Signal Processing: *Image Communication* 39 (2015) 17–25

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

Secure spread-spectrum data embedding with PN-sequence masking

Ming Li, Yanqing Guo, Bo Wang *, Xiangwei Kong

School of Information and Communication Engineering, Dalian University of Technology, Dalian, Liaoning 116024, PR China

ARTICLE INFO

Article history:
Received 21 January 2015
Received in revised form
30 July 2015
Accepted 30 July 2015
Available online 10 August 2015

Keywords:
Data hiding
Information hiding
Pseudo-noise masking
Signal-to-interference-plus-noise ratio (SINR)
Spread-spectrum embedding
Steganography

ABSTRACT

Conventional additive spread-spectrum (SS) data embedding has a dangerous security flaw that unauthorized receivers can blindly extract hidden information without the knowledge of carrier(s). In this paper, pseudo-noise (PN) masking technique is adopted as an efficient security measure against illegitimate data extraction. The proposed PN-sequence masked SS embedding can offer efficient security against current SS embedding analysis without inducing any additional distortion to host nor notable recovery performance loss. To further improve recovery performance, optimal carrier design for PN-masked SS embedding is also developed. With any given host distortion budget, we aim at designing a carrier to maximize the output signal-to-interference-plus-noise ratio (SINR) of the corresponding maximum-SINR linear filter. Then, we present jointly optimal carrier and linear processor designs for PN-masked SS embedding in linearly modified transform domain host data. Finally, PN-masked multi-carrier/multi-message SS embedding is studied as well. The extensive experimental studies confirm our analytical performance predictions and illustrate the benefits of the designed PN masked optimal SS embedding.

1. Introduction

Information hiding, which is also called as digital data embedding, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio [1,2]. Applications may vary from annotation, copyright-marking, and watermarking to single-stream media merging (text, audio, image) and covert communication [3–8]. As a general encompassing comment, different applications of information hiding, such as the ones identified above, require different satisfactory tradeoffs between the following four basic attributes of data hiding [9]: (i) payload – information delivery rate; (ii) robustness – hidden data resistance to noise/disturbance; (iii) transparency – low host distortion for concealment purposes; and (iv) security – inability by unauthorized users to detect/access the covert communication channel.

The data hiding performance in terms of above four attributes depends directly on how the data is inserted in the host. Therefore, it is a crucial step to determine the embedding process in the design of a data hiding system. Data embedding can be performed either directly in the time (audio) or spatial (image) domain [10–14] or in a transform domain [15–26]. While direct embedding in the original host signal domain may be desirable for system complexity purposes, embedding in a transform domain may take advantage of the particular transform domain properties [27] and enables the powerful notion of spread-spectrum

* Corresponding author.
E-mail addresses: mli@dlut.edu.cn (M. Li), guoyq@dlut.edu.cn (Y. Guo), bowang@dlut.edu.cn (B. Wang), kongxw@dlut.edu.cn (X. Kong).

http://dx.doi.org/10.1016/j.image.2015.07.014
0923-5965/

(SS) data embedding when the secret signal is spread over a wide range of host frequencies [28–32].

In this paper, we focus our attention on additive SS embedding in transform domain host. In direct analogy to SS digital communication systems [33], conventional additive SS embedding methods use an equal-amplitude modulated carrier/signature to deposit one information symbol across a group of host data coefficients or a linearly transformed version of the host data coefficients. Recently, a dangerous security flaw of SS embedding has been alerted and investigated. Embedding a number of information symbols with a same carrier will create a strong basis/subspace of the hidden signal which can be tracked and analyzed. Therefore, even without the knowledge of carrier (s), unauthorized receivers can still blindly extract the embedded data by blind signal separation (BBS) methods [34–37] or novel iterative generalized least square (IGLS) approaches [38,39]. The illegitimate blind hidden data extraction has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context [34–37]. Thus, it raises the concerns of making SS embedding more difficult to be extracted by the illegitimate users. Two interesting SS embedding schemes were proposed in [40] which attempt to withstand SS embedding analysis by using random-like amplitudes. However, these SS embedding schemes sacrifice recovery performance to enhance the security and consequently are sensitive to noise which would lead to high recovery error rates by intended recipients. More importantly, information leakage cannot be fully prevented because information symbols are still embedded by the same carrier.

Pseudo-noise (PN) masking technique has been proven to be an effective technique against unauthorized data collection (eavesdropping) in the context of secure wireless communications. Typical examples of PN masking technique are military-grade communications and global-positioning systems (GPS). In this work, we first develop a PN-masked secure SS embedding approach in which the embedded SS single is scrambled by random-like PN masks such that no subspace of embedded signal can be found and tracked in the data-embedded host. With our proposed PN masked SS embedding scheme, the performance in terms of recovery bit-error-rate (BER) at the intended receiver is maintained at almost the same level as the conventional SS embedding (i.e. almost no performance loss), while the unauthorized users will have BER close to 0.5 (i.e. almost perfect security). Since the proposed PN masked SS embedding schemes can efficiently minimize the likelihood that embedded data are "stolen" by the unauthorized users, they are suitable for the applications with high security requirement, such as steganography and covert communications.

It should also be understood that the host, which acts as a source of interference to the secret message of interest, is known to the message embedder. Such knowledge can be exploited appropriately to facilitate the task of the blind receiver at the other end and minimize the recovery error rate for a given host distortion level, minimize host distortion for a given target recovery error rate, maximize the Shannon capacity of the covert channel, etc. By exploiting the knowledge of the second order statistics (SOS) of host, the recently presented Gkizeli–Pados–Medley eigen-design optimal carrier [29,30] can maximize the signal-to-interference-noise-ratio (SINR) at the output of the corresponding maximum-SINR linear filter. Benefiting from the legacy of [29,30], the optimal carrier design for PN-masked SS embedding is also studied.

The rest of the paper is organized as follows. Section 2 briefly reviews the prior art on additive SS embedding. PN-masked SS embedding is present in Section 3. These results are generalized to multi-carrier embedding in Section 4. Section 5 is devoted to experimental studies and comparisons. A few concluding remarks are drawn in Section 6.

The following notation is used throughout the paper. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{R}$ denotes the set of all real 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.

2. Prior art of additive SS embedding

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 M local non-overlapping blocks of size $N_1 N_2/M$. Each block, $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_M$, is to carry one hidden information bit $b_i \in \{\pm 1\}$, $i = 1, 2, \ldots, M$, respectively. Embedding is performed in a 2-D transform domain $\mathcal{T}$ (such as the discrete cosine transform and a wavelet transform). After transform calculation and vectorization (for example by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_i) \in \mathbb{R}^{N_1 N_2/M}, i = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_i)$ we choose a fixed subset of $L \le N_1 N_2/M$ coefficients (bins) to form the final host vectors $\mathbf{x}_i \in \mathbb{R}^L$, $i = 1, 2, \ldots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

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 host). 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

$$\mathbf{y}_i = A b_i \mathbf{s} + \mathbf{x}_i + \mathbf{n}_i, \quad i = 1, \ldots, M, \tag{1}$$

where information bit $b_i \in \{\pm 1\}$ is embedded in the transform domain host vector $\mathbf{x}_i \in \mathbb{R}^L$ via additive SS embedding by means of a (normalized) spreading sequence (carrier/signature) $\mathbf{s} \in \mathbb{R}^L$, $\|\mathbf{s}\| = 1$, 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 $\sigma_n^2 \mathbf{I}_L$, $\sigma_n^2 > 0$.

