Circuits Syst Signal Process (2016) 35:1333–1353
DOI 10.1007/s00034-015-0124-3

Optimal M-PAM Spread-Spectrum Data Embedding with Precoding

Ming Li[1] · Qian Liu[2] · Yanqing Guo[1] · Bo Wang[1]

Received: 15 September 2014 / Revised: 1 July 2015 / Accepted: 2 July 2015 /
Published online: 11 July 2015

Abstract We consider M-level pulse amplitude modulation (M-PAM) spread-spectrum (SS) data embedding in transform domain host data. The process of data embedding can be viewed as delivering information through the channel including additive interference from host that is known to the embedder. We first utilize the knowledge of second-order statistics of host to design optimal carrier that maximizes the signal-to-interference-plus-noise ratio at the decoder end. Then, inspired by Tomlinson–Harashima precoding used in communication systems, a symbol-by-symbol precoding scheme is developed for M-PAM SS embedding to alleviate the impact of the interference which is explicitly known to embedder. For any given embedding carrier and host data, we aim at designing precoding algorithm to minimize the receiver bit error rate (BER) with any given host distortion budget, and conversely minimize the distortion at any target BER. Experimental studies demonstrate that the proposed precoded SS embedding approach can significantly improve BER performance over conventional SS embedding schemes.

✉ Bo Wang
bowang@dlut.edu.cn

Ming Li
mli@dlut.edu.cn

Qian Liu
qianliu@buffalo.edu

Yanqing Guo
guoyq@dlut.edu.cn

[1] School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, Liaoning, People's Republic of China

[2] Department of Computer Science and Engineering, University of New York at Buffalo, Buffalo, NY 14260, USA

Keywords Authentication · Data embedding · Data hiding · Dirty paper coding · Information hiding · Spread-spectrum embedding · Tomlinson–Harashima precoding · Watermarking

1 Introduction

Data embedding has raised extensive attention in recent years with the increasing demand of security and privacy in digital media services. Various applications emerge along with the blooming of this technology such as annotation, copyright marking, watermarking, ownership protection, authentication, digital fingerprint, as well as covert communications and steganography [8,10,16,19–21,28,29,38]. As a general encompassing comment, different applications of data embedding require different satisfactory trade-offs between the following four basic attributes [35]: Payload—data delivery rate; robustness—embedded data resistance to noise and disturbance; transparency—low host distortion for concealment purposes; and security—inability by unauthorized users to detect and access the embedded data.

Embedding process is a crucial step in the design of data embedding systems because distortion, payload, embedded data detector design, and recovery performance depend heavily on how the data are inserted in the host. Data embedding can be performed either directly in the time/spatial domain [5,9,17,23,32] or in a transform domain (for example, for images, we may consider full-frame discrete Fourier transform (DFT) [3,4,7], block DFT or DCT [2,15,26,30,39], or discrete wavelet transforms (DWT) [24,25,37]).

Spread-spectrum (SS) data embedding [11,12,22,34,36] is a branch of transform domain data embedding family tree and enjoys wide popularity in data embedding community, especially for watermarking-related applications. It is derived from SS digital communication systems [13] and utilizes a modulated carrier to deposit one information symbol across a group of host data coefficients or a linearly transformed version of them. In direct analogy to SS digital communication systems, the information inserted into the host data is considered as the desired signal, while the host media are treated as interference during SS data embedding procedure. However, unlike SS communications, this interference is explicitly known to the embedder. With proper design, this unique characteristic can play an important role in host distortion reduction and embedding message recovery.

In this paper, we investigate M-level pulse amplitude modulation (M-PAM) SS data embedding in transform domain host. In particular, the adoption of M-PAM can allow the host to accommodate more embedded data during embedding procedure and therefore provides higher payload rate than the existing binary symbol SS embedding algorithms. However, challenges always come along with opportunities. The introduction of M-PAM also arouses a crucial problem to the current SS embedding system: While higher-order modulation allows higher payload rate, detection error will also increase. Therefore, in this paper, we develop new optimal carrier and precoding designs for M-PAM SS data embedding which can minimize the bit error rate (BER) at a given host distortion budget. The contributions of this paper are summarized in the following.

- We propose optimal carrier design for M-PAM SS data embedding.

Recently, an optimal carrier for binary symbol data embedding was presented in [11,12] by exploiting the second-order statistics (SOS) of the host data. Inspired by this result, we develop an eigen-based optimal carrier design for M-PAM SS embedding in linear-transform host media by considering the characteristic of SOS of the host data. The proposed design can maximize the signal-to-interference-noise ratio (SINR) at a given host distortion budget, which is equivalent to minimize the BER of the embedded data at a given host distortion budget.

- We develop a novel precoding design for M-PAM SS data embedding.

The proposed precoding design is inspired by the idea of "Dirty Paper Coding" (DPC) and can be utilized with or without the proposed optimal carrier scheme in SS embedding systems. In the next two paragraphs, we shall demonstrate the motivation and the design of the proposed precoding algorithm.

As is known, in SS data embedding systems, the impact of interference from the host signal is explicitly known to the embedders and therefore can be further alleviated by performing precoding at the embedder side. In Costa's seminal paper "Writing on dirty paper" [6], this scenario is modeled as a writer who strategically adapts his writing in order to avoid the dirt (interference) on a piece of paper and help the reader decode the message without knowing where the dirt is. The Costas dirty paper coding (DPC) scheme can theoretically achieve the same capacity of the channel in which the interference was not present. However, Costa's DPC scheme is not impractical for real-world implementation since it requires an infinite length of codewords and codebooks. In [1], a dirty trellis embedding algorithm is proposed with a theoretical capacity close to Costa's scheme in the moderate-to-low bit error rate regime. Since this approach is based on serially concatenated convolutional coding, the encoder and decoder are relatively complicated compared with the existing binary symbol embedding schemes. Tomlinson–Harashima precoding (THP), initially proposed for temporal inter-symbol interference mitigation [14,31], is a well-known practical DPC scheme with simple implementation structure. Since the THP precancels the interference of each symbol individually, it can be considered as a one-dimensional implementation of DPC.

Inspired by THP in communication systems, we develop a symbol-by-symbol precoding scheme for M-PAM SS data embedding in this paper. The proposed scheme can extensively reduce the influence of host media (interference) to the embedded data. For any given embedding carrier/signature and the host data, the proposed precoding algorithm aims at minimizing the receiving BER with a given host distortion budget, or conversely minimizing the distortion at a target BER. Experimental studies demonstrate that the proposed precoding design can significantly improve the BER performance of M-PAM SS data embedding systems.

The rest of the paper is organized as follows. In Sect. 2, the M-PAM SS embedding is presented, and optimal carrier design is proposed. Then, M-PAM SS embedding with precoding is developed in Sect. 3. Section 4 is devoted to experimental studies and comparisons. A few concluding remarks are drawn in Sect. 5.

The following notation is used throughout the paper. Boldface lowercase letters indicate column vectors and boldface uppercase letters indicate matrices; $\mathbb{R}$ denotes

the set of all real numbers; $\mathbb{Z}$ denotes the set of all integer numbers; $()^T$ denotes matrix transpose; $\mathbf{I}_L$ is the $L \times L$ identity matrix; sgn$\{\cdot\}$ denotes zero-threshold quantization; $\mathbb{E}\{\cdot\}$ represents statistical expectation; $\|\cdot\|$ is vector norm; round(x) denotes as rounding a real number x to the nearest integer value; mod(x, y) denotes modulo operation that finds the remainder of division of x by y, $y \neq 0$.

