Jan L. Camenisch
Christian S. Collberg
Neil F. Johnson
Phil Sallee (Eds.)

LNCS 4437

Information Hiding

8th International Workshop, IH 2006
Alexandria, VA, USA, July 2006
Revised Selected Papers

Springer

Jan L. Camenisch   Christian S. Collberg
Neil F. Johnson   Phil Sallee (Eds.)

Information Hiding

8th International Workshop, IH 2006
Alexandria, VA, USA, July 10-12, 2006
Revised Selcted Papers

Springer

Volume Editors

Jan L. Camenisch
IBM Research
CH-8803 Rüschlikon, Switzerland
E-mail: jca@zurich.ibm.com

Christian S. Collberg
The University of Arizona
Tucson, AZ 85721, USA
E-mail: collberg@cs.arizona.edu

Neil F. Johnson
Johnson & Johnson Technology Consultants
Vienna, VA 22183, USA
E-mail: nfi@jjtc.com
and
Booz Allen Hamilton
B-8042, 8283 Greensboro Drive, MCLean
VA 22102, USA
E-mail: Johnson_neil@bah.com

Phil Sallee
Booz Allen Hamilton
B-8042, 8283 Greensboro Drive, MCLean
VA 22102, USA
E-mail: sallee_phil@bah.com

Library of Congress Control Number: 2007935081

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-74123-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74123-7 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12104833 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4437

Preface

These proceedings contain the 25 papers that were accepted for presentation at the Eighth Information Hiding Conference, held July 10–12, 2006 in Old Town Alexandria, Virginia. The papers were selected by the Program Committee from more than 70 submissions on the basis of their novelty, originality, and scientific merit. We are grateful to all authors who submitted their work for consideration. The papers were divided into ten sessions [Watermarking, Information Hiding and Networking, Data Hiding in Unusual Content (2 sessions), Fundamentals, Software Protection, Steganalysis, Steganography (2 sessions), and Subliminal Channels], showing the breadth of research in the field. This year was an important one in the history of the IHW: "Workshop" was dropped from the name to show that the field has matured and that the conference has become the premier venue for the dissemination of new results.

The conference employed a double-blind reviewing process. Each paper was examined by at least three reviewers. Papers submitted by Program Committee members were held to a higher standard. We relied on the advice of outside colleagues and would like to extend our thanks for their contribution to the paper selection process and their dedication to excellence in research.

We thank our sponsors Booz Allen Hamilton and Johnson & Johnson Technology Consultants for their financial and logistic support, including local arrangements, printing the pre-proceedings, and organizing the registration. The walking tour of Old Town Alexandria organized by Ira Moskowitz and the dessert cruise on board the Miss Christin were enjoyable highlights of the social program and we thank the organizers! Roger Zimmermann helped to run the submission server and without the help of Björn Assmann you would not be holding these proceedings in your hands. Thank you guys!

Finally, we wish to thank the many researchers who have contributed to extending the state of the art for information hiding research and hope these proceedings will be helpful for future developments.

January 2007

Jan Camenisch
Christian Collberg
Neil F. Johnson
Phil Sallee

Organization

Program Committee

Ross J. Anderson (University of Cambridge, UK)
Mauro Barni (Università di Siena, Italy)
Jack Brassil (HP Laboratories, USA)
Jan Camenisch (IBM Zurich Research Laboratory, Switzerland)
Christian Collberg (University of Arizona, USA)
Ee-Chien Chang (National University of Singapore, Singapore)
Ingemar J. Cox (University College London, UK)
Jessica Fridrich (SUNY Binghamton, USA)
Neil F. Johnson (Booz Allen Hamilton and JJTC, USA)
John McHugh (SEI/CERT, USA)
Ira S. Moskowitz (Naval Research Laboratory, USA)
Stefan Katzenbeisser (Philips Research, The Netherlands)
Darko Kirovski (Microsoft Research, USA)
Richard C. Owens (University of Toronto, Canada)
Andreas Pfitzmann (Dresden University of Technology, Germany)
Phil Sallee (Booz Allen Hamilton, USA)
Michiel van der Veen (Philips Research, The Netherlands)

