Signal Processing 113 (2015) 250–258

Contents lists available at ScienceDirect

Signal Processing

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

Matrix embedding in finite abelian group

Xiaolong Li [a], Siren Cai [a], Weiming Zhang [b], Bin Yang [a,*]

[a] Institute of Computer Science and Technology, Peking University, Beijing 100871, China
[b] School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China

ARTICLE INFO

Article history:
Received 8 June 2014
Received in revised form
30 November 2014
Accepted 9 February 2015
Available online 17 February 2015

Keywords:
Steganography
Matrix embedding
Finite abelian group
Covering sequence

ABSTRACT

Matrix embedding (ME) is a well-known steganographic scheme that can improve the embedding efficiency of steganography. In ME, the sender and recipient agree on a matrix in advance, and the message will be embedded into the cover data according to the matrix. In this paper, we propose a general framework for ME based on covering sequence (CS) of finite abelian group. By the proposed approach, the to-be-embedded message is regraded as an element of a finite abelian group, and it can be embedded into the cover data according to a CS of the group. It can be verified that many previous works, including the conventional ME (binary and ternary) and the sum and difference covering set based steganography, are special cases of the proposed general framework. The proposed CS-based ME formally extends these classical algorithms, and it provides a general way for designing efficient steganography. Some examples of CS-based ME and their performance evaluation are also given for a better illustration.

1. Introduction

Steganography studies secure secret communication [1,2]. By this means, a secret message is embedded into a cover by slightly modifying its content. The most important requirement for a steganographic scheme is its security, i.e., the perceptual and statistical undetectability of the hidden message.

There are mainly two ways to improve the stego-security. On one hand, less changes can be made to the cover for the same embedding capacity, which can be realized by, for example, matrix embedding (ME) [3–6]. The ME technique was firstly proposed by Crandall [3], and was made popular by the F5 algorithm of Westfeld [4]. Thereafter, the ME technique was systematically investigated by Fridrich et al. [7–9], in which they proved that the theoretical upper bound of embedding efficiency of the LSB-based steganography can be achieved by using binary codes. In ME, the sender and recipient agree on a parity check matrix (PCM) in advance, and then the embedded message is extracted by the recipient as the syndrome of the received stego data. In particular, to minimize the embedding distortion, the sender usually chooses a coset leader as the modification to the cover data. Besides ME using binary linear codes, ternary ME (± 1 embedding) is also studied in the literature [8,10,11]. Moreover, as an extension of the classical LSB matching and Mielikainen's algorithm [12], a variant of ME based on the sum and difference covering set (SDCS) of cyclic groups is proposed [13–15]. By the SDCS-based approach, the embedding distortion is reduced compared with LSB matching and [12]. In another work, Zhang and Wang proposed a new steganographic method based on exploiting modification direction (EMD) [16]. The EMD method and its related works such as [17–23] are also designed to reduce the embedding distortion and enhance the embedding efficiency.

On the other hand, given a content-adaptive distortion measurement, more appropriate changes can be made by a well designed embedding method. For example, it is obvious that embedding modifications operated in rough regions of a natural image are less perceptible than that in flat regions.

* Corresponding author.
Tel.: +86 10 82529693; fax: +86 10 82529207.
E-mail addresses: lixiaolong@pku.edu.cn (X. Li), caisiren@pku.edu.cn (S. Cai), zhangwm@ustc.edu.cn (W. Zhang), yang_bin@pku.edu.cn (B. Yang).

http://dx.doi.org/10.1016/j.sigpro.2015.02.007
0165-1684/© 2015 Elsevier B.V. All rights reserved.

Besides, the slight modifications to rough regions cannot be easily perceived by analyzing normal image statistics since the embedding noise is covered by the inherent noise. Thus the content-adaptive approach for steganography has the potential to provide a high level of security. Based on this consideration, Wu et al. proposed the so-called pixel-value-differencing (PVD) steganography [24], in which the difference value of a pixel pair is considered as the smoothness measurement and more data bits will be embedded into a pair if its difference is relatively larger. To the best of our knowledge, the PVD-based approach is the first attempt to realize content-adaptive steganography, and it is extensively studied in the literature including both performance enhancement and security discussions [25–32]. Later on, Fridrich et al. proposed the wet paper code (WPC) based steganography [33,34]. Imagine that we have a cover image exposed to rain and the sender can only slightly modify the dry spots of the image but cannot change the wet ones. During data transmission, the stego image dries out, and thus the receiver cannot identify which pixels were dry. However, with WPC, the positions of dry spots are unnecessary for the receiver to recover the embedded message. The WPC-based embedding is a fundamental work of content-adaptive steganography. After that, many other content-adaptive and effective steganographic methods are also proposed [35–41]. Particularly, in a recent work [42], Filler et al. proposed a practical approach to minimize the embedding impact measured by a content-adaptive cost function quantifying the effect of making modification to cover pixels. This method is based on syndrome coding using linear convolutional codes with the optimal binary quantizer implemented using the Viterbi algorithm. Nowadays, it is a hot topic to explore a reasonable image-dependent distortion measurement for enhancing the stego-security.