2 M-PAM SS Embedding

2.1 Signal Model and Notation

Consider a host image $\mathbf{H} \in \mathcal{M}^{N_1 \times N_2}$ where $\mathcal{M}$ is the finite image alphabet and $N_1 \times N_2$ is the image size in pixels. Without loss of generality, the image $\mathbf{H}$ is partitioned into N local non-overlapping blocks of size $\frac{N_1 N_2}{N}$. Each block, $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_N$, is to carry one information bit $b_i, i = 1, 2, \ldots, N$, respectively. Embedding is performed in a 2D transform domain $\mathcal{T}$ (such as the discrete cosine transform and a wavelet transform). After transform calculation and vectorization (for example by conventional zigzag scanning), we obtain $\mathcal{T}(\mathbf{H}_i) \in \mathbb{R}^{\frac{N_1 N_2}{N}}, i = 1, 2, \ldots, N$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_i)$, we choose a fixed subset of $L \leq \frac{N_1 N_2}{N}$ coefficients (bins) to form the final host vectors $\mathbf{x}_i \in \mathbb{R}^L, i = 1, 2, \ldots, N$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes in the dc value.

The autocorrelation matrix of the host data $\mathbf{x}$ is an important statistical quantity for our developments and is defined as

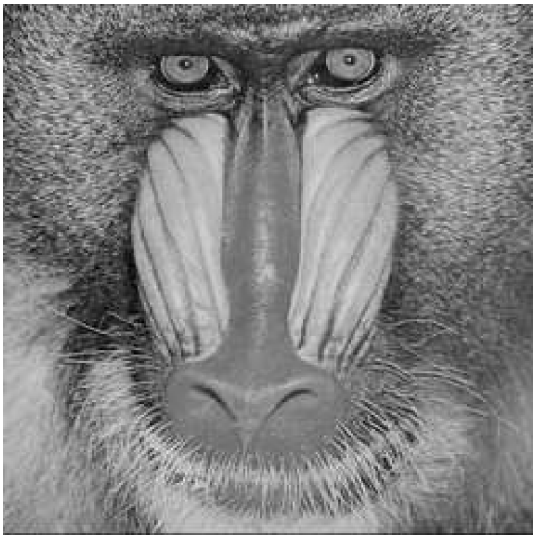
$$\mathbf{R}_{\mathrm{x}} \triangleq \mathbb{E}\{\mathbf{x}\mathbf{x}^T\} = \frac{1}{N}\sum_{i=1}^{N} \mathbf{x}_i \mathbf{x}_i^T. \tag{1}$$

It is easy to verify that in general $\mathbf{R}_{\mathrm{x}} \neq \alpha \mathbf{I}_L, \alpha > 0$, that is, $\mathbf{R}_{\mathrm{x}}$ is *not* constant-value diagonal or "white" in field language. For example, 8×8 DCT with 63-bin host data formation (excluding only the dc coefficient) for the 256×256 gray-scale Baboon image in Fig. 1a gives the host autocorrelation matrix $\mathbf{R}_{\mathrm{x}}$ in Fig. 1b [12].

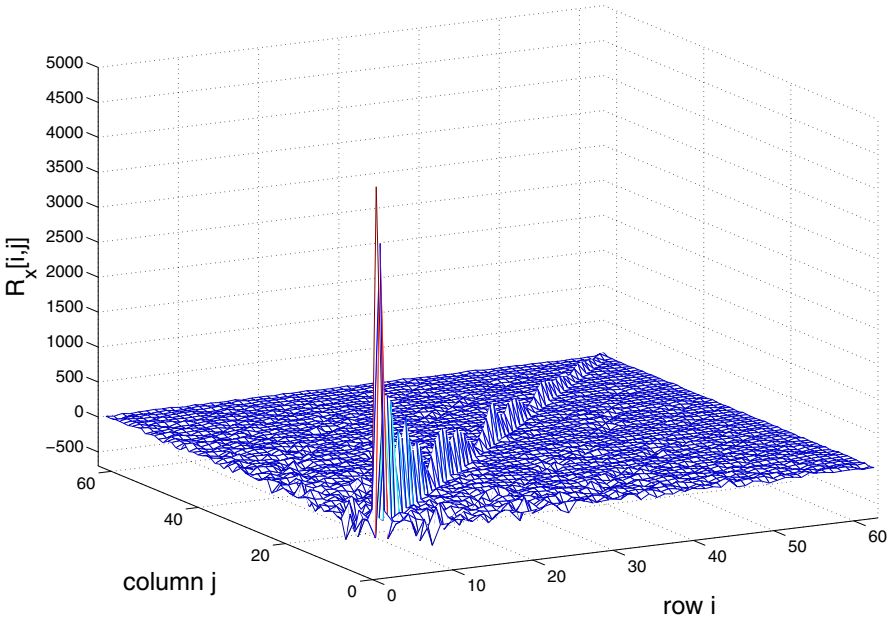
2.2 M-PAM SS Embedding

To draw a parallelism with SS communication systems, conventional SS embedding treats embedded message as the SS signal of interest transmitted through a noisy "channel." The disturbance to the SS signal of interest is the host data themselves plus potential external noise due to physical transmission of the watermarked data and/or processing/attacking. In particular, conventional additive SS embedding is carried out in the transform domain by

$$\mathbf{y}_i = Ab_i\mathbf{s} + \mathbf{x}_i + \mathbf{n}_i, \quad i = 1, \ldots, N, \tag{2}$$



(a)



(b)

Fig. 1 **a** Baboon image example $\mathbf{H} \in \{0, 1, \ldots, 255\}^{256\times256}$. **b** Host data autocorrelation matrix (8×8 DCT, 63-bin host) [12]

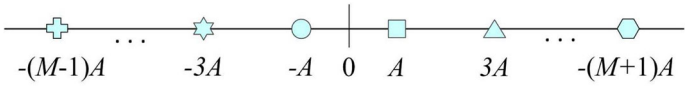


Fig. 2 M-PAM constellation

where information symbol b_i is embedded in the transform domain host vector $\mathbf{x}_i \in \mathbb{R}^L$ via additive SS embedding by means of a carrier $\mathbf{s} \in \mathbb{R}^L$, $\|\mathbf{s}\| = 1$, with a corresponding embedding amplitude $A > 0$. For the sake of generality, $\mathbf{n}_i$ represents potential external white Gaussian noise[1] of mean $\mathbf{0}$ and autocorrelation matrix $\sigma_n^2 \mathbf{I}_L$, $\sigma_n^2 > 0$.

While binary symbol $b_i \in \{\pm 1\}$ is the simplest and most common case in previous works; in this paper, we extend our scope to use more symbol alphabets in order to provide SS embedding with ability to embed/deliver more data. M-level pulse amplitude modulation (M-PAM) is adopted, and the information symbol b_i to be embedded is selected from an M alphabet set $\mathcal{A}_{\mathcal{M}} \triangleq \{\pm(2m-1), m = 1, \ldots, M/2,\ M \text{ is even}\}$. With an amplitude A, the constellation points are $\{\pm A(2m-1), m = 1, 2, \ldots, M/2\}$ as shown in Fig. 2.