External Reviewers

Farid Ahmed
Richard Bergmair
Mike Bergmann
Rainer Boehme
Roberto Caldelli
Mehmet Celik
Massimiliano Corsini
Scott Craver
Alessia De Rosa
Shan He
Susan Hohenberger
Andrew Ker
Johannes Kinder
Patty Lafferty
Aweke Lemma
Keye Martin
Ginger Myles
Alessandro Piva
Mila dalla Preda
Victor Raskin
Antje Schneidewind
Franz Schneidewind
Dagmar Schönfeld
Ashwin Swaminathan
Morton Swimmer
James Troupe
Dan Wallach
Andreas Westfeld
Greg Zaverucha
Min Wu

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Krügel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

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

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

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

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

Vol. 4237: H. Leitold, E.P. 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. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y A Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

Table of Contents

Hamiltonian Mechanics

Video Watermarking by Using Geometic Warping Without Visible Artifacts

Natural Watermarking: A Secure Spread Spectrum Technique for WOA

Patrick Bas[1,2] and François Cayre[2]

[1] CIS / Helsinki University of Technology
P.O. Box 5400
FI-02015 HUT FINLAND
[2] LIS/INPG
961, rue de la Houille Blanche BP 46
F-38042 St. Martin d'Hères Cedex, France

Abstract. This paper presents a spread spectrum (SS) watermarking technique that is secure against carriers estimation in a Watermark Only Attack framework. After reviewing the sufficient conditions to design secure algorithms for watermarking and steganography, we present a setup based on Blind Source Separation (BSS) theory to assess the lack of security of classical SS techniques such as classical SS or ISS. We motivate a new SS watermarking algorithm called Natural Watermarking (NW) where the estimation of the secret carriers is impossible and which achieves perfect secrecy thanks to unchanged Gaussian distributions of the secret carriers. The theoretical evaluation of the NW security is carried out and the case of multi-bit embedding is addressed. Finally, a robust extension of NW is presented and the properties of NW and Robust-NW are both practically verified.

1 Introduction

Robustness, *capacity* and *imperceptibility* have always been considered, since the very beginning of watermarking, as the main three constraints to respect in order to build a valuable watermarking scheme. Recently the watermarking community has thrown light on the problem of *security* which appears also to be a fundamental constraint to respect in order to guaranty the usability of a watermarking technology. Several authors [1][2][3] showed that some information about the secret key may leak from several observations of watermarked pieces of content. Using this information, it may be possible to estimate the secret key, and then to destroy the security of the considered scheme by removing, copying or altering the embedded messages. Several studies address also the security of practical watermarking techniques for digital images [4][5].

In this paper, we tackle the problem of security for the well-known class of spread spectrum (SS) watermarking schemes. In this case, the secret key which practically is the seed of a random generator, corresponds to the set of secret carriers that is used to convey the information. It is important to note that an attacker does not need the seed used to initialiaze the random number generator: the secret carriers are good enough to attack the watermark. We propose a

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 1–14, 2007.

watermarking scheme that is secure (e.g. it does not offer information leakage of the secret key) for the class of Watermark Only Attacks (WOA). This class of attacks, proposed by [1], considers an attack that is based on the observation of watermarked contents, watermarked with the same key but conveying different messages. We named the proposed scheme *natural spread spectrum watermarking* because embedding is achieved without altering the natural distribution of each secret carrier before and after embedding. As shown in the paper, this characteristic enables to achieve perfect secrecy. Moreover, when embedding several bits, we show that if each carrier is embedded in the contents with an amplitude following a Gaussian distribution, it is impossible to individually estimate the carriers.

The rest of the paper is divided into five sections. First, the security of classical SS techniques for WOA are analysed as a Blind Source Separation (BSS) problem: in section 2 we show that the characterisation of the distributions of each carrier for the observed contents enables to estimate the different carriers. Section 3 presents the constraints, principles and characteristics of Natural Watermarking (NW). The embedding, decoding and distortion related to NW are presented and the link with the Scalar Costa's Scheme, another scheme preserving perfect secrecy, is outlined. An extension of NW to increase the robustness is presented in section 4, the implications in term of security are also mentioned. Section 5 presents a comparison between the estimations of the secret carriers for different SS watermarking schemes including NW. We show that for NW it is impossible to estimate the carriers. For Robust-NW only the estimation of the watermark subspace is possible. Finally section 6 concludes this paper and presents open research lines for future works.

