Mauro Barni
Jordi Herrera-Joancomartí
Stefan Katzenbeisser
Fernando Pérez-González (Eds.)

LNCS 3727

Information Hiding

7th International Workshop, IH 2005
Barcelona, Spain, June 2005
Revised Selected Papers

Springer

Mauro Barni Jordi Herrera-Joancomartí
Stefan Katzenbeisser
Fernando Pérez-González (Eds.)

Information Hiding

7th International Workshop, IH 2005
Barcelona, Spain, June 6-8, 2005
Revised Selected Papers

Springer

Volume Editors

Mauro Barni
Università di Siena
Dipartimento di Ingegneria dell'Informazione
Siena, Italy
E-mail: barni@dii.unisi.it

Jordi Herrera-Joancomartí
Universitat Oberta de Catalunya
Estudis d'Informàtica i Multimèdia
Barcelona, Spain
E-mail: jherreraj@uoc.edu

Stefan Katzenbeisser
Technische Universität München
Institut für Informatik
München, Germany
E-mail: katzenbe@in.tum.de

Fernando Pérez-González
Universidad de Vigo
Signal Processing in Communications Group
Vigo, Spain
E-mail: fperez@tsc.uvigo.es

Library of Congress Control Number: 2005936733

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, H.3, H.5.1

ISSN 0302-9743
ISBN-10 3-540-29039-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-29039-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11558859 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3727

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

Editorial Board

Preface

It is our pleasure to present in this volume the proceedings of the 7th International Workshop on Information Hiding (IH 2005), held in Barcelona, Catalonia, Spain, during June 6–8, 2005. The workshop was organized by the Department of Computer Science and Multimedia, Universitat Oberta de Catalunya (UOC).

Continuing the tradition of previous workshops, we sought a balanced program, containing talks on various aspects of data hiding, anonymous communication, steganalysis, and watermarking. Although the protection of digital intellectual property has up to now motivated most of our research, there are many other upcoming fields of application. We were delighted to see that this year's workshop presented numerous new and unconventional approaches to information hiding.

The selection of the program was a very challenging task. In total, we received 90 submissions from 21 countries. At this point we want to thank all authors who submitted their latest work to IH 2005—and thus assured that the Information Hiding Workshop continues to be the top forum of our community. Each submission was refereed by three reviewers. Due to the space limitations of a single-track workshop, we could only accept 28 papers, keeping the high quality of previous workshops. We would like to thank all members of the Program Committee and all external reviewers for the enormous efforts they put into the review process. In addition to the regular presentations, an invited lecture entitled "On Joint Coding for Watermarking and Encryption" was given by Neri Merhav. Furthermore, to open the floor to additional ideas, we arranged a rump session.

Finally, we want to thank the Organizing Committee for handling all local organizational issues and the European Office of Aerospace Research and Development for their financial support.

We hope that you will enjoy reading these proceedings and that they will inspire your own research in the area of information hiding.

July 2005

Mauro Barni
Jordi Herrera Joancomartí
Stefan Katzenbeisser
Fernando Pérez-González

7th International Workshop on Information Hiding

June 6–8, 2005, Barcelona (Spain)

General Chairs

Jordi Herrera-Joancomartí, Universitat Oberta de Catalunya, Spain
Fernando Pérez-González, University of Vigo, Spain

Program Chairs

Mauro Barni, Università di Siena, Italy
Stefan Katzenbeisser, Technische Universität München, Germany

Program Committee

Ross J. Anderson, University of Cambridge, UK
Mauro Barni, Università di Siena, Italy
Jan Camenisch, IBM Zurich Research Laboratory, Switzerland
Christian Collberg, University of Arizona, USA
Ingemar J. Cox, University College London, UK
Jessica Fridrich, SUNY Binghamton, USA
Jordi Herrera-Joancomartí, Universitat Oberta de Catalunya, Spain
John McHugh, SEI/CERT, USA
Ira Moskowitz, Naval Research Laboratory, USA
Stefan Katzenbeisser, Technische Universität München, Germany
Darko Kirovski, Microsoft Research, USA
Richard C. Owens, University of Toronto, Canada
Fernando Pérez-González, University of Vigo, Spain
Andreas Pfitzmann, Dresden University of Technology, Germany
Michiel van der Veen, Philips Research, Netherlands

