Extracting Spread-Spectrum Hidden Data Based on Better Lattice Decoding

Fan Yang, Hao Cheng, and Shanxiang Lyu(✉)

College of Cyber Security, Jinan University, Guangzhou 510632, China
lsx07@jnu.edu.cn

Abstract. This paper considers the blind extraction of hidden data embedded by the multi-carrier spread-spectrum scheme. Since the conventional multi-carrier iterative generalize least-squares (M-IGLS) scheme suffers from performance degradation when the carriers lack sufficient orthogonality, we develop a novel blind extraction scheme called multi-carrier iterative successive interference cancellation (M-ISIC). M-ISIC is formulated from the perspective of lattices, and it employs a successive interference cancellation subroutine to solve the lattice decoding problem. We show that M-ISIC outperforms M-IGLS by both theoretical justification and numerical simulations.

Keywords: blind extraction · spread spectrum · lattices · successive interference cancellation

1 Introduction

Steganography describes the act of secretly embedding messages into various forms of multimedia (also called the cover data) [7,9,19,20]. It has a close connection to data hiding and watermarking, as they all resemble the variants of communication with side information [5]. Their research goals include reducing the amount of distortion to the cover data so as to get unnoticeable, improving the amount of embedded bits, and rising the security level of the embedding scheme.

Many Steganography/data-hiding schemes have been developed in the past three decades (see, e.g., [1,4,6,12,14]), in which the spread-spectrum (SS) scheme and its variants are among the most popular ones. By using a similar principle as in spread-spectrum communication, the SS method was originally introduced by Cox et al. [3]. In SS, the message is dispersed into many frequency bins contained in the host signal, which makes the energy in each one extremely

This work was supported in part by the National Natural Science Foundation of China under Grants 61902149 and 62032009, the Natural Science Foundation of Guangdong Province under Grant 2020A1515010393, and the Major Program of Guangdong Basic and Applied Research under Grant 2019B030302008.

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 169–182, 2023.
https://doi.org/10.1007/978-3-031-36574-4_10

small and certainly undetectable. SS has been improved in many aspects. E.g, using the technique of minimum-mean-square error to reduce the interference caused by the host itself [15], improving signature design to reduce the decoding error rate [1], and using multi-carriers instead of a single carrier to improve the number of payloads [10,11].

In recent years, the steganalysis of SS has drawn more attention, especially from the perspective of "Watermarked Only Attack" (WOA). In WOA neither the original host nor the embedding carriers (i.e., the spreading sequences) are assumed known, as its goal is to fully extract the embedded data. To crack the single-carrier SS method, an iterative generalize least squares (IGLS) was proposed in [8], which shows remarkable recovery performance and low complexity. Since an embedder may favor multi-carrier SS transform-domain embedding to increase security/payload, its corresponding steganalysis seems more important. As the underlying mathematical problem is akin to blind source separation (BSS) in speech signal processing, celebrated BSS algorithms such as independent component analysis (ICA) [2] and Joint Approximate Diagonalization of Eigenmatrix (JADE) [18] may be utilized to extract the hidden data. Nevertheless, these BSS algorithms are far from being effective as the multi-carrier SS problem exhibits correlated signal interference [10]. In this regard, Li Ming et al. [10] developed an improved IGLS scheme referred to as multi-carrier iterative generalized least-squares (M-IGLS), whose recovery error probability is close to those of non-blind extraction algorithms.

What motivates this work is that we notice the problem of cracking multi-carrier SS parallels lattice decoding in part. Lattice decoding asks to find the closest lattice vector to a given query vector, in which the message space is the integer set. Multi-carrier SS only involves a special case of lattice decoding where the message space is $\{\pm 1\}$. In addition, since the extraction performance of M-IGLS hinges on a simple lattice decoding algorithm referred to as zero-forcing (ZF), M-IGLS can exhibit satisfactory performance only when the carriers/signatures show sufficient orthogonality. For instance, the simulation of M-IGLS [10] only consider the case of embedding (and extracting) 4 data streams by modifying 63 host coefficients. If the multi-carrier SS has a larger number of embedded data streams within the same number host coefficients, then more sophisticated lattice decoding algorithms become beneficial. By addressing the above issues, the contributions of this work are summarized as follows:

– First, we formulate the problem of cracking multi-carrier SS as a lattice decoding problem. To be concise, the problem can be regarded as the blind extraction of integer sources under the noisy setting, which asks to find the mixing matrix and the integer messages. In an alternating minimization principle, the extraction algorithm should estimate the mixing matrix and the integer messages iteratively. Then with the availability of the mixing matrix, estimating the integer messages is exactly what lattice decoding favors. The term "Least Square" in IGLS and M-IGLS originates from detection design of using no prior information on the source messages, this makes them naturally suboptimal as the prior information for integer sources ($\{\pm 1\}$) has been omitted.

In addition, the part of "Least Square" in M-IGLS is conceived as the ZF algorithm in lattice decoding.
- Second, we propose a new hidden data extraction referred to as multi-carrier iterative successive interference cancellation (M-ISIC). We show that M-ISIC outperforms M-IGLS by both theoretical justification and numerical simulations, where the performance improvement is due to a better lattice algorithm used in the subroutine. Thanks to the lattice-based formulation, the proposed algorithm can also address the scenario when the number of signatures is unknown.

The rest of this paper is organized as follows. In Sect. 2, preliminaries on SS embedding and blind extraction are briefly introduced. In Sect. 3, the proposed algorithm is introduced and comparisons are made. Simulation results are shown in Sect. 4 and Sect. 5 concludes this paper.