In an effort to reduce the interference effect of the host signal, the host vectors $\mathbf{x}_i$, $i = 1, \ldots, M$, can be steered away from the embedding carrier using an operator of the form

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

$(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)$ with parameter $c \in \mathbb{R}$, $i = 1, \ldots, M$, and the carrier $\mathbf{s} \in \mathbb{R}^L$. In parallel to (1), the composite signal of additive SS embedding on linearly transformed host data is [28,30]

$$\mathbf{y}_i = Ab_i\mathbf{s} + (\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i + \mathbf{n}_i, \quad i = 1, \ldots, M, \tag{2}$$

where information symbol bit $b_i \in \{\pm 1\}$ 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 optimal carrier $\mathbf{s}$ and transform parameter c to maximize the output SINR are presented in Proposition 3 of [30].

The SS embedding schemes (1) and (2) have been shown to have a dangerous security flaw. Using the same carrier $\mathbf{s}$ to embed all information bits can generate a strong basis/subspace of embedded signal in data-embedded host $\mathbf{y}_i$, $i = 1, \ldots, M$. By analyzing observation signal $\mathbf{y}_i$ with BBS-based algorithms [34–37] or a novel IGLS approach [39], embedded information bits can be blindly extracted by unauthorized users without the knowledge of carrier $\mathbf{s}$. Using random-like amplitudes [40] can weaken SS embedding analysis to a certain degree, but still has the problem of information leakage and suffers from loss of recovery performance. To practically provide a secure SS embedding, in the next section we adopt PN-sequence masking technique on SS embedding to protect the secret data without any notable performance loss.

3. PN-sequence masked SS embedding

Let $\mathbf{m} = [m_1, m_2, \ldots, m_N]^T \in \{\pm 1\}^N$ be a PN-sequence (such as m-sequence or Gold code) of large length $N \geq LM$. We select M non-overlap segments from $\mathbf{m}$ as mask vectors $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_M$ of length L each

$$\mathbf{m}_i \triangleq [m_{(i-1)L+1}, \ldots, m_{iL}]^T, \quad i = 1, \ldots, M. \tag{3}$$

The PN-mask vector $\mathbf{m}_i$ is used to scramble the SS signal of interest $Ab_i\mathbf{s}$ by component-wise multiplication of carrier $\mathbf{s}$ and $\mathbf{m}_i$. PN-masked carrier for the ith bit b_i is defined as

$$\mathbf{c}_i \triangleq \mathbf{s} \odot \mathbf{m}_i \triangleq [\mathbf{s}(1)\mathbf{m}_i(1), \mathbf{s}(2)\mathbf{m}_i(2), \ldots, \mathbf{s}(L)\mathbf{m}_i(L)]^T \tag{4}$$

where $\odot$ denotes component-wise vector multiplication. Since the mask vector $\mathbf{m}_i$ just pseudo-randomly flips each element of $\mathbf{s}$, then with a normalized regular carrier $\|\mathbf{s}\| = 1$, the PN-masked carriers are also normalized $\|\mathbf{c}_i\| = 1$, $i = 1, \ldots, M$.

Instead of using the same carrier $\mathbf{s}$, information bit $b_i \in \{\pm 1\}$ is embedded in host $\mathbf{x}_i$ by means of a PN-masked carrier $\mathbf{c}_i \in \mathbb{R}^L$, $\|\mathbf{c}_i\| = 1$

$$\mathbf{y}_i = Ab_i\mathbf{c}_i + \mathbf{x}_i + \mathbf{n}_i, \quad i = 1, \ldots, M, \tag{5}$$

with an embedding amplitude $A > 0$. With random-like PN-masked carriers, the SS signal of interest $Ab_i\mathbf{c}_i$ behaves like white noise and no subspace of embedded signal can be tracked from the observation data $\mathbf{y}_i$. Therefore, PN-masked SS embedding in (5) can efficiently prevent illegitimate data extraction by unauthorized users who have no knowledge of PN masks.

Squared Euclidean metric is rudimentary but common choice to measure the distortion to host. The mean-squared (MS) distortion to the host *due to the embedded data only* is

$$\mathcal{D} = \mathbb{E}\,\|(Ab_i\mathbf{c}_i + \mathbf{x}_i) - \mathbf{x}_i\|^2 = A^2. \tag{6}$$

The MS distortion of PN-masked SS embedding depends only on the embedding amplitudes and PN-sequence masking operation would not induce any more distortion to host.

Recovery of the embedded information bits at the intended receiver requires use of a replica PN generator to "strip-off" the mask by following operation:

$$\begin{aligned}\tilde{\mathbf{y}}_i &= \mathbf{y}_i \odot \mathbf{m}_i \\ &= Ab_i\mathbf{s} \odot \mathbf{m}_i \odot \mathbf{m}_i + \mathbf{x}_i \odot \mathbf{m}_i + \mathbf{n}_i \odot \mathbf{m}_i \\ &= Ab_i\mathbf{s} + \tilde{\mathbf{x}}_i + \tilde{\mathbf{n}}_i\end{aligned} \tag{7}$$

where $\tilde{\mathbf{x}}_i \triangleq \mathbf{x}_i \odot \mathbf{m}_i$ is PN-masked host vector, $\tilde{\mathbf{n}}_i \triangleq \mathbf{n}_i \odot \mathbf{m}_i$. After mask removal, the PN-masked SS embedding in (7) has a similar form to the conventional SS embedding in (1) with PN-masked host $\tilde{\mathbf{x}}_i$ instead of original host vector $\mathbf{x}_i$. Since PN masking operation at the intended receiver just randomly flips the host coefficients and the external noise, the total disturbance $(\tilde{\mathbf{x}}_i + \tilde{\mathbf{n}}_i)$ to the signal of interest $Ab_i\mathbf{s}$ would not be amplified.

The embedded bits can be recovered by looking at the sign of the output of a filter $\mathbf{w} \in \mathbb{R}^L$

$$\hat{b}_i = \mathrm{sgn}\{\mathbf{w}^T\tilde{\mathbf{y}}_i\}. \tag{8}$$

In current data hiding applications, simple matched filter (MF)

$$\mathbf{w}_{\mathrm{MF}} = \mathbf{s} \tag{9}$$

has been widely used by the intended receiver to recover embedded bits. With signal of interest $Ab_i\mathbf{s}$ and total disturbance $(\tilde{\mathbf{x}}_i + \tilde{\mathbf{n}}_i)$ in (7) after mask removal operation at the intended receiver, the output SINR of filter $\mathbf{w}$ is

$$\mathrm{SINR} = \frac{\mathbb{E}\{\|Ab_i(\mathbf{w}^T\mathbf{s})\|^2\}}{\mathbb{E}\{\|\mathbf{w}^T(\tilde{\mathbf{x}}_i + \tilde{\mathbf{n}}_i)\|^2\}} = \frac{A^2\mathbf{w}^T\mathbf{s}\mathbf{s}^T\mathbf{w}}{\mathbf{w}^T(\mathbf{R}_{\tilde{\mathbf{x}}} + \sigma_n^2\mathbf{I}_L)\mathbf{w}} \tag{10}$$

where

$$\mathbf{R}_{\tilde{\mathbf{x}}} \triangleq \mathbb{E}\{\tilde{\mathbf{x}}_i\tilde{\mathbf{x}}_i^T\} = \frac{1}{M}\sum_{i=1}^{M}\tilde{\mathbf{x}}_i\tilde{\mathbf{x}}_i^T \tag{11}$$

is the autocorrelation matrix of PN-masked host vectors. The linear filter that offers maximum SINR at its output is [41]

$$\mathbf{w}_{\mathrm{maxSINR}} = (\mathbf{R}_{\tilde{\mathbf{x}}} + \sigma_n^2\mathbf{I}_L)^{-1}\mathbf{s}. \tag{12}$$