Squared Euclidean metric is rudimentary but common choice to measure the distortion. The mean-squared (MS) distortion to each host vector (i.e., each block of image) *due to embedding only* is

$$\mathcal{D} = \mathbb{E}\,\|(Ab_i\mathbf{s} + \mathbf{x}_i) - \mathbf{x}_i\|^2 = \mathbb{E}\{b_i\}A^2 = \frac{M^2-1}{3}A^2. \tag{3}$$

The intended recipient of the message can perform matched filtering (MF)

$$r_i = \mathbf{s}^T \mathbf{y}_i \tag{4}$$

and then recovers the embedded symbols by

$$\hat{b}_i = \arg\min_{b \in \mathcal{A}_M} |r_i - Ab|\,. \tag{5}$$

Or equivalently, embedded symbols can be recovered by following simple operation

$$\hat{b}_i = \begin{cases} M-1, & \text{if } r_i > (M-1)A; \\ -(M-1), & \text{if } r_i < -(M-1)A; \\ \text{round}\,((r_i/A+1)/2)\,2-1, & \text{else.} \end{cases} \tag{6}$$

[1] Additive white Gaussian noise is frequently viewed as a suitable model for malicious or accidental attacks, such as quantization errors, channel transmission disturbances, and/or image processing attacks.

2.3 Carrier Optimization

With the signal of interest $Ab_i\mathbf{s}$ and total disturbance $(\mathbf{x}_i + \mathbf{n}_i)$ in (2), the SINR of the output of matched filter in (4) is

$$\mathrm{SINR} = \frac{\mathbb{E}\{\|Ab_i(\mathbf{s}^T\mathbf{s})\|^2\}}{\mathbb{E}\{\|\mathbf{s}^T(\mathbf{x}_i + \mathbf{n}_i)\|^2\}} = \frac{\frac{M^2-1}{3}A^2}{\mathbf{s}^T(\mathbf{R}_{\mathrm{x}} + \sigma_n^2\mathbf{I}_L)\mathbf{s}}.$$

It is understood that the host $\mathbf{x}_i$, which is interference to the signal of interest, is known to the embedder. By exploiting $\mathbf{R}_{\mathrm{x}}$, i.e., the SOS of the host, optimal carrier that maximizes the output SINR has been presented in Proposition 1 whose proof is straightforward and omitted.

Proposition 1 *Consider additive SS embedding according to (2). Let* $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_L$ *be eigenvectors of* $\mathbf{R}_{\mathrm{x}}$ *in (1) with corresponding eigenvalues* $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$. *For any hidden message-induced distortion level* $\mathcal{D}$, *a carrier that maximizes the output SINR of the matched filter is*

$$\mathbf{s}^{\mathrm{opt}} = \mathbf{q}_L. \tag{7}$$

With this optimal carrier, the matched filter is also a maximum SINR filter, and the output SINR is maximized at

$$\mathrm{SINR}_{\max} = \frac{\frac{M^2-1}{3}A^2}{\lambda_L + \sigma_n^2} = \frac{\mathcal{D}}{\lambda_L + \sigma_n^2}. \tag{8}$$

If we are allowed to assume that $\mathbf{x}_i$ is Gaussian, the symbol error rate (SER) of the recovered message is

$$\mathrm{SER} = \frac{2(M-1)}{M}Q\left(\sqrt{\frac{3}{M^2-1}\mathrm{SINR}}\right) \tag{9}$$

where $Q(a) = \int_a^\infty \frac{1}{\sqrt{2\pi}}e^{-\tau^2/2}d\tau$. With Gray-coded symbol, the bit error rate (BER) is

$$\mathrm{BER} = \frac{\mathrm{SER}}{\log_2 M}. \tag{10}$$

We see that SER and BER are monotonically decreasing functions of SINR, and then, the optimization on maximizing SINR is equivalent to minimize probability of error.

2.4 SS Embedding on Linearly Transformed Host

In an effort to reduce the interference effect of the host signal, the host vectors $\mathbf{x}_i$, $i = 1, \ldots, N$, can be steered away from the embedding carrier using an operator of the form $(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)$ with a parameter $c \in \mathbb{R}$ and the carrier $\mathbf{s} \in \mathbb{R}^L$. In parallel to

(2), the composite signal of additive SS embedding on linearly transformed host data is [11,12,22]

$$\mathbf{y}_i = Ab_i\mathbf{s} + (\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i + \mathbf{n}_i, \quad i = 1, \ldots, N, \tag{11}$$

where information symbol b_i is embedded, using amplitude $A > 0$ and (normalized) carrier $\mathbf{s} \in \mathbb{R}^L$, $\|\mathbf{s}\| = 1$, in the ith linearly transformed host data vector $(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i$. The output SINR of MF is

$$\text{SINR} = \frac{\mathbb{E}\{\|Ab_i\|^2\}}{\mathbb{E}\{\|\mathbf{s}^T((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i + \mathbf{n})\|^2\}}. \tag{12}$$

The mean-squared distortion *due to the embedding operation only* is

$$\begin{aligned}\mathcal{D} &= \mathbb{E}\left\{\|\left(Ab_i\mathbf{s} + (\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i\right) - \mathbf{x}_i\|^2\right\} \\ &= \frac{M^2-1}{3}A^2 + c^2\mathbf{s}^T\mathbf{R}_x\mathbf{s}.\end{aligned} \tag{13}$$

It should be noticed that, in contrast to (3), the distortion level is controlled not only by A but by c and $\mathbf{s}$ as well. Comparing to conventional SS embedding in (2), SS embedding on linearly transformed host utilizes part of available distortion to presuppress the interference at the embedding side and then uses the remaining distortion to embed information bits. With any given distortion budget, the transform parameter c, amplitude A, and optimal carrier $\mathbf{s}$ to maximize the output SINR are presented in Proposition 2 whose proof is offered in the "Appendix."

Proposition 2 *Consider additive SS embedding in linearly transformed host data by (11), and secret message is recovered by matched filter. For any hidden message-induced distortion budget $\mathcal{D}$ and any carrier $\mathbf{s}$, the optimal amplitude A and transformation parameter c to maximize the SINR of matched filter are*

$$c^{\text{opt}} = \frac{\alpha + \sigma_n^2 + \mathcal{D} - \sqrt{(\alpha + \sigma_n^2 + \mathcal{D})^2 - 4\alpha\mathcal{D}}}{2\alpha}, \tag{14}$$

$$A^{\text{opt}} = \sqrt{\frac{3}{M^2-1}\left(\mathcal{D} - {c^{\text{opt}}}^2\alpha\right)}, \tag{15}$$

where $\alpha \triangleq \mathbf{s}^T\mathbf{R}_x\mathbf{s}$. The output SINR is maximized to

$$\text{SINR}_{\max} = \frac{\mathcal{D} - {c^{\text{opt}}}^2\alpha}{\alpha(1 - c^{\text{opt}})^2 + \sigma_n^2}. \tag{16}$$

Let $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_L$ be eigenvectors of $\mathbf{R}_x$ in (1) with corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$. The optimal carrier to maximize output SINR is

$$\mathbf{s}^{\text{opt}} = \mathbf{q}_L. \tag{17}$$

With this optimal carrier $\mathbf{s}^{\text{opt}}$*, the corresponding optimal c and A can be calculated by (14) and (15) with* $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\text{x}}\mathbf{s} = \lambda_L$*, and the matched filter is also a maximum SINR filter.*

The effort on optimal carrier design developed in this section attempts to maximize SINR by utilizing the SOS of the host $\mathbf{R}_{\text{x}}$. It should be noticed that the impact of interference from the explicitly known host signal can be further alleviated if each symbol is precoded adaptively to precancel interference at the embedder side. In next section, we pursue further optimal symbol-by-symbol adaptive precoding for M-PAM SS embedding to compensate for the known interference.

3 M-PAM SS Embedding with Precoding

With precoding scheme, instead of embedding the information symbol b_i directly, we precode b_i to u_i and then embed u_i into host $\mathbf{x}_i$ via a carrier $\mathbf{s}$. The M-PAM SS embedding with precoding is modeled in a form of

$$\mathbf{y}_i = u_i\mathbf{s} + \mathbf{x}_i + \mathbf{n}_i \tag{18}$$

where u_i is precoded symbol based on information symbol b_i and host/interference $\mathbf{x}_i$. We need to choose u_i (as a function of b_i and $\mathbf{x}_i$) such that the embedded information symbol b_i can be decoded as the host signal (interference) $\mathbf{x}_i$ is present and unknown.