The following notation is used throughout the paper. Boldface upper-case and lower-case letters represent matrices and column vectors, respectively. $\mathbb{R}$ denotes the set of real numbers, while $\mathbf{I}$ denotes an identity matrix. $(\cdot)^\top$ is the matrix transpose operator, and $||\cdot||$, $||\cdot||_F$ denote vector norm, and matrix Frobenius norm, respectively. sign$(\cdot)$ represents a quantization function with respect to $\{-1, 1\}$.

2 Preliminaries

2.1 SS Embedding and Legitimate Extraction

Without loss of generality, we consider a gray-scale host image $\mathbf{H} \in \mathcal{M}^{N_1 \times N_2}$, where $\mathcal{M}$ denotes the image alphabet and $N_1 \times N_2$ denotes the size of the image. Then $\mathbf{H}$ is partitioned into M non-overlapping blocks $\mathbf{H}_1, ..., \mathbf{H}_M$ (of size $\frac{N_1 \times N_2}{M}$). By performing DCT transformation and zig-zag scanning for each block, the cover object in each block can be generated as $\mathbf{x}(m) \in \mathbb{R}^L$, $m = 1, ..., M$. By excluding the DC coefficient, L can be set as $1 \leq L \leq \frac{N_1 \times N_2}{M}$.

In multi-carrier SS, it employs K distinct carriers (signatures) $\mathbf{s}_1, ..., \mathbf{s}_K$ to embed K bits of messages $b_1, ..., b_K \in \{\pm 1\}$ to each $\mathbf{x}(m)$. In general $K \leq L$ such that these signature vectors can exhibit sufficient mutual orthogonality in the L dimensional space. Subsequently, the modified cover (stego) is generated by

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m) \mathbf{s}_k + \mathbf{x}(m) + \mathbf{n}(m), \ m = 1, 2, ..., M, \tag{1}$$

where A_k denotes the embedding amplitude of $\mathbf{s}_k$, $b_k(m)$ denotes the messages of the mth block, and $\mathbf{n}(m)$ represents the additive white Gaussian noise vector of mean $\mathbf{0}$ and covariance $\sigma_n^2 \mathbf{I}_L$. By taking expectation over the randomness of $\mathbf{s}_k$, the embedding distortion due to $A_k b_k(m) \mathbf{s}_k$ is

$$D_k = \mathbb{E}\{||A_k b_k(m) \mathbf{s}_k||^2\} = A_k^2, \ k = 1, 2, ..., K. \tag{2}$$

Algorithm 1: The M-IGLS data extraction algorithm.

Input: $\mathbf{Y}$, $\mathbf{R_y}$.
Output: $\hat{\mathbf{V}} = \mathbf{V}^{(d)}$, $\hat{\mathbf{B}} = \mathbf{B}^{(d)}$.
$d = 0$, $\mathbf{B}^{(0)} \sim \{\pm 1\}^{K \times M}$;
while *a stopping criterion has not been reached* **do**
  $d \leftarrow d + 1$;
  $\mathbf{V}^{(d)} \leftarrow \mathbf{Y}(\mathbf{B}^{(d-1)})^{\mathrm{T}}[\mathbf{B}^{(d-1)}(\mathbf{B}^{(d-1)})^{\mathrm{T}}]^{-1}$;
  $\mathbf{B}^{(d)} \leftarrow \text{sign}\left\{\left((\mathbf{V}^{(d)})^{\mathrm{T}}\mathbf{R}_{\mathbf{y}}^{-1}\mathbf{V}^{(d)}\right)^{-1}(\mathbf{V}^{(d)})^{\mathrm{T}}\mathbf{R}_{\mathbf{y}}^{-1}\mathbf{Y}\right\}$; ▷ Approximate lattice decoding via GLS/ZF.

Based on the statistical independence of signatures $\mathbf{s}_k$, the averaged total distortion per block is defined as $D = \sum_{k=1}^{K} D_k = \sum_{k=1}^{K} A_k^2$.

In the receivers' side, legitimate users can employ the pre-shared secrets/signatures $\mathbf{s}_k$ to generate high-quality estimates of messages $b_k(m)$. Define the auto-correlation matrix of $\mathbf{y}(m)$ from that of the host auto-correlation $\mathbf{R_x}$ and noise auto-correlation as:

$$\mathbf{R_y} = \mathbf{R_x} + \sum_{k=1}^{K} A_k^2 \mathbf{s}_k \mathbf{s}_k^{\top} + \sigma_n^2 \mathbf{I}_L. \tag{3}$$

Then the minimum-mean-square-error (MMSE) estimation of the messages is given by

$$\hat{b}_k(m) = \text{sign}\{\mathbf{s}_k^{\top} \mathbf{R}_{\mathbf{y}}^{-1} \mathbf{y}(m)\}. \tag{4}$$

2.2 Blind SS Extraction

The observation Eq. (1) can be written in the form of matrices:

$$\mathbf{Y} = \mathbf{V}\mathbf{B} + \mathbf{Z} \tag{5}$$

where $\mathbf{Y} \triangleq [\mathbf{y}(1), ..., \mathbf{y}(M)] \in \mathbb{R}^{L \times M}$, $\mathbf{B} \triangleq [\mathbf{b}(1), ..., \mathbf{b}(M)] \in \{\pm 1\}^{K \times M}$, $\mathbf{V} \triangleq [A_1 \mathbf{s}_1, ..., A_M \mathbf{s}_M] \in \mathbb{R}^{L \times K}$, $\mathbf{Z} \triangleq [\mathbf{x}(1) + \mathbf{n}(1), ..., \mathbf{x}(M) + \mathbf{n}(M)] \in \mathbb{R}^{L \times M}$.

