SECURITY ANALYSIS OF OPTIMAL MULTI-CARRIER SPREAD-SPECTRUM EMBEDDING

Ming Li, Lingyun Li, Yanqing Guo, Bo Wang, and Xiangwei Kong

School of Information and Communication Engineering
Dalian University of Technology
Dalian, Liaoning, 116024, P. R. China
E-mail: {mli,guoyq,bowang,kongxw}@dlut.edu.cn,lingyunli@mail.dlut.edu.cn

ABSTRACT

This paper considers optimal multi-carrier (multiple messages) spread-spectrum (SS) data embedding on linearly-transformed host. We present information-theoretic security analysis for the optimal SS embedding. The security is quantified by both the Kullback-Leibler distance and Bhattacharyya distance between the cover and stego probability distributions. The main results of this paper permit to establish fundamental security limits for the optimal SS embedding. Theoretical analysis and experimental results show the impact of the number of embedding messages, the embedding distortion, and the host transformation in the security level.

Index Terms–Bhattacharyya distance, covert communications, data hiding, Kullback-Leibler distance, steganography.

1. INTRODUCTION

Steganography, which literally means “covered writing” in Greek, is an important sub-discipline of data embedding [1]-[6]. The purpose of steganography is to embed secret messages within an innocuous looking cover medium in order to conceal the existence of embedded messages and establish secret communication between trusting parties. If any suspicion about the hidden secret messages is raised, then the goal of establishing a covert communication link is defeated. Undetectability, i.e. hiding data perceptually as well as statistically, is a critical security issue and the primary requirement in steganographic applications.

The security/undetectability of steganographic systems can be evaluated in an information-theoretic framework. The Kullback-Leibler (KL) distance between cover distribution P_c and stego distribution P_s has become a popular metric for analyzing and assessing the security of practical steganographic schemes [7]-[10]. In information theory, the KL distance $D_{KL}(P_c||P_s) \triangleq \mathbb{E}_{P_c}\{\log(P_c) - \log(P_s)\}$ can be viewed as a measure of difference/similarity between P_c and P_s. If $P_c = P_s$, i.e. cover and stego are statistically identical, then $D_{KL}(P_c||P_s) = 0$ and the steganogrphic system is perfectly secure. The larger difference between P_c and P_s, the larger KL distance and the presence of embedded data is easier to be detected. A steganographic system is called ϵ-secure if $D_{KL}(P_c||P_s) \leq \epsilon$. Since KL distance is not a symmetric function and sometimes it cannot reasonably reflect the difference between the cover and stego distributions, Korzhik *et al.* proposed to use Bhattacharyya distance (BD) as the measure of steganography security [11]. BD between P_c and P_s is denoted as $D_B(P_c||P_s) \triangleq -\ln(BC(P_c, P_s))$, where $BC(P_c, P_s) \triangleq \int \sqrt{BC(P_c(x)P_s(x))}dx$.

As one of the most popular approaches, spread-spectrum (SS) embedding has been widely used in many data hiding applications [12]-[18]. Recently, a novel optimal multi-carrier (multiple message) SS embedding on the linearly transformed host was proposed [19], [20]. This new approach exploits the statistics of the host signals and designs optimal carriers and transformation operator that maximize the output signal-to-interference-plus-noise ratio (SINR) of the maximum-SINR data receiver filter or, equivalently, minimize the average embedding distortion for any target message extraction error rate. It has been shown that the optimal multi-carrier SS embedding is superior to its counterpart, the conventional SS embedding and Improved SS (ISS) embedding [17], in terms of recovery performance.

However, the security of this optimal multi-carrier SS embedding scheme has not been investigated. Since its security/undetectability is unknown, we are always in fear of stanalysis attacks if we apply this optimal SS embedding scheme in steganographic applications. In this paper, we aim to analyze the information-theoretic security of the optimal multi-carrier data embedding scheme by evaluating both the KL distance and the Bhattacharyya distance between the cover and stego distributions. The main results of this paper permit to establish fundamental security limits for the optimal multi-carrier SS embedding and to draw conclusions about the tradeoffs between robustness and security. Specifically, theoretical analysis and experimental results show the impact of the number of embedding messages, the dimensionality of the embedding,

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. 61172109 and 61402079).

the host transformation, and the embedding distortion in the security level.