In this work, we focus on the first approach that improves the stego-security based on making less modification to the cover data. We conduct a further study on ME systematically and provide a general framework for ME based on the covering sequence (CS) of finite abelian group. Referred to this framework, it can be verified that many previous works, including the conventional ME (binary and ternary) and the SDCS-based steganography, are special cases of the proposed general framework. Moreover, the proposed new approach leads to some theoretical (somewhat interesting) problems beyond the steganography scope as well. Some examples of CS-based ME are also given for a better illustration.

The rest of this paper is organized as follows. We first introduce the general framework for CS-based ME in finite abelian group in Section 2. Some examples of CS-based ME and discussions are presented in Section 3. Some numerical results demonstrating the embedding performance of CS-based ME are also reported in Section 3. The final conclusion is drawn in the last section.

2. General framework for matrix embedding in finite abelian group

In this section, based on summarizing and extending the conventional ME and some previously proposed steganographic methods such as [8,12,14,16,43], we propose a general framework for designing steganography. Our approach is based on CS of finite abelian group. For a cover sequence $X=(x_1,\ldots,x_N)\in\mathbb{Z}^N$, the to-be-embedded message is regarded as an element of a finite abelian group G. Then, by the proposed framework utilizing a predetermined CS of G, we can derive the stego sequence $Y=(y_1,\ldots,y_N)\in\mathbb{Z}^N$ such that the embedding distortion (measured by l^2-norm)

$$\|X-Y\|_{l^2}=\left(\sum_{i=1}^{N}(x_i-y_i)^2\right)^{1/2} \tag{1}$$

is minimized.

We start our presentation by reviewing some basic concepts of group theory.

A group $(G,+)$ is a set of elements together with an operation "+" (also called the group operation) satisfying the following four properties:

- Closure: If $a,b\in G$, then $a+b\in G$.
- Associativity: The group operation is associative, i.e., for any $a,b,c\in G$, $(a+b)+c=a+(b+c)$.
- Identity: There is an identity element denoted as "0" such that $0+a=a+0=a$ holds for every $a\in G$.
- Invertibility: For each $a\in G$, there exists $a^*\in G$ such that $a+a^*=a^*+a=0$. Here, a^* is called the inverse of a and denoted as $-a$.

The cardinal number of G is called the order of G. In addition, if $a+b=b+a$ holds for any $a,b\in G$, G is called an abelian group (also called a commutative group). For example, the cyclic group $\mathbb{Z}_M=\{0,1,\ldots,M-1\}$ is an abelian group with order M, where the group operation "+" is just the addition operation modulo M (e.g., $3+4=2$ in $\mathbb{Z}_5$, $3+(-4)=5$ in $\mathbb{Z}_6$).

For a given finite abelian group $(G,+)$ with order M, a sequence $A=(a_1,\ldots,a_N)$ of G with $a_i\neq 0$ is called a CS if, for each $g\in G$, there exists an integer sequence $S=(s_1,\ldots,s_N)$ such that

$$g=s_1a_1+\cdots+s_Na_N \tag{2}$$

holds. Notice that the multiplication here is realized by addition of a_i if s_i is positive and otherwise addition of $-a_i$ (inverse of a_i in the group G). In other words, A is a CS if every element in G can be represented by the linear combination of elements in A, i.e., using the terminology of algebra, A is a CS if $\{a_1,\ldots,a_N\}$ is a generating set of G.

A CS can lead to a steganographic method. We first give some definitions. For $g\in G$, we define

$$C_g=\{(s_1,\ldots,s_N)\in\mathbb{Z}^N: s_1a_1+\cdots+s_Na_N=g\}, \tag{3}$$

$$d_g=\min\{s_1^2+\cdots+s_N^2:(s_1,\ldots,s_N)\in C_g\}, \tag{4}$$

$$D_g=\{(s_1,\ldots,s_N)\in C_g: s_1^2+\cdots+s_N^2=d_g\}. \tag{5}$$

Here, C_g is the set of all linear representations of g, d_g stands for the smallest cost in l^2-norm of all these linear representations, and D_g denotes the set of linear representations of g with the smallest cost. According to the condition in (2), C_g is non-empty and thus d_g and D_g are well-defined. In addition, D_g is a subset of C_g.

We then define a steganographic method based on (G, A). For a cover sequence $X=(x_1,\ldots,x_N)\in\mathbb{Z}^N$ and a secret data $g\in G$, the corresponding stego sequence $Y=(y_1,\ldots,y_N)$ is taken as $X+S$, where S is randomly chosen from the set D_{g*} with

$$g^* = g-(x_1a_1+\cdots+x_Na_N). \tag{6}$$

In this case, for the stego sequence Y, the embedded data g can be extracted by computing $\sum_{i=1}^N y_ia_i$ since

$$\begin{aligned}\sum_{i=1}^N y_ia_i &= \sum_{i=1}^N (x_i+s_i)a_i = \sum_{i=1}^N x_ia_i + \sum_{i=1}^N s_ia_i \\ &= \sum_{i=1}^N x_ia_i + \left(g-\sum_{i=1}^N x_ia_i\right) = g.\end{aligned} \tag{7}$$

Here, we remark that, instead of D_{g*}, S can be taken as any element of C_{g*} which contains D_{g*} as a subset, and the extraction phase in (7) still works. However, since $S=Y-X$ is the modification generated by data embedding, we then take S from the set D_{g*} to minimize the embedding distortion.