The difference between legitimate extraction and blind extraction lies in the availability of $\mathbf{V}$. The task of a blind extraction requires estimating both $\mathbf{V}$ and $\mathbf{B}$ from the observation $\mathbf{Y}$, which is known as the noisy BSS problem:

$$\mathcal{P}_1 : \min_{\substack{\mathbf{B} \in \{\pm 1\}^{K \times M} \\ \mathbf{V} \in \mathbb{R}^{L \times K}}} ||\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})||_F^2, \tag{6}$$

where $\mathbf{R_z} \triangleq \mathbf{R_x} + \sigma_n^2 \mathbf{I}_L$ denotes the pre-whitening matrix. Nevertheless, enumerating all the feasible candidates of $\mathbf{V}$ and $\mathbf{B}$ is infeasible as it incurs exponential complexity.

The M-IGLS proposed by Li et al. can approximately solve (6) efficiently. The pseudo-code of M-IGLS is shown in Algorithm 1. Specifically, M-IGLS estimates $\mathbf{V}$ and $\mathbf{B}$ iteratively by using an MMSE criterion: by either fixing $\mathbf{B}^{(d)}$ or $\mathbf{V}^{(d)}$ and using convex optimization, the formulas for $\mathbf{B}^{(d)}$ or $\mathbf{V}^{(d)}$ are derived.

2.3 Lattice Decoding

To inspect M-IGLS, we review some basic knowledge of lattices as follows. Lattices are discrete additive subgroups. Given K linearly independent vectors $\mathbf{g}_1, ..., \mathbf{g}_K \in \mathbb{R}^L$ with $L \geq K$, they can define a lattice as

$$\mathcal{L}(\mathbf{G}) = \left\{ \sum_{k=1}^{K} x_k \mathbf{g}_k \mid x_k \in \mathbb{Z} \right\} \tag{7}$$

where $\mathbf{G} \triangleq [\mathbf{g}_1, ..., \mathbf{g}_K]$ is called lattice basis.

Many computationally hard problems can be defined over lattices. The one related to this work is called the closest vector problem (CVP) [16]: given a query vector $\mathbf{t}$, it asks to find the closest vector to $\mathbf{t}$ from the set of lattice vectors $\mathcal{L}(\mathbf{G})$. Let the closest vector be $\mathbf{Gx}$, $\mathbf{x} \in \mathbb{Z}^K$, then we have

$$\|\mathbf{Gx} - \mathbf{t}\| \leq \|\mathbf{G}\tilde{\mathbf{x}} - \mathbf{t}\|, \forall \tilde{\mathbf{x}} \in \mathbb{Z}^K. \tag{8}$$

After the detour, consider the step of estimating $\mathbf{B}^{(d)}$ in Algorithm 1, which asks to solve the following problem:

$$\mathcal{P}_2 : \min_{\mathbf{B} \in \{\pm 1\}^{K \times M}} ||\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} \mathbf{Y} - \mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} \mathbf{VB}||_F^2. \tag{9}$$

Since $\{\pm 1\}^{K \times M} \in \mathbb{Z}^{K \times M}$, $\mathcal{P}_2$ is a special case of CVP, which asks to find M closest lattice vectors to $\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} \mathbf{Y}$, and the lattice is defined by basis $\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} \mathbf{V}$.

In general solving CVP for a random lattice basis incurs exponential computational complexity in the order of $\mathcal{O}(2^K)$, but for lattice basis whose $\mathbf{g}_1, ..., \mathbf{g}_K$ are close to being orthogonal, fast low-complexity algorithm can approximately achieve the performance of maximum likelihood decoding. One of such algorithm is called ZF [13]. Considering $\mathcal{P}_2$, define the set of query vectors as $\overline{\mathbf{Y}} \triangleq \mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} \mathbf{Y}$, and the lattice basis as $\overline{\mathbf{V}} \triangleq \mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} \mathbf{V}$, then the ZF estimator is

$$\begin{aligned} \hat{\mathbf{B}}_{\mathrm{ZF}} &= \overline{\mathbf{V}}^{\dagger} \overline{\mathbf{Y}}^{\mathrm{T}} \\ &= (\overline{\mathbf{V}}^{\mathrm{T}} \overline{\mathbf{V}})^{-1} \overline{\mathbf{V}}^{\mathrm{T}} \overline{\mathbf{Y}}^{\mathrm{T}}. \end{aligned} \tag{10}$$

In Appendix A, we show that the geometric least square (GLS) step in line 5 of M-IGLS is the same as ZF. The ZF estimator is linear, which behaves like a linear filter and separates the data streams and thereafter independently decodes each stream. The drawback of ZF is the effect of noise amplification when the lattice basis $\overline{\mathbf{V}}$ is not orthogonal.

3 The Proposed Method

From the viewpoint of lattices, we can improve the ZF detector in M-IGLS by using other lattice decoding algorithms. Based on this idea, a novel hidden data extraction algorithm is proposed. In the following subsections, we will present our scheme and analyze its performance.