The signal after matched filtering can be expressed as

$$\begin{aligned} r_i &= \mathbf{s}^T\mathbf{y}_i && (19)\\ &= u_i\mathbf{s}^T\mathbf{s} + \mathbf{s}^T\mathbf{x}_i + \mathbf{s}^T\mathbf{n}_i && (20)\\ &= u_i + z_i + n_i && (21) \end{aligned}$$

where we define $z_i \triangleq \mathbf{s}^T\mathbf{x}_i$, $n_i \triangleq \mathbf{s}^T\mathbf{n}_i$. The application of data embedding is considered to convey information symbols b_i by u_i to the receiver in the presence of interference z_i and noise n_i. In particular, interference z_i can be approximately viewed as having generalized Gaussian distribution [26] or Laplace distribution [18] with zero mean and variance $\sigma_z^2 \triangleq \mathbb{E}\{z_i^2\} = \mathbf{s}^T\mathbf{R}_{\text{x}}\mathbf{s}$. Additive white Gaussian noise n_i has zero mean and variance σ_n^2.

With a determined carrier $\mathbf{s}$ and host vectors $\mathbf{x}_i$, $i = 1, \ldots, N$, the interference z_i, $i = 1, \ldots, N$, is explicitly known and can be precanceled at the embedder side. The simplest way to compensate for the interference z_i is to select u_i such that the symbol b_i is modulated into the corresponding constellation point Ab_i, i.e.,

$$u_i + z_i = Ab_i, \quad i = 1, \ldots, N. \tag{22}$$

Thus, the precoded symbol for interference precancelation is

$$u_i = Ab_i - z_i, \quad i = 1, \ldots, N. \tag{23}$$

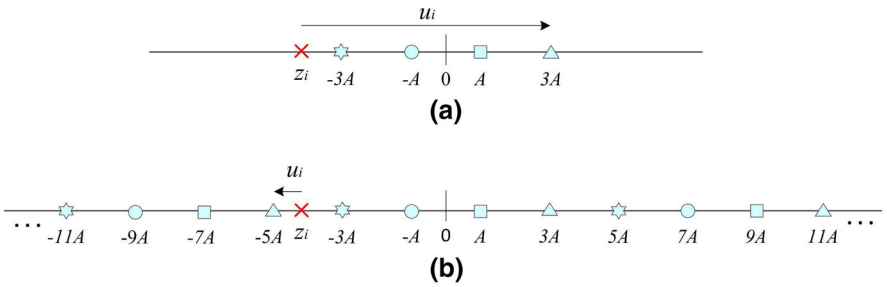


Fig. 3 **a** Four-point constellation. **b** Four-point constellation is replicated along the entire *line*

The squared distortion to the ith host vector due to the embedded data only is

$$\mathcal{D}_i = \|(u_i \mathbf{s} + \mathbf{x}_i) - \mathbf{x}_i\|^2 = u_i^2, \quad i = 1, \ldots, N. \tag{24}$$

The MS host distortion is

$$\mathcal{D} = \mathbb{E}\{\mathcal{D}_i\} = \mathbb{E}\{u_i^2\} = \mathbb{E}\{(Ab_i - z_i)^2\} = \frac{M^2 - 1}{3} A^2 + \sigma_z^2. \tag{25}$$

The SER of the recovered message is

$$\text{SER} = \frac{2(M-1)}{M} Q\left(\frac{A}{\sigma_n}\right). \tag{26}$$

With Gray-coded symbol, the BER is

$$\text{BER} = \frac{\text{SER}}{\log_2 M} = \frac{2(M-1)}{M \log_2 M} Q\left(\frac{A}{\sigma_n}\right). \tag{27}$$

The problem of the interference precancelation for regular modulation in (23) is that the interference z_i may be arbitrarily far away from desired constellation points. Here is an example shown in Fig. 3a for 4-PAM case. We want to modulate symbol to constellation point $3A$, while the interference is z_i. To precancel a large interference z_i, we need a precoded symbol u_i with a large absolute value and consequently introduce strong distortion to the host. Actually, even for the worst case $A = 0$ which results BER $= 0.5$, we still have to induce distortion at a level $\mathcal{D} = \sigma_z^2 = \mathbf{s}^T \mathbf{R}_{\mathrm{x}} \mathbf{s}$. Therefore, host-adaptive optimal carrier is still favorable in this interference precancelation scheme to minimize the variance of interference σ_z^2. However, regretfully, host-adaptive optimal carrier is not always applicable for all data embedding applications.

We utilize the idea of Tomlinson–Harashima precoding and replicate the constellation along the entire length of the real line to obtain an infinite extended constellation, as shown in Fig. 3b for 4-PAM case. Each of the M information symbols b_i now corresponds to the equivalence class of points $(2nM + b_i)A$, $n \in \mathbb{Z}$ is an integer, in the replicated constellation points instead of a single point.

To minimize distortion $\mathcal{D}_i = u_i^2$ to the ith host vector, we choose u_i with minimum absolute value such that $u_i + z_i$ is a representation point in its equivalence class $(2nM + b_i)A$,

$$\min|u_i|, \quad \text{s. t. } u_i + z_i = (2nM + b_i)A, \quad n \in \mathbb{Z}. \tag{28}$$

To solve (28), we need to first find the representation point in its equivalence class which is closest to the interference, that is, $(2n'M + b_i)A$, where $n' = \text{round}(\frac{z_i - b_i A}{2AM})$. To let $u_i + z_i = (2n'M + b_i)A$, we then find the optimal u_i by calculating the difference

$$u_i = (2n'M + b_i)A - z_i, \quad n' = \text{round}\left(\frac{z_i - b_i A}{2AM}\right). \tag{29}$$

The maximum-likelihood (ML) detector of embedded symbols can be mathematically expressed in a form of

$$\hat{b}_i = \arg\min_{b \in \mathcal{A}_\mathcal{M}} |r_i - (2nM + b)A|, \quad \text{for any integer } n. \tag{30}$$

Or equivalently, recovery can be performed by finding the point $n''A$ in the infinite replicated constellation that is closest to received signal r_i:

$$n'' = \text{round}\left((r_i/A + 1)/2\right) 2 - 1 \tag{31}$$

and then decoding n'' to the corresponding symbol in the alphabet set $\mathcal{A}_\mathcal{M}$:

$$\hat{b}_i = \text{mod}\left(n'' + M - 1, 2M\right) - (M - 1). \tag{32}$$

The M-PAM SS embedding with precoding has just slightly more complexity on encoder and decoder than conventional SS embedding. But the decoder needs the knowledge of the modulation separation A which can be predesigned with the estimation of external noise intensity (i.e., the variance σ_n^2) and preshared to both encoder and decoder. If σ_n^2 changes significantly, we can adaptively increase A to reduce the BER, or decrease A to reduce the distortion of image. While such adaptive scheme can provide better BER distortion performance, it requires updating amplitude A between encoder and decoder via a secure channel which may cost much more complexity.

