Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®
Signal Processing 86 (2006) 893–914
SIGNAL PROCESSING
www.elsevier.com/locate/sigpro

An overview of scalar quantization based data hiding methods

Husrev T. Sencar[a,*], Mahalingam Ramkumar[b], Ali N. Akansu[a]

[a]New Jersey Institute of Technology, Department of Electrical and Computer Engineering, Newark, NJ 07102, USA
[b]Mississippi State University, Department of Computer Science & Engineering, Mississippi State, MS 39762, USA

Received 5 July 2004; received in revised form 9 July 2005; accepted 9 July 2005
Available online 18 August 2005

Abstract

In Ref. [Costa, Writing on dirty paper, IEEE Trans. Inform. Theory 29 (1983) 439–441.], Costa presented a communications framework that provided useful insights into the study of data hiding. We present an alternate and equivalent framework with a more direct data hiding perspective. The difference between the two frameworks is in how channel dependent nature is reflected in optimal encoding and decoding operations. The connection between the suggested encoding/decoding scheme and practical embedding/detection techniques is examined. We analyze quantization based embedding/detection techniques in terms of the proposed framework based on three key aspects. The first aspect is the type of postprocessing utilized at the embedder (i.e. distortion compensation [Chen, Wornell, Preprocessed and postprocessed quantization index modulation methods for digital watermarking, in: Proceedings of SPIE: Security and Watermarking of Multimedia Contents II, vol. 3971, 2000, pp. 48–59; Eggers, Su, Girod, A blind watermarking scheme based on structured codebooks, IEE Colloq. Secure Images Image Authentication 4 (2001) 1–6.], thresholding [Ramkumar, Akansu, Self-noise suppression schemes for blind image steganography, in: Proceedings of SPIE International Workshop on Voice, Video and Data Communication, Multimedia Applications, vol. 3845, 1999.], Gaussian mapping [Perez-Gonzalez, Balado, Hernandez Martin, Performance analysis of existing and new methods for data hiding with known-host information in additive channels, IEEE Trans. Signal Process. 51(4) (2003) 960–980].). The second key aspect is the form of demodulation used at the extractor. The third is the criteria used to optimize the embedding/detection parameters. The embedding/detection techniques are compared in terms of probability of error, correlation, and mutual information (hiding rate) performance merits.

Keywords: Data hiding; Embedder/detector; Quantization; Postprocessing; Thresholding; Distortion compensation; Gaussian mapping

1. Introduction

The study of data hiding (watermarking) tries to establish the achievable limits and the design of

*Corresponding author.
E-mail addresses: taha.sencar@njit.edu (H.T. Sencar), ramkumar@cse.msstate.edu (M. Ramkumar), ali@oak.njit.edu (A.N. Akansu).

0165-1684/$ - see front matter
doi:10.1016/j.sigpro.2005.07.018

methods for conveying a message signal, embedded within a host (cover) signal, in an imperceptible and reliable way. One conservative assumption in data hiding is that the embedder has no access to the host signal (oblivious data hiding). Though, not all data hiding applications are necessarily oblivious, our focus is the oblivious one.

The theory of data hiding has been developed mainly through employing analytical tools of communication theory. This is achieved by reinterpreting and adapting basic concepts such as channel, side information, and power constraints within the context of data hiding. In data hiding, channel is the medium between the hider and extractor, and it includes all forms of disturbances that affect the *stego* signal, which is an *intelligent* combination of the host signal and the message to be conveyed. Side information available at the encoder in a communication channel model, is associated with the host signal at the embedder in the equivalent data hiding model. Similarly, encoder/decoder pair is functionally equivalent to embedder/detector pair. Power constraints in a channel communication scenario are analogous to the perceptual distortion limits that are determined based on the features of the host signal. The bandwidth is somewhat dual to embedding signal size, and signal-to-noise ratio (SNR) measure corresponds to embedding distortion to attack distortion ratio (WNR) measure. Table 1 shows the relationship between the communications and data hiding frameworks. Aside from the analogies between the two frameworks, the analytical formulation of data hiding problem further requires consideration of the interactions between information hider/extractor and attacker.

Table 1
Relationship between communications and data hiding frameworks

Communications framework	Data hiding framework
Side information	Host signal
Encoder/decoder	Embedder/detector
Channel noise	All forms of modification on the stego signal (Attack)
Power constraints	Perceptual distortion limits
Bandwidth	Embedding signal size
Signal-to-noise ratio	Embedding distortion to attack distortion ratio

Performance of data hiding methods is usually restricted by the maximum amount of distortion that may be introduced to the host signal with no perceptual distortion. The embedding distortion is ideally derived from a perceptual distortion measure, and it is a resource of the communication between the embedder and detector. The information hider needs to design the embedder/detector pair that makes the most effective use of this core resource.

The design principle that governs the operation of the embedder/detector pair is the most important characteristic of a data hiding method. Among a variety of research approaches the ones that draw a lot of attention are inspired from *communication with side information* [1–4]. Costa [5] introduced the notion that, in a communication channel, a side information *available to encoder but not to decoder* does not necessarily causes a reduction in the communication rate. His results, when evaluated within data hiding context, encouraged researchers in designing practical oblivious data hiding schemes that can achieve the hiding capacity.

To achieve the hiding rates that are closer to the upper capacity bound, several implementations are proposed [1,6–9]. These techniques are characterized by the use of enhanced quantization procedures in order to design embedding/detection techniques that approximate the performance of optimal encoding/decoding. In this class of methods, the optimal implementation requires higher dimensional quantization for embedding. In [10], Zamir et al. show that nested lattices can be used to construct optimum codes. However, a satisfactory performance is also achievable through scalar quantization or unidimensional lattices. On the other hand, the extraction of the hidden message is achieved, most generally, by employing minimum distance decoding due to the use of lattice structures in embedding.

Chen and Wornell [6] provide a formal treatment of data hiding methods that use quantizers to embed signals, that is called quantization index modulation (QIM). In this class of methods, quantization is used to force the host signal