2 Assessing the Security of Spread-Spectrum Techniques Using BSS Techniques

2.1 Notations

Vectors are denoted in bold face ($\mathbf{v}$) and coefficients of vectors with parenthesis ($\mathbf{v}(i)$ is the coefficient number i in vector $\mathbf{v}$). Matrices are denoted in capital bold face and are generally composed of several realizations of vectors of the same name, column-wise: the columns of $\mathbf{V}$ are several realizations $\mathbf{v}_1 \ldots \mathbf{v}_N$ of a "template" vector $\mathbf{v}$.

Let us denote $\mathbf{x}$ the host vector of N_v coefficients into which we want to hide a binary message vector $\mathbf{m}$ of N_c bits. The resulting watermarked vector is denoted $\mathbf{y}$. To this aim, we use $\mathbf{u}_i$ orthogonal carriers, $1 \leq i \leq N_c$. The decoded message is denoted $\hat{\mathbf{m}}$. It is to be estimated from $\mathbf{y}'$, a potentially degraded version of $\mathbf{y}$. Let us further denote $z_{\mathbf{v},\mathbf{u}_i}$ the correlation between a vector $\mathbf{v}$ and a carrier $\mathbf{u}_i$:

$$z_{\mathbf{v},\mathbf{u}_i} =< \mathbf{v}|\mathbf{u}_i >= \frac{1}{N_v}\sum_{k=1}^{N_v} \mathbf{v}(k)\mathbf{u}_i(k) \tag{1}$$

2.2 Information Theoretical Constraints for Perfect Secrecy

Perfect secrecy has different meanings according to the domain of application. For steganography, perfect secrecy means the impossibility to distinguish between an original content ($\mathbf{x}$) and a stego content ($\mathbf{y}$). Cachin studied the necessary conditions to obtain a secure steganographic scheme and claims that a scheme is secure if the Kullback-Leibler divergence D_{KL} between the distributions $P_{\mathbf{x}}$ and $P_{\mathbf{y}}$ of $\mathbf{x}$ and $\mathbf{y}$ is null. The quantity D_{KL} is defined by:

$$D_{KL}(P_{\mathbf{x}}||P_{\mathbf{y}}) = \sum_i P_{\mathbf{x}}(i) \log \frac{P_{\mathbf{x}}(i)}{P_{\mathbf{y}}(i)} \tag{2}$$

which means that perfect secrecy may be achieved if and only if the distributions of $\mathbf{x}$ and $\mathbf{y}$ are identical. A practical implementation of a steganographic scheme satisfying the perfect secrecy constraint has been proposed in [6].

For robust watermarking, the problem does not concern a possible distinction between the original and the watermarked content: it is not important to know wether a content is watermarked or not, but is it important not to disclose the secret carriers based on observations of pieces of watermarked contents. The concept of information leakage in the context of robust watermarking has been proposed in [1] and developed in [2][3]. The notion of information leakage stems from the definition of the mutual information between N_o watermarked contents $\mathbf{Y}$ and the secret carriers $\mathbf{U}$ (where the $\mathbf{u}_i$ are the columns of $\mathbf{U}$ and the N_o observed $\mathbf{y}$ are the columns of $\mathbf{Y}$):

$$I(\mathbf{U}, \mathbf{Y}) = H(\mathbf{Y}) - H(\mathbf{Y}|\mathbf{U}) = H(\mathbf{U}) - H(\mathbf{U}|\mathbf{Y}) \tag{3}$$

then a watermarking scheme is secure if the mutual information between $\mathbf{U}$ and $\mathbf{Y}$ is null: in this case there is no information leakage.

2.3 Spread Spectrum Carriers Estimation

As mentioned previously, a SS watermarking scheme is secure if it is impossible to estimate the secret carriers using observed signals. On the contrary, if a given technique enables to estimate the secret carriers $\mathbf{u}_i$ based only on the observations of $\mathbf{y}$, then the security of the watermarking scheme is greatly reduced. Such a tool can be provided using BSS theory. The goal of BSS is to decompose the observations as a mixture of signals having special statistical properties.