Local Organization

Joan Arnedo, Universitat Oberta de Catalunya, Spain
David Megías, Universitat Oberta de Catalunya, Spain
Julià Minguillón, Universitat Oberta de Catalunya, Spain
Emma Pedrol, Universitat Oberta de Catalunya, Spain
Jordi Serra, Universitat Oberta de Catalunya, Spain
Michael Tautschnig, Technische Universität München, Germany

External Reviewers

Michael A. Colón
Andre Adelsbach
Farid Ahmed
Felix Balado
Richard Bergmair
Mike Bergmann
Rainer Böhme
Roberto Caldelli
Mehmet Celik
R. Chandramouli
Sebastian Clauss
Pedro Comesaña Alfaro
Scott Craver
George Danezis
Alessia De Rosa
Josep Domingo-Ferrer
Sorina Dumitrescu
Hany Farid
Elke Franz
Shan He
Peter Hon Wah Wong
Mark Horgan
Neil Hurley
Myong Kang
Andrew Ker
Dogan Kesdogan
Farinaz Koushanfar
Thomas Kriegelstein
Ginger M. Myles
John McDermott
Catherine Meadows
David Megías
Nasir Memon
Juliá Minguillón
Steven Murdoch
Aweke N. Lemma
Jasvir Nagra
Richard Newman
Luis Perez-Freire
Alessandro Piva
Miodrag Potkonjak
Gang Qu
Majid Rabbani
Victor Raskin
Ahmad-Reza Sadeghi
Phil Sallee
Elisa Sayrol
Dagmar Schönfeld
G.C.M. Silvestre
Sandra Steinbrecher
Kenneth Sullivan
Ashwin Swaminathan
Paul Syverson
Cuneyt Taskiran
Clark Thomborson
Roman Tzschoppe
José Emilio Vila-Forcén
Renato Villán
Changjie Wang
Ying Wang
Brent Waters
Andreas Westfeld
Kevin Whelan
Jennifer Wong
Min Wu
Li Wu Chang
Yacov Yacobi
Hong Zhao

Lecture Notes in Computer Science

For information about Vols. 1–3712

please contact your bookseller or Springer

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Subseries LNAI).

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Subseries LNAI).

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Subseries LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005.

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3796: N.P. Smart (Ed.), Cryptography and Coding. XI, 461 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Subseries LNAI).

Vol. 3788: B. Roy (Ed.), Advances in Cryptology - ASIACRYPT 2005. XIV, 703 pages. 2005.

Vol. 3785: K.-K. Lau, R. Banach (Eds.), Formal Methods and Software Engineering. XIV, 496 pages. 2005.

Vol. 3784: J. Tao, T. Tan, R.W. Picard (Eds.), Affective Computing and Intelligent Interaction. XIX, 1008 pages. 2005.

Vol. 3781: S.Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, D. Zhang (Eds.), Advances in Biometric Person Authentication. XI, 250 pages. 2005.

Vol. 3780: K. Yi (Ed.), Programming Languages and Systems. XI, 435 pages. 2005.

Vol. 3779: H. Jin, D. Reed, W. Jiang (Eds.), Network and Parallel Computing. XV, 513 pages. 2005.

Vol. 3777: O.B. Lupanov, O.M. Kasim-Zade, A.V. Chaskin, K. Steinhöfel (Eds.), Stochastic Algorithms: Foundations and Applications. VIII, 239 pages. 2005.

Vol. 3775: J. Schönwälder, J. Serrat (Eds.), Ambient Networks. XIII, 281 pages. 2005.