3.1 M-ISIC

By using decision feedback in the decoding process, the nonlinear Successive Interference Cancellation (SIC) detector has better performance than ZF. Recall that for $\mathcal{P}_2$, the lattice basis is $\overline{\mathbf{V}}$, and the set of query vectors are $\overline{\mathbf{Y}}$. The SIC algorithm consists of the following steps:

Step i) Use QR decomposition to factorize $\overline{\mathbf{V}}$: $\overline{\mathbf{V}} = \mathbf{QR}$[1], where $\mathbf{Q} \in \mathbb{R}^{L\times L}$ denotes a unitary matrix and $\mathbf{R} \in \mathbb{R}^{L\times K}$ is an upper triangular matrix of the form:

$$\mathbf{R} = \begin{bmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,K} \\ 0 & R_{2,2} & \cdots & R_{2,K} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R_{K,K} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{11}$$

Step ii) Construct $\mathbf{Y}^{'} = \mathbf{Q}^{\top}\overline{\mathbf{Y}} \in \mathbb{R}^{L\times M}$, which consists of vectors $\mathbf{y}^{'}(1), ..., \mathbf{y}^{'}(M)$.

Step iii) For $m = 1, ..., M$, generate the estimation as

$$\hat{b}_K(m) = \text{sign}\left(\frac{y'_K(m)}{R_{K,K}}\right), \tag{12}$$

$$\hat{b}_k(m) = \text{sign}\left(\frac{y'_k(m) - \sum_{l=k+1}^{K} R_{k,l}\hat{b}_l(m)}{R_{k,k}}\right), \tag{13}$$

where $k = K-1, K-2, ..., 1$, and $y'_k(m)$ denotes the kth component of $\mathbf{y}^{'}(m)$.

By substituting the Step 5 in Algorithm 1 with the SIC steps, we obtain a new algorithm referred to as multi-carrier iterative successive interference cancellation (M-ISIC). Its pseudo-codes are presented in Algorithm 2. Notably, $\mathbf{V}^{(d)}$ is estimated in the same way as that of M-IGLS, and the performance improvements rely on SIC decoding. The stopping criterion can be set as when $||\mathbf{B}^{(d)} - \mathbf{B}^{(d-1)}||_F^2 < 10^{-5}$.

Remark 1. The rationale of SIC is explained as follows. When detecting multiple symbols, if one of them can be estimated first, the interference caused by the already decoded can be eliminated when solving another, so as to reduce the effective noise of the symbol to be solved and to improve the bit error rate performance. To be concise, denote the observation equation corresponding to $\mathcal{P}_2$ as

$$\overline{\mathbf{Y}} = \overline{\mathbf{V}}\mathbf{B} + \overline{\mathbf{Z}}, \tag{14}$$

[1] For better performance, this paper adopts a sorted version of QR decomposition, where the column vectors in $\overline{\mathbf{V}}$ are sorted from short to long.

Algorithm 2: The M-ISIC data extraction algorithm.

Input: $\mathbf{Y}$, $\mathbf{R_z}$.
Output: $\hat{\mathbf{V}} = \mathbf{V}^{(d)}$, $\hat{\mathbf{B}} = \mathbf{B}^{(d)}$.
$d = 0$, $\mathbf{B}^{(0)} \sim \{\pm 1\}^{K \times M}$;
while *a stopping criterion has not been reached* **do**
  $d \leftarrow d + 1$;
  $\mathbf{V}^{(d)} \leftarrow \mathbf{Y}(\mathbf{B}^{(d-1)})^{\mathrm{T}}[\mathbf{B}^{(d-1)}(\mathbf{B}^{(d-1)})^{\mathrm{T}}]^{-1}$;
  Employ Steps i)-iii) of SIC to estimate $\mathbf{B}^{(d)}$ ▷ Approximate lattice decoding via SIC.

with $\overline{\mathbf{Z}}$ being the effective noise. Then the multiplication of $\mathbf{Q}^{\top}$ to (14) is simply a rotation, which maintain the Frobenius norm of the objective function:

$$||\overline{\mathbf{Y}} - \overline{\mathbf{V}}\mathbf{B}||_F^2 = ||\overline{\mathbf{Z}}||_F^2 \tag{15}$$

$$= ||\mathbf{Q}^{\top}\overline{\mathbf{Z}}||_F^2 \tag{16}$$

$$= ||\mathbf{Q}^{\top}\overline{\mathbf{Y}} - \mathbf{R}\mathbf{B}||_F^2. \tag{17}$$

Regarding Step iii), $\hat{b}_K(m), ..., \hat{b}_1(m)$ are estimated in descending order because the interference caused by these symbols can be canceled. Moreover, the divisions of $R_{K,K}, ..., R_{1,1}$ in Eqs. (12) (13) imply that the effective noise level hinges on the quality of $R_{K,K}, ..., R_{1,1}$.

3.2 Performance Analysis

We argue that M-ISIC theoretically outperforms M-IGLS, as SIC has better decoding performance than ZF when approximately solving $\mathcal{P}_2$. With a slight abuse of notations, $\mathcal{P}_2$ can be simplified as M instances of the following observation:

$$\mathbf{y} = \mathbf{R}'\mathbf{b}^* + \mathbf{z} \tag{18}$$

where $\mathbf{y} \in \mathbb{R}^K$, $\mathbf{b}^* \in \{\pm 1\}^K$ is the transmitted message, $\mathbf{R}' \in \mathbb{R}^{K \times K}$ includes only the first K rows of (11), and we assume that $\mathbf{z}$ also admits a Gaussian distribution with mean $\mathbf{0}$ and covariance $\sigma_n^2\mathbf{I}_K$. Then the lattice decoding task becomes

$$\mathcal{P}_3 : \min_{\mathbf{b} \in \{\pm 1\}^K} ||\mathbf{y} - \mathbf{R}\mathbf{b}||^2. \tag{19}$$

It has been shown in the literature [13,21] that SIC outperforms ZF if the constraint of $\mathbf{b}$ in $\mathcal{P}_3$ is an integer set $\mathbb{Z}^K$ and a box-constrained (truncated continuous integer) set $\mathcal{B}$. Therefore, we employ a model reduction technique to show that SIC has higher success probability when decoding $\mathcal{P}_3$.