The SER of the SS embedding with precoding is

$$\text{SER} = 2Q\left(\frac{A}{\sigma_n}\right) \tag{33}$$

, and the BER with Gray-coded symbol is

$$\text{BER} = \frac{\text{SER}}{\log_2 M} = \frac{2}{\log_2 M} Q\left(\frac{A}{\sigma_n}\right). \tag{34}$$

Therefore, given a target BER, the required constellation separation is

$$A \geq \sigma_n Q^{-1}\left(\frac{\text{BER}}{2}\log_2 M\right). \tag{35}$$

Unlike the precancelation with regular modulation scheme in (23), the distortion induced by SS embedding with precoding is

$$\mathcal{D}_i = u_i^2 \leq M^2 A^2 \tag{36}$$

which does not grow unbounded with the interference z_i. If interference z_i is assumed having uniform distribution, then the MS distortion to the host is

$$\mathcal{D} = \mathbb{E}\{u_i^2\} = \frac{1}{3}M^2 A^2. \tag{37}$$

Generally, the distribution of interference z_i from the host is not uniform but can be modeled as generalized Gaussian or Laplace distribution with zero mean and variance $\sigma_z^2 > 0$. If $\sigma_z^2 = 0$ which means no interference presents, from (25) the distortion is $\mathcal{D} = \left(\frac{1}{3}M^2 - \frac{1}{3}\right)A^2$; if $\sigma_z^2 \to \infty$ which means the distribution of interference approaches to uniform, then $\mathcal{D} = \frac{1}{3}M^2A^2$. Thus, with a given A, the induced distortion has upper and lower bounds as

$$\left(\frac{1}{3}M^2 - \frac{1}{3}\right)A^2 \leq \mathcal{D} \leq \frac{1}{3}M^2A^2. \tag{38}$$

The closed-form relationship between distortion $\mathcal{D}$ and modulation separation A is too complicated for practical use, even host is modeled as generalized Gaussian or Laplace distribution. Therefore, we introduce instead following simple approximated expression

$$\mathcal{D} = \left(\frac{1}{3}M^2 - \frac{1}{3}e^{-\frac{\sigma_z}{4}}\right)A^2. \tag{39}$$

To validate this approximation, we carried out an experiment in Fig. 4 over more than 1,500 8-bit gray-scale photographic images ([27] and [33] combined). With a modulation separation A varying from 0.5 to 5, the true distortion obtained empirically and the distortion predicted by (39) are shown in Fig. 4 for both arbitrary carrier and optimal carrier cases. It can be concluded that the approximated form (39) can accurately illustrate the relationship between distortion $\mathcal{D}$ and modulation separation A. Given a distortion budget $\mathcal{D}$, we can use (39) to obtain an optimal constellation separation

$$A = \sqrt{\frac{3\mathcal{D}}{M^2 - e^{-\frac{\sigma_z}{4}}}} \tag{40}$$

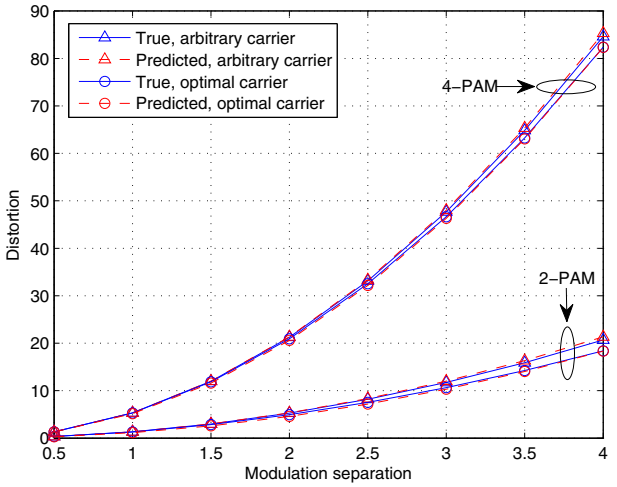


Fig. 4 Distortion versus modulation separation A, (average findings over a data set of more than 1500 images [27,33], 8×8 block partition, $L = 63$)

such that the induced distortion would not exceed the budget, and the probability of error is minimized at

$$\mathrm{BER} = \frac{2}{\log_2 M} Q\left(\sqrt{\frac{3\mathcal{D}}{\left(M^2 - e^{-\frac{\sigma_z}{4}}\right)\sigma_n^2}}\right). \tag{41}$$

When 2-PAM is used and the variance of interference σ_z^2 is small enough (close to zero), the BER for SS embedding with precoding in (41) can be approximated as $\mathrm{BER} = 2Q\left(\frac{\sqrt{\mathcal{D}}}{\sigma_n}\right)$. But for the precancelation with regular modulation (23) or SS embedding on linearly transformed host (11), the error probability can be approximated as $\mathrm{BER} = Q\left(\frac{\sqrt{\mathcal{D}}}{\sigma_n}\right)$, which is smaller by a factor of 1/2. The probability of error of SS embedding with precoding is larger because there is an additional possibility of confusion across replicas. However, the variance of interference is in general large enough such that SS embedding with precoding is superior in most cases. Even when small interference variance occurs (generally only when the optimal carrier is adopted), the performance degradation due to precoding is very small and negligible.

We evaluate the performance of six different embedding schemes: (i) SS embedding in (2) with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$, (ii) SS embedding in (2) with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$ in (7), (iii) SS embedding on linearly transformed host in (11) with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$ and an optimal transform parameter c^{opt} in (14), (iv) SS embedding on linearly transformed host in (11) with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$ in (17) and an optimal transform parameter c^{opt} in (14), (v) precoded SS embedding with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$, and (vi) precoded SS embedding with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$ in (7).

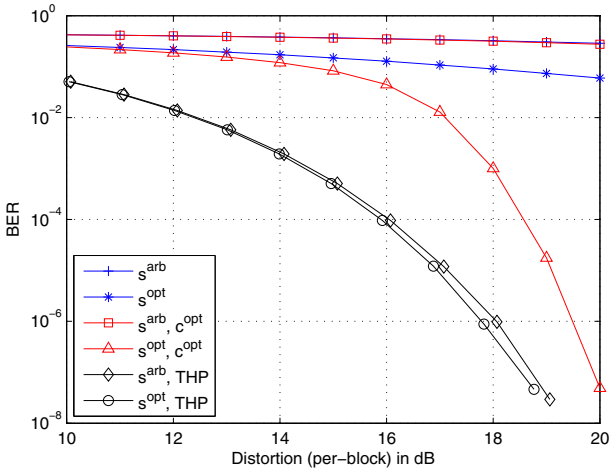


Fig. 5 BER versus per-block distortion, 2-PAM, (512 × 512 Baboon, 8 × 8 block partition, 4096 bits are embedded, $L = 63$, $\sigma_n^2 = 3$dB)

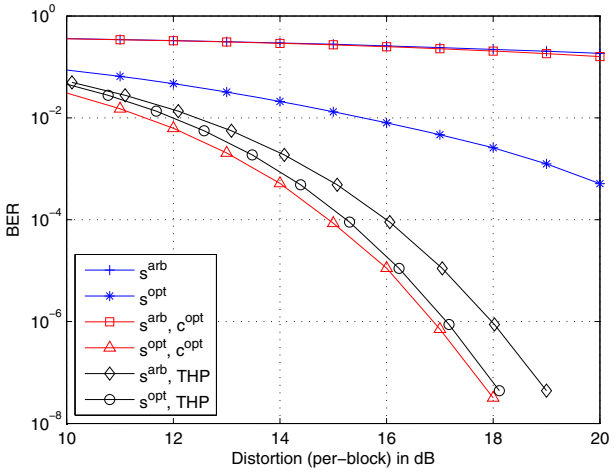


Fig. 6 BER versus per-block distortion, 2-PAM, (512 × 512 Boat, 8 × 8 block partition, 4096 bits are embedded, $L = 63$, $\sigma_n^2 = 3$dB)

4 Experimental Studies

To carry out an experimental study of the developments presented in the previous sections, we consider the familiar gray-scale 512 × 512 "Baboon" image as a host example. We perform 8 × 8 block DCT embedding over all 63 bins except the dc coefficient. For the sake of generality, we also incorporate white Gaussian noise of variance $\sigma_n^2 = 3$dB.

