furthermore, 13 of the 34 papers were arranged in a poster session in order to facilitate more efficient and interactive information exchange.

Our deep appreciation goes to all of the authors who submitted papers to IWDW 2006, the invited lecturers, the panelists and the participants, who all contributed to IWDW 2006. We are grateful to the members of the Technical Program Committee and all the invited reviewers, since IWDW 2006 would not have been successful without their efforts and time — they finished their high-quality evaluation of the submitted papers in a professional and timely fashion. In addition, we are grateful to the kind sponsors of IWDW 2006, including Digital Times, Electronics and Telecommunications Research Institute (ETRI), Korea Advanced Institute of Science and Technology (KAIST), Korea University, and Sung Kyun Kwan University in Korea. Our appreciation goes to the General Chair, JooSeok Song, President of Korea Institute of Information Security and Cryptology, for his leadership, and to the Organizing Committee led by Jeho Nam for its excellent job in financing, publicity, publication, and registration. Last but not the least, our thanks go to Victoria Kim for her professional perfectionism in managing and assisting us as the Conference Secretary.

September 2006

Yun-Qing Shi
Byeungwoo Jeon

Organization

Committee List

Technical Program Committee

Mauro Barni (University of Siena, Italy)

Jeffrey Bloom (Thomson Corporate Research, USA)

Jana Dittmann (Otto-von-Guericke-University of Magdeburg, Germany)

Jean-Luc Dugelay (Institut EURECOM, France)

Teddy Furon (INRIA, France)

Miroslav Goljan (State University of New York, USA)

Jiwu Huang (Sun Yat-Sen University, China)

Mohan Kankanhalli (National University of Singapore, Singapore)

Stefan Katzenbeisser (Philips Research, Netherlands)

Hyoung-Joong Kim (Korea University, Korea)

C.-C. Jay Kuo (University of Southern California, USA)

Inald Lagendijk (Delft University of Technology, Netherlands)

Heung-Kyu Lee (Korea Advanced Institute of Science and Technology, Korea)

Zheming Lu (Harbin Institute of Technology, China)

Benoit Macq (Université Catholique de Louvain, Belgium)

Nasir Memon (Polytechnic University, USA)

M. Kivanc Mihcak (Bogazici University, Turkey)

Matt Miller (NEC, USA)

Hideki Noda (Kyushu Institute of Technology, Japan)

Jeng-Shyang Pan (National Kaohsiung University of Applied Sciences, Taiwan)

Fernando Perez-Gonzalez (University of Vigo, Spain)

Raphael C.-W. Phan (Swinburne University of Technology, Malaysia)

Ioannis Pitas (University of Thessaloniki, Greece)

Alessandro Piva (University of Florence, Italy)

Yong-Man Ro (Information and Communication University, Korea)

Ahmad-Reza Sadeghi (Ruhr University Bochum, Germany)

Kouichi Sakurai (Kyushu University, Japan)

Qibin Sun (Institute for Infocomm Research, Singapore)

Sviatoslav Voloshynovskiy (CUI-University of Geneva, Switzerland)

Chee Sun Won (Dongguk University, Korea)

Min Wu (University of Maryland, USA)

Additional Reviewer List

Roberto Caldelli (Swinburne University of Technology, Malaysia)

Chunhua Chen (New Jersey Institute of Technology, USA)

Wen Chen (New Jersey Institute of Technology, USA)

Dongdong Fu (New Jersey Institute of Technology, USA)

Hongmei Gou (University of Maryland, USA)

Anthony TS Ho (University of Surrey, UK)

Keiichi Iwamura (Science Univ. of Tokyo, Japan)

Xiangui Kang (Sun Yat-Sen University, China)

Oleksiy Koval (CUI-University of Geneva, Switzerland)

Minoru Kuribayashi (Swinburne University of Technology, Malaysia)

Hongmei Liu (Sun Yat-Sen University, China)

Yinian Mao (University of Maryland, USA)

Zhicheng Ni (World Gate Communications, USA)

Maria Paula Queluz (Swinburne University of Technology, Malaysia)

Shunquan Tan (Sun Yat-Sen University, China)

Francesca Uccheddu (Swinburne University of Technology, Malaysia)

Yoshifumi Ueshige (Institute of Systems and Information Technology/KYUSHU, Japan)

Avinash Varna (University of Maryland, USA)

Guorong Xuan (Tongji University, China)

Dekun Zou (Thomson Corporate Research, USA)

Lecture Notes in Computer Science

For information about Vols. 1–4199

please contact your bookseller or Springer

Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part II. XXXII, 906 pages. 2006.

Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part I. XXXI, 916 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), Theoretical Aspects of Computing - ICTAC. XV, 371 pages. 2006.

Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II. XLV, 1004 pages. 2006.

Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems: OTM 2006 Workshops, Part I. XLV, 1009 pages. 2006.

Vol. 4276: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II. XXXII, 752 pages. 2006.

Vol. 4275: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I. XXXI, 1115 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4271: F.V. Fomin (Ed.), Graph-Theoretic Concepts in Computer Science. XIII, 358 pages. 2006.

Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), Interactive Technologies and Sociotechnical Systems. XVI, 547 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4265: N. Lavrač, L. Todorovski, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006. (Sublibrary LNAI).

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006. (Sublibrary LNAI).

Vol. 4263: A. Levi, E. Savas, H. Yenigün, S. Balcisoy, Y. Saygin (Eds.), Computer and Information Sciences – ISCIS 2006. XXIII, 1084 pages. 2006.

Vol. 4261: Y. Zhuang, S.-Q. Yang, Y. Rui, Q. He (Eds.), Advance in Multimedia Information Processing - PCM 2006. XXII, 1040 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006. (Sublibrary LNAI).

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), Web Information Systems – WISE 2006 Workshops. XIV, 320 pages. 2006.

Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), Web Information Systems – WISE 2006. XIV, 563 pages. 2006.

Vol. 4254: T. Grust, H. Höpfner, A. Illarramendi, S. Jablonski, M. Mesiti, S. Müller, P.-L. Patranjan, K.-U. Sattler, M. Spiliopoulou (Eds.), Current Trends in Database Technology – EDBT 2006. XXXI, 932 pages. 2006.

Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. XXXII, 1301 pages. 2006. (Sublibrary LNAI).

Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. XXXIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXVI, 1297 pages. 2006. (Sublibrary LNAI).

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Engineering Knowledge in the Age of the Semantic Web. XIV, 400 pages. 2006. (Sublibrary LNAI).

Vol. 4247: T.-D. Wang, X. Li, S.-H. Chen, X. Wang, H. Abbass, H. Iba, G. Chen, X. Yao (Eds.), Simulated Evolution and Learning. XXI, 940 pages. 2006.

Vol. 4246: M. Hermann, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIII, 588 pages. 2006. (Sublibrary LNAI).

Vol. 4245: A. Kuba, L.G. Nyúl, K. Palágyi (Eds.), Discrete Geometry for Computer Imagery. XIII, 688 pages. 2006.

Vol. 4244: S. Spaccapietra (Ed.), Journal on Data Semantics VII. XI, 267 pages. 2006.

Vol. 4243: T. Yakhno, E.J. Neuhold (Eds.), Advances in Information Systems. XIII, 420 pages. 2006.

Vol. 4241: R.R. Beichel, M. Sonka (Eds.), Computer Vision Approaches to Medical Image Analysis. XI, 262 pages. 2006.

Vol. 4239: H.Y. Youn, M. Kim, H. Morikawa (Eds.), Ubiquitous Computing Systems. XVI, 548 pages. 2006.

Vol. 4238: Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services. XVIII, 605 pages. 2006.

Vol. 4237: H. Leitold, E. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4234: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part III. XXII, 1227 pages. 2006.

Vol. 4233: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part II. XXII, 1203 pages. 2006.

Vol. 4232: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part I. XLVI, 1153 pages. 2006.

Vol. 4231: J. F. Roddick, R. Benjamins, S. Si-Saïd Cherfi, R. Chiang, C. Claramunt, R. Elmasri, F. Grandi, H. Han, M. Hepp, M. Hepp, M. Lytras, V.B. Mišić, G. Poels, I.-Y. Song, J. Trujillo, C. Vangenot (Eds.), Advances in Conceptual Modeling - Theory and Practice. XXII, 456 pages. 2006.

Vol. 4229: E. Najm, J.F. Pradat-Peyre, V.V. Donzeau-Gouge (Eds.), Formal Techniques for Networked and Distributed Systems - FORTE 2006. X, 486 pages. 2006.

Vol. 4228: D.E. Lightfoot, C.A. Szyperski (Eds.), Modular Programming Languages. X, 415 pages. 2006.

Vol. 4227: W. Nejdl, K. Tochtermann (Eds.), Innovative Approaches for Learning and Knowledge Sharing. XVII, 721 pages. 2006.

Vol. 4226: R.T. Mittermeir (Ed.), Informatics Education – The Bridge between Using and Understanding Computers. XVII, 319 pages. 2006.