The exact maximum output SINR value attained is

$$\mathrm{SINR}_{\max} = A^2\mathbf{s}^T(\mathbf{R}_{\tilde{\mathbf{x}}} + \sigma_n^2\mathbf{I}_L)^{-1}\mathbf{s}. \tag{13}$$

We can view $\mathrm{SINR}_{\max}$ as a function of the embedding carrier $\mathbf{s}$ and identify the signature that maximizes the SINR at the output of the maximum SINR filter. Our findings are presented in the form of a proposition below that parallels the developments in [30] for the conventional SS embedding case. The proof is straightforward and omitted.

Proposition 1. *Consider PN-masked SS embedding by (5). The optimal carrier* $\mathbf{s}^{\mathrm{opt}} \in \mathbb{R}^L$ *that maximizes the output SINR*

of the maximum-SINR filter $\mathbf{w}_{\text{maxSINR}}$ *is*

$$\mathbf{s}^{\text{opt}} = \mathbf{q}_L \tag{14}$$

where $\mathbf{q}_L$ *is the eigenvector of autocorrelation matrix* $\mathbf{R}_{\tilde{x}}$ *in (11) with the smallest corresponding eigenvalue* λ_L. *When* $\mathbf{s}^{\text{opt}} = \mathbf{q}_L$, *the maximum-SINR filter with this optimal carrier is also a matched filter*

$$\mathbf{w}_{\text{maxSINR}} \equiv \mathbf{w}_{\text{MF}} = \mathbf{q}_L. \square \tag{15}$$

Now we turn our attention on PN-masked SS embedding on linearly transformed SS embedding which is modeled in a form of

$$\mathbf{y}_i = Ab_i\mathbf{c}_i + (\mathbf{I}_L - c\mathbf{c}_i\mathbf{c}_i^T)\mathbf{x}_i + \mathbf{n}_i,\ i = 1, \ldots, M, \tag{16}$$

where $\mathbf{c}_i \triangleq \mathbf{s} \odot \mathbf{m}_i$ is the PN-masked carrier. The host vector $\mathbf{x}_i$ is linearly transformed by $(\mathbf{I}_L - c\mathbf{c}_i\mathbf{c}_i^T)$ which is formed by the corresponding PN-masked carrier $\mathbf{c}_i$.

The intended receiver first removes the masks from $\mathbf{y}_i$ by

$$\begin{aligned}\tilde{\mathbf{y}}_i &= \mathbf{y}_i \odot \mathbf{m}_i \\ &= (Ab_i\mathbf{c}_i + \mathbf{x}_i - c\mathbf{c}_i\mathbf{c}_i^T\mathbf{x}_i + \mathbf{n}_i) \odot \mathbf{m}_i \\ &= Ab_i\mathbf{c}_i \odot \mathbf{m}_i + \mathbf{x}_i \odot \mathbf{m}_i - c(\mathbf{c}_i^T\mathbf{x}_i)(\mathbf{c}_i \odot \mathbf{m}_i) + \mathbf{n}_i \odot \mathbf{m}_i.\end{aligned} \tag{17}$$

With $\mathbf{c}_i^T\mathbf{x}_i = (\mathbf{s} \odot \mathbf{m}_i)^T\mathbf{x}_i = \mathbf{s}^T(\mathbf{m}_i \odot \mathbf{x}_i)$ and $\mathbf{c}_i \odot \mathbf{m}_i = \mathbf{s}$, mask-removed signal in (17) can be rewritten as

$$\begin{aligned}\tilde{\mathbf{y}}_i &= Ab_i\mathbf{s} + \mathbf{x}_i \odot \mathbf{m}_i - c(\mathbf{s}^T(\mathbf{m}_i \odot \mathbf{x}_i))\mathbf{s} + \mathbf{n}_i \odot \mathbf{m}_i \\ &= Ab_i\mathbf{s} + \tilde{\mathbf{x}}_i - c(\mathbf{s}^T\tilde{\mathbf{x}}_i)\mathbf{s} + \tilde{\mathbf{n}}_i \\ &= Ab_i\mathbf{s} + (\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\tilde{\mathbf{x}}_i + \tilde{\mathbf{n}}_i\end{aligned} \tag{18}$$

where $\tilde{\mathbf{x}}_i \triangleq \mathbf{x}_i \odot \mathbf{m}_i$, $\tilde{\mathbf{n}}_i \triangleq \mathbf{n}_i \odot \mathbf{m}_i$. Now PN-masked SS embedding on linearly transformed host is similar to the non-PN-masked one in (2).

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

$$\begin{aligned}\mathcal{D} &= \mathbb{E}\left\{ \| \left(Ab_i\mathbf{c}_i + (\mathbf{I}_L - c\mathbf{c}_i\mathbf{c}_i^T)\mathbf{x}_i\right) - \mathbf{x}_i \|^2 \right\} \\ &= \mathbb{E}\left\{ \| \left(Ab_i - c\mathbf{c}_i^T\mathbf{x}_i\right)\mathbf{c}_i \|^2 \right\} \\ &= \mathbb{E}\left\{ \| Ab_i - c\mathbf{s}^T\tilde{\mathbf{x}}_i \|^2 \right\} \\ &= A^2 + c^2\mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s}.\end{aligned} \tag{19}$$

It should be noticed that, in contrast to (6), the distortion level is controlled not only by A but also by c. Compared to conventional SS embedding in (5), SS embedding on linearly transformed host uses part of available distortion to pre-suppress the interference at the embedding side and then utilizes the remaining distortion to embed information bits. The joint optimal carrier $\mathbf{s}$, amplitude A, and transformation parameter c design to maximize output SINR are summarized in Proposition 2 below whose proof is similar to Proposition 3 in [30] and omitted.

Proposition 2. *Consider PN-masked SS embedding in linearly transformed host data by (16). Let* $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_L$ *be eigenvectors of* $\mathbf{R}_{\tilde{x}}$ *in (11) with corresponding eigenvalues* $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$. *For any hidden message-induced distortion budget* $\mathcal{D}$, *the optimal carrier* $\mathbf{s}$, *amplitude* A, *and transformation parameter* c *to maximize SINR are*

$$\mathbf{s}^{\text{opt}} = \mathbf{q}_L, \tag{20}$$

$$c^{\text{opt}} = \frac{\lambda_L + \sigma_n^2 + \mathcal{D} - \sqrt{(\lambda_L + \sigma_n^2 + \mathcal{D})^2 - 4\lambda_L\mathcal{D}}}{2\lambda_L}, \tag{21}$$

$$A = \sqrt{\mathcal{D} - c^2\lambda_L}. \tag{22}$$

When $\mathbf{s}^{\text{opt}} = \mathbf{q}_L$ *and* $c = c^{\text{opt}}$, *then maximum SINR filter simplifies to*

$$\mathbf{w}_{\text{maxSINR}} = \mathbf{w}_{\text{MF}} = \mathbf{q}_L. \square \tag{23}$$

Adaptive optimal carrier design can significantly improve recovery performance. However, when host image is changed, the embedder needs to re-design the optimal carrier and re-transmit it to the intended receiver via a secure channel. This operation may be not applicable for some data hiding applications. In the most common data hiding cases, the carrier is pre-defined and known for both embedder and receiver. For any arbitrary carrier $\mathbf{s}$, the optimal separation of distortion budget to maximize the output SINR is presented in the form of a proposition below.