For example, a Principal Component Analysis decomposes observations into orthogonal components according to their variances, and an Independent Component Analysis decomposes the observations into independent signals. Making connections between BSS and SS watermarking is straightforward. A noteworthy property of the class of spread spectrum watermarking schemes is the fact that the embedding part of a SS scheme can be formulated exactly as a blind source separation problem:

$$\mathbf{Y} = \mathbf{X} + \mathbf{U}\mathbf{S}_{\mathbf{m}}. \tag{4}$$

In this equation, the matrix $\mathbf{U}$ is an $N_v \times N_c$ matrix called the mixing matrix (in a BSS framework) and which represents in our case the different carriers $\mathbf{u}_i$ column-wise. The matrix $\mathbf{S_m}$ denotes the different sources that have to be extracted and represents the modulation signal for each carrier that is a function of the embedded message $\mathbf{m}$. The matrix $\mathbf{X}$ represents the host signals (column-wise) and shall be considered as noise in a BSS framework. The goal of BSS is to estimate the matrices $\mathbf{U}$ (the secret carriers) and $\mathbf{S_m}$ according to the observation matrix $\mathbf{Y}$.

In the case of WOA, this decomposition is possible thanks to the fact that each message is embedded independently from another one. It is consequently possible to use Independent Component Analysis techniques to break the security of many spread spectrum watermarking schemes.

The principle of ICA techniques is to find directions in the observed data space whose projections give singular distributions [7]. Based on the fact that the sum of independent variables tends to a Gaussian law, independent components are defined as the most "non-gaussian" components. Moreover, if the watermark components have a different variance than the host data, principal component analysis can be used to perform a reduction of dimension that makes the search of independent components easier.

We now focus on the estimation process of the secret carriers for two popular SS schemes (classical SS and ISS). The ability to estimate their secret carriers is presented.

Classical Spread Spectrum Watermarking. In the case of classical SS, the embedding is given for each vector by:

$$\mathbf{y} = \mathbf{x} + \sum_{i=1}^{N_c} \mathbf{b}(i)\mathbf{u}_i \qquad (5)$$

where $\mathbf{b} \in \{-1; +1\}^{N_c}$ is the BPSK modulation of the embedded message $\mathbf{m}$.

Improved Spread Spectrum Watermarking (ISS). ISS was proposed in [8], it can be considered an informed-embedding variation of classical SS. The embedding is given in this case by:

$$\mathbf{y} = \mathbf{x} + \sum_{i=1}^{N_c} (\alpha \mathbf{b}(i) - \lambda \frac{z_{\mathbf{x},\mathbf{u}_i}}{||\mathbf{u}_i||})\mathbf{u}_i \qquad (6)$$

where α and λ are respectively calculated to respect the targeted distortion and to achieve the most little error probability after addition of white Gaussian noise.

Eq. 5 and Eq. 6 can be easily transposed in the multidimensional case to obtain a formulation similar to Eq. 4: the matrix $\mathbf{U}$ still contains the carriers and the matrix $\mathbf{S_m}$ contains the modulation signals for each carrier.

To assess the security of a SS-based technique, we have decided to adopt the following methodology which is generally used in BSS benchmarks:

1. We generate N_o observa tions of watermarked contents and generate the matrix of observations $\mathbf{Y}$.
2. We whiten the observed signals using principal component analysis. To reduce the searching time, a reduction of dimension is therefore performed. If we consider that the host signal is generated from an i.i.d. process, the subspace containing the watermark generated by N_c carriers will be included into a N_c-dimensional space of different variance [9]. We consequently select the subspace generated by eigenvectors presenting singular (lower or higher) eigenvalues.
3. We run the FastICA algorithm [10] on this subspace to estimate the independent components and the independent basis vectors (e.g. the secret carriers).
4. We compute the normalized correlation c between each original and estimated carriers. A value of c close to 1 means that the estimation of the component is accurate. An estimation close to 0 means that the estimation is erroneous. If $N_c = 2$, we evaluate the estimation accuracy by plotting a 2D constellation of points of coordinates $(c_1; c_2)$. A successful estimation will then provide a point close to one of the four cardinal points $(0,1)$, $(0,-1)$, $(1,0)$, $(-1,0)$[1].