Vol. 3773: A. Sanfeliu, M.L. Cortés (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XX, 1094 pages. 2005.

Vol. 3772: M. Consens, G. Navarro (Eds.), String Processing and Information Retrieval. XIV, 406 pages. 2005.

Vol. 3771: J.M.T. Romijn, G.P. Smith, J. van de Pol (Eds.), Integrated Formal Methods. XI, 407 pages. 2005.

Vol. 3770: J. Akoka, S.W. Liddle, I.-Y. Song, M. Bertolotto, I. Comyn-Wattiau, W.-J. van den Heuvel, M. Kolp, J. Trujillo, C. Kop, H.C. Mayr (Eds.), Perspectives in Conceptual Modeling. XXII, 476 pages. 2005.

Vol. 3768: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part II. XXVIII, 1088 pages. 2005.

Vol. 3767: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part I. XXVIII, 1022 pages. 2005.

Vol. 3766: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 231 pages. 2005.

Vol. 3765: Y. Liu, T. Jiang, C. Zhang (Eds.), Computer Vision for Biomedical Image Applications. X, 563 pages. 2005.

Vol. 3764: S. Tixeuil, T. Herman (Eds.), Self-Stabilizing Systems. VIII, 229 pages. 2005.

Vol. 3762: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops. XXXI, 1228 pages. 2005.

Vol. 3761: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part II. XXVII, 653 pages. 2005.

Vol. 3760: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part I. XXVII, 921 pages. 2005.

Vol. 3759: G. Chen, Y. Pan, M. Guo, J. Lu (Eds.), Parallel and Distributed Processing and Applications - ISPA 2005 Workshops. XIII, 669 pages. 2005.

Vol. 3758: Y. Pan, D.-x. Chen, M. Guo, J. Cao, J.J. Dongarra (Eds.), Parallel and Distributed Processing and Applications. XXIII, 1162 pages. 2005.

Vol. 3757: A. Rangarajan, B. Vemuri, A.L. Yuille (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 666 pages. 2005.

Vol. 3756: J. Cao, W. Nejdl, M. Xu (Eds.), Advanced Parallel Processing Technologies. XIV, 526 pages. 2005.

Vol. 3754: J. Dalmau Royo, G. Hasegawa (Eds.), Management of Multimedia Networks and Services. XII, 384 pages. 2005.

Vol. 3753: O.F. Olsen, L.M.J. Florack, A. Kuijper (Eds.), Deep Structure, Singularities, and Computer Vision. X, 259 pages. 2005.

Vol. 3752: N. Paragios, O. Faugeras, T. Chan, C. Schnörr (Eds.), Variational, Geometric, and Level Set Methods in Computer Vision. XI, 369 pages. 2005.

Vol. 3751: T. Magedanz, E.R. M. Madeira, P. Dini (Eds.), Operations and Management in IP-Based Networks. X, 213 pages. 2005.

Vol. 3750: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part II. XL, 1018 pages. 2005.

Vol. 3749: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part I. XXXIX, 942 pages. 2005.

Vol. 3748: A. Hartman, D. Kreische (Eds.), Model Driven Architecture – Foundations and Applications. IX, 349 pages. 2005.

Vol. 3747: C.A. Maziero, J.G. Silva, A.M.S. Andrade, F.M.d. Assis Silva (Eds.), Dependable Computing. XV, 267 pages. 2005.

Vol. 3746: P. Bozanis, E.N. Houstis (Eds.), Advances in Informatics. XIX, 879 pages. 2005.

Vol. 3745: J.L. Oliveira, V. Maojo, F. Martín-Sánchez, A.S. Pereira (Eds.), Biological and Medical Data Analysis. XII, 422 pages. 2005. (Subseries LNBI).

Vol. 3744: T. Magedanz, A. Karmouch, S. Pierre, I. Venieris (Eds.), Mobility Aware Technologies and Applications. XIV, 418 pages. 2005.