Vol. 4225: J.F. Martínez-Trinidad, J.A. Carrasco Ochoa, J. Kittler (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XIX, 995 pages. 2006.

Vol. 4224: E. Corchado, H. Yin, V. Botti, C. Fyfe (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2006. XXVII, 1447 pages. 2006.

Vol. 4223: L. Wang, L. Jiao, G. Shi, X. Li, J. Liu (Eds.), Fuzzy Systems and Knowledge Discovery. XXVIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4222: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part II. XLII, 998 pages. 2006.

Vol. 4221: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part I. XLI, 992 pages. 2006.

Vol. 4219: D. Zamboni, C. Kruegel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4218: S. Graf, W. Zhang (Eds.), Automated Technology for Verification and Analysis. XIV, 540 pages. 2006.

Vol. 4217: P. Cuenca, L. Orozco-Barbosa (Eds.), Personal Wireless Communications. XV, 532 pages. 2006.

Vol. 4216: M.R. Berthold, R. Glen, I. Fischer (Eds.), Computational Life Sciences II. XIII, 269 pages. 2006. (Sublibrary LNBI).

Vol. 4215: D.W. Embley, A. Olivé, S. Ram (Eds.), Conceptual Modeling - ER 2006. XVI, 590 pages. 2006.

Vol. 4213: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Knowledge Discovery in Databases: PKDD 2006. XXII, 660 pages. 2006. (Sublibrary LNAI).

Vol. 4212: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Machine Learning: ECML 2006. XXIII, 851 pages. 2006. (Sublibrary LNAI).

Vol. 4211: P. Vogt, Y. Sugita, E. Tuci, C. Nehaniv (Eds.), Symbol Grounding and Beyond. VIII, 237 pages. 2006. (Sublibrary LNAI).

Vol. 4210: C. Priami (Ed.), Computational Methods in Systems Biology. X, 323 pages. 2006. (Sublibrary LNBI).

Vol. 4209: F. Crestani, P. Ferragina, M. Sanderson (Eds.), String Processing and Information Retrieval. XIV, 367 pages. 2006.

Vol. 4208: M. Gerndt, D. Kranzlmüller (Eds.), High Performance Computing and Communications. XXII, 938 pages. 2006.

Vol. 4207: Z. Ésik (Ed.), Computer Science Logic. XII, 627 pages. 2006.

Vol. 4206: P. Dourish, A. Friday (Eds.), UbiComp 2006: Ubiquitous Computing. XIX, 526 pages. 2006.

Vol. 4205: G. Bourque, N. El-Mabrouk (Eds.), Comparative Genomics. X, 231 pages. 2006. (Sublibrary LNBI).

Vol. 4204: F. Benhamou (Ed.), Principles and Practice of Constraint Programming - CP 2006. XVIII, 774 pages. 2006.

Vol. 4203: F. Esposito, Z.W. Raś, D. Malerba, G. Semeraro (Eds.), Foundations of Intelligent Systems. XVIII, 767 pages. 2006. (Sublibrary LNAI).

Vol. 4202: E. Asarin, P. Bouyer (Eds.), Formal Modeling and Analysis of Timed Systems. XI, 369 pages. 2006.

Vol. 4201: Y. Sakakibara, S. Kobayashi, K. Sato, T. Nishino, E. Tomita (Eds.), Grammatical Inference: Algorithms and Applications. XII, 359 pages. 2006. (Sublibrary LNAI).

Vol. 4200: I.F.C. Smith (Ed.), Intelligent Computing in Engineering and Architecture. XIII, 692 pages. 2006. (Sublibrary LNAI).

Table of Contents

Watermarking Is Not Cryptography

Ingemar J. Cox[1], Gwenaël Doërr[1], and Teddy Furon[2]

[1] University College London
Adastral Park, Ross Building 2
Martlesham IP5 3RE, United Kingdom
{i.cox, g.doerr}@adastral.ucl.ac.uk
http://www.adastral.ucl.ac.uk
[2] INRIA / TEMICS
Campus Universitaire de Beaulieu
35042 Rennes Cedex, France
teddy.furon@irisa.fr
http://www.irisa.fr

Abstract. A number of analogies to cryptographic concepts have been made about watermarking. In this paper, we argue that these analogies are misleading or incorrect, and highlight several analogies to support our argument. We believe that the fundamental role of watermarking is the reliable embedding and detection of information and should therefore be considered a form of communications. We note that the fields of communications and cryptography are quite distinct and while communications *systems* often combine technologies from the two fields, a layered architecture is applied that requires no knowledge of the layers above. We discuss how this layered approach can be applied to watermarking applications.