2. OPTIMAL MULTI-CARRIER 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 $b_i \in \{\pm 1\}$, $i = 1, 2, \dots, M$, 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 $\mathcal{T}(\mathbf{H}_i) \in \mathbb{R}^{\frac{N_1 N_2}{M}}, i = 1, 2, \dots, M$. 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 $\mathbf{x}_i \in \mathbb{R}^L$, $i = 1, 2, \dots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value. The autocorrelation matrix of the host data $\mathbf{x}$ is defined as

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

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.

We first review the optimal multi-carrier/multi-message SS embedding on the linearly modified transform domain of host[20]:

$$\mathbf{y}_i = \sum_{k=1}^{K} A_k b_{k,i} \mathbf{s}_k + (\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)\mathbf{x}_i + \mathbf{n} \tag{2}$$

where information bits $\{b_{1,i}, b_{2,i}, \dots, b_{K,i}\}$, belonging potentially to K distinct messages, are embedded simultaneously in the linearly transformed host $(\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)\mathbf{x}_i$, of block $i = 1, \dots, M$, with corresponding amplitudes $A_k > 0$ and embedding carriers $\mathbf{s}_k \in \mathbb{R}^L$, $\|\mathbf{s}_k\| = 1$, $k = 1, 2, \dots, K$. In an effort to reduce the interference effect of the host signal, the host vectors $\mathbf{x}_i$ is steered away from the embedding carriers using an operator of the form $(\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)$.

Under statistical independence across messages, the mean-square-error (MSE) distortion per-block induced by each individual message is

$$\begin{aligned} \mathcal{D}_k &= \mathbb{E}\left\{\left\|\left(A_k b_{k,i} \mathbf{s}_k + (\mathbf{I}_L - c_k \mathbf{s}_k \mathbf{s}_k^T)\mathbf{x}_i\right) - \mathbf{x}_i\right\|^2\right\} \\ &= A_k^2 + c_k^2 \mathbf{s}_k^T \mathbf{R}_{\mathrm{x}} \mathbf{s}_k. \end{aligned} \tag{3}$$

The intended receiver of the kth-message bits will use a linear filter $\mathbf{w}_k$ to recover the corresponding embedded bits

$$\hat{b}_{k,i} = \operatorname{sgn}\left\{\mathbf{w}_k^T \mathbf{y}_i\right\}. \tag{4}$$

The linear filter that operates on $\mathbf{y}_i$ and offers maximum SINR at its output to the kth-message recipient is

$$\mathbf{w}_{maxSINR,k} = \mathbf{R}_{/k}^{-1} \mathbf{s}_k. \tag{5}$$

where $\mathbf{R}_{/k} \triangleq \sum_{i \neq k}^{K} A_i \mathbf{s}_i \mathbf{s}_i^T + (\mathbf{I}_L - \sum_{i=1}^{K} c_i \mathbf{s}_i \mathbf{s}_i^T)\ \mathbf{R}_x$ $(\mathbf{I}_L - \sum_{i=1}^{K} c_i \mathbf{s}_i \mathbf{s}_i^T) + \sigma_n^2 \mathbf{I}_L$ denotes the "exclude-k" data autocorrelation matrix. The output SINR value attained by $\mathbf{w}_{maxSINR,k}$ is

$$\mathrm{SINR}_{maxSINR,k} = A_k^2 \mathbf{s}_k^T \mathbf{R}_{/k}^{-1} \mathbf{s}_k\ . \tag{6}$$

If we view $\mathrm{SINR}_{maxSINR,k}$ as a function of the embedding carrier $\mathbf{s}_k$ and the transformation parameter c_k, then we can identify $\mathbf{s}_k$ and c_k that maximize the SINR value. The findings in [20] are summarized in the following Proposition.