Vol. 3742: J. Akiyama, M. Kano, X. Tan (Eds.), Discrete and Computational Geometry. VIII, 213 pages. 2005.

Vol. 3740: T. Srikanthan, J. Xue, C.-H. Chang (Eds.), Advances in Computer Systems Architecture. XVII, 833 pages. 2005.

Vol. 3739: W. Fan, Z.-h. Wu, J. Yang (Eds.), Advances in Web-Age Information Management. XXIV, 930 pages. 2005.

Vol. 3738: V.R. Syrotiuk, E. Chávez (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XI, 360 pages. 2005.

Vol. 3735: A. Hoffmann, H. Motoda, T. Scheffer (Eds.), Discovery Science. XVI, 400 pages. 2005. (Subseries LNAI).

Vol. 3734: S. Jain, H.U. Simon, E. Tomita (Eds.), Algorithmic Learning Theory. XII, 490 pages. 2005. (Subseries LNAI).

Vol. 3733: P. Yolum, T. Güngör, F. Gürgen, C. Özturan (Eds.), Computer and Information Sciences - ISCIS 2005. XXI, 973 pages. 2005.

Vol. 3731: F. Wang (Ed.), Formal Techniques for Networked and Distributed Systems - FORTE 2005. XII, 558 pages. 2005.

Vol. 3729: Y. Gil, E. Motta, V. R. Benjamins, M.A. Musen (Eds.), The Semantic Web – ISWC 2005. XXIII, 1073 pages. 2005.

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3727: M. Barni, J. Herrera-Joancomartí, S. Katzenbeisser, F. Pérez-González (Eds.), Information Hiding. XII, 414 pages. 2005.

Vol. 3726: L.T. Yang, O.F. Rana, B. Di Martino, J.J. Dongarra (Eds.), High Performance Computing and Communications. XXVI, 1116 pages. 2005.

Vol. 3725: D. Borrione, W. Paul (Eds.), Correct Hardware Design and Verification Methods. XII, 412 pages. 2005.

Vol. 3724: P. Fraigniaud (Ed.), Distributed Computing. XIV, 520 pages. 2005.

Vol. 3723: W. Zhao, S. Gong, X. Tang (Eds.), Analysis and Modelling of Faces and Gestures. XI, 4234 pages. 2005.

Vol. 3722: D. Van Hung, M. Wirsing (Eds.), Theoretical Aspects of Computing – ICTAC 2005. XIV, 614 pages. 2005.

Vol. 3721: A.M. Jorge, L. Torgo, P.B. Brazdil, R. Camacho, J. Gama (Eds.), Knowledge Discovery in Databases: PKDD 2005. XXIII, 719 pages. 2005. (Subseries LNAI).

Vol. 3720: J. Gama, R. Camacho, P.B. Brazdil, A.M. Jorge, L. Torgo (Eds.), Machine Learning: ECML 2005. XXIII, 769 pages. 2005. (Subseries LNAI).

Vol. 3719: M. Hobbs, A.M. Goscinski, W. Zhou (Eds.), Distributed and Parallel Computing. XI, 448 pages. 2005.

Vol. 3718: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XII, 502 pages. 2005.

Vol. 3717: B. Gramlich (Ed.), Frontiers of Combining Systems. X, 321 pages. 2005. (Subseries LNAI).

Vol. 3716: L. Delcambre, C. Kop, H.C. Mayr, J. Mylopoulos, Ó. Pastor (Eds.), Conceptual Modeling – ER 2005. XVI, 498 pages. 2005.

Vol. 3715: E. Dawson, S. Vaudenay (Eds.), Progress in Cryptology – Mycrypt 2005. XI, 329 pages. 2005.

Vol. 3714: H. Obbink, K. Pohl (Eds.), Software Product Lines. XIII, 235 pages. 2005.

Vol. 3713: L.C. Briand, C. Williams (Eds.), Model Driven Engineering Languages and Systems. XV, 722 pages. 2005.