With (G, A), one can get a steganographic method based on the aforementioned embedding and extraction procedures. In this case, $\log_2 M$ bits are embedded into N pixels, and thus the embedding rate denoted as ER is

$$\mathrm{ER} = \frac{\log_2 M}{N}. \tag{8}$$

And, according to the definition of S, the embedding distortion denoted as ED can be computed as

$$\mathrm{ED} = \frac{\sum_{g\in G} d_{g-(x_1a_1+\cdots+x_Na_N)}}{MN} = \frac{\sum_{g\in G} d_g}{MN}. \tag{9}$$

As a result, the embedding efficiency denoted as EE is

$$\mathrm{EE} = \frac{\mathrm{ER}}{\mathrm{ED}} = \frac{M\log_2 M}{\sum_{g\in G} d_g}. \tag{10}$$

The classical LSB matching steganography is a special case of the proposed CS-based ME. By taking $G=\mathbb{Z}_2=\{0,1\}$ and $A=(1)$, one can verify that $D_0=\{0\}$ and $D_1=\{\pm 1\}$. According to (6), for a cover $X\in\mathbb{Z}$ and a message $g\in\{0,1\}$, we have $g^*=g-X$. Then, the stego data is X itself if X and g have the same parity, otherwise, the stego data will be randomly taken as $X+1$ or $X-1$.

As another example illustrating the CS-based embedding procedure, we introduce the method proposed by Mielikainen [12]. This method is also a special case of the proposed general framework. Actually, we may take $G=\mathbb{Z}_4$ and $A=(1,2)$. In this case, the corresponding set D_g can be computed as $D_0=\{(0,0)\}$, $D_1=\{(1,0)\}$, $D_2=\{(0,1),(0,-1)\}$ and $D_3=\{(-1,0)\}$. For a cover pixel pair such as $X=(10,12)$ and a message g=0, we first compute $g^*=g-(x_1a_1+x_2a_2)=2$. Then, by randomly taking an element from D_{g*}, e.g., $S=(0,-1)$, we can determine the stego pixel pair as $Y=X+S=(10,11)$. In addition, the embedding rate, distortion, and efficiency, are clearly $\mathrm{ER}=(\log_2 4)/2=1$, $\mathrm{ED}=(0+1+1+1)/8=0.375$, and $\mathrm{EE}=\mathrm{ER}/\mathrm{ED}=8/3$.

By the fundamental theorem of finite abelian groups, any finite abelian group is isomorphic to a direct product of cyclic groups of prime power order, then we can rewrite G as $\mathbb{Z}_{q_1}\oplus\cdots\oplus\mathbb{Z}_{q_K}$, where each q_i corresponds to a prime power. In this situation, each element of A can be expressed as $a_j=(a_{1,j},\ldots,a_{K,j})$ where $a_{i,j}\in\mathbb{Z}_{q_i}$. Thus, for $g=(g_1,\ldots,g_K)\in G$, (2) equivalents to

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,N} \\ \ldots & \ldots & \ldots \\ a_{K,1} & \ldots & a_{K,N}\end{pmatrix}\begin{pmatrix} s_1 \\ \ldots \\ s_N\end{pmatrix} = \begin{pmatrix} g_1 \\ \ldots \\ g_K\end{pmatrix}. \tag{11}$$

With this form, the CS A can be viewed as a $K\times N$ matrix $(a_{i,j})$, and the proposed general framework is in fact a natural extension of the conventional ME. Here, $N\ge K$ is not required to be satisfied, and the smallest N is the size of the minimal generating set of G. For example, for $G=\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_3$ where K=4, the size of the minimal generating set of G is 3. Notice that, G can be written as the Smith canonical form of $\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_L}$ where $n_1,\ldots,n_L$ are integers greater than 1 and $n_i|n_{i+1}$ holds for $1\le i\le L-1$. Using this form, L is actually the size of the minimal generating set of G.

For CS-based ME, a basic problem is the existence of CS, i.e., how to find a CS and decide whether a given sequence is a CS or not. We can give the solution to this question for a simple case where G is a cyclic group.

Theorem 1. *For a cyclic group $G=\mathbb{Z}_M$, $A=(a_1,\ldots,a_N)$ is a CS of G if and only if one of the following two conditions holds*: (1) *there exists an index $i\in\{1,\ldots,N\}$ such that* $\gcd(a_i,M)=1$, (2) $\gcd(a_1,\ldots,a_N,M)=1$ *and* $\gcd(a_i,M)>1$ *hold for each* $i\in\{1,\ldots,N\}$. *Here,* gcd *means the greatest common divisor of integers.*

Proof. Suppose that $(a_1,\ldots,a_N)$ is a CS of $\mathbb{Z}_M$. Then, there is an integer sequence $(s_1,\ldots,s_N)$ satisfying $1=s_1a_1+\cdots+s_Na_N$. In this case, if $\gcd(a_i,M)>1$ for each $i\in\{1,\ldots,N\}$, one must have $\gcd(a_1,\ldots,a_N,M)=1$. Otherwise, there exists $i\in\{1,\ldots,N\}$ such that $\gcd(a_i,M)=1$ and thus the condition (1) holds.