1 Introduction

Digital watermarking has received considerable attention as a complement to cryptography for the protection of digital content such as music, video and images. Cryptography provides a means for secure delivery of content to the consumer. Legitimate consumers are explicitly or implicitly provided with a key to decrypt the content in order to view or listen to it. Unfortunately, not all legitimate consumers are trustworthy and an untrustworthy consumer may alter or copy the decrypted content in a manner that is not permitted by the content owner. However, cryptography provides no protection once the content is decrypted, which is required for human perception. Watermarking complements cryptography by embedding a message within the content. If properly designed, the message remains in the content after decryption and, more importantly, after digital-to-analog and analog-to-digital conversion. By so doing, watermarking can be used to close the 'analog hole'[1].

[1] Not only must the digital content be decrypted, but it must also be converted to an analog signal in order for a person to see or hear it. This gives rise to the 'analog hole', which refers to the fact that all digital protection is lost at the point of perception. And this analog signal may be re-digitized by an untrustworthy consumer in order to obtain an unprotected digital copy of the content.

Y.Q. Shi and B. Jeon (Eds.): IWDW 2006, LNCS 4283, pp. 1–15, 2006.

Since the primary motivation for watermarking has been for security, numerous analogies have been made between watermarking and cryptography. In this paper, we argue that many of these analogies are for the moment misleading or incorrect. We argue that watermarking should only be viewed as a means for reliably embedding and decoding information hidden in a cover Work. As such, it is a communication system, often modeled as spread spectrum communications or communications with side information. A system incorporating watermarking may also use cryptography but we argue that, up to now, a layered model has been much more successful than intermingling the two concepts.

To support our argument, we first provide a brief introduction to key concepts in communications (Section 2) and cryptography (Section 3). We then discuss the security requirements associated with watermarking. Section 4 highlights a number of cryptographic analogies used within the watermarking community and discusses the weaknesses of these analogies. A contrario, Section 5 shows that the layered model offers much safer designs with the examples of watermarking-based content authentication and watermarking-based traitor tracing. The last section extends this discussion to signal processing other than watermarking.

2 Communications

Communications is concerned with *reliable* transmission of a message from Alice to Bob over an *unreliable* channel. A channel is considered unreliable if there is a finite probability that an error will occur between the points of transmission and reception, e.g. Alice sends a '0'-bit, but Bob decodes a '1'-bit. Reliable communications is concerned with bandwidth, power or signal-to-noise ratio (SNR), channel coding and bit error rate (BER).

It was, of course, Shannon [1] who showed that the maximum rate of error free transmission, i.e. the channel capacity (in bits per second), is given by:

$$C = 2B \log_2 \left(1 + \frac{s}{n}\right) \tag{1}$$

where B denotes bandwidth in hertz, and s and n the signal and white Gaussian noise powers respectively. In order to approach this limit, it is necessary to encode the message m, prior to transmission. This channel code provides a level of redundancy that is measured by the code rate, R. For example, if every k-bits of the message are represented by an n-bit code, then the rate is $R = k/n$, where $n > k$. Finally the BER is a direct measure of the error rate achieved by a particular code and is usually plotted as a function of the SNR.

The sources of bit errors are many. The most common error model is Gaussian noise, but there are many other error sources. However, all such sources are usually considered to be naturally occurring and not due to the effects of an adversary. In fact, it is very rare for a civilian communications system to consider a hostile channel. However, military communications must do so. In a hostile military environment, the two primary concerns are (i) jamming and (ii) detection. Jamming refers to attempts by an active adversary to prevent Bob receiving a signal. Detection refers to an adversary's efforts to detect (and localize)

enemy communications. If this is successfully achieved then military firepower may be used to destroy the communications. Note that at this level, the concern is with the delivery of bits, not with the security of the bits (which is discussed in the next section). Secure communication is irrelevant if Bob never receives the communications!

Spread spectrum (SS) communications was originally developed to protect military communications from detection and jamming [2], although it is now widely used in many civilian applications, e.g. mobile phones. The basic principle behind SS communications is that each message bit is multiplied by a (pseudo random) chip sequence that spreads the message bit over a much broader spectrum. For example, consider an implementation of SS communications based on frequency hopping. Here, the original message bit is transmitted as n lower power bits (the chip sequence), each of which is transmitted over a separate frequency band that is pseudo-randomly chosen. The receiver is synchronized with the transmitter and also has knowledge of the pseudo-random sequence of frequency bands being used. Thus, Bob is able to sum the lower energy in each of the individual bands to produce a good signal-to-noise ratio (SNR) at the receiver.

