Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®

Signal Processing 84 (2004) 1429–1445

SIGNAL PROCESSING

www.elsevier.com/locate/sigpro

Performance analysis and error exponents of asymmetric watermarking systems

Qiang Cheng[a,*], Yingge Wang[b], Thomas S. Huang[c]

[a] *ECE Department, Wayne State University, 3119 Engineering Building, Detroit, MI 48202, USA*
[b] *240 Biltmore Blvd, Troy, MI 48084, USA*
[c] *Coordinated Science Laboratory, ECE Department, Beckman Institute, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA*

Received 11 July 2003; received in revised form 22 April 2004

Abstract

Digital watermarking is an important technique to protect intellectual property right and to transmit useful secondary data. This paper investigates the performance analysis and error exponents of asymmetric watermarking systems. Asymmetric watermarking provides potentially better levels of security. Its detection is much different from commonly used watermarking detectors, particularly when both gain factors and exact values of the watermark are not known to the detector. Optimum detectors are constructed in this paper. To handle unwieldy computations of large matrices, we develop equivalent yet more practical detectors in the frequency domain using asymptotic analysis techniques. Due to the nonlinearity nature of these detectors, their performance analysis is challenging, especially when the size of the watermark becomes large. Gaussian approximations using the central limit theorem is limited in modeling the performance. To obtain fundamental performance limits, we go a step further to make use of asymptotic statistical analysis techniques to derive the exact error exponents. The analytical method gives insights into the performance of asymmetric watermarking, and paves the way toward seeking efficient watermarks for more general asymmetric watermarking systems.

Keywords: Asymmetric watermarking; Locally optimum detector; Asymptotic performance analysis; Exponential level; Exponential power; Exponents characteristic curve

1. Introduction

Watermarking is an important technique for intellectual property right protection or content authentication of digital media, and for secure delivery of useful secondary information by seamlessly embedding data into multimedia content in a seemingly innocuous and standards-compliant fashion. It can be described using a communication model in the presence of side information. An embedder encodes secret messages into watermarks by taking into account host media, which may be considered as side information from the perspective of sending secret messages. The original media seamlessly combined with the watermark are sent through a watermarking channel, in which an attacker attempts to disrupt the watermark by introducing noise as well as other

* Corresponding author. Tel.: +1-313-577-3530.
E-mail addresses: qcheng@ece.eng.wayne.edu (Q. Cheng), yinggewang@hotmail.com (Y. Wang), huang@ifp.uiuc.edu (T.S. Huang).

0165-1684/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2004.05.017

distortions, such as irregular resampling and cropping. At the receiving end, a receiver decodes the transmitted message or identifies the watermarking pattern.

To optimize the message transmission rate in the presence of side information, for Gaussian channel with mean squared error distortion measure, Costa proposed an information-theoretic scheme which has been widely applied in watermarking research [4,12,16,30,35]. Practical watermarking schemes, such as sign embedding and look-up-table mapping [34,43], have been designed. A verification model taking into account side information has also been proposed by Steinberg and Merhav [38]. Practical schemes have been developed, utilizing spread spectrum embedding, human perceptual models, and oblivious detection or decoding [13,39,42,44]. Statistical modeling and performance analysis have also been developed [1,5–9,25]. A particular class of methods in the verification model is asymmetric watermarking. It is designed in a way analogous to asymmetric cryptographic systems [36]. Several methods have been proposed in the literature, please refer to [17,19,20,23,32,37,40] and the references therein. These asymmetric watermarking schemes use different keys at the ends of the sender and receiver. A notable feature of these methods is that, often times, a particular statistical property or random process is used as a watermark, and the detector needs to verify the presence of the watermark without its exact values. The commonly used detection algorithm for asymmetric watermarks is a quadratic detector (an exception is [32], where neural networks are used. Please see [17,19,20,23,32,37,40] and the references therein). The quadratic detector is much deviated from the common linear correlation detector. In this paper, we first examine the uniformly most powerful detector (UMP) of an asymmetric watermarking system, and develop a practical detector in the frequency domain. Usually, the strengths of the watermark are controlled by gain factors, and adapted to local host characteristics for a given spectral structure of stochastic signals. The gain factors are needed to utilize the uniformly most powerful detector, but in many practical applications, they are often unavailable at the detector end. To efficiently handle this situation, we construct a locally optimum detector (LOD) in a way similar to our previous works for symmetric watermarking [6,8,9]. This LOD detector does not need the knowledge of the gain factor, but it involves the cumbersome manipulation of large matrices. To overcome this computational difficulty, we devise an equivalent LOD by exploiting the frequency-domain representation. The equivalent LOD does not need to manipulate the large matrices, thus, is more practical. Then, we focus on the performance analysis of an asymmetric watermarking scheme. Especially, we are concerned with the asymptotic error exponents, since they dominate the performance when the size of the watermark becomes large. For both the UMP and LOD detectors, we first use the central limit theorem to approximate the error probabilities. Their performance is found not very accurate, and more accurate performance analysis has yet to be developed. To obtain the fundamental limits of the performance, we make use of their frequency-domain representations and large deviations techniques (please see [2,3,14,15] and the references therein) to find the exact error coefficients. An error exponent characteristic curve is proposed as a global performance index of different detection algorithms. It is independent of the thresholds or the decision boundaries, and indicates the intrinsic detection capability. Numerical results are provided to corroborate the above theoretical analysis. This paper provides insights into the performance of asymmetric watermarking, and paves a way toward devising asymmetric watermarking schemes that optimize the asymptotic exponential decreasing rates of the detection errors.

The rest of the paper is organized as follows: Section 2 presents problem formulation for asymmetric watermark detection. Optimum detectors and practical ones for asymmetric watermarking are constructed in Sections 3 and 4. Section 5 develops performance analysis using Gaussian approximations. Error exponent analyses for these detectors are developed in Sections 6 and 7. Experimental results are provided in Section 8 to confirm the effectiveness of theoretical analyses. Section 9 concludes the paper and points out future research lines.

The following notation is used. Underlined letters denote vectors with the exception of 0: it will be clear in the context whether 0 is a scalar or vector. Underlined upper case letters denote vectors of random variables. $\mathscr{R}^N$ and $\mathscr{C}^N$ denote the set of N-dimensional vectors with real- and complex-valued entries, respectively. The superscripts of a vector or matrix $(\cdot)^{\mathrm{T}}$ and