Proposition 3. *Consider PN-masked SS embedding in linearly transformed host data by (16) and matched filter* $\mathbf{w}_{\text{MF}} = \mathbf{s}$ *is used for embedded bits recovery. For any hidden message-induced distortion budget* $\mathcal{D}$ *and carrier* $\mathbf{s}$, *the optimal amplitude* A *and transformation parameter* c *to maximize SINR are*

$$c^{\text{opt}} = \frac{\alpha + \sigma_n^2 + \mathcal{D} - \sqrt{(\alpha + \sigma_n^2 + \mathcal{D})^2 - 4\alpha\mathcal{D}}}{2\alpha}, \tag{24}$$

$$A = \sqrt{\mathcal{D} - c^2\alpha}, \tag{25}$$

where $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s}$. $\square$

Proof. With SS embedding signal (17) after mask removal, the output SINR of MF is

$$\text{SINR} = \frac{\mathbb{E}\{\| Ab_i \|^2\}}{\mathbb{E}\{\| \mathbf{s}^T((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i + \mathbf{n}) \|^2\}} \tag{26}$$

$$\begin{aligned}&= \frac{A^2}{\mathbf{s}^T((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{R}_{\tilde{x}}(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T) + \sigma_n^2\mathbf{I})\mathbf{s}} \\ &= \frac{A^2}{\mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s} - 2c\mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s} + c^2\mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s} + \sigma_n^2} \\ &= \frac{A^2}{\alpha - 2c\alpha + c^2\alpha + \sigma_n^2}\end{aligned} \tag{27}$$

where we define $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s}$. By Applying $\mathcal{D} = A^2 + c^2\mathbf{s}^T\mathbf{R}_{\tilde{x}}\mathbf{s} = A^2 + c^2\alpha$ into (27), we obtain

$$\text{SINR} = \frac{\mathcal{D} - c^2\alpha}{\alpha - 2c\alpha + c^2\alpha + \sigma^2} \tag{28}$$

By direct differentiation of (28) with respect to c and root selection, we obtain $c = \frac{\alpha + \sigma_n^2 + \mathcal{D} - \sqrt{(\alpha + \sigma_n^2 + \mathcal{D})^2 - 4\alpha\mathcal{D}}}{2\alpha}$ in (24). $\square$

4. Multi-carrier PN-masked SS embedding

In this section, we extend our studies to the emerging concept of multi-carrier/multi-message SS embedding. We consider K distinct message bit sequences, $\{b_{k,1}, b_{k,2}, \ldots, b_{k,M}\}$, $k=1,2,\ldots,K$, $b_{k,i} \in \{\pm 1\}$, $i=1,\ldots,M$, each of length M bits. The K message sequences may be to be delivered to K distinct corresponding recipients or they are just K portions of one large message sequence to be transmitted to one recipient. In particular, the ith bit from each of K sequences, $b_{1,i},\ldots,b_{K,i}$, is simultaneously embedded in the ith transform-domain host vector $\mathbf{x}_i$ with corresponding amplitude $A_{k,i} \geq 0$ and PN-masked carrier $\mathbf{c}_{k,i} = \mathbf{s}_k \odot \mathbf{m}_i$, $\mathbf{m}_i \in \{\pm 1\}^L, \mathbf{s}_k \in \mathbb{R}^L$, $\|\mathbf{s}_k\| = 1$, $k=1,\ldots,K$, $i=1,\ldots,M$:

$$\begin{aligned}\mathbf{y}_i &= \sum_{k=1}^{K} A_{k,i} b_{k,i} \mathbf{c}_{k,i} + \mathbf{x}_i + \mathbf{n} \\ &= \left(\sum_{k=1}^{K} A_{k,i} b_{k,i} \mathbf{s}_k \right) \odot \mathbf{m}_i + \mathbf{x}_i + \mathbf{n}, \quad i=1,2,\ldots,M. \end{aligned} \tag{29}$$

The contribution of each individual embedded message bit $b_{k,i}$ to the composite signal is $A_{k,i} b_{k,i} \mathbf{c}_{k,i}$ and the MS distortion to the original host data *due to the embedded message-k alone* is

$$\mathcal{D}_k = \mathbb{E}\{\| A_{k,i} b_{k,i} \mathbf{c}_{k,i} \|^2\} = \frac{1}{M} \sum_{i=1}^{M} A_{k,i}^2, \quad k=1,\ldots,K.$$

Under a statistical independence assumption across message bits, the mean-squared distortion of the original image due to the total multi-message insertion is

$$\mathcal{D}^t = \sum_{k=1}^{K} \mathcal{D}_k = \frac{1}{M} \sum_{k=1}^{K} \sum_{i=1}^{M} A_{k,i}^2. \tag{30}$$

After PN-mask removal, the intended receiver of the kth message can use a filter $\mathbf{w}_k \in \mathbb{R}^L$ to recover embedded bits

$$\begin{aligned}\hat{b}_{k,i} &= \mathrm{sgn}\{\mathbf{w}_k^T (\mathbf{y}_i \odot \mathbf{m}_i)\} \\ &= \mathrm{sgn}\left\{ \mathbf{w}_k^T \left(\sum_{k=1}^{K} A_{k,i} b_{k,i} \mathbf{s}_k + \mathbf{x}_i \odot \mathbf{m}_i + \mathbf{n} \odot \mathbf{m}_i \right) \right\} \\ &= \mathrm{sgn}\left\{ A_{k,i} b_{k,i} (\mathbf{w}_k^T \mathbf{s}_k) + \sum_{j=1, j\neq k}^{K} A_{k,i} b_{k,i} \mathbf{w}_k^T \mathbf{s}_j + \mathbf{w}_k^T \tilde{\mathbf{x}}_i + \mathbf{w}_k^T \tilde{\mathbf{n}}_i \right\} \end{aligned} \tag{31}$$

where $\tilde{\mathbf{x}}_i \triangleq \mathbf{x}_i \odot \mathbf{m}_i$, $\tilde{\mathbf{n}}_i \triangleq \mathbf{n}_i \odot \mathbf{m}_i$. Similar to the finding in Proposition 6 of [30], the conditionally optimal carriers are summarized in the form of Proposition 4 below.