We now consider the inverse. If there exists $i\in\{1,\ldots,N\}$ such that $\gcd(a_i,M)=1$, there exists $b\in\mathbb{Z}$ satisfying ba_i=1 in $\mathbb{Z}_M$. As a result, any $g\in\mathbb{Z}_M$ can be written as $g=gba_i$ and thus $(a_1,\ldots,a_N)$ is a CS of $\mathbb{Z}_M$. On the other hand, if $\gcd(a_1,\ldots,a_N,M)=1$, according to Bézout's identity, there exists an integer sequence $(s_1,\ldots,s_N)$ satisfying $1=s_1a_1+\cdots+s_Na_N$. Consequently, any $g\in\mathbb{Z}_M$ can be written as $g=gs_1a_1+\cdots+gs_Na_N$ and thus A is also a CS of $\mathbb{Z}_M$. □

By this theorem, in terms of equivalence (here, two CSs of a given group G are regraded equivalent if they have the same embedding rate and distortion), we can only consider the CSs $A=(a_1,\ldots,a_N)$ that satisfy one of the following two conditions:

1. $1=a_1\le a_2\le\cdots\le a_N\le M/2$.
2. $1<a_1\le a_2\le\cdots\le a_N\le M/2$, $\gcd(a_1,\ldots,a_N,M)=1$ and $\gcd(a_i,M)>1$ hold for each $i\in\{1,\ldots,N\}$.

It gives all CSs of $\mathbb{Z}_M$.

Finally, we give an estimation for the lower bound of the embedding distortion when M and N are fixed. The estimation is straightforward. First, for $k\ge 0$, we define

$$E_k=\{(s_1,\ldots,s_N)\in\mathbb{Z}^N : s_1^2+\cdots+s_N^2=k\}. \tag{12}$$

Then, we have the following estimation for the embedding distortion.

Theorem 2. *Suppose* $T \ge 0$ *is the unique positive integer satisfying* $\sum_{k=0}^{T}|E_k| < M \le \sum_{k=0}^{T+1}|E_k|$, *where* $|\cdot|$ *means the cardinal number of a set. Then, we have*

$$\mathrm{ED} \ge \frac{1}{MN}\left(\sum_{k=0}^{T} k|E_k| + (T+1)\left(M - \sum_{k=0}^{T}|E_k|\right)\right). \tag{13}$$

Proof. According to the definition of ED in (9), we need to prove that

$$\sum_{g\in G} d_g \ge \sum_{k=0}^{T} k|E_k| + (T+1)\left(M - \sum_{k=0}^{T}|E_k|\right). \tag{14}$$

For every $k \ge 0$, consider the set $F_k = \{g \in G: d_g = k\}$, we have $G = \cup_{k\ge 0} F_k$ and

$$\sum_{g\in G} d_g = \sum_{k\ge 0}\sum_{g\in F_k} d_g = \sum_{k\ge 0} k|F_k|. \tag{15}$$

Notice that, for any $g_1 \ne g_2 \in G$, $C_{g_1} \cap C_{g_2} = \varnothing$. Thus, the mapping $\sigma_k: F_k \to E_k$ defined by taking $\sigma_k(g)$ as an (arbitrary) element of D_g is an injective. It yields that $|F_k| \le |E_k|$. On the other hand, as $\sum_{k\ge 0}|F_k| = |G| = M$, we have

$$\begin{aligned}\sum_{k\ge 0} k|F_k| &- \left(\sum_{k=0}^{T} k|E_k| + (T+1)\left(M - \sum_{k=0}^{T}|E_k|\right)\right)\\ &\ge \left(\sum_{k=0}^{T} k|F_k| + (T+1)\left(M - \sum_{k=0}^{T}|F_k|\right)\right)\\ &- \left(\sum_{k=0}^{T} k|E_k| + (T+1)\left(M - \sum_{k=0}^{T}|E_k|\right)\right)\\ &= \sum_{k=0}^{T}(T+1-k)(|E_k| - |F_k|) \ge 0.\end{aligned}$$

The theorem is finally proved according to the above equation and (14) and (15). □

By definition (12), we know that $E_0 = \{(0,\ldots,0)\}$ and

$$\begin{aligned}E_1 &= \{(s_1,\ldots,s_N) \in \mathbb{Z}^N: s_i\\ &= \pm 1 \text{ for an index } i,\ s_j = 0 \text{ for each } j \ne i\}.\end{aligned} \tag{16}$$

Then we get $|E_0| = 1$ and $|E_1| = 2C_N^1 = 2N$. As a result, for $M \in (1, 1+2N]$, we have $T=0$ and

$$\mathrm{ED} \ge \frac{M-1}{MN}. \tag{17}$$

With (17), we know that the embedding distortion can be minimized for a CS if $d_g \in \{0,1\}$ holds for every $g \in G$.