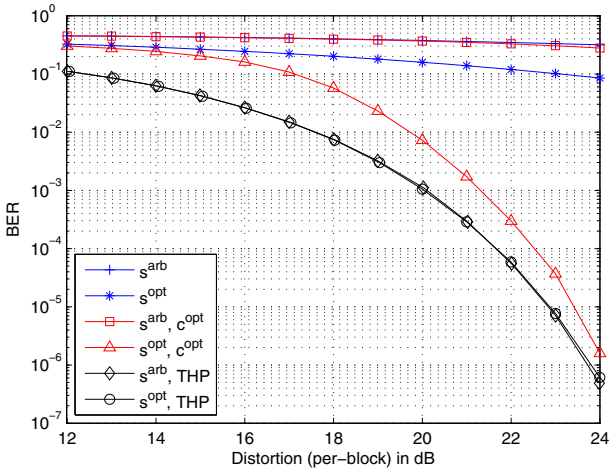


Fig. 7 BER versus per-block distortion, 4-PAM, (512×512 Baboon, 8×8 block partition, 8192 bits are embedded, $L = 63$, $\sigma_n^2 = 3$dB)

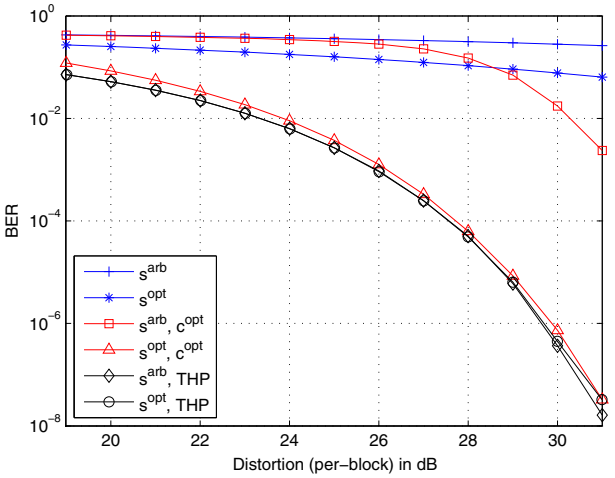


Fig. 8 BER versus per-block distortion, 8-PAM, (512×512 Baboon, 8×8 block partition, 12,288 bits are embedded, $L = 63$, $\sigma_n^2 = 3$dB)

Figure 5 shows the recovery BER for SS embedding with 2-PAM as a function of the MS per-block distortion.[2] Totally, 4096 bits are embedded in the Baboon image. It is demonstrated that the use of proposed symbol-by-symbol precoding can significantly improve the BER performance over traditional SS embedding schemes as well as recently developed SS embedding in transform domain host data with optimal

[2] With block MS distortion $\mathcal{D}$, the peak signal-to-noise ratio (PSNR) of the image due to embedding can be calculated by PSNR $= 20\log_{10}(255) - 10\log_{10}(\mathcal{D}/64)$. The embedding (watermarking) distortion to attack noise ratio (WNR) measure can also be easily obtained by WNR $= 10\log_{10}(\mathcal{D}/64/\sigma_n^2)$.

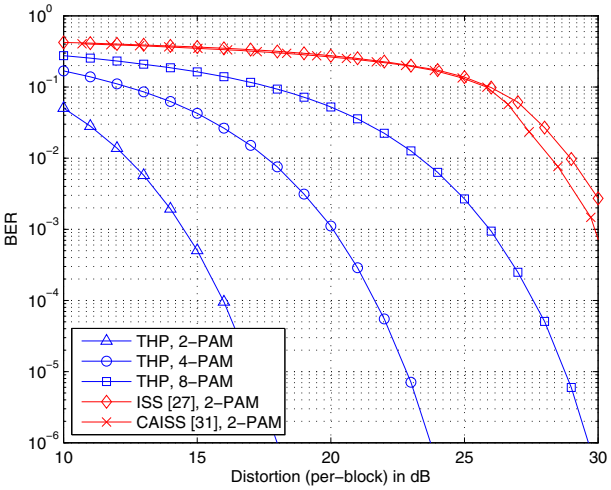


Fig. 9 BER versus per-block distortion (512 × 512 Baboon, 8 × 8 block partition, $L = 63$, $\sigma_n^2 = 3$dB)

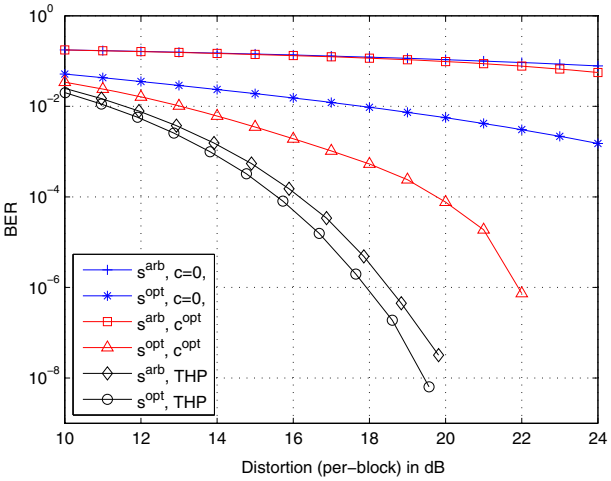


Fig. 10 BER versus per-block distortion, 2-PAM, (average findings over a data set of more than 1500 images [27,33], 8 × 8 block partition, $L = 63$, $\sigma_n^2 = 3$dB)

projection-like linear operator. It can also be observed that for precoded SS embedding, the recovery performance gap between arbitrary carrier and optimal carrier is very small while optimal carrier can significantly improve the recovery performance than arbitrary carrier for other SS embedding schemes. This implies that the performance of SS embedding with precoding is not notably affected by the selection of carrier.

In Fig. 6, we repeat the same experiment for gray-scale 512 × 512 "Boat" image. We notice that, when optimal carrier is used, SS embedding with precoding is slightly worse than SS embedding on linear transformed host. This is because that, as we discussed in the previous section, the variance of interference σ_z^2 is very low for Boat

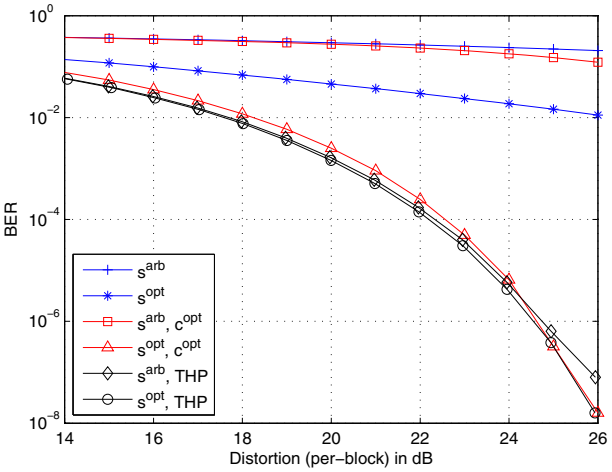


Fig. 11 BER versus per-block distortion, 4-PAM, (average findings over a data set of more than 1500 images [27,33], 8×8 block partition, $L = 63$, $\sigma_n^2 = 3$dB)

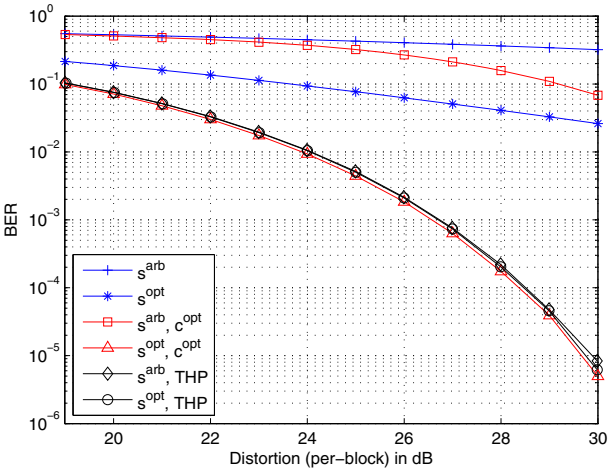


Fig. 12 BER versus per-block distortion, 8-PAM, (average findings over a data set of more than 1500 images [27,33], 8×8 block partition, $L = 63$, $\sigma_n^2 = 3$dB)

image when optimal carrier is adopted. But the performance gap is negligible, and SS embedding with precoding is still worth using.