Proposition 1. *Let the SIC and ZF estimates of* $\mathcal{P}_3$ *be* $\mathbf{b}^{\mathrm{SIC}}$ *and* $\mathbf{b}^{\mathrm{ZF}}$*, respectively. Then the averaged decoding success probability of SIC is higher than that of ZF:*

$$\mathbb{E}_{\mathbf{b}^*}\{\Pr(\mathbf{b}^{\mathrm{SIC}} = \mathbf{b}^*)\} \geq \mathbb{E}_{\mathbf{b}^*}\{\Pr(\mathbf{b}^{\mathrm{ZF}} = \mathbf{b}^*)\}, \tag{20}$$

where the expectation is taken over uniform random $\mathbf{b}^* \in \{\pm 1\}^K$.

Proof. Firstly, Eq. (18) is rewritten as

$$(\mathbf{y} + \mathbf{R} \times \mathbf{1})/2 = \mathbf{R}(\mathbf{b}^* + \mathbf{1})/2 + \mathbf{z}/2. \tag{21}$$

By updating the query vector $\mathbf{y}$ as $\mathbf{y}' \triangleq (\mathbf{y} + \mathbf{R} \times \mathbf{1})/2$, the bipolar constraint model $\mathcal{P}_3$ is transformed to the following box-constrained model $\mathcal{P}_4$:

$$\mathcal{P}_4 : \min_{\mathbf{b} \in \mathcal{B}} ||\mathbf{y}' - \mathbf{R}\mathbf{b}||^2, \tag{22}$$

where the constraint of the variable is $\mathcal{B} = \{0, 1\}^K$. Since [21][Thm. 9] has shown that Eq. (20) holds in this type of box-constrained model, the proposition is proved.

If $\overline{\mathbf{V}}$ is close to being an orthogonal matrix, then ZF and SIC detection can both achieve maximum likelihood estimation. The reason is that they are all solving a much simpler quantization problem $\min_{\mathbf{b} \in \{\pm 1\}^K} ||\mathbf{y} - \mathbf{I}_K \mathbf{b}||^2$. In general, the performance gap between ZF and SIC depends on the degree of orthogonality of the lattice basis $\overline{\mathbf{V}}$. To quantify this parameter, we introduce the normalized orthogonality defect of a matrix as

$$\delta(\overline{\mathbf{V}}) = \left(\frac{\prod_{k=1}^{K} ||\overline{\mathbf{v}}_k||}{\sqrt{\det(\overline{\mathbf{V}}^\top \overline{\mathbf{V}})}} \right)^{1/K}, \tag{23}$$

where the column vectors of $\overline{\mathbf{V}} = [\overline{\mathbf{v}}_1, ..., \overline{\mathbf{v}}_K]$ are linear independent. From Hardamard's inequality, $\delta(\overline{\mathbf{V}})$ is always larger than or equal to 1, with equality if and only if the columns are orthogonal to each other. Summarizing the above, SIC performs better than ZF in general, and their performance gap decreases as $\delta(\overline{\mathbf{V}}) \to 1$.

3.3 Unknown Number of Signatures

In real-world scenarios it may be more reasonable to assume that the number of carriers/signatures (i.e., K) is unknown. Fortunately, our lattice-based formulation can incorporate this setting in a straightforward manner. The observation equation can still be written as Eq. (5), but the constraints are changed to

$$\mathbf{V} \in \mathbb{R}^{L \times L}, \mathbf{B} \in \{-1, 0, 1\}^{L \times M}. \tag{24}$$

Then the objective function becomes

$$\mathcal{P}_5 : \min_{\substack{\mathbf{B} \in \{-1,0,1\}^{L \times M} \\ \mathbf{V} \in \mathbb{R}^{L \times L}}} ||\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}} (\mathbf{Y} - \mathbf{V}\mathbf{B})||_F^2, \tag{25}$$

Here $\mathbf{R}_{\mathbf{z}}$ can be set as an identity matrix if it cannot be available. By solving $\mathcal{P}_5$, the non-zero messages indicate the number of signatures. For instance, when $\hat{b}_k(m) = 0$, it implies that the kth column of $\mathbf{V}$ is redundant and inactivated.

Both M-ISIC and M-IGLS can be slightly modified to address $\mathcal{P}_5$, where the needed modification is to change the quantization function from the binary quantization $\text{sign}(\cdot)$ to a ternary quantization $\mathcal{Q}_{\{-1,0,1\}}(\cdot)$. In the same vein, Proposition 1 also holds when the number of signatures is unknown.

3.4 Computational Complexity

To compare with M-IGLS and exiting schemes, we give the computational complexity of M-ISIC based on the following conditions:

- The complexity of the multiplication of two matrices $\mathbf{A} \in \mathbb{R}^{M\times N}$ and $\mathbf{B} \in \mathbb{R}^{N\times K}$ is $\mathcal{O}(MNK)$.
- The complexity of an inversion over the square matrix $\mathbf{A} \in \mathbb{R}^{N\times N}$ is $\mathcal{O}(N^3)$.
- The complexity of performing QR decomposition on matrix $\mathbf{A} \in \mathbb{R}^{M\times N}$, $M > N$, is $\mathcal{O}(2MN^2)$.