For another example, as $|E_2| = 2N^2 - 2N$, we have $T=1$ for $M \in (1+2N, 1+2N^2]$, and in this case,

$$\mathrm{ED} \ge 2\frac{M-N-1}{MN}. \tag{18}$$

3. Examples of CS-based ME

Some examples of CS-based ME are presented in this section. The comments and discussions are also given in the context. Since the proposed CS-based ME only depends on the group G and its CS A, and the detailed data embedding and extraction procedures have already been given in the previous section, we simply give here the definition of (G, A) in each example. Moreover, at the end of this section, some numerical results demonstrating the embedding performance of CS-based ME are presented as well.

Example 1. According to (11), the proposed CS-based ME includes binary ME [7,8,44–46] and ternary ME [8,10,11] as special cases, by taking G as $\mathbb{Z}_2^K$ and $\mathbb{Z}_3^K$, respectively. The proposed general embedding scheme formally extends these classical algorithms. For $G = \mathbb{Z}_2^K$, the matrix A can be viewed as the PCM of a binary linear code $\mathcal{C}$ with length N and dimension $N-K$. By this means, determining the set D_g defined in (5) is equivalent to finding a coset leader, i.e., the vector in the coset which has the minimal Hamming weight. Moreover, one can prove that $\mathrm{ED} = R_a(\mathcal{C})/N$, where $R_a(\mathcal{C})$ is the average distance to code defined by

$$R_a(\mathcal{C}) = \frac{\sum_{g\in G}\mathrm{dis}(g, \mathcal{C})}{2^K} \tag{19}$$

with $\mathrm{dis}(g, \mathcal{C}) = \min_{c\in\mathcal{C}}|g - c|$ which is the distance from g to $\mathcal{C}$. It should be mentioned that the problem of minimizing ED (equivalently, minimizing the average distance to code) is different from the covering radius problem extensively studied in coding theory [47]. The latter aims at minimizing the covering radius $R(\mathcal{C})$ which is defined by

$$R(\mathcal{C}) = \max_{g\in G} \mathrm{dis}(g, \mathcal{C}). \tag{20}$$

For a given G, finding the optimal CS, i.e., the CS minimizing ED, is a new and challenging problem. For $G = \mathbb{Z}_2^K$ or $\mathbb{Z}_3^K$, only some special cases have been solved for this problem in some recent works [11,48,49].

Example 2. The SDCS-based steganography [13–15] is a special case of the proposed CS-based ME. For SDCS-based steganography, the maximum modification to each image pixel value is limited to 1, and it extends the classical LSB matching and Mielikainen's method [12] by achieving higher embedding efficiency. The CS-based ME is degraded to SDCS-based steganography if taking $G = \mathbb{Z}_M$ and restricting $s_i \in \{0, \pm 1\}$ in (2). Moreover, it should be mentioned that, in [50], a new steganographic method is proposed by Lisoněk using the sum covers of a cyclic group. This approach is exactly the same as the one based on SDCS.

Example 3. In [43], Hong and Chen proposed a new data hiding method based on the so-called pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. As a matter of fact, their method is just a specific case of CS-based ME with $G = \mathbb{Z}_M$ and $A = (a_1, a_2)$ where a_1 is fixed as 1. Notice that, according to Theorem 1 (see the subsequent discussion part of this theorem), there are actually two types of CSs for cyclic group. However, only the first type of CS with the condition $1 = a_1 \le a_2 \le M/2$ is investigated in Hong and Chen's method. The second type of CS, e.g., $G = \mathbb{Z}_{12}$ and $A = (2, 3)$, is not taken into account in their work.

Example 4. We consider the case that $M \le 1+2N$ in this example. By taking $G = \mathbb{Z}_M$ and $A = (1, \ldots, N)$, one can verify that $d_0 = 0$ and $d_g = 1$ for each $g \ne 0$. Then, in this CS-based ME, only one element of the cover sequence is modified at most by 1 in value. Thus, the similarity between cover and stego data measured by embedding change is well guaranteed. Moreover, according to (17), this CS-based ME is optimal in the sense that the embedding distortion is minimized for fixed (M, N). When taking $M=1+2N$ in this example, it is in fact the EMD method of Zhang and Wang [16] and the grid coloring steganography of Fridrich and Lisoněk [51].