Proposition 4. *Consider additive SS embedding by (29). Let $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_L$ be eigenvectors of $\mathbf{R}_{\tilde{x}}$ with corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$. Orthogonal carriers that conditionally maximize the output SINR of the maximum SINR filter $\mathbf{w}_{\mathrm{maxSINR},k}$ are*

$$\mathbf{s}_k^{\mathrm{opt}} = \mathbf{q}_{L-k+1}, k=1,\ldots,K. \tag{32}$$

When $\mathbf{s}_k^{\mathrm{opt}} = \mathbf{q}_{L-k+1}$, maximum SINR filter simplifies to matched filter

$$\mathbf{w}_{\mathrm{maxSINR},k} \equiv \mathbf{w}_{\mathrm{MF},k} = \mathbf{s}_k^{\mathrm{opt}}. \square \tag{33}$$

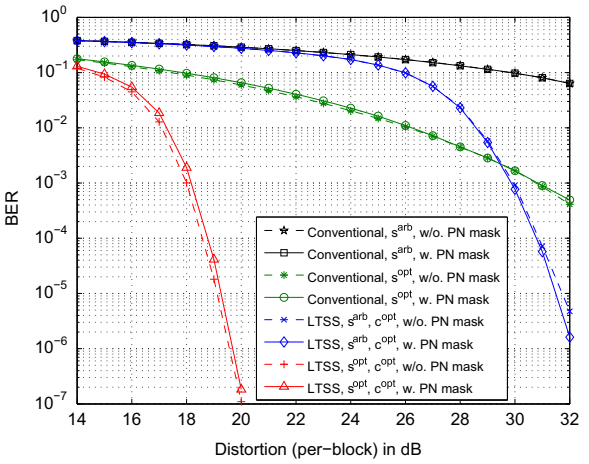

Fig. 1. BER versus per-block distortion due to embedding (512×512 Baboon, $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

5. 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 single-carrier embedding over all 63 bins except the dc coefficient. Hence, our carrier length is $L=63$ and we embed $512^2/8^2 = 4096$ bits. For the sake of generality, we also incorporate white Gaussian external noise of variance $\sigma_n^2 = 3$ dB. We evaluate the performance of eight different embedding schemes: (i) conventional SS embedding in (1) with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$, (ii) PN-masked conventional SS embedding in (5) with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$, (iii) conventional SS embedding in (1) with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$, (iv) PN-masked conventional SS embedding in (5) with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$, (v) linearly transformed SS (LTSS) embedding in (2) with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$ and the optimal transformation parameter c^{opt}, (vi) PN-masked LTSS embedding in (16) with an arbitrary carrier $\mathbf{s}^{\mathrm{arb}}$ and the optimal transformation parameter c^{opt}, (vii) LTSS embedding in (2) with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$ and the optimal transformation parameter c^{opt}, (viii) PN-masked LTSS embedding in (16) with an optimal carrier $\mathbf{s}^{\mathrm{opt}}$ and the optimal transform parameter c^{opt}. In all examined SS embedding schemes, MF is utilized to recover embedded bits.

Fig. 1 shows the recovery BER created by the embedded message for above six embedding schemes as a function of the MS distortion $\mathcal{D}$ per-block.[2]

We recall that the per-block distortion is due to the embedding only (see (6)) and the variance of external noise is fixed at $\sigma_n^2 = 3$ dB in the experiment.[3] It is demonstrated from Fig. 1 that the proposed PN-masked SS embedding

[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 distortion to attack distortion ratio (WNR) measure can also be easily obtained by $WNR = 10\log_{10}(\mathcal{D}/64/\sigma_n^2)$.

[3] With $\sigma_n^2 = 3$ dB, the initial peak signal-to-noise ratio (PSNR) of image (i.e. no hidden data, only external noise) is 45.1 dB.

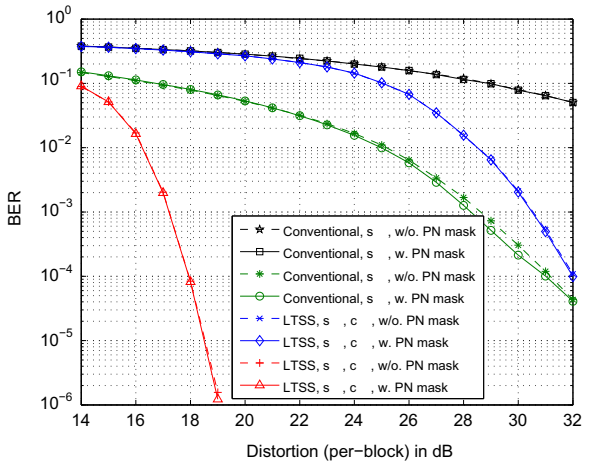

Fig. 2. BER versus per-block distortion due to embedding (512×512 Bridge, $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

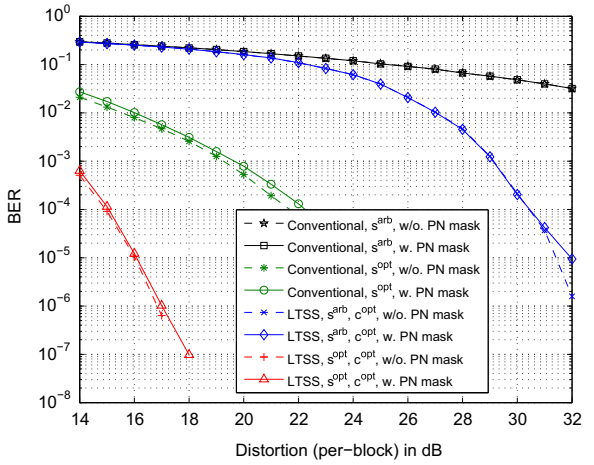

Fig. 3. BER versus per-block distortion due to embedding (512×512 Boat, $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

schemes have almost the same BER performance as their corresponding conventional SS embedding counterparts (see the same color curves). This observation means that the use of PN-sequence mask would not notably affect the BER performance of SS embedding, i.e., no obvious performance loss. In Figs. 2 and 3, we repeat the same experiment for gray-scale 512×512 "Bridge" and "Boat" images and the same conclusions can be drawn. Now we examine the average performance of the proposed PN-masked SS embedding algorithms over a large image database. The experimental image data set consists of more than 1500 8-bit gray-scale photographic images ([42,43] combined) which have great varieties (e.g. outdoor/indoor, daylight/night, natural/man-made) and different sizes. Recovery performance plots are given in Fig. 4. Similar conclusion can be drawn as in previous individual image host experimentations.