Table of Contents

Invited Talk

Anonymity

Watermarking

Theory

Watermark Attacks

Steganography

Hiding in Unusual Content

Steganalysis

Software Watermarking

Fingerprinting

On Joint Coding for Watermarking and Encryption

Neri Merhav

Department of Electrical Engineering,
Technion – Israel Institute of Technology,
Technion City, Haifa 32000, Israel
merhav@ee.technion.ac.il

Abstract. In continuation to earlier works where the problem of joint information embedding and lossless compression (of the composite signal) was studied in the absence [6] and in the presence [7] of attacks, here we consider the additional ingredient of protecting the secrecy of the watermark against an unauthorized party, which has no access to a secret key shared by the legitimate parties. In other words, we study the problem of joint coding for three objectives: information embedding, compression, and encryption. Our main result is a coding theorem that provides a single–letter characterization of the best achievable tradeoffs among the following parameters: the distortion between the composite signal and the covertext, the distortion in reconstructing the watermark by the legitimate receiver, the compressibility of the composite signal (with and without the key), and the equivocation of the watermark, as well as its reconstructed version, given the composite signal. In the attack–free case, if the key is independent of the covertext, this coding theorem gives rise to a *threefold* separation principle that tells that asymptotically, for long block codes, no optimality is lost by first applying a rate–distortion code to the watermark source, then encrypting the compressed codeword, and finally, embedding it into the covertext using the embedding scheme of [6]. In the more general case, however, this separation principle is no longer valid, as the key plays an additional role of side information used by the embedding unit.

1 Introduction

It is common to say that encryption and watermarking (or information hiding) are related but they are substantially different in the sense that in the former, the goal is to protect the secrecy of the *contents* of information, whereas in the latter, it is the very *existence* of this information that is to be kept secret. In the last few years, however, we are witnessing increasing efforts around the *combination* of encryption and watermarking (WM), which is motivated by the desire to further enhance the security of sensitive information that is being hidden in the host signal. This is to guarantee that even if the watermark is somehow detected by a hostile party, its contents still remain secure due to the encryption. This combination of WM and encryption can be seen both in recently reported

M. Barni et al. (Eds.): IH 2005, LNCS 3727, pp. 1–10, 2005.

research work (see, e.g., [1],[2],[4],[5],[9],[11] and references therein) and in actual technologies used in commercial products with a copyright protection framework, such as the CD and the DVD.

This paper is devoted to the information–theoretic aspects of joint WM and encryption together with lossless compression of the composite signal that contains the encrypted watermark. Specifically, we extend the framework studied in [6] and [7] of joint WM and compression, so as to include encryption using a secret key. Before we describe the setting concretely, we pause then to give some more detailed background on the work reported in [6] and [7].

In [6], the following problem was studied: Given a covertext source vector $X^n = (X_1, \ldots, X_n)$, generated by a discrete memoryless source (DMS), and a message m, uniformly distributed in $\{1, 2, \ldots, 2^{nR_e}\}$, independently of X^n, with R_e designating the embedding rate, we wish to generate a composite (stegotext) vector $Y^n = (Y_1, \ldots, Y_n)$ that satisfies the following requirements: (i) Similarity to the covertext, in the sense that a distortion constraint, $Ed(X^n, Y^n) = \sum_{t=1}^{n} Ed(X_t, Y_t) \leq nD$, holds, (ii) compressibility, in the sense that the normalized entropy, $H(Y^n)/n$, does not exceed some threshold R_c, and (iii) reliability in decoding the message m from Y^n, in the sense that the decoding error probability is arbitrarily small for large n. A single–letter characterization of the best achievable tradeoffs among R_c, R_e, and D was given in [6], and was shown to be achievable by an extension of the ordinary lossy source coding theorem, giving rise to the existence of 2^{nR_e} *disjoint* rate–distortion codebooks (one per each possible watermark message) as long as R_e does not exceed a certain fundamental limit. In [7], this setup was extended to include a given memoryless attack channel, $P(Z^n|Y^n)$, where item (iii) above was redefined such that the decoding was based on Z^n rather than on Y^n. This extension required a completely different approach, which was in the spirit of the Gel'fand–Pinsker coding theorem for a channel with non–causal side information (SI) at the transmitter [3]. The role of SI, in this case, was played by the covertext.