Notice that $\mathbf{Y} \in \mathbb{R}^{L\times M}$, $\mathbf{V} \in \mathbb{R}^{L\times K}$ and $\mathbf{B} \in \mathbb{R}^{K\times M}$, the computational complexity of Step 4 in M-ISIC is

$$\mathcal{O}(K^3 + K^2(L + M) + LMK).$$

The computational complexity of Step 5 is dominated by the QR decomposition, which is

$$\mathcal{O}\left(K^2L + M(LK + K)\right).$$

The computational complexity of each iteration of the algorithm is summarized as

$$\mathcal{O}\left(K^3 + 2LMK + K^2(3L + M) + KM\right).$$

With a total of T iterations, the overall complexity is

$$\mathcal{O}\left(T(K^3 + 2LMK + K^2(3L + M) + KM)\right).$$

4 Experimental Studies

This section performs numerical simulations to verify the effectiveness and accuracy of our scheme. Benchmark algorithms include: *i)* M-IGLS [10], *ii)* sample-matrix-inversion minimum mean square error (SMI-MMSE) [10], *iii)* ideal minimum mean square error (ideal MMSE) [10], *iv)* JADE [18]. The following experiments are run on Matlab R2018b. To ensure fair comparisons, M-IGLS and M-ISIC are initialized with the same $\mathbf{B}^{(0)}$.

Without loss of generality, the carrier images are taken from the BOWS-2 database [17], composed of 10,000 grey-level images, with different statistical properties. Some typical images are displayed in Fig. 1. We employ 8×8 block-wise DCT transform on the original images and select all bins except the DC value to embed message sequences. The simulations investigate the scenarios with known and unknown number of carriers separately. The normalized orthogonality defect of the simulated carriers are shown in Table 1. The entries in the matrix $\overline{\mathbf{V}}$ are taken from standard Gaussian distribution, and by varying the size of $L \times K$, the carriers exhibit different $\delta(\overline{\mathbf{V}})$.

The bit-error-rate (BER), as a common performance index, is employed to measure the decoding performance. The noise power is fixed as $\sigma_n^2 = 1$ and the signal-to-noise ratio is controlled by varying the distortion D.

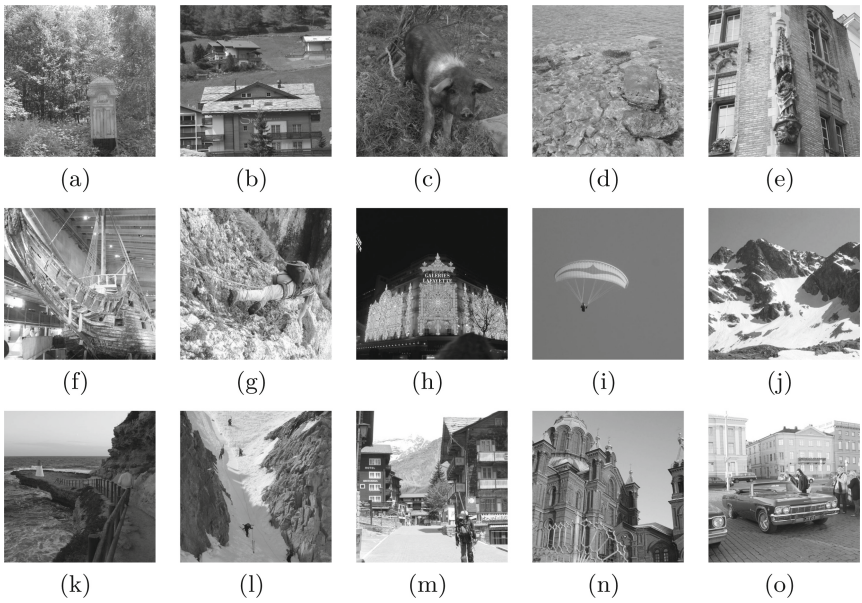

Fig. 1. Some representative images in the BOWS-2 database.

Table 1. The normalized orthogonality defect of the simulated carriers.

Knowledge of K	Known			Unknown	
$L \times K$	8×8	32×28	32×20	20×8	16×4
$\delta(\overline{\mathbf{V}})$	2.2123	1.4420	1.2297	1.1171	1.0582

4.1 Known Number of Carriers

In the following, we consider the cases with $\delta(\overline{\mathbf{V}}) = 2.2123, 1.4420, 1.2297$ for the sake of exploring the influence of the lattice bases.

In the first example, we consider the case with $L = 8$, $K = 8$, $\delta(\overline{\mathbf{V}}) = 2.2123$. The BER versus distortion performance of different algorithms are plotted in Fig. 2. With the exact carriers' information, the SMI-MMSE and Ideal-MMSE algorithms serve as the performance upper bounds. The BSS approach, JADE fails to exhibit satisfactory performance. Moreover, M-ISIC outperforms M-IGLS in the whole distortion range of 24–38 dB, over which the improvement can be as large as 4 dB.

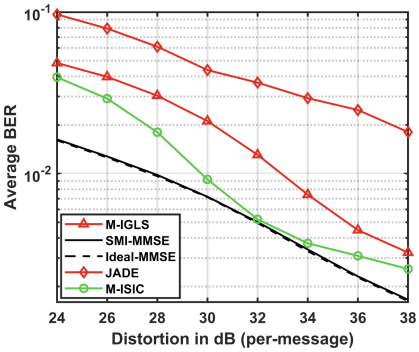

Fig. 2. BER versus distortion ($L = 8$, $K = 8$, $\delta(\overline{\mathbf{V}}) = 2.2123$).