To assess the perceptual quality of the data-embedded images, in Fig. 5 we repeat the experiment in Fig. 4, but use structural similarity (SSIM) index [44] as perceptual criterion instead of the per-block distortion. The proposed similar

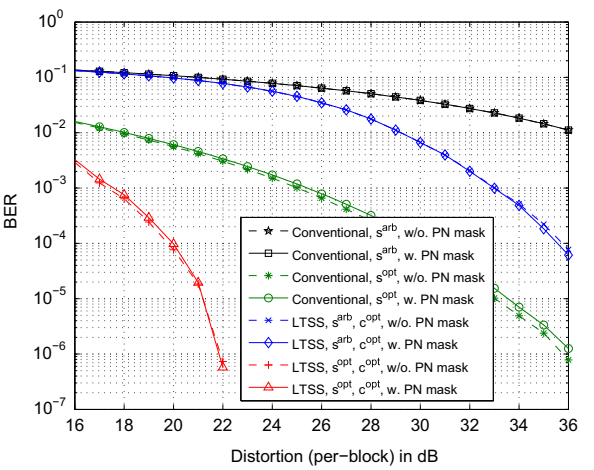

Fig. 4. BER versus per-block distortion due to embedding (average findings over a data set of more than 1500 images [42,43], $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

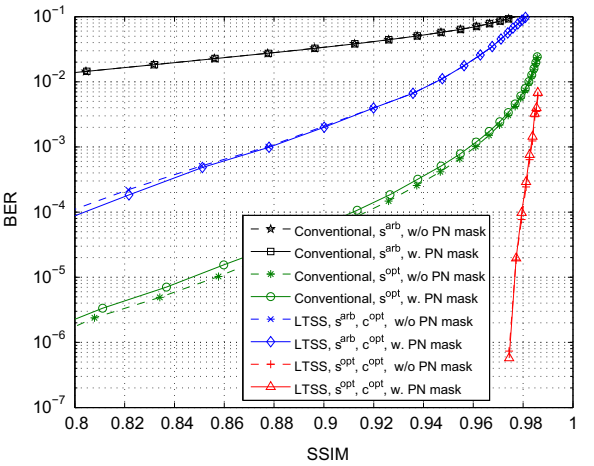

Fig. 5. BER versus SSIM (average findings over a data set of more than 1500 images [42,43], $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

conclusion can be drawn. To further illustrate the perceptual distortion due to the SS embedding, in Fig. 6 we display some meaningful images. Fig. 6(a) is the original clean 512×512 Baboon image, Fig. 6(b) is the stego image with data embedded by optimal LTSS, and Fig. 6(c) is the stego image with data embedded by proposed optimal PN-masked LTSS. From Fig. 6, we do not observe obvious perceptual distortion. All these results illustrate that the proposed PN mask method would not introduce any additional distortion than the conventional SS embedding. To show the suitability of the proposed PN masked SS embedding scheme for different transform domains, in Fig. 7 we repeat the same experiment of Fig. 1 but data are embedding on the discrete wavelet transform (DWT) domain. Comparing Fig. 7 with Fig. 1, it can be found that the performance is almost the same which means that the proposed PN masked SS embedding scheme is also suitable for other transform domains. To evaluate robustness of the proposed PN-

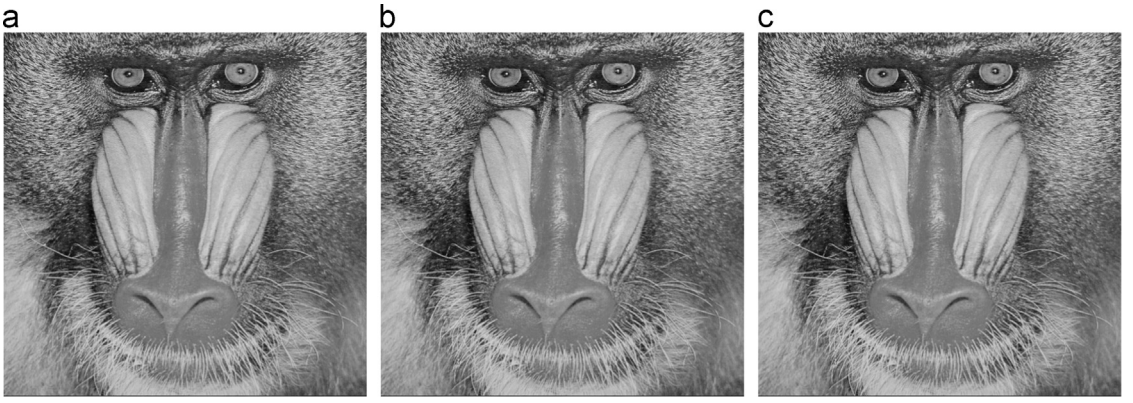

Fig. 6. (a) Original 512 × 512 Baboon image, (b) image with 4096 bits data embedded by optimal LTSS method (per-block distortion is $\mathcal{D}=20$ dB), (c) image with 4096 bits data embedded by PN-masked optimal LTSS method (per-block distortion is $\mathcal{D}=20$ dB).

masked embedding schemes and investigate the effect of the external noise on the performance, in Fig. 8 we keep the distortion at $\mathcal{D}=20$ dB and show the BER of each embedding scheme as a function of external noise variance σ_n^2 varying from 0 dB to 10 dB. First of all, at different noise levels, the proposed PN mask schemes would not notably degrade the performance comparing their counterparts. Moreover, as the noise level increases, the performance of $(\mathbf{s}^{\text{opt}}, c^{\text{opt}})$ embedding schemes (i.e. red curves) becomes worse. This means that, for a larger noise level, we need to increase the distortion to maintain the same BER performance. For other six embedding schemes (black, green, and blue curves), since the interference from the host to the embedded signal is very large and dominant, performances of these six schemes do not notable change with varying noise level.

To demonstrate the security offered by PN-sequence masking, we adopt IGLS-based algorithm [39] which has been shown to have better performance than BSS-based algorithms. We keep the Baboon image as the host and data are embedded with optimal carrier via (i) Circular Watermarking (CW) scheme proposed in [40] to enhance SS embedding security, (ii) non-PN-masked SS embedding, and (iii) PN-masked SS embedding. The intended receiver knows carrier and uses *non-blind* matched filter to recover embedded bits. The unauthorized/adversary receiver has no knowledge of carrier and uses IGLS-based algorithm to *blindly* extract embedded bits. The BER performances of intended receiver and unauthorized receiver are shown in Fig. 9. If the intended receiver and the unauthorized receiver have similar BER, then the embedding scheme has a low security level; If the intended receiver has low BER and the unauthorized receiver has much higher BER, then the embedding scheme has a high security level; If the unauthorized receiver has BER as high as 0.5 which means that what he received are garbage, then the embedding scheme has perfect security. While the unauthorized receiver can successfully recover data hidden by CW scheme and non-PN-masked SS embedding (almost the same BER as the intended receiver), PN-masked SS can fail the unauthorized receiver and provides perfect security for SS embedding. In Fig. 10, we repeat the same experimentation with arbitrary carrier and the same results can be found. In Fig. 11, instead

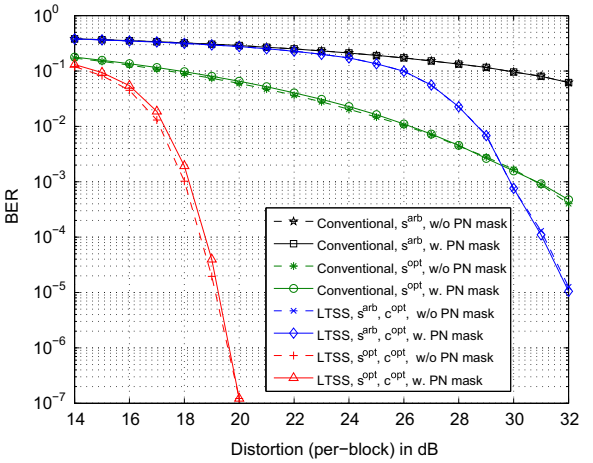

Fig. 7. BER versus per-block distortion due to embedding (512 × 512 Baboon, embedding on DWT domain, carrier of length $L=63$, external noise variance is fixed at $\sigma_n^2=3$ dB).