In this paper, we extend the settings of [6] and [7] to include encryption. For the sake of clarity, we do that in several steps. First, we extend the attack–free setting of [6]: In addition to including encryption, we also extend the model of the watermark message source to be an arbitrary DMS, $U_1, U_2, \ldots$, independent of the covertext, and not necessarily a binary symmetric source (BSS) as in [6] and [7]. Specifically, we now assume that the encoder has three inputs: The covertext source vector, X^n, an independent (watermark) message source vector $U^N = (U_1, \ldots, U_N)$, where N may differ from n if the two sources operate in different rates, and a secret key (shared also with the legitimate decoder) $K^n = (K_1, \ldots, K_n)$, which, for mathematical convenience, is assumed to operate at the same rate as the covertext. It is assumed, at this stage, that K^n is independent of U^N and X^n. Now, in addition to requirements (i)-(iii), we impose a requirement on the equivocation of the message source relative to an eavesdropper that has access to Y^n, but not to K^n. Specifically, we would like the normalized conditional entropy, $H(U^N|Y^n)/N$, to exceed a prescribed threshold, h (e.g., $h = H(U)$ for perfect secrecy). Our first result is a coding theorem

that gives a set of necessary and sufficient conditions, in terms of single–letter inequalities, such that a triple (D, R_c, h) is achievable, while maintaining reliable reconstruction of U^N at the legitimate receiver.

In the second step, we relax the requirement of perfect (or almost perfect) watermark reconstruction, and assume that we are willing to tolerate a certain distortion between the watermark message U^N and its reconstructed version $\hat{U}^N$, that is, $Ed'(U^N, \hat{U}^N) = \sum_{i=1}^{N} Ed'(U_i, \hat{U}_i) \leq ND'$. For example, if d' is the Hamming distortion measure then D', of course, designates the maximum allowable bit error probability (as opposed to the block error probability requirement of [6] and [7]). Also, in this case, it makes sense, in some applications, to impose a requirement regarding the equivocation of the *reconstructed* message, $\hat{U}^N$, namely, $H(\hat{U}^N|Y^n)/N \geq h'$, for some prescribed constant h'. The rationale is that it is $\hat{U}^N$, not U^N, that is actually conveyed to the legitimate receiver. For the sake of generality, however, we will take into account both equivocation requirements, with the understanding that if one of them is superfluous, then the corresponding threshold (h or h' accordingly) can always be set to zero. Our second result then extends the above–mentioned coding theorem to a single–letter characterization of achievable quintuples (D, D', R_c, h, h'). As will be seen, this coding theorem gives rise to a threefold separation theorem, that separates, without asymptotic loss of optimality, between three stages: rate–distortion coding of U^N, encryption of the compressed bitstream, and finally, embedding the resulting encrypted version using the embedding scheme of [6]. The necessary and sufficient conditions related to the encryption are completely decoupled from those of the embedding and the stegotext compression.

In the third and last step, we drop the assumption of an attack–free system and we assume a memoryless attack channel, in analogy to [7]. As it will turn out, in this case there is an interaction between the encryption and the embedding, even if the key is still assumed independent of the covertext. In particular, it will be interesting to see that the key, in addition to its original role in encryption, serves as SI that is available to both encoder and decoder. Also, because of the dependence between the key and the composite signal, and the fact that the key is available to the legitimate decoder as well, it may make sense, at least in some applications, to let the compressibility constraint correspond to the the conditional entropy of Y^n given K^n. Again, for the sake of generality, we will consider both the conditional and the unconditional entropies of Y^n, i.e., $H(Y^n)/n \leq R_c$ and $H(Y^n|K^n)/n \leq R_c'$.