However, an adversary has much greater difficulty detecting the transmission, since Eve does not know the pseudo-random frequency hopping sequence. If Eve monitors just one frequency band, she cannot be confident that there is any communication, since the signal transmitted is very weak and only persists for a short time. Furthermore, Eve cannot jam the channel as a precaution against possible communications. This is because the power needed to confidently jam all the frequency channels would be impractically large.

Another communications model that has received recent interest is known as communications with side information. Here the channel has two noise sources, both of which are unknown to the receiver, but the first of which is entirely known to the transmitter. Under these circumstances, which arise in mobile telephony and digital watermarking, how much information can Alice reliably transmit to Bob? Costa [3] proved that the channel capacity is the same as if the first noise source is absent.

3 Cryptography

Cryptography is concerned with the *secure* transmission of a message from a sender, Alice, to a recipient, Bob, over an insecure channel. A channel is considered insecure if the bits sent by Alice may be read or altered by an adversary, Eve, prior to receipt by Bob. It is important to realize that an insecure channel is not an unreliable channel. In fact, cryptography often assumes reliable communications, i.e. Bob receives exactly the same bits sent by either Alice or Eve - there are no unintentional errors.

A secure transmission is concerned with (i) privacy, (ii) integrity and (iii) authentication. Privacy is concerned with ensuring that an adversary, Eve, can learn nothing about the message intended for Bob, by examining the encrypted

bits sent by Alice. Integrity is concerned with ensuring that Bob can be confident that the message has not been altered by Eve prior to receipt. And authentication is concerned with guaranteeing that the sender of the message is actually Alice and not an impostor.

To ensure privacy, cryptography assumes the existence of an encryption function , E(.), which takes a message, m, and a key, K, and outputs an encrypted message, c, i.e. $c = \mathrm{E}(m, K)$. It further assumes a decryption function, D(.) that takes an encrypted message, c and a key, K, and outputs a cleartext message, m, i.e. $m = \mathrm{D}(c, K) = \mathrm{D}(\mathrm{E}(m, K), K)$.

Shannon [4] defined perfect security as an encryption function in which an adversary, Eve, learns nothing about the message, m, by inspection of the ciphertext, c. Perfect security can be realized using a one-time pad. Unfortunately, a one-time pad is not practical in most situations. Consequently, modern cryptography is therefore concerned with the design of cryptographic algorithms which approximate perfect security while re-using a shared key, K. It is assumed that the encryption and decryption algorithms are known to all parties, including the adversary, Eve. This is known as Kerckhoffs' Principle [5] and reduces Eve's cryptanalysis problem to inferring the key, K.

If the length of the binary key is n-bits, the total number of keys is 2^n and is called the keyspace. For sufficiently large n, the keyspace is enormous and exhaustive enumeration or brute force search is infeasible. Note that cryptography assumes that Eve learns nothing about the true key, K, by trying a key, K', that is close to K in the sense of say Hamming distance. In other words, if Alice encodes a message twice, once using key, K and once using a key, K', that differs by only one bit from K, then the two encrypted ciphertexts will be completely different with no correlation between them. In reality, modern cryptographic algorithms only approximate these assumptions.

Cryptographic systems in which the encryption and decryption algorithm share the same key are known as symmetric key or private key systems. One problem with such is how to initiate the system, i.e. how do Alice and Bob agree on a key without sharing this knowledge with Eve? Public key or asymmetric key cryptography solves this problem by assigning two keys to each individual: a public one (PK) that is published on a database and a secret one (SK) which is never disclosed. Everybody knows the public key of everybody. The main feature of public key watermarking lies in the asymmetry of the keys used during encryption and decryption, namely $m = \mathrm{D}(\mathrm{E}(m, PK), SK)$. For instance, Alice can encrypt the message she wishes to transmit with Bob's public key (PK_B). The resulting ciphertext $c = \mathrm{E}(m, PK_B)$ can then only be decrypted with Bob's secret key (SK_B) i.e. by Bob himself. In other words, the message m has been sent securely without agreeing on a secret key beforehand[2].

Integrity is guaranteed through the use of another cryptographic primitive known as a one-way hash function. This is a function that takes an arbitrarily

[2] However, for practical reasons, public key cryptography is usually used to exchange a key at the beginning of a transmission. The subsequent messages are then encrypted/decrypted with a private key crypto-system using the agreed session key.