In Figs. 7 and 8, we repeat the same experiment as Fig. 5 for 4-PAM and 8-PAM with Gray coding, respectively. The sizes of embedded data for these two experiments are 8192 and 12,288 bits, respectively. We notice that, when modulation order increases, $(\mathbf{s}^{\text{opt}}, c^{\text{opt}})$ embedding has performance close to the precoding approach. Yet, we should emphasize that the performance of precoding is almost independent of the carrier, i.e., as we can found from the figures, arbitrary carrier and optimal carrier have similar performance for the THP. This means that precoding scheme can simply use a preshared and fixed carrier for any image, and the performance can be always

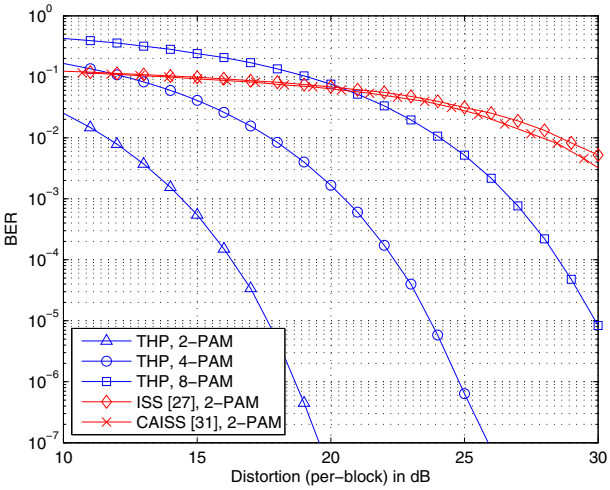


Fig. 13 BER versus per-block distortion, (average findings over a data set of more than 1500 images [27,33], 8×8 block partition, $L = 63$, $\sigma_n^2 = 3$dB)

maintained at a satisfactory level. However, to achieve such good performance, the $(\mathbf{s}^{\text{opt}}, c^{\text{opt}})$ embedding needs to re-calculate the optimal carrier for each image and sends it to the receiver via a secure channel which is complex and may not always be available. Therefore, SS embedding with precoding is always suggested due to its simplicity (no need of a secure channel), superior performance, and carrier independence. To further illustrate the recovery performances for different modulation orders, in Fig. 9, we show the performance curves of precoded SS embedding using 2-PAM, 4-PAM, and 8-PAM. For the comparison purpose, we also include the famous improved spread-spectrum (ISS) embedding [22] and recently proposed correlation-aware improved spread-spectrum (CAISS) embedding [34]. We can found that the SS embedding with precoding has much better recovery performance than ISS and CAISS.

To address the need for experimental verification of highest credibility, now we examine the average performance of the proposed precoded SS embedding algorithm over a large image database. The experimental image data set consists of more than 1500 8-bit gray-scale photographic images ([27] and [33] combined) which have great variety (e.g., outdoor/indoor, daylight/night, and natural/man-made) and different sizes. Recovery performance plots are given in Figs. 10, 11 and 12. Similar conclusion can be drawn as in previous individual image host experimentations. Finally, in Fig. 13, we show the average BER performance of THP with 2-PAM, 4-PAM, and 8-PAM and also include the SS embedding algorithms in [22] and [34]. We can conclude that the SS embedding with TH precoding is superior to other counterparts.

5 Conclusion

In this work, we focused on additive M-PAM spread-spectrum (SS) data embedding in transform domain host data. We utilized the idea of Tomlinson–Harashima precod-

ing (THP) which is a practical dirty paper coding implementation for communication systems. A symbol-by-symbol precoding approach was designed for SS embedding to minimize BER with any given distortion budget, and conversely minimize the distortion at any target BER. Experimental studies demonstrated that this symbol-by-symbol precoded SS embedding approach can significantly improve the BER performance and is superior over other conventional SS embedding schemes.

Acknowledgments This work is supported by the Fundamental Research Funds for the Central Universities (Grant No. DUT14RC(3)103), the Research Fund for the Doctoral Program of Liaoning Province (Grant No. 20131014), the National Natural Science Foundation of China (Grant No. 61402079).

Appendix

Proof of Proposition 2 With SS embedding signal (11), the output SINR of MF is

$$\begin{aligned}\mathrm{SINR} &= \frac{\mathbb{E}\{\|Ab_i\|^2\}}{\mathbb{E}\left\{\|\mathbf{s}^T((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i + \mathbf{n})\|^2\right\}} \qquad (42)\\ &= \frac{\frac{3}{M^2-1}A^2}{\mathbf{s}^T\left((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{R}_{\mathrm{x}}(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T) + \sigma_n^2\mathbf{I}\right)\mathbf{s}}\\ &= \frac{\frac{3}{M^2-1}A^2}{\mathbf{s}^T\mathbf{R}_{\mathrm{x}}\mathbf{s} - 2c\mathbf{s}^T\mathbf{R}_{\mathrm{x}}\mathbf{s} + c^2\mathbf{s}^T\mathbf{R}_{\mathrm{x}}\mathbf{s} + \sigma_n^2}\\ &= \frac{\frac{3}{M^2-1}A^2}{\alpha - 2c\alpha + c^2\alpha + \sigma_n^2} \qquad (43)\end{aligned}$$

where we define $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\mathrm{x}}\mathbf{s}$. By applying $\mathcal{D} = \frac{3}{M^2-1}A^2 + c^2\mathbf{s}^T\mathbf{R}_{\mathrm{x}}\mathbf{s} = \frac{3}{M^2-1}A^2 + c^2\alpha$ into (43), we obtain

$$\mathrm{SINR} = \frac{\mathcal{D} - c^2\alpha}{\alpha - 2c\alpha + c^2\alpha + \sigma^2} \qquad (44)$$

By direct differentiation of the (44) with respect to c and root selection, we obtain $c^{\mathrm{opt}} = \frac{\alpha+\sigma_n^2+\mathcal{D}-\sqrt{(\alpha+\sigma_n^2+\mathcal{D})^2-4\alpha\mathcal{D}}}{2\alpha}$ in (14). With optimal transform parameter c^{opt}, the optimal amplitude A^{opt} and the maximum SINR can be easily calculated.