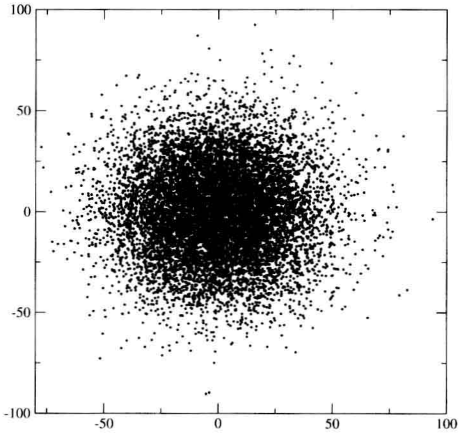


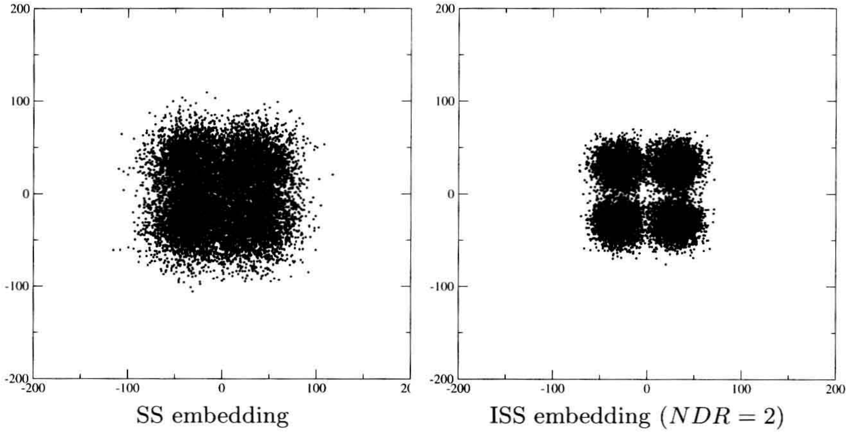
Fig. 1. Joint distributions of two carriers for original contents. $N_o = 10000$, $N_v = 512$, $\sigma_{\mathbf{x}}^2 = 1$.

We have depicted the empirical joint distributions of two carriers in the observed watermarked signals (see Fig. 2) and applied our estimation setup for $N_c = 2$ secret carriers (see Fig. 3). In both cases the host vectors are Gaussian

[1] We use $N_c = 2$ for illustration purposes, hiding more bits would require to use the Hungarian method [11] to assign original and estimated carriers prior to the computation of the normalized correlation c.

i.i.d. signals of law $\mathcal{N}(0,1)$ and two carriers where used during the embedding. The Watermark to Content Ratio (WCR) was fixed in both case to $-21dB$. For each SS scheme, the joint distribution of the carriers in the observed content is the sum of four bi-dimensional Gaussian distributions. Note that the variance of each distribution is less important for ISS embedding than for SS because of the embedding optimization performed by ISS. Note also that the global variance of the distribution for SS is more important than for ISS. For each distribution, the directions of the two carriers (horizontal and vertical axis) are easily identifiable by the ICA algorithm.

Additionally we see that the Cachin criterion which considers the distributions of original and watermarked contents is not fulfilled for this two schemes. Fig. 1 depicts the distribution of the two same carriers for original contents. This distribution is rather different than the distributions after SS watermarking.