Example 5. As a continuation of the previous example, we consider here a little more difficult case with $1+2N< M\le 1+2N^2$. By the CS-based ME of this example, only two elements of the cover sequence are modified at most by 1 in value, and the similarity between cover and stego data is also well guaranteed. We first consider the case that $1+2N<M\le N^2+3N-1$. In this case, we take $G=\mathbb{Z}_M$ and $A=(1,2,\ldots,k,3k,5k+1,\ldots,(2m+1)k+m-1)$, where $k+m=N$ and $k>0$. With this example, one can verify that it is optimal by taking a proper k. We now consider the case that $M=\frac{4}{3}N^2+O(N)$. This construction is inspired by our previous work [13] (see Theorem 1 of [13]). For convenience, denote here $(a,d)_k$ a k term arithmetic progression $a,a+d,\ldots,a+(k-1)d$. Then, we take $G=\mathbb{Z}_M$ and consider that A is composed of three arithmetic progressions $(a_1,d_1)_{k_1}$, $(a_2,d_2)_{k_2}$ and $(a_3,d_3)_{k_3}$. Next, we take

- if $N\equiv 0 (\text{mod } 3)$: $(a_1,d_1)=(1,1)$, $(a_2,d_2)=(N/3+1,2N+3)$, $(a_3,d_3)=(5N/3+1,2N+1)$, and $k_1=k_2=k_3=N/3$;
- if $N\equiv 1(\text{mod } 3)$: $(a_1,d_1)=(1,2)$, $(a_2,d_2)=(2(N-1)/3+1,2N+3)$, $(a_3,d_3)=(4(N-1)/3+2,2N-1)$, and $k_1=k_2=(N-1)/3$ and $k_3=(N-1)/3+1$;
- if $N\equiv 2(\text{mod } 3)$: $(a_1,d_1)=(1,1)$, $(a_2,d_2)=((N+1)/3,2N+1)$, $(a_3,d_3)=(5(N+1)/3-2,2N-1)$, and $k_1=(N-2)/3$ and $k_2=k_3=(N+1)/3$.

Finally, with this choice of A, one can verify that it is an optimal CS of $\mathbb{Z}_M$ where M is

$$\begin{cases} \frac{4}{3}N^2+\frac{4}{3}N+1 & \text{if } N\equiv 0,2 \text{ (mod 3)} \\ (2N+1)^2/3 & \text{if } N\equiv 1 (\text{mod } 3). \end{cases} \tag{21}$$

According to the above construction, for $G=\mathbb{Z}_M$ with order $M=\frac{4}{3}N^2+O(N)$, we know that there exists a CS $A=(a_1,\ldots,a_N)$ such that each element of G can be written as $s_ia_i+s_ja_j$ with $a_i,a_j\in\{0,\pm 1\}$. In other words, each element of $\mathbb{Z}_M$ can be represented by the sum or difference of at most two elements of A. For a fixed N, denote λ_N as the largest integer M such that $\mathbb{Z}_M$ contains such a CS. Then, $\lambda_N\ge\frac{4}{3}N^2+O(N)$. On the other hand, we clearly have $\lambda_N\le 1+2N^2$. Based on this discussion, a natural problem is, what is the asymptotic expression of λ_N when $N\to+\infty$? Or, in a weak sense, can we determine two constants C_1 and C_2 such that $C_1N^2\le\lambda_N\le C_2N^2$ holds for a sufficient large N? This problem is difficult and we cannot give a response even for the extreme case where $M=1+2N^2$. It is an interesting problem for the future work. Moreover, we remark that the sum or difference covers of finite abelian group are also studied in the literature [13,52–56], in which one concerns to cover the group G by either $A+A=\{a_i+a_j: a_i,a_j\in A\}$ or $A-A=\{a_i-a_j: a_i,a_j\in A\}$ for a subset $A\subset G$. For the minimal sum or difference covers problem, i.e., finding the set A with minimal cardinal number such that $G=A+A$ or $G=A-A$ holds, only some numerical results are known and it lacks solid theoretical study.

Example 6. In this example, we use the q-ary notational system to construct CS. We take $G=\mathbb{Z}_{q^N}$ and $A=(q^0,q^1,\ldots,q^{N-1})$, where q is a positive odd number. Notice that, for any integer $g\in[-(q^N-1)/2,(q^N-1)/2]$, it can be uniquely represented by $g=\sum_{i=1}^{N}s_iq^{i-1}$ with $s_i\in\{0,\pm 1,\ldots,\pm(q-1)/2\}$. Thus, the sequence A is a CS of G. The corresponding embedding rate and distortion can be computed as $\mathrm{ER}=\log_2 q$ and $\mathrm{ED}=(q^2-1)/12$. With this example, a high embedding rate can be achieved by taking a large q.

Example 7. We consider the CS composed of prime numbers, i.e., we take $G=\mathbb{Z}_M$ and $A=(a_1,\ldots,a_N)$ where a_i is the ith prime number less than $M/2$. According to the classical theorem describing the asymptotic distribution of prime numbers, we have $N\sim M/2/\log(M/2)$. On the other hand, according to Vinogradov's theorem (each odd integer no less than 7 can be written as a sum of three prime numbers), we know that for each odd integer $g\in G$, it can be written as the forms of $\pm(3a_i)$, $\pm(2a_i+a_j)$, or $\pm(a_i+a_j+a_k)$. Moreover, since Goldbach's conjecture is verified true for sufficient large even numbers (about 4×10^{18}) and generally assumed to be true, for each even integer $g\in G$, it can be written as the forms of $\pm(2a_i)$ or $\pm(a_i+a_j)$. As a result, A is a CS of G with $d_g\le 9$ holds for each $g\in G$.