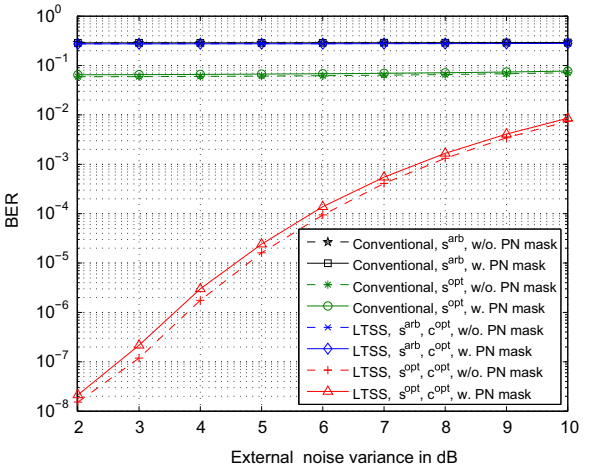

Fig. 8. BER versus external noise level (512 × 512 Baboon, embedding on DCT domain, carrier of length $L=63$, distortion is fixed at 20 dB).

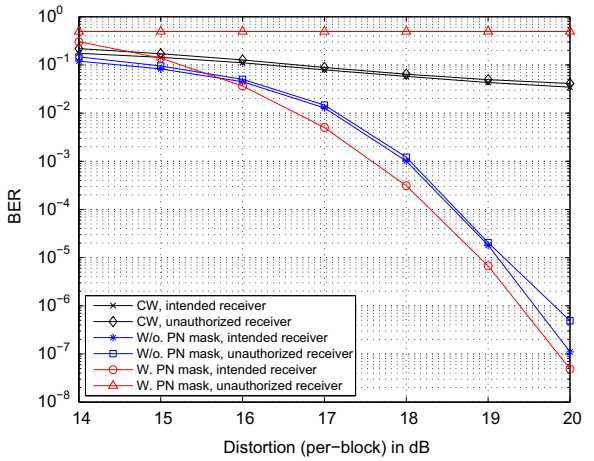

Fig. 9. BER versus per-block distortion due to embedding (512×512 Baboon, optimal carrier of length $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

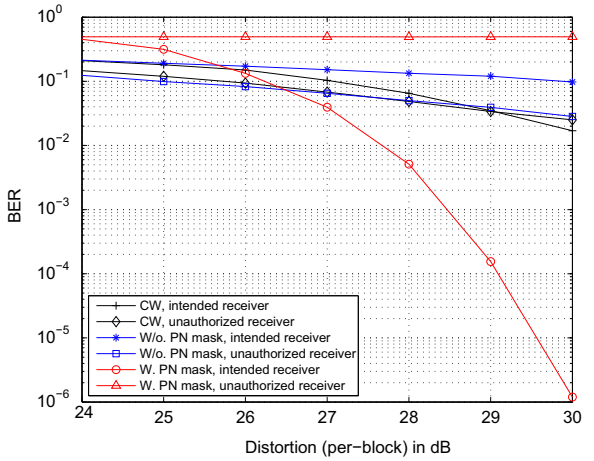

Fig. 10. BER versus per-block distortion due to embedding (512×512 Baboon, arbitrary carrier of length $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

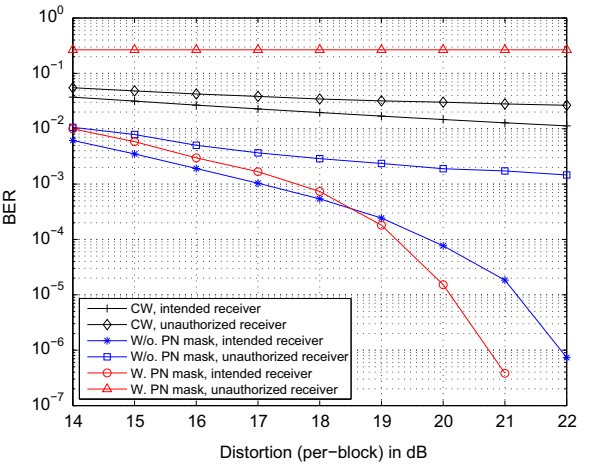

Fig. 11. BER versus per-block distortion due to embedding (average findings over a data set of more than 1500 images [42,43], optimal carrier of length $L=63$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

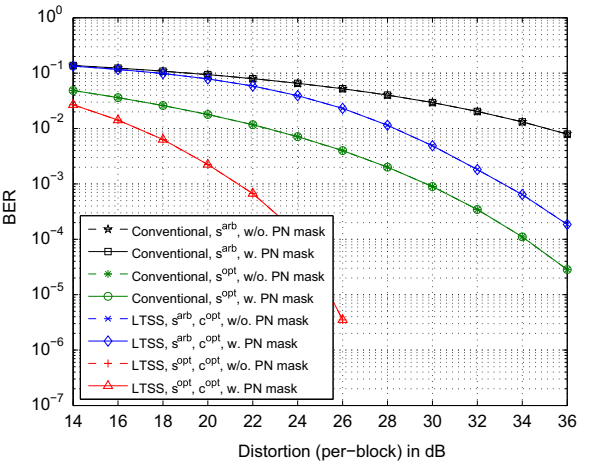

Fig. 12. BER versus allowable per-message per-block distortion (average findings over a data set of more than 1500 images [42,43], $L=63$, $K=16$, external noise variance is fixed at $\sigma_n^2 = 3$ dB).

of focusing on one image, we carry out the experiment with image data set consisting of more than 1500 images. The average performance results shown in Fig. 11 illustrate that our proposed PN masking SS embedding can efficiently improve the security.

Finally, we consider the problem of multi-carrier SS embedding. We wish to hide $K=16$ data messages with each message having its own individual orthogonal embedding carrier. In Fig. 12 we examine the average performance of the proposed multi-carrier SS embedding algorithms over a large image database. The results in Fig. 12 reiterate the importance of PN masking operation and jointly optimized carrier and host-data manipulation.

6. Conclusions

We considered the problem of embedding data in a digital host via SS embedding in an arbitrary transform domain. PN-sequence masked SS embedding was first proposed to enhance the security and prevent illegitimate data extraction by unauthorized users. Then, adaptive optimal carrier design was developed to maximize the output SINR with any given total distortion budget. To take these findings one step further, we also extended our effort to cover multi-carrier/multi-message embedding and developed carrier optimization algorithm which can, once again, improve the probability of error as well as enhance the security. As a brief concluding remark, PN-sequence masked SS embedding is a very efficient secure data hiding approach to protect embedded data without inducing more distortion to host nor affecting recovery performance. Optimal carrier design utilizes SOS of host and can significantly improve SINR and consequently reduce BER.

Acknowledgments

This work is supported by the Fundamental Research Funds for the Central Universities (Grant no. DUT14RC(3)

103), the Open Fund of Artificial Intelligence Key Laboratory of Sichuan Province (Grant no. 2012RZJ01), the National Natural Science Foundation of China (Grant no. 61172109 and 61402079), and the Foundation for Innovative Research Groups of the NSFC (Grant no. 71421001).