SS embedding

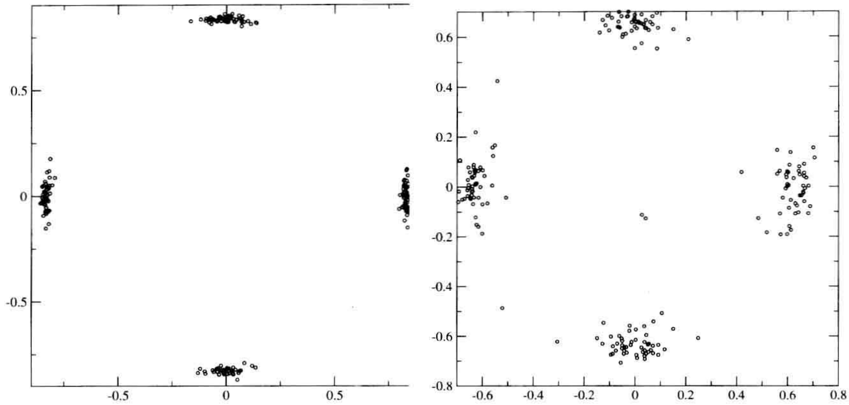
ISS embedding ($NDR = 2$)

Fig. 2. Joint distributions of two carriers for SS and ISS schemes. For both schemes $N_o = 10000$, $WCR = -21dB$ and $N_v = 512$, $\sigma_{\mathbf{x}}^2 = 1$.

Fig. 3 depicts the normalized correlation between the original and estimated carriers for 100 trials considering every 1000 watermarked vectors. We can notice that the estimations are globally more accurate for SS than for ISS. In this case, this is mainly due to the fact that the variance of the embedding for ISS is lower than for SS and consequently the estimation of the subspace relative to the watermark is less accurate in the second case.

3 Natural Spread Spectrum Watermarking

In this section, we show how to build a SS-based watermarking scheme in such a way that the identification of the watermarking subspace spanned by the secret carriers is impossible.



SS embedding ISS embedding ($NDR = 2$)

Fig. 3. Normalized correlations between the two estimated carriers and the real ones. For both schemes $N_o = 1000$, $WCR = -21dB$ and $N_v = 512$.

3.1 Embedding and Decoding

If we consider a carrier $\mathbf{u}_i$ such that its coefficients follows a Gaussian model ($\mathbf{u}_i \sim \mathcal{N}(0, \sigma^2_{\mathbf{u}_i})$), and host signals $\mathbf{x} \sim \mathcal{N}(0, \sigma^2_{\mathbf{x}})$ then the random variable $z_{\mathbf{x},\mathbf{u}_i}$ follows a Gaussian law of parameters $z_{\mathbf{x},\mathbf{u}_i} \sim \mathcal{N}(0, \sigma^2_{\mathbf{u}_i}\sigma^2_{\mathbf{x}})$. Note that this property is true because of the Central limit theorem as far as N_v is important. Moreover, this property is still valid if $\mathbf{x}$ does not follow a Gaussian model. The goal of NW is to design the embedding in such a way that the distribution of $z_{\mathbf{x},\mathbf{u}_i}$ before and after embedding will remain identical. Moreover, as it is shown at the end of this section, the fact that each carrier follows a Gaussian distribution prevents the estimation of the different carriers and guarantees the security of the scheme.

The decoding rule remains the same than for usual SS schemes:

$$\hat{\mathbf{m}}(i) = 1 \text{ if } z_{\mathbf{y}',\mathbf{u}_i} > 0 \tag{7}$$

$$\hat{\mathbf{m}}(i) = 0 \text{ if } z_{\mathbf{y}',\mathbf{u}_i} < 0 \tag{8}$$

The watermarked vector $\mathbf{y}$ is:

$$\mathbf{y} = \mathbf{x} + \mathbf{w} \tag{9}$$

where the watermark signal $\mathbf{w}$ is computed as follows:

$$\mathbf{w} = -\sum_{i=1}^{N_c} \left(1 + (-1)^{\mathbf{m}(i)} \mathrm{sign}(z_{\mathbf{x},\mathbf{u}_i})\right) \frac{z_{\mathbf{x},\mathbf{u}_i}}{\|\mathbf{u}_i\|^2} \mathbf{u}_i \tag{10}$$

which means that the watermark $\mathbf{w}_i$ associated to each carrier $\mathbf{u}_i$ follows this simple embedding rule:

$$\mathbf{w}_i = 0 \quad \text{if} \quad \mathbf{m}(i) = 1 \; ; \; z_{\mathbf{x},\mathbf{u}_i} > 0 \tag{11}$$