The SINR in (44) is a monotonically decreasing function of $\alpha \geq 0$. Therefore, the optimal carrier $\mathbf{s}$, which minimizes $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\mathrm{x}}\mathbf{s}$, is the eigenvector of $\mathbf{R}_{\mathrm{x}}$ with minimum eigenvalue

$$\mathbf{s}^{\mathrm{opt}} = \mathbf{q}_L. \qquad (45)$$

With this optimal carrier, the identity of match filter and maximum SINR filter has be proved in Proposition 3 in [12]. □

References

1. A. Abrardo, M. Barni, A new watermarking scheme based on antipodal binary dirty paper coding. IEEE Trans. Inf. Forensics Secur. **9**(6), 1380–1393 (2014)

2. C.B. Adsumilli, M.C.Q. Farias, S.K. Mitra, M. Carli, A robust error concealment technique using data hiding for image and video transmission over lossy channels. IEEE Trans. Circuits Syst. Video Technol. **15**(11), 1394–1406 (2005)
3. M. Barni, F. Bartolini, A. De Rosa, A. Piva, A new decoder for the optimum recovery of nonadditive watermarks. IEEE Trans. Image Process. **10**(8), 755–766 (2001)
4. M. Barni, F. Bartolini, A. De Rosa, A. Piva, Optimum decoding and detection of multiplicative watermarks. IEEE Trans. Signal Process. **51**(5), 1118–1123 (2003)
5. H. Cao, A.C. Kot, On establishing edge adaptive grid for bilevel image data hiding. IEEE Trans. Inf. Forensics Secur. **8**(9), 1508–1518 (2013)
6. M.H.M. Costa, Writing on dirty paper. IEEE Trans. Inf. Theory **29**(3), 439–441 (1983)
7. I.J. Cox, J. Kilian, F.T. Leighton, T. Shannon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. **6**(12), 1673–1687 (1997)
8. X. Feng, H. Zhang, H.-C. Wu, Y. Wu, A new approach for optimal multiple watermarks injection. IEEE Signal Proc. Lett. **18**(10), 575–578 (2011)
9. B. Feng, W. Lu, W. Sun, Secure binary image steganography based on minimizing the distortion on the texture. IEEE Trans. Inf. Forensics Secur. **10**(2), 243–255 (2015)
10. J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications* (Cambridge Univeristy Press, Cambridge, 2010)
11. M. Gkizeli, D.A. Pados, M.J. Medley, SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography, in *Proceedings IEEE International Conference on Image Processing (ICIP)*, Singapore, Oct. 2004, pp. 1561–1564
12. M. Gkizeli, D.A. Pados, M.J. Medley, Optimal signature design for spread-spectrum steganography. IEEE Trans. Image Process. **16**(2), 391–405 (2007)
13. S. Glisic, B. Vucetic, *Spread Spectrum CDMA Systems for Wireless Communications* (Artech House, Norwood, MA, 1997)
14. H. Harashima, H. Miyakawa, Matched-transmission technique for channels with intersymbol interference. IEEE Trans. Commun. **20**(4), 774–780 (1972)
15. J. Hernandez, M. Amado, F. Pérez-González, DCT-domain watermarking techniques for still images: detector performance analysis and a new structure. IEEE Trans. Image Process. **9**(1), 55–68 (2000)
16. Y. Huang, C. Liu, S. Tang, S. Bai, Steganography integration into a low-bit rate speech codec. IEEE Trans. Inf. Forensics Secur. **7**(6), 1865–1875 (2012)
17. M. Kutter, S. Winkler, A vision-based masking model for spreadspectrum image watermarking. IEEE Trans. Image Process. **11**(1), 16–25 (2002)
18. E.Y. Lam, J.W. Goodman, A mathematical analysis of the DCT coefficient distributions for images. IEEE Trans. Image Process. **9**(10), 1661–1666 (2000)
19. M. Li, M. Kulhandjian, D.A. Pados, S.N. Batalama, M.J. Medley, J.D. Matyjas, On the extraction of spread-spectrum hidden data in digital media, in *Proceedings on International Conference on Communications (ICC)*, Ottawa, Canada, June 2012, pp. 1046–1050
20. M. Li, M. Kulhandjian, D.A. Pados, S.N. Batalama, M.J. Medley, Extracting spread-spectrum hidden data from digital media. IEEE Trans. Inf. Forensics Secur. **8**(7), 1201–1210 (2013)
21. S.-C. Liu, W.-H. Tsai, Line-based cubism-like image—a new type of art image and its application to lossless data hiding. IEEE Trans. Inf. Forensics Secur. **7**(5), 1448–1458 (2012)
22. H.S. Malvar, D.A. Florencio, Improved spread spectrum: a new modulation technique for robust watermarking. IEEE Trans. Signal Process. **51**(4), 898–905 (2003)
23. L.M. Marvel Jr, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography. IEEE Trans. Image Process. **8**, 1075–1083 (1999)
24. P. Moulin, A. Ivanović, The zero-rate spread-spectrum watermarking game. IEEE Trans. Signal Process. **51**(4), 1098–1117 (2003)
25. S. Pereira, S. Voloshynovskiy, T. Pun, Optimized wavelet domain watermark embedding strategy using linear programming, in *Proceedings on SPIE Wavelet Applications Conference*, Orlando, FL, April 2000, vol. 4056, pp. 490–498
26. C. Qiang, T.S. Huang, An additive approach to transform-domain information hiding and optimum detection structure. IEEE Trans. Multimed. **3**(3), 273–284 (2001)
27. G. Schaefer, M. Stich, UCID–an uncompressed colour image database, in *Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multimedia*, San Jose, CA, Jan. 2004, pp. 472–480
28. M.D. Swanson, M. Kobayashi, A.H. Tewfik, Multimedia data-embedding and watermarking technologies. Proc. IEEE **86**(6), 1064–1087 (1998)

29. Y. Tew, K. Wong, An overview of information hiding in H.264/AVC compressed video. IEEE Trans. Circuits Syst. Video Technol. **24**(2), 305–319 (2014)
30. H. Tian, Y. Zhao, R. Ni, L. Qin, X. Li, LDFT-based watermarking resilient to local desynchronization attacks. IEEE Trans. Cybern. **43**(6), 2190–2201 (2013)
31. M. Tomlinson, New automatic equalizer employing modulo arithmetic. Electron. Lett. **7**(5), 138–139 (1971)
32. H.-W. Tseng, H.-S. Leng, High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion. IET Image Process. **8**(11), 647–654 (2014)
33. *USC-SIPI Image Database*. Available: http://sipi.usc.edu/database/database.cgi?volume=misc
34. A. Valizadeh, Z.J. Wang, Correlation-and-bit-aware spread spectrum embedding for data hiding. IEEE Trans. Inf. Forensics Secur. **6**(2), 267–282 (2011)
35. Y. Wang, P. Moulin, Perfectly secure steganography: capacity, error exponents, and code constructions. IEEE Trans. Inf. Theory **54**(6), 2706–2722 (2008)
36. L. Wei, D.A. Pados, S.N. Batalama, M.J. Medley, Sum-SINR/sum-capacity optimal multisignature spread-spectrum steganography, in *Proceedings of SPIE, Mobile Multimedia/Image Processing, Security, and Applications Conference, SPIE Defense and Security Symposium*, Orlando, FL, March 2008, vol. 6982, pp. 0D1–0D10
37. X.G. Xia, C.G. Boncelet, G.R. Arce, A multiresolution watermark for digital images, in *Proceedings IEEE International Conference on Image Processing (ICIP)*, Santa Barbara, CA, Oct. 1997, vol. 1, pp. 548–551
38. Y. Yi, R. Li, F. Chen, A.X. Liu, Y. Lin, A digital watermarking approach to secure and precise range query processing in sensor networks, in *Proceedings on IEEE INFOCOM*, Turin, Italy, April 2013, pp. 1950–1958
39. M. Zareian, H.R. Tohidypour, Robust quantisation index modulation-based approach for image watermarking. IET Image Process. **7**(5), 432–441 (2013)