Example 8. This example is somewhat similar to the previous one. In number theory, Waring's problem, proposed in 1770 by Edward Waring, asks whether for every natural number k there exists an associated positive integer s such that every natural number is the sum of at most s kth powers of natural numbers. The response is positive and it is firstly proved by David Hilbert in 1909. For every $k\ge 1$, we denote by $f(k)$ the minimum number of kth powers needed to represent all integers, for examples, $f(1)=1$, $f(2)=4$, and $f(3)=9$. In this light, the set of powers of natural numbers can lead to a CS. Specifically, we take $G=\mathbb{Z}_M$, $A=(a_1,\ldots,a_N)$ where $a_i=i^k$ and N is determined such that N^k is the largest kth power less than $M/2$. According to Hilbert–Waring's theorem, A is a CS of G with $d_g\le f(k)^2$. By Examples 7 and 8, we see a connection between two different scientific domains, information hiding and number theory. We believe that advanced results in number theory may provide advisable designs in steganography, and it should be investigated in the future work.

Example 9. In this example, by exhaustive search considering all non-isomorphic finite abelian groups of small order, all optimal CSs are computed for $2\le N\le 5$ and $4\le M\le 100$. For given M and N, in most cases, there is a CS A of the cyclic group $\mathbb{Z}_M$ such that $(\mathbb{Z}_M,A)$ leads to an optimal embedding where the distortion is minimized among all possible choices of (G,A). The exceptions where (G,A) is optimal with (1) $G\ne\mathbb{Z}_M$, (2) $(\mathbb{Z}_M,A)$ is not optimal for each CS A of $\mathbb{Z}_M$ are listed in Table 1. The cyclic group and its CS can lead to optimal embedding in most tested cases, however, with limited experimental results and without theoretical analysis, the impact of the group structure on the embedding performance is still unclear.

Example 10. In this example, we give a CS based on a specific matrix construction using the PCM of convolutional q-ary codes. Our idea derives from the previous works of syndrome-trellis-based decoding [42,57]. Specifically, for a positive odd number q, we take $G=\mathbb{Z}_q^K$ and the $K\times N$ matrix $(a_{i,j})$ (see (11)) as the following form, by placing respectively two $a\times b$ sub-matrices A_1 and A_2 along its main and minor diagonals

$$\begin{pmatrix} A_1 & & & \cdots & & \\ A_2 & A_1 & & \cdots & & \\ & A_2 & A_1 & \cdots & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & \cdots & A_1 & \\ & & & \cdots & A_2 & A_1 \end{pmatrix} \tag{22}$$

where A_1 is in systematic form as (I, R), I is an identical matrix of $a\times a$ and R is an $a\times(b-a)$ matrix. The nonsingularity of A_1 ensures that (11) has a solution for every $g=(g_1,\ldots,g_K)\in G$. And, using the syndrome-trellis-based decoding methods [42,57], the computation complexity for processing one pixel in data embedding procedure is $\mathcal{O}(q^{2a+1})$ and thus q and a should be small. Suppose that the number of matrix A_1 in the main diagonal is k, we then have $N=kb$ and $K=ka$, and the embedding rate is clearly

$$\frac{\log_2 M}{N}=\frac{K}{N}\log_2 q=\frac{a}{b}\log_2 q. \tag{23}$$

The embedding rate is fixed whatever k is. However, for the distortion, one has a desirable property when increasing k. Denote for convenience the embedding distortion as ED_k, then we have, for any $k_1,k_2\geq 2$

$$\mathrm{ED}_{k_1+k_2}\leq\frac{k_1}{k_1+k_2}\mathrm{ED}_{k_1}+\frac{k_2}{k_1+k_2}\mathrm{ED}_{k_2}. \tag{24}$$

By taking $k_1=k_2=k$, (24) yields that

$$\mathrm{ED}_{2k}\leq\mathrm{ED}_k. \tag{25}$$

It says, the distortion is either unchanged or decreased by doubling k. This property guarantees the validity of employing large k. See appendix for the proof of (24).

Table 1
Exceptional optimal (G, A). Here, "exceptional" means that $G\neq\mathbb{Z}_M$ and, for given M and N, $(\mathbb{Z}_M, A)$ is not optimal for each CS A of $\mathbb{Z}_M$.