Our final result then is a coding theorem that provides a single–letter characterization of the region of achievable six–tuples $(D, D', R_c, R_c', h, h')$. Interestingly, this characterization remains essentially unaltered even if there is dependence between the key and the covertext, which is a reasonable thing to have once the key and the stegotext interact anyhow.[1] In this context, the system designer confronts an interesting dilemma regarding the desirable degree of statistical dependence between the key and the covertext, which affects the

[1] In fact, the choice of the conditional distribution $P(K^n|X^n)$ is a degree of freedom that can be optimized subject to the given randomness resources.

dependence between the key and the stegotext. On the one hand, strong dependence can reduce the entropy of Y^n given K^n (and thereby reduce R'_c), and can also help in the embedding process: For example, the extreme case of $K^n = X^n$ (which corresponds to *private* WM since the decoder actually has access to the covertext) is particularly interesting because in this case, for the encryption key, there is no need for any external resources of randomness, in addition to the randomness of the covertext that is already available. On the other hand, when there is strong dependence between K^n and Y^n, the secrecy of the watermark might be sacrificed since $H(K^n|Y^n)$ decreases as well. An interesting point, in this context, is that the Slepian–Wolf encoder [10] is used to generate, from K^n, random bits that are essentially independent of Y^n (as Y^n is generated only after the encryption).

2 Results

We begin by establishing some notation conventions. Throughout this paper, scalar random variables (RV's) will be denoted by capital letters, their sample values will be denoted by the respective lower case letters, and their alphabets will be denoted by the respective calligraphic letters. A similar convention will apply to random vectors and their sample values, which will be denoted with same symbols superscripted by the dimension. Thus, for example, A^ℓ (ℓ – positive integer) will denote a random ℓ-vector $(A_1, ..., A_\ell)$, and $a^\ell = (a_1, ..., a_\ell)$ is a specific vector value in $\mathcal{A}^\ell$, the ℓ-th Cartesian power of $\mathcal{A}$. Sources and channels will be denoted generically by the letter P, or Q, subscripted by the name of the RV and its conditioning, if applicable, e.g., $P_U(u)$ is the probability function of U at the point $U = u$, $P_{K|X}(k|x)$ is the conditional probability of $K = k$ given $X = x$, and so on. Whenever clear from the context, these subscripts will be omitted. Information theoretic quantities like entropies and mutual informations will be denoted following the usual conventions of the Information Theory literature, e.g., $H(U^N)$, $I(X^n; Y^n)$, and so on. For single–letter information quantities (i.e., when $n = 1$ or $N = 1$), subscripts will be omitted, e.g., $H(U^1) = H(U_1)$ will be denoted by $H(U)$, similarly, $I(X^1; Y^1) = I(X_1; Y_1)$ will be denoted by $I(X; Y)$, and so on.

We now turn to the formal description of the problem setting for step 1, as described in the Introduction. A source P_X, henceforth referred to as the *covertext source* generates a sequence of independent copies, $\{X_t\}_{t=-\infty}^{\infty}$, of a finite–alphabet RV, $X \in \mathcal{X}$. At the same time and independently, another source P_U, henceforth referred to as the *message source* generates a sequence of independent copies, $\{U_i\}_{i=-\infty}^{\infty}$, of a finite–alphabet RV, $U \in \mathcal{U}$. The relative rate between the message source and the covertext source is λ message symbols per covertext symbol. This means that while the covertext source generates a block of n symbols, say, $X^n = (X_1, \ldots, X_n)$, the message source generates a block of $N = \lambda n$ symbols, $U^N = (U_1, \ldots, U_N)$. In addition to the covertext source and the message source, yet another source, P_K, henceforth referred to as the *key source*, generates a sequence of independent copies, $\{K_t\}_{t=-\infty}^{\infty}$, of a finite–