References

[1] M.D. Swanson, M. Kobayashi, A.H. Tewfik, Multimedia data-embedding and watermarking technologies, Proc. IEEE 86 (June) (1998) 1064–1087.
[2] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding: a survey, Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information) 87 (July) (1999) 1062–1078.
[3] I.J. Cox, M.L. Miller, J.A. Bloom, Digital Watermarking, Morgan-Kaufmann, San Francisco, CA, 2002.
[4] G.C. Langelaar, I. Setyawan, R.L. Lagendijk, Watermarking digital image and video data: a state-of-the-art overview, IEEE Signal Process. Mag. 17 (September) (2000) 20–46.
[5] N.F. Johnson, S. Katzenbeisser, A survey of steganographic techniques, in: S. Katzenbeisser, F. Petitcolas (Eds.), Information Hiding, Artech House, Norwood, MA, 2000, pp. 43–78.
[6] C. Cachin, An information-theoretic model for steganography, in: Proceedings of 2nd International Workshop on Information Hiding, Portland, OR, April 1998, pp. 306–318.
[7] G.J. Simmons, The prisoner's problem and the subliminal channel, in: Advances in Cryptology, Proceedings of CRYPTO'83, Plenum, New York, NY, 1984, pp. 51–67.
[8] J. Fridrich, Steganography in Digital, Media, Principles, Algorithms and Applications, Combridge Univeristy Press, Combridge, UK, 2010.
[9] Y. Wang, P. Moulin, Perfectly secure steganography: capacity, error exponents, and code constructions, IEEE Trans. Inf. Theory 54 (June) (2008) 2706–2722.
[10] L.M. Marvel Jr., C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Proc. 8 (August) (1999) 1075–1083.
[11] M. Kutter, S. Winkler, A vision-based masking model for spread-spectrum image watermarking, IEEE Trans. Image Proc. 11 (January) (2002) 16–25.
[12] J.R. Smith, B.O. Comiskey, Modulation and Information Hiding in Images, Lecture Notes on Computer Science 1174 (1996) 207–226.
[13] M. Wu, B. Liu, Data hiding in binary image for authentication and annotation, IEEE Trans. Multimed. 6 (August) (2004) 528–538.
[14] N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain, Signal Proc. 66 (May) (1998) 385–403.
[15] I.J. Cox, J. Kilian, F.T. Leighton, T. Shannon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Proc. 6 (December) (1997) 1673–1687.
[16] M. Barni, F. Bartolini, A. De Rosa, A. Piva, Optimum decoding and detection of multiplicative watermarks, IEEE Trans. Signal Proc. 51 (April) (2003) 1118–1123.
[17] M. Barni, F. Bartolini, A. De Rosa, A. Piva, A new decoder for the optimum recovery of nonadditive watermarks, IEEE Trans. Image Proc. 10 (May) (2001) 755–766.
[18] M. Barni, F. Bartolini, A. De Rosa, A. Piva, Capacity of full frame DCT image watermarks, IEEE Trans. Image Proc. 9 (August) (2000) 1450–1455.
[19] J. Hernandez, M. Amado, F. Pérez-González, DCT-domain watermarking techniques for still images: detector performance analysis and a new structure, IEEE Trans. Image Proc. 9 (January) (2000) 55–68.
[20] C. Qiang, T.S. Huang, An additive approach to transform-domain information hiding and optimum detection structure, IEEE Trans. Multimed. 3 (September) (2001) 273–284.
[21] 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 (November) (2005) 1394–1406.
[22] J.J. Eggers, B. Girod, Quantization effects on digital watermarks, Signal Proc. 81 (February) (2001) 239–263.
[23] P. Moulin, M.K. Mihçak, A framework for evaluating the datahiding capacity of image sources, IEEE Trans. Image Proc. 11 (September) (2002) 1029–1042.
[24] S. Pereira, S. Voloshynovskiy, T. Pun, Optimized wavelet domain watermark embedding strategy using linear programming, In: Proceedings of SPIE Wavelet Applications Conference, vol. 4056, Orlando, FL, April 2000, pp. 490–498.
[25] P. Moulin, A. Ivanović, The zero-rate spread-spectrum watermarking game, IEEE Trans. Signal Proc. 51 (April) (2003) 1098–1117.
[26] X.G. Xia, C.G. Boncelet, G.R. Arce, A multiresolution watermark for digital images, In: Proceedings of IEEE International Conference on Image Processing (ICIP), vol. 1, Santa Barbara, CA, October 1997, pp. 548–551.
[27] C. Fei, D. Kundur, R.H. Kwong, Analysis and design of watermarking algorithms for improved resistance to compression, IEEE Trans. Image Proc. 13 (February) (2004) 126–144.
[28] H.S. Malvar, D.A. Florencio, Improved spread spectrum: a new modulation technique for robust watermarking, IEEE Trans. Signal Proc. 51 (April) (2003) 898–905.
[29] M. Gkizeli, D.A. Pados, M.J. Medley, SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography, In: Proceedings of IEEE International Conference on Image Processing (ICIP), Singapore, October 2004, pp. 1561–1564.
[30] M. Gkizeli, D.A. Pados, M.J. Medley, Optimal signature design for spread-spectrum steganography, IEEE Trans. Image Proc. 16 (February) (2007) 391–405.
[31] 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 & Security Symposium, vol. 6982, Orlando, FL, March 2008, pp. 0D1–0D10.
[32] A. Valizadeh, Z.J. Wang, Correlation-and-bit-aware spread spectrum embedding for data hiding, IEEE Trans. Inf. Forensics Secur. 6 (June) (2011) 267–282.
[33] S. Glisic, B. Vucetic, Spread Spectrum CDMA Systems for Wireless Communications, Artech House, Norwood, MA, 1997.
[34] F. Cayre, C. Fontaine, T. Furon, Watermarking security: theory and practice, IEEE Trans. Signal Proc. 53 (October) (2005) 3976–3987.
[35] L. Pérez-Freire, P. Comesana, J.R. Troncoso-Pastoriza, F. Pérez-González, Watermarking security: a survey, LNCS Trans. Data Hiding Multimed. Secur., 4300(October), 2006, 41–72.
[36] M. Barni, F. Bartolini, T. Furon, A general framework for robust watermarking security, ACM J. Signal Proc. – Spec. Sect.: Secur. Data Hiding Technol. 83 (October) (2003) 2069–2084.
[37] L. Pérez-Freire, F. Pérez-González, Spread-spectrum watermarking security, IEEE Trans. Inf. Forensics Secur. 4 (March) (2009) 2–24.
[38] M. Gkizeli, D.A. Pados, S.N. Batalama, M.J. Medley, Blind iterative recovery of spread-spectrum steganographic messages, In: Proceedings of IEEE International Conference on Image Processing (ICIP), vol. 2, Genova, Italy, 11–14 September, 2005, pp. 1098–1101.
[39] 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 of International Conference on Communications (ICC), Ottawa, Canada, June 2012.
[40] P. Bas, F. Cayre, Achieving subspace or key security for WOA using natural or circular watermarking, In: Proceedings of ACM Multimedia and Security Workshop, Geneva, Switzerland, September 2006.
[41] D.G. Manolakis, V.K. Ingle, S.M. Kogon, Statistical and Adaptive Signal Processing, McGraw-Hill, New York, 2000.
[42] 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, January 2004, pp. 472–480.
[43] USC-SIPI Image Database. Available: ⟨http://sipi.usc.edu/database/database.cgi?volume=misc⟩.
[44] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Trans. Image Process. 13 (April (4)) (2004) 600–612.