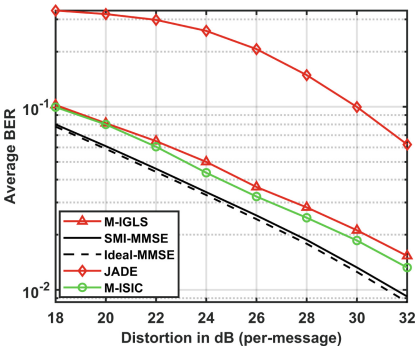

Fig. 3. BER versus distortion ($L = 32$, $K = 28$, $\delta(\overline{\mathbf{V}}) = 1.4420$).

The second example examines the case with $L = 32$, $K = 28$, $\delta(\overline{\mathbf{V}}) = 1.4420$. As depicted in Fig. 3, when the carriers become more orthogonal, both M-IGLS and M-ISIC get closer to SMI-MMSE and Ideal-MMSE. The performance gap between M-IGLS and M-ISIC has become smaller, in which the improvement is about 1 dB. Similar results can be replicated when we further reduce the normalized orthogonality defect. We post one of such figures in Fig. 4 without further comments.

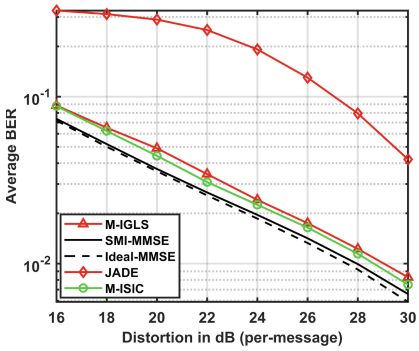

Fig. 4. BER versus distortion ($L = 32$, $K = 20$, $\delta(\overline{\mathbf{V}}) = 1.2297$).

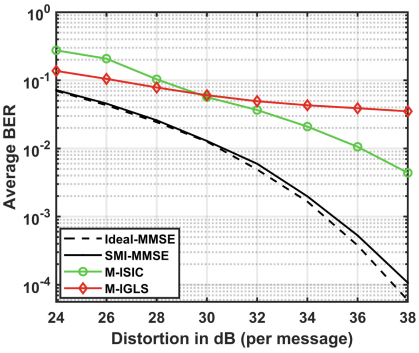

Fig. 5. BER versus distortion ($L = 20$, $K = 8$ is unknown, $\delta(\overline{\mathbf{V}}) = 1.1171$).

From the above, we observe that the performance of M-ISIC is generally not worse than that of M-IGLS. When the carriers $\overline{\mathbf{V}}$ represents a bad lattice basis, M-ISIC apparently outperforms M-IGLS. On the other hand, when the carriers are highly orthogonal, the decision regions of M-IGLS and M-ISIC become similar in shape, then the performance of the two algorithms tends to be the same.

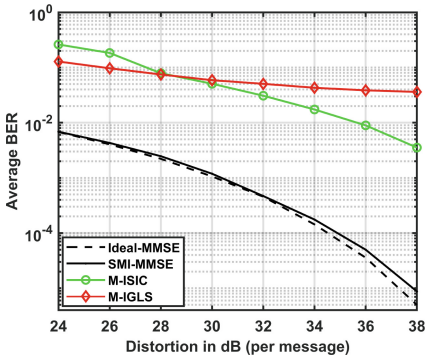

Fig. 6. BER versus distortion ($L = 16$, $K = 4$ is unknown, $\delta(\overline{\mathbf{V}}) = 1.0582$).

4.2 Unknown Number of Carriers

Hereby we investigate the performance of different algorithms for the more realistic scenario with K being unknown. As mentioned in Sect. 3.3, the setting of M-ISIC and M-IGLS are as follows. Initialize $\mathbf{V}$ and $\mathbf{B}$ as matrices with size $L \times L$ and $L \times M$ respectively, and then calculate $\mathbf{B}$ in the same way, except that the quantization function is slightly modified. Here $\mathbf{R}_z$ is replaced by an identity matrix for performance enhancement.

Figures 5 and 6 plot the BER figures with $\delta(\overline{\mathbf{V}}) = 1.1171$ and 1.0582. It turns out that our method still outperforms M-IGLS in most of the distortion range. Since K and the carriers' information are known for ideal-MMSE and SMI-MMSE, they significantly outperform M-IGLS and M-ISIC. As the constraint of the lattice decoding algorithms has increased from binary alphabets to ternary alphabets, the performance degradation of M-ISIC and M-IGLS are reasonable. Nevertheless, sine M-ISIC can generally achieve a small BER of about 10^{-2}, it justifies that multi-carrier SS can be cracked even when K is unknown.

5 Conclusions

This paper explores the issue of extracting spread-spectrum hidden data from digital media and proposes an accurate and more general algorithm based on better lattice decoding. To verify the superiority of our algorithm, M-ISIC is compared with M-IGLS and other non-blind algorithms. The experimental results demonstrate that M-ISIC enjoys better decoding performance especially when the normalized orthogonality defect of the carriers becomes large.