(N, M)	G	A	ER	EE
(2,60)	$\mathbb{Z}_2^2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5$	$\begin{pmatrix}1&0\\0&1\\1&2\\1&1\end{pmatrix}$	2.9534	0.6111
(2,92)	$\mathbb{Z}_2^2\oplus\mathbb{Z}_{23}$	$\begin{pmatrix}1&0\\0&1\\1&5\end{pmatrix}$	3.2618	0.4413
(3,64)	$\mathbb{Z}_2\oplus\mathbb{Z}_{32}$	$\begin{pmatrix}1&0&0\\4&1&14\end{pmatrix}$	2.0000	1.5868
(3,81)	$\mathbb{Z}_9^2$	$\begin{pmatrix}1&0&2\\0&1&4\end{pmatrix}$	2.1133	1.4506
(3,84)	$\mathbb{Z}_2^2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_7$	$\begin{pmatrix}1&0&0\\0&0&1\\0&1&2\\1&1&1\end{pmatrix}$	2.1308	1.4056
(4,36)	$\mathbb{Z}_3^2\oplus\mathbb{Z}_4$	$\begin{pmatrix}1&0&0&1\\0&0&1&2\\0&1&1&1\end{pmatrix}$	1.2925	2.8633
(4,48)	$\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_8$	$\begin{pmatrix}0&0&1&0\\1&0&1&1\\0&1&1&3\end{pmatrix}$	1.3962	2.6542
(4,98)	$\mathbb{Z}_2\oplus\mathbb{Z}_7^2$	$\begin{pmatrix}1&1&1&1\\0&1&2&3\\1&0&3&5\end{pmatrix}$	1.6537	2.1974
(5,60)	$\mathbb{Z}_2^2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5$	$\begin{pmatrix}0&1&0&1&0\\0&0&1&0&1\\1&0&0&1&2\\0&1&1&2&2\end{pmatrix}$	1.1814	3.0035

Finally, before closing this section, some preliminary numerical results illustrating the performance of CS-based ME are reported. We give the embedding rate versus embedding efficiency in Fig. 1, for the following CSs:

- The CS presented in Example 4, where $G=\mathbb{Z}_{1+2N}$ and $A=(1,\ldots,N)$. This CS-based ME is just the EMD embedding method [16] and the grid coloring steganography [51].
- The CS presented in Example 5, where $G=\mathbb{Z}_M$ with M defined in (21) and A composed of the three arithmetic progressions. These CSs are based on our previous work [13].
- The CS presented in Example 7 using prime numbers, where $G=\mathbb{Z}_M$ and $A=(a_1,\ldots,a_N)$ with a_i as the ith prime number less than $M/2$. For example, $A=(2,3,5,7)$ when $M=16$.
- The CS presented in Example 8 using square numbers, where $G=\mathbb{Z}_M$ and $A=(a_1,\ldots,a_N)$ with $a_i=i^2\leq M/2$. For example, $A=(1,4,9)$ when $M=25$.
- The CS presented in Example 8 using cubic numbers, where $G=\mathbb{Z}_M$ and $A=(a_1,\ldots,a_N)$ with $a_i=i^3\leq M/2$. For example, $A=(1,8,27,64,125)$ when $M=256$.
- The optimal $(\mathbb{Z}_M, A)$ with $N\in\{2,3,4\}$ and $M\in\{2,\ldots,2^{2N}\}$. In this case, for each (N, M), according to

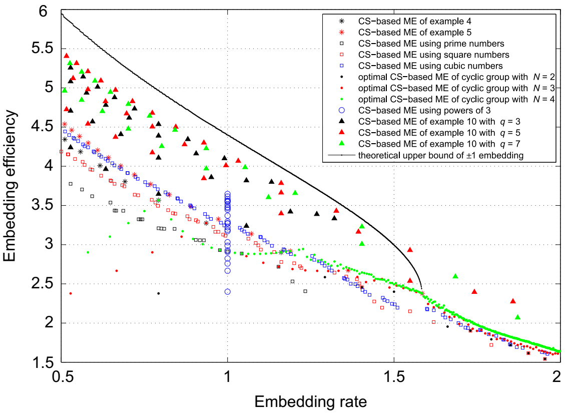

Fig. 1. Embedding rate versus embedding efficiency for some CS-based ME. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

Theorem 1, all CSs sized N of $\mathbb{Z}_M$ are tested to get the optimal one such that the distortion is minimized. For reference, the optimal CS of $\mathbb{Z}_M$ for $N \in \{2, 3\}$ and $M \in \{2, \ldots, 2^{2N}\}$ are listed in Tables 2 and 3.

- The CS composed of powers of 3 with an embedding rate of 1, i.e., we take $G = \mathbb{Z}_{2^N}$ with the specific CS $A = (3^0, 3^1, \ldots, 3^{N-1})$. This CS-based ME is previously presented in our work of SDCS-based steganography [14].
- The CSs presented in Example 10. Here, k is fixed as 2^{10}. And, we take $q=3$ with $a \in \{2, 3, 4, 5\}$, $q=5$ with $a \in \{2, 3, 4\}$, $q=7$ with $a \in \{2, 3\}$, and $b \geq a+1$. For each (q, a, b), the sub-matrices A_1 and A_2 are randomly selected for 100 times, and the embedding distortion is averaged as the final result. This type of CS is motivated by the syndrome-trellis-codes-based steganography [42] and the decoding method [57].

Also, for a better illustration, the theoretical upper bound of "± 1 embedding" is plotted as well in this figure. The "± 1 embedding" means that in the embedding process, each pixel value is allowed to be modified at most by 1 [58]. According to this figure, one can observe that the CS-based ME can provide different embedding efficiencies based on different CS constructions. However, both the presented CS-based ME can provide good embedding efficiencies. For example, when the embedding rate is 1, the embedding efficiency of LSB matching and Mielikainen's method [12] is 2 and 8/3, respectively. However, with the CