PN-sequence Masked Spread-Spectrum Data Embedding

Ming Li†, Qian Liu‡, Bo Wang†, Yanqing Guo†, and Xiangwei Kong†

†School of Information and Communication
Engineering, Dalian University of Technology, Dalian, Liaoning, China, 116024
E-mail: {mli,bowang,guoyq,kongxw}@dlut.edu.cn
‡Department of Computer Science and Engineering
The State University of New York at Buffalo, Buffalo, NY 14260, USA
E-mail: qianliu@buffalo.edu

***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. The extensive experimental studies confirm our analytical performance predictions and illustrate the benefits of the designed PN masked optimal SS embedding.**

***Index Terms*—Data hiding, information hiding, pseudo-noise masking, signal-to-interference-plus-noise ratio (SINR), spread-spectrum embedding, steganography, watermarking.**

I. Introduction

The rapid advances in information and communication technologies allow people to easily transfer and exchange massive amounts of digital multimedia, such as digital images, video, and audio. Consequently, it has become extremely important to ensure the security of the exchanged information. As a result, digital data embedding has raised extensive attention in recent years with the development of various security/privacy protection applications, such as annotation, copyright marking, watermarking, ownership protection, authentication, digital fingerprint, and covert communications or steganography. As a general encompassing comment, different applications of information hiding, such as the ones described above, require different satisfactory tradeoffs between the following four basic attributes of data hiding [1]: Payload, robustness, transparency, and security.

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 Natural Science Foundation of Liaoning Province (Grant No. 2015020043), and the Natural Science Foundation of China (Grant No. 61172109 and 61402079).

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 or in a transform domain [2]-[10]. 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 [11] and enables the powerful notion of spread-spectrum (SS) data embedding when the secret signal is spread over a wide range of host frequencies [12]-[16].

In this paper, we focus our attention on additive SS embedding in transform domain host. In direct analogy to SS digital communication systems [17], 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 [18]-[21] or novel iterative generalized least square (IGLS) approaches [22],[23]. The illegitimate blind hidden data extraction has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context [18]-[21]. 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 [24] 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

978-1-5090-0243-6/15/$31.00 ©2015 IEEE

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. Without any notable performance loss, this PN-masked SS embedding can efficiently provide almost perfect security and minimize the likelihood that embedded data are "stolen" by unauthorized users.

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 [13], [14] can maximize the signal-to-interference-noise-ratio (SINR) at the output of the corresponding maximum-SINR linear filter. Benefiting from the legacy of [13], [14], the optimal carrier design for PN-masked SS embedding is also studied.

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; $\mathrm{sgn}\{\cdot\}$ denotes zero-threshold quantization; $\mathbb{E}\{\cdot\}$ represents statistical expectation; $\|\cdot\|$ is vector norm.

II. 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 $\frac{N_1 N_2}{M}$. Each block, $\mathbf{H}_1, \mathbf{H}_2, ..., \mathbf{H}_M$, 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, a wavelet transform, etc.). After transform calculation and vectorization (for example by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_i) \in \mathbb{R}^{\frac{N_1 N_2}{M}}, i = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_i)$ we choose a fixed subset of $L \leq \frac{N_1 N_2}{M}$ 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

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

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 $(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)$ 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 [12], [14]

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

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 is presented in Proposition 3 of [14].

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 [18]-[21] or a novel IGLS approach [23], embedded information bits can be blindly extracted by unauthorized users without the knowledge of carrier $\mathbf{s}$. Using random-like amplitudes [24] 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.

III. 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

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

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

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

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

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 $\mathbf{c}_i \in \mathbb{R}^L$, $\|\mathbf{c}_i\| = 1$

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

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

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

where $\widetilde{\mathbf{x}}_i \triangleq \mathbf{x}_i \odot \mathbf{m}_i$ is PN-masked host vector, $\widetilde{\mathbf{n}}_i \triangleq \mathbf{n}_i \odot \mathbf{m}_i$. 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 $\widetilde{\mathbf{x}}_i$ 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, then the total disturbance $(\widetilde{\mathbf{x}}_i + \widetilde{\mathbf{n}}_i)$ 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 $\mathbf{w} \in \mathbb{R}^L$

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

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 $(\widetilde{\mathbf{x}}_i + \widetilde{\mathbf{n}}_i)$ in (7) after mask removal operation at the intended receiver, the output SINR of filter $\mathbf{w}$ is

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

where

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

is the autocorrelation matrix of PN-masked host vectors. The linear filter offers maximum SINR at its output is [25]

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

The exact maximum output SINR value attained is

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

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 [14] 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 $\mathbf{w}_{\mathrm{maxSINR}}$ is

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

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

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

■

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

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

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

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

where $\widetilde{\mathbf{x}}_i \triangleq \mathbf{x}_i \odot \mathbf{m}_i$, $\widetilde{\mathbf{n}}_i \triangleq \mathbf{n}_i \odot \mathbf{m}_i$. 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

$$\begin{aligned}\mathcal{D} &= \mathbb{E}\left\{\|\left(Ab_i\mathbf{c}_i + (\mathbf{I}_L - c\mathbf{c}_i\mathbf{c}_i^T)\mathbf{x}_i\right) - \mathbf{x}_i\|^2\right\} \\ &= \mathbb{E}\left\{\|\left(Ab_i - c\mathbf{c}_i^T\mathbf{x}_i\right)\mathbf{c}_i\|^2\right\} \\ &= \mathbb{E}\left\{\|Ab_i - c\mathbf{s}^T\widetilde{\mathbf{x}}_i\|^2\right\} \\ &= A^2 + c^2\mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s}. \end{aligned} \tag{18}$$

It should be noticed that, in contrast to (6), the distortion level is controlled not only by A but also by c. Comparing 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 is summarized in Proposition 2 below whose proof is similar to Proposition 3 in [14] 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 $\mathbf{R}_{\widetilde{\mathbf{x}}}$ in (11) with corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_L$. For any hidden message-induced distortion budget $\mathcal{D}$, the optimal carrier $\mathbf{s}$, amplitude A, and transformation parameter c to maximize SINR are

$$\mathbf{s}^{\rm opt} = \mathbf{q}_L, \tag{19}$$

$$c^{\rm opt} = \frac{\lambda_L+\sigma_n^2+\mathcal{D}-\sqrt{(\lambda_L+\sigma_n^2+\mathcal{D})^2-4\lambda_L\mathcal{D}}}{2\lambda_L}, \tag{20}$$

$$A = \sqrt{\mathcal{D}-c^2\lambda_L}. \tag{21}$$

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

$$\mathbf{w}_{\rm maxSINR} = \mathbf{w}_{\rm MF} = \mathbf{q}_L. \tag{22}$$

■

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 $\mathbf{w}_{\rm MF} = \mathbf{s}$ 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

$$c^{\rm opt} = \frac{\alpha+\sigma_n^2+\mathcal{D}-\sqrt{(\alpha+\sigma_n^2+\mathcal{D})^2-4\alpha\mathcal{D}}}{2\alpha}, \tag{23}$$

$$A = \sqrt{\mathcal{D}-c^2\alpha}, \tag{24}$$

where $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s}$. ■

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

$$\begin{aligned} \text{SINR} &= \frac{\mathbb{E}\{\|Ab_i\|^2\}}{\mathbb{E}\{\|\mathbf{s}^T((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{x}_i + \mathbf{n})\|^2\}} \qquad (25)\\ &= \frac{A^2}{\mathbf{s}^T((\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T)\mathbf{R}_{\widetilde{\mathbf{x}}}(\mathbf{I}_L - c\mathbf{s}\mathbf{s}^T) + \sigma_n^2\mathbf{I})\mathbf{s}}\\ &= \frac{A^2}{\mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s} - 2c\mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s} + c^2\mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s} + \sigma_n^2}\\ &= \frac{A^2}{\alpha - 2c\alpha + c^2\alpha + \sigma_n^2} \qquad (26) \end{aligned}$$

where we define $\alpha \triangleq \mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s}$. By Applying $\mathcal{D} = A^2 + c^2\mathbf{s}^T\mathbf{R}_{\widetilde{\mathbf{x}}}\mathbf{s} = A^2 + c^2\alpha$ into (26), we obtain

$$\text{SINR} = \frac{\mathcal{D} - c^2\alpha}{\alpha - 2c\alpha + c^2\alpha + \sigma^2} \tag{27}$$

By direct differentiation of the (27) 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 (23). ■

IV. 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 $\mathbf{s}^{\rm arb}$, *ii*) PN-masked conventional SS embedding in (5) with an arbitrary carrier $\mathbf{s}^{\rm arb}$, *iii*) conventional SS embedding in (1) with an optimal carrier $\mathbf{s}^{\rm opt}$, *iv*) PN-masked conventional SS embedding in (5) with an optimal carrier $\mathbf{s}^{\rm opt}$, *v*) linearly transformed SS (LTSS) embedding in (2) with an arbitrary carrier $\mathbf{s}^{\rm arb}$ and the optimal transformation parameter $c^{\rm opt}$, *vi*) PN-masked LTSS embedding in (16) with an arbitrary carrier $\mathbf{s}^{\rm arb}$ and the optimal transformation parameter $c^{\rm opt}$, *vii*) LTSS embedding in (2) with an optimal carrier $\mathbf{s}^{\rm opt}$ and the optimal transformation parameter $c^{\rm opt}$, *viii*) PN-masked LTSS embedding in (16) with an optimal carrier $\mathbf{s}^{\rm opt}$ and the optimal transform parameter $c^{\rm opt}$. 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]. It is demonstrated that use of PN-sequence mask would not evidently affect the BER performance of SS embedding. 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

[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 $WNR = 10\log_{10}(\mathcal{D}/64/\sigma_n^2)$.

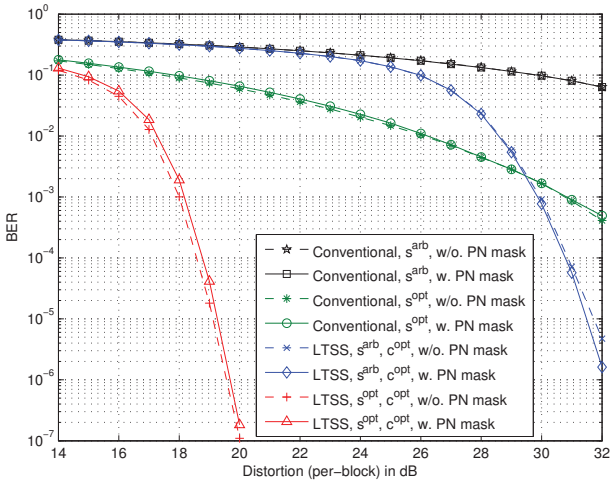

Fig. 1. BER versus allowable per-block distortion, (512×512 Baboon, $L = 63$, $\sigma_n^2 = 3$dB).

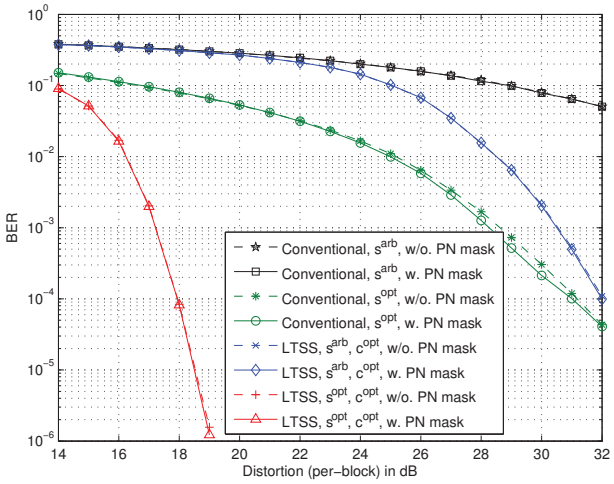

Fig. 2. BER versus allowable per-block distortion, (512×512 Bridge, $L = 63$, $\sigma_n^2 = 3$dB).

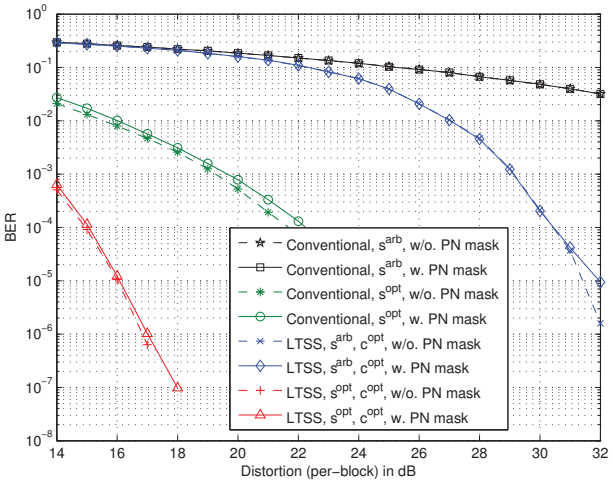

Fig. 3. BER versus allowable per-block distortion, (512×512 Boat, $L = 63$, $\sigma_n^2 = 3$dB).

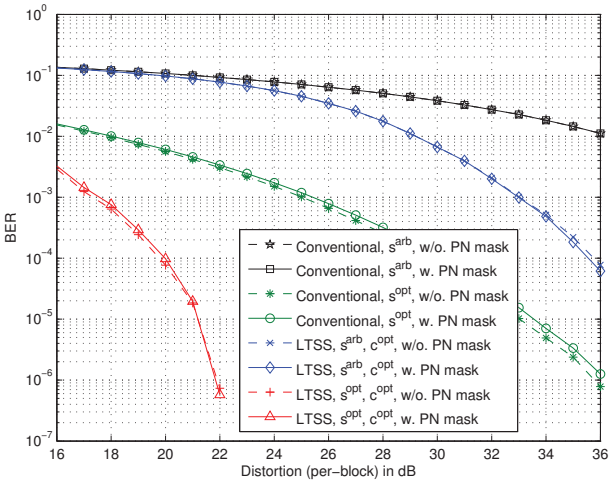

Fig. 4. BER versus allowable per-block distortion, (average findings over a data set of more than $1,500$ images [26], [27], $L = 63$, $\sigma_n^2 = 3$dB).

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 $1,500$ 8-bit gray-scale photographic images ([26] and [27] combined) which have great variety (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 demonstrate the security offered by PN-sequence mask, we adopt IGLS-based algorithm [23] 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 [24] 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 performance of blind and non-blind recovery algorithms are shown in Fig. 5. While IGLS blind data extraction algorithm can successfully recover data hidden by CW scheme and non-PN-masked SS embedding (almost the same BER as non-blind one), PN-masked SS can fail the blind data extraction (0.5 BER) and provides perfect security for SS embedding. In Fig. 6, we repeat the same experimentation with arbitrary carrier and the same results can be found.

V. 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

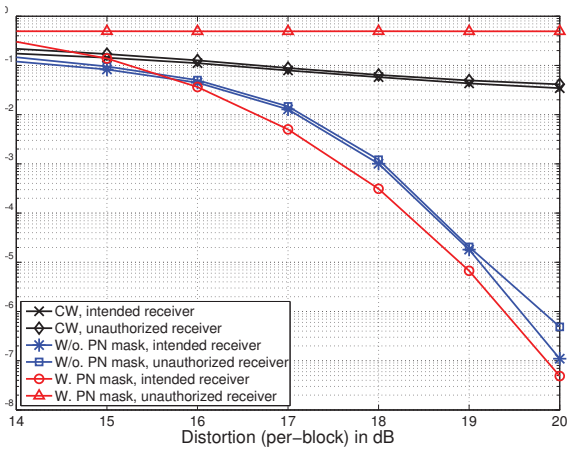

Fig. 5. BER versus allowable per-block distortion, (512×512 Baboon, optimal carrier of length $L = 63$, $\sigma_n^2 = 3$dB).

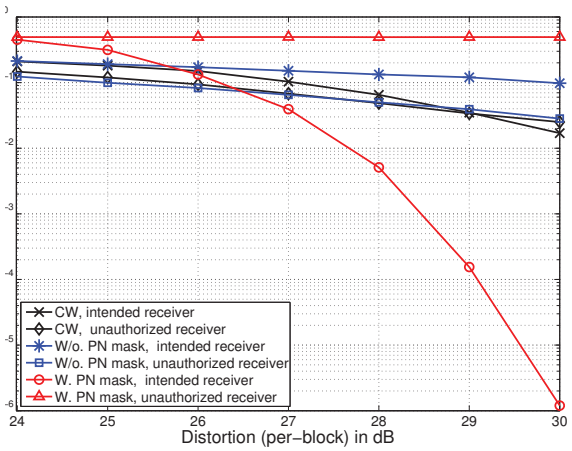

Fig. 6. BER versus allowable per-block distortion, (512×512 Baboon, arbitrary carrier of length $L = 63$, $\sigma_n^2 = 3$dB).

unauthorized users. Then, adaptive optimal carrier design was developed to maximize the output SINR with any given total distortion budget. 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.

REFERENCES

[1] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2706-2722, June 2008.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, pp. 1673-1687, Dec. 1997.

[3] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, pp. 1118-1123, Apr. 2003.

[4] J. Hernandez, M. Amado, and F. Pérez-González, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Process.*, vol. 9, pp. 55-68, Jan. 2000.

[5] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, pp. 273-284, Sept. 2001.

[6] C. B. Adsumilli, M. C. Q. Farias, S. K. Mitra, and M. Carli, "A robust error concealment technique using data hiding for image and video transmission over lossy channels," *IEEE Trans. Circuits System Video Technol.*, vol. 15, pp. 1394-1406, Nov. 2005.

[7] P. Moulin and M. K. Mihçak, "A framework for evaluating the datahiding capacity of image sources," *IEEE Trans. Image Process.*, vol. 11, pp. 1029-1042, Sept. 2002.

[8] S. Pereira, S. Voloshynovskiy, and T. Pun, "Optimized wavelet domain watermark embedding strategy using linear programming," in *Proc. SPIE Wavelet Applications Conf.*, Orlando, FL, Apr. 2000, vol. 4056, pp. 490-498.

[9] P. Moulin and A. Ivanović, "The zero-rate spread-spectrum watermarking game," *IEEE Trans. Signal Proc.*, vol. 51, pp. 1098-1117, Apr. 2003.

[10] X. G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," in *Proc. IEEE Intern. Conf. Image Process. (ICIP)*, Santa Barbara, CA, Oct. 1997, vol. 1, pp. 548-551.

[11] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression," *IEEE Trans. Image Process.*, vol. 13, pp. 126-144, Feb. 2004.

[12] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Process.*, vol. 51, pp. 898-905, Apr. 2003.

[13] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in *Proc. IEEE Intern. Conf. Image Process. (ICIP)*, Singapore, Oct. 2004, pp. 1561-1564.

[14] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Process.*, vol. 16, pp. 391-405, Feb. 2007.

[15] L. Wei, D. A. Pados, S. N. Batalama, and M. J. Medley, "Sum-SINR/sum-capacity optimal multisignature spread-spectrum steganography," in *Proc. SPIE, Mobile Multimedia/Image Processing, Security, and Applications Conf., SPIE Defense & Security Symposium*, Orlando, FL, Mar. 2008, vol. 6982, pp. 0D1-0D10.

[16] A. Valizadeh, Z. J. Wang, "Correlation-and-bit-aware spread spectrum embedding for data hiding," *IEEE Trans. Inf. Forensics and Security*, vol. 6 , pp. 267-282, June 2011.

[17] S. Glisic and B. Vucetic, *Spread Spectrum CDMA Systems for Wireless Communications*. Norwood, MA: Artech House, 1997.

[18] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Process.*, vol. 53, pp. 3976-3987, Oct. 2005.

[19] L. Pérez-Freire, P. Comesana, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Watermarking security: A survey," *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.

[20] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," *ACM Journal Signal Proc. - Special Section: Security of Data Hiding Technologies*, vol. 83, pp. 2069-2084, Oct. 2003.

[21] L. Pérez-Freire and F. Pérez-González, "Spread-spectrum watermarking security," *IEEE Trans. Inf. Forensics and Security*, vol. 4, pp. 2-24, Mar. 2009.

[22] M. Gkizeli, D. A. Pados, S. N. Batalama, and M. J. Medley, "Blind iterative recovery of spread-spectrum steganographic messages," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Genova, Italy, Sept. 11-14, 2005, vol. 2, pp. 1098-1101.

[23] M. Li, M. Kulhandjian, D. A. Pados, S. N. Batalama, M. J. Medley, and J. D. Matyjas, "On the extraction of spread-spectrum hidden data in digital media," in *Proc. Int. Conf. Commun.(ICC)*, Ottawa, Canada, June 2012.

[24] P. Bas and F. Cayre, "Achieving subspace or key security for WOA using natural or circular watermarking," in *Proc. ACM Multimedia and Security Workshop*, Geneva, Switzerland, Sept. 2006.

[25] D. G. Manolakis, V. K. Ingle, and S. M. Kogon, *Statistical and Adaptive Signal Processing*. New York: McGraw-Hill, 2000.

[26] G. Schaefer and M. Stich, "UCID–An uncompressed colour image database," in *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, San Jose, CA, Jan. 2004, pp. 472-480.

[27] *USC-SIPI Image Database*. Available: http://sipi.usc.edu/database/database.cgi?volume=misc