A The Equivalence of GLS and ZF

Assuming $\mathbf{V}$ is known, the least-squares estimation [10] of $\mathbf{B}$ used in Step 5 of Algorithm 1 is:

$$\begin{aligned}
\hat{\mathbf{B}}_{\mathrm{GLS}} &= \left(\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{y}}^{-1}\mathbf{V}\right)^{-1}\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{y}}^{-1}\mathbf{Y} \\
&= \left(\left(\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{z}}^{-1}\mathbf{V}\right)^{-1} + \mathbf{I}\right)\mathbf{V}^{\top} \\
&\quad \times \left(\mathbf{R}_{\mathbf{z}}^{-1} - \mathbf{R}_{\mathbf{z}}^{-1}\mathbf{V}\left(\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{z}}^{-1}\mathbf{V} + \mathbf{I}\right)^{-1}\mathbf{V}^{\top}\mathbf{R}_{\mathbf{z}}^{-1}\right) \\
&= \left(\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{z}}^{-1}\mathbf{V}\right)^{-1}\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{z}}^{-1}\mathbf{Y} \\
&= \left(\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{V}\right)^{-1}\mathbf{V}^{\mathrm{T}}\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{Y} \\
&= \left[(\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{V})^{\mathrm{T}}(\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{V})\right]^{-1}(\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{V})^{\mathrm{T}}(\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{Y}). \qquad (26)
\end{aligned}$$

In the language of ZF, recall that $\overline{\mathbf{Y}} = \mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{Y}$, and $\overline{\mathbf{V}} = \mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{V}$. Thus Eq. (26) equals to $(\overline{\mathbf{V}}^{\mathrm{T}}\overline{\mathbf{V}})^{-1}\overline{\mathbf{V}}^{\mathrm{T}}\overline{\mathbf{Y}}^{\mathrm{T}}$, which justifies $\hat{\mathbf{B}}_{\mathrm{GLS}} = \hat{\mathbf{B}}_{\mathrm{ZF}}$.

References

1. Bailey, C.P., Chamadia, S., Pados, D.A.: An alternative signature design using L1 principal components for spread-spectrum steganography. In: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2020, Barcelona, Spain, pp. 2693–2696. IEEE (2020)
2. Bingham, E., Hyvärinen, A.: A fast fixed-point algorithm for independent component analysis of complex valued signals. Int. J. Neural Syst. **10**(1), 1–8 (2000)
3. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. **6**(12), 1673–1687 (1997)
4. Cox, I.J., Miller, M.L., Bloom, J.A., Honsinger, C.: Digital Watermarking, vol. 53. Springer, Cham (2002)
5. Cox, I.J., Miller, M.L., McKellips, A.L.: Watermarking as communications with side information. Proc. IEEE **87**(7), 1127–1141 (1999)
6. Du, Y., Yin, Z., Zhang, X.: High capacity lossless data hiding in JPEG bitstream based on general VLC mapping. IEEE Trans. Dependable Secur. Comput. **19**(2), 1420–1433 (2022)
7. Fridrich, J.: Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge (2009)
8. Gkizeli, M., Pados, D.A., Batalama, S.N., Medley, M.J.: Blind iterative recovery of spread-spectrum steganographic messages. In: Proceedings of the 2005 International Conference on Image Processing, ICIP 2005, Genoa, Italy, pp. 1098–1100. IEEE (2005)
9. Huang, J., Shi, Y.Q.: Reliable information bit hiding. IEEE Trans. Circuits Syst. Video Technol. **12**(10), 916–920 (2002)
10. Li, M., Kulhandjian, M., Pados, D.A., Batalama, S.N., Medley, M.J.: Extracting spread-spectrum hidden data from digital media. IEEE Trans. Inf. Forensics Secur. **8**(7), 1201–1210 (2013)

11. Li, M., Liu, Q.: Steganalysis of SS steganography: hidden data identification and extraction. Circuits Syst. Signal Process. **34**(10), 3305–3324 (2015)
12. Lin, J., Qin, J., Lyu, S., Feng, B., Wang, J.: Lattice-based minimum-distortion data hiding. IEEE Commun. Lett. **25**(9), 2839–2843 (2021)
13. Ling, C.: On the proximity factors of lattice reduction-aided decoding. IEEE Trans. Signal Process. **59**(6), 2795–2808 (2011)
14. Lu, W., Zhang, J., Zhao, X., Zhang, W., Huang, J.: Secure robust JPEG steganography based on autoencoder with adaptive BCH encoding. IEEE Trans. Circuits Syst. Video Technol. **31**(7), 2909–2922 (2021)
15. Malvar, H.S., Florêncio, D.A.: Improved spread spectrum: a new modulation technique for robust watermarking. IEEE Trans. Signal Process. **51**(4), 898–905 (2003)
16. Micciancio, D., Goldwasser, S.: Complexity of Lattice Problems. Springer, Boston (2002)
17. Bas, P., Furon, T.: Image database of bows-2. https://bows2.ec-lille.fr/
18. Sheinvald, J.: On blind beamforming for multiple non-Gaussian signals and the constant-modulus algorithm. IEEE Trans. Signal Process. **46**(7), 1878–1885 (1998)
19. Simmons, G.J.: The Prisoners' problem and the subliminal channel. In: Chaum, D. (ed.) Advances in Cryptology, pp. 51–67. Springer, Boston (1984). https://doi.org/10.1007/978-1-4684-4730-9_5
20. Tao, J., Li, S., Zhang, X., Wang, Z.: Towards robust image steganography. IEEE Trans. Circuits Syst. Video Technol. **29**(2), 594–600 (2019)
21. Wen, J., Chang, X.: On the success probability of three detectors for the box-constrained integer linear model. IEEE Trans. Commun. **69**(11), 7180–7191 (2021)