Proposition 1: Let $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_L$ denote the eigenvectors of $\mathbf{R}_x$ with corresponding eigenvalues $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_L$, then for any given kth-message-induced distortion level $\mathcal{D}_k$, the optimal carriers and transformation parameters $(\mathbf{s}_k^{\mathrm{opt}}, c_k^{\mathrm{opt}})$, $k = 1, \dots, K$, that conditionally maximize the output SINR of the maximum SINR filters

$$\mathbf{s}_k^{\mathrm{opt}} = \mathbf{q}_k, \tag{7}$$

$$c_k^{\mathrm{opt}} = \frac{\lambda_k + \sigma_n^2 + \mathcal{D}_k - \sqrt{(\lambda_k + \sigma_n^2 + \mathcal{D}_k)^2 - 4\lambda_k \mathcal{D}_k}}{2\lambda_k}, \tag{8}$$
$$k = 1, \dots, K.$$

The target per-message distortion $\mathcal{D}_k$ is achieved when the embedding amplitude is set to $A_k = \sqrt{\mathcal{D}_k - c_k^{\mathrm{opt}\,2} \lambda_k}$, $k = 1, \dots, K$. ■

3. INFORMATION-THEORETIC SECURITY ANALYSIS

If we can model the cover vector $\mathbf{x}$ as correlated (colored) Gaussian distribution with zero mean and autocorrelation $\mathbf{R}_x$, then the probability density function of the cover data is

$$P_c(\mathbf{z}) = \frac{1}{(2\pi)^{\frac{L}{2}} \det(\mathbf{R}_x)^{\frac{1}{2}}} \exp\left(-\frac{1}{2} \mathbf{z}^T \mathbf{R}_x^{-1} \mathbf{z}\right). \tag{9}$$

Since we attempt to evaluate the impact on the host distribution *due to embedding optation only*, the external noise term in (2) can be ignored and the stego data has a form of

$$\begin{aligned} \mathbf{y}_i &= \sum_{k=1}^{K} A_k b_{k,i} \mathbf{s}_k + (\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)\mathbf{x}_i \\ &= \sum_{k=1}^{K} A_k b_{k,i} \mathbf{s}_k + \widetilde{\mathbf{x}}_i \end{aligned} \tag{10}$$

where $\widetilde{\mathbf{x}}_i \triangleq (\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)\mathbf{x}_i$ is the linearly transformed host data which also has Gaussian distribution with zero mean and autocorrelation $\mathbf{R}_{\widetilde{x}} \triangleq \mathbb{E}\{(\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)$ $\mathbf{x}\mathbf{x}^T (\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)^T\} = (\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)\, \mathbf{R}_x (\mathbf{I}_L - \sum_{k=1}^{K} c_k \mathbf{s}_k \mathbf{s}_k^T)$. Then, under the assumption that the embedded bits are independent identically distributed (i.i.d.), the probability density function of the stego data can be expressed as

$$P_s(\mathbf{z}) \quad = \quad \frac{1}{B} \sum_{j=1}^{B} \frac{1}{(2\pi)^{\frac{L}{2}} \det(\mathbf{R}_{\widetilde{x}})^{\frac{1}{2}}} \times$$

$$\exp\left(-\frac{1}{2}(\mathbf{z}-\mathbf{u}_j)^T\mathbf{R}_{\widetilde{x}}^{-1}(\mathbf{z}-\mathbf{u}_j)\right) \quad (11)$$

where, $\mathbf{u}_j = \sum_{k=1}^{K} A_k b_i^j \mathbf{s}_k$, $j = 1,\ldots,B$, is one of $B = 2^K$ possible embedded vectors, $b_k^j \in \{\pm 1\}$, $k = 1,\ldots,K$, $[b_1^j, b_2^j, \ldots, b_K^j]$ represents the jth distinct combination of K bits.

3.1. KL Distance

The probability density function of the stego data (11) can be viewed as Gaussian Mixed Model (GMM). Then, the KL distance between P_c and P_s can be calculated by

$$D_{KL}(P_c||P_s) \approx \frac{1}{B}\sum_{j=1}^{B} D_{KL}(P_c||(P_s|\mathbf{u}_j)). \quad (12)$$

The KL distance between the Gaussians $\mathcal{N}(0,\mathbf{R}_{\mathrm{x}})$ and $\mathcal{N}(\mathbf{u}_j,\mathbf{R}_{\widetilde{\mathrm{x}}})$ has the following closed form expression:

$$\begin{aligned} D_{KL}(P_c||(P_s|\mathbf{u}_j)) &= \frac{1}{2}\log\frac{\det(\mathbf{R}_{\widetilde{\mathrm{x}}})}{\det(\mathbf{R}_x)} + \frac{1}{2}\mathrm{Tr}(\mathbf{R}_{\widetilde{\mathrm{x}}}^{-1}\mathbf{R}_x) \\ &\quad + \frac{1}{2}\mathbf{u}_j^T\mathbf{R}_{\widetilde{\mathrm{x}}}^{-1}\mathbf{u}_j - \frac{L}{2}. \quad (13) \end{aligned}$$

Now we attempt to evaluate the KL distance when the optimal carriers and transformation parameters in Proposition 1 are used in the data embedding. The autocorrelation matrix $\mathbf{R}_x$ can be decomposed as $\mathbf{R}_x = \mathbf{Q}\mathbf{\Lambda}\mathbf{Q}^T$ where $\mathbf{\Lambda} \triangleq \mathrm{diag}\{\lambda_1,\lambda_2,\ldots,\lambda_L\}$, $\lambda_1 \le \lambda_2 \le \ldots \le \lambda_L$ are eigenvlues, $\mathbf{Q} = [\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_L]$ is an eigenvector matrix. With the optimal carriers $\mathbf{s}_k^{\mathrm{opt}} = \mathbf{q}_k$, $k = 1,\ldots,K$, we have property that $\mathbf{s}_k^T\mathbf{R}_x = \lambda_k\mathbf{s}_k^T$. Then, the autocorrelation matrix $\mathbf{R}_{\widetilde{x}}$ can be rewritten as

$$\begin{aligned} \mathbf{R}_{\widetilde{x}} &\triangleq (\mathbf{I}_L - \sum_{k=1}^{K} c_k\mathbf{s}_k\mathbf{s}_k^T)\mathbf{R}_x(\mathbf{I}_L - \sum_{k=1}^{K} c_k\mathbf{s}_k\mathbf{s}_k^T) \\ &= \mathbf{R}_x - 2\sum_{k=1}^{K} c_k\lambda_k\mathbf{s}_k\mathbf{s}_k^T + \sum_{k=1}^{K} c_k^2\lambda_k\mathbf{s}_k\mathbf{s}_k^T \\ &= \mathbf{Q}\widetilde{\mathbf{\Lambda}}\mathbf{Q}^T \quad (14) \end{aligned}$$

where $\widetilde{\mathbf{\Lambda}} = \mathrm{diag}\{\widetilde{\lambda_1},\widetilde{\lambda_2},\ldots,\widetilde{\lambda_L}\}$, $\widetilde{\lambda_i} = (1-c_i)^2\lambda_i$ if $i \le K$, $\widetilde{\lambda_i} = \lambda_i$ if $i > K$, $i = 1,2,\ldots,L$.

With (14), the first term in (13) can be simplified as

$$\begin{aligned} \frac{1}{2}\log\frac{\det(\mathbf{R}_{\widetilde{x}})}{\det(\mathbf{R}_x)} &= \frac{1}{2}\log\frac{\prod_{i=1}^{L}\widetilde{\lambda}_i}{\prod_{i=1}^{L}\lambda_i} = \frac{1}{2}\log\prod_{k=1}^{K}\frac{\widetilde{\lambda}_k}{\lambda_k} \\ &= \frac{1}{2}\log\prod_{k=1}^{K}(1-c_k)^2 = \sum_{k=1}^{K}\log(1-c_i). \quad (15) \end{aligned}$$

The second term in (13) can also be rewritten as

$$\frac{1}{2}\mathrm{Tr}\left(\mathbf{R}_{\widetilde{x}}^{-1}\mathbf{R}_x\right) = \frac{1}{2}\mathrm{Tr}\left(\mathbf{Q}\widetilde{\mathbf{\Lambda}}^{-1}\mathbf{\Lambda}\mathbf{Q}^T\right) = \frac{1}{2}\mathrm{Tr}\left(\widetilde{\mathbf{\Lambda}}^{-1}\mathbf{\Lambda}\right)$$

$$= \frac{1}{2}\left(L - K + \sum_{k=1}^{K}\frac{1}{(1-c_k)^2}\right). \quad (16)$$

We also can re-formulate the third term in (13) into following form

$$\begin{aligned} \frac{1}{2}\mathbf{u}_j^T\mathbf{R}_{\widetilde{x}}^{-1}\mathbf{u}_j &= \frac{1}{2}(\sum_{k=1}^{K} A_k b_k^j\mathbf{s}_k)^T\mathbf{R}_{\widetilde{x}}^{-1}(\sum_{k=1}^{K} A_k b_k^j\mathbf{s}_k) \\ &= \frac{1}{2}\sum_{k=1}^{K}\frac{A_k^2}{(1-c_k)^2\lambda_k}. \quad (17) \end{aligned}$$

By applying (15), (16), and (17) into (13) and then (12), we finally obtain the KL distance of the optimal SS embedding

$$\begin{aligned} D_{KL}(P_c||P_s) &\approx D_{KL}(P_c||(P_s|\mathbf{u}_j)) \\ &= \sum_{k=1}^{K}\log(1-c_k) + \frac{1}{2}\left(L - K + \sum_{i=1}^{K}\frac{1}{(1-c_k)^2}\right) \\ &\quad + \frac{1}{2}\sum_{k=1}^{K}\frac{A_k^2}{(1-c_k)^2\lambda_k} - \frac{L}{2} \\ &= \sum_{k=1}^{K}\log(1-c_k) + \frac{1}{2}\sum_{k=1}^{K}\frac{\lambda_k + A_k^2}{(1-c_k)^2\lambda_k} - \frac{K}{2}. \quad (18) \end{aligned}$$

The KL distance is proportional to embedding amplitude A_i and the number of messages K, but independent with the dimensionality of the embedding L. This result accords with our intuition on the SS embedding security. However, it is also well known that KL distance is not a symmetric function. Moreover, sometimes it cannot reasonably represent the difference between the host and stego distributions. As shown in (18), when the transformation operator c_k is selected close to 1, D_{KL} goes to a very large value.

3.2. Bhattacharyya Distance

To find more appropriate security measure to replace KL distance, Korzhik *et al.* proposed to use Bhattacharyya distance. With cover distribution P_c in (9) and stego distribution P_s in (11), the Bhattacharyya distance $D_B(P_c||P_s)$ is

$$D_B(P_c||P_s) = \frac{1}{8}\mathbf{u}_j^T\mathbf{R}_{\widetilde{x}}\mathbf{u}_j + \frac{1}{2}\log\frac{\det(\mathbf{R})}{\sqrt{\det(\mathbf{R}_x)\det(\mathbf{R}_{\widetilde{x}})}} \quad (19)$$

where

$$\mathbf{R} \triangleq \frac{1}{2}(\mathbf{R}_x + \mathbf{R}_{\widetilde{x}}) = \frac{1}{2}\mathbf{Q}\overline{\mathbf{\Lambda}}\mathbf{Q}^T, \quad (20)$$

$\overline{\mathbf{\Lambda}} \triangleq \mathrm{diag}\{\overline{\lambda}_1,\overline{\lambda}_2,\ldots,\overline{\lambda}_L\}$, $\overline{\lambda_i} = \frac{1}{2}(\lambda_i + (1-c_i)^2\lambda_i)$ if $i \le K$, $\overline{\lambda_i} = \lambda_i$ if $i > K$, $i = 1,2,\ldots,L$.

The first term in (19) can be rewritten as

$$\begin{aligned} \frac{1}{8}\mathbf{u}_j^T\mathbf{R}_{\widetilde{x}}\mathbf{u}_j &= \frac{1}{8}(\sum_{k=1}^{K} A_k b_k^j\mathbf{s}_k)^T\mathbf{R}^{-1}(\sum_{k=1}^{K} A_k b_k^j\mathbf{s}_k) \quad (21) \\ &= \frac{1}{8}\sum_{k=1}^{K}\frac{2A_k^2}{\lambda_k + (1-c_k)^2\lambda_k}. \quad (22) \end{aligned}$$

Since we also have

$$\det(\mathbf{R}) = \prod_{i=K+1}^{L} \lambda_i \prod_{i=1}^{K} \frac{1}{2}(\lambda_i + (1-c_i)^2\lambda_i), \quad (23)$$

$$\det(\mathbf{R}_x) = \prod_{i=1}^{L} \lambda_i, \quad (24)$$

$$\det(\mathbf{R}_{\widetilde{x}}) = \prod_{i=K+1}^{L} \lambda_i \prod_{i=1}^{K} (1-c_i)^2\lambda_i, \quad (25)$$

the second term in (19) can be re-formulated as

$$\frac{1}{2}\log\frac{\det(\mathbf{R})}{\sqrt{\det(\mathbf{R}_x)\det(\mathbf{R}_{\widetilde{x}})}} = \frac{1}{2}\log\frac{\prod_{k=1}^{K}\frac{1}{2}(1+(1-c_k)^2)\lambda_k}{\prod_{k=1}^{K}(1-c_k)\lambda_k}$$

$$= \frac{1}{2}\log\prod_{k=1}^{K}\left(\frac{1}{2(1-c_k)} + \frac{(1-c_i)}{2}\right). \quad (26)$$

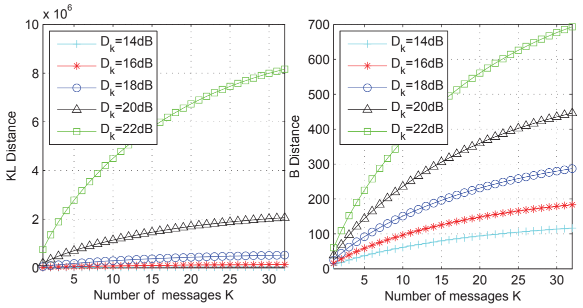
Applying (22) and (26) into (19), we finally obtain the BD expression for optimal SS embedding in a form of

$$D_B = \frac{1}{4}\sum_{k=1}^{K}\frac{A_k^2}{\lambda_k + (1-c_k)^2\lambda_k} + \frac{1}{2}\sum_{k=1}^{K}\log\left(\frac{1}{2(1-c_i)} + \frac{(1-c_i)}{2}\right). \quad (27)$$

4. EXPERIMENTAL STUDIES AND DISCUSSION

To carry out an experimental study of the security analysis, we consider data set which consists of $10,000$ 8-bit grayscale photographic images [23]. We perform 8×8 block DCT embedding over all 63 bins except the dc coefficient (i.e. $L = 63$) and embed K messages via the optimal multi-carrier SS embedding. The per-message distortion $\mathcal{D}_k$ is set at five levels $\mathcal{D}_k = \{12, 14, 16, 20, 22\}$dB. The KL distance and the Bhattacharyya distance are shown n Fig. 1 as a function of the number of carriers/messages K. It can be observed that the larger number of messages K (i.e. payload) or the larger distortion $\mathcal{D}_k$ (i.e. embedding intensity) lead to a larger distance, i.e. the less security. This results coincide our intuition about the security of SS embedding. However, we also note that KL distance is too sensitive to the distortion while Bhattacharyya distance seems is more reasonable to evaluate the security of the SS embedding with different numbers of messages and distortion levels.

To further evaluate the security of the optimal SS embedding scheme and validate the theoretic security shown in Fig. 1, we carry out experiments of a typical steganalysis attack. The same image dataset is used and $K = 4, 16, 32$ messages are embed messages via the optimal multi-carrier SS embedding with per-message distortion $\mathcal{D}_k = 14, 20$dB, respectively. Therefore, six embedding settings are considered. A popular feature [22] and support vector machine (SVM) classifier are selected in our experiment. In Fig. 2, we plot the "receiver operating characteristic" (ROC) curves that show the probability of correct identification (P_C) versus the probability of false alarm (P_{FA}). Embedding scheme with higher security can provide lower P_C with a certain P_{FA}. It can be observed from Fig. 2 that the larger number of messages K (i.e. payload) or the larger distortion $\mathcal{D}_k$ (i.e. embedding intensity) lead to higher detection rate and result in less security. This experimental results coincide with the theoretic security results shown in Fig. 1. Moreover, we notice that embedding with $K = 32$ and $D_k = 14$dB has ROC curve close to embedriding with $K = 4$ and $D_k = 20$dB. The finding is similar to the results in Fig. 1(a) and implies that Bhattacharyya distance is more appropriate for evaluating the theoretic security of the optimal multi-carrier SS embedding.



(a) (b)

Fig. 1. KL divergence versus number of messages K.

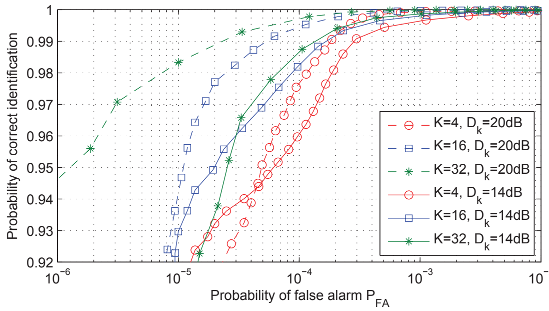


Fig. 2. ROC curves of SS steganalysis ($\mathcal{D}_k$ = 14dB, 20dB, $K = 4, 16, 32$).

5. CONCLUSION

We considered optimal multi-carrier (multiple messages) spread-spectrum (SS) data embedding and evaluated its security which quantified by both the Kullback-Leibler (KL) distance and Bhattacharyya distance. Theoretical analysis and experimental results demonstrated the impact on the security due to the number of embedding messages, the embedding distortion, and the host transformation. Bhattacharyya distance is more appropriate for evaluating the theoretic security of the optimal SS embedding.

6. REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[2] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[3] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[4] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*. New York, NY: Plenum, 1984, pp. 51-67.

[5] Y. Huang, C. Liu, S. Tang, and S. Bai, "Steganography integration into a low-bit rate speech codec," *IEEE Trans. Inf. Forens. and Security*, vol. 7, no. 6, pp. 1865-1875, Dec. 2012.

[6] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.

[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Int. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.

[8] C. Cachin, "An information-theoretic model for steganography," *Information and Computation*, vol. 192, no. 1, pp. 41?6, Jul. 2004.

[9] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563-593, March 2003.

[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2706-2722, June 2008.

[11] V. Korzhik, H. Imai, and J. Shikata, G. Morales-Luna, and E. Gerling, "On the use of Bhattacharyya Distance as a measure of the detectability of steganographic systems," *Trans. DHMS III, LNCS 4920, Heidelberg: Springer-Verlag*, pp. 23-32, 2008.

[12] L. M. Marvel, C. G. Boncelet Jr., and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Image Process.*, vol. 8, no. 8, pp. 1075-1083, Aug. 1999.

[13] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[14] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Process.*, vol. 9, no. 1, pp. 55-68, Jan. 2000.

[15] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, no. 3, pp. 273-284, Sept. 2001.

[16] 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, no. 2, pp. 126-144, Feb. 2004.

[17] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 898-905, Apr. 2003.

[18] A. Valizadeh and Z. J. Wang, "Correlation-and-bit-aware spread spectrum embedding for data hiding," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 2, pp. 267-282, June 2011.

[19] 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 Proce. (ICIP)*, Singapore, Oct. 2004, pp. 1561-1564.

[20] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 391-405, Feb. 2007.

[21] J. R. Hershey and P. A. Olsen, "Approximating the Kullback Leibler divergence between Gaussian mixture models," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP)*, Honolulu, HI, April 2007, vol. 4, pp. 317-320.

[22] T. Pevny and P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forens. and Security*, vol. 5, no. 2, pp. 215-224, Feb. 2010.

[23] T. Filler, T. Pevny, and P. Bas. *BOSS, Break Our Steganography System*. [Online]. Available: http://www.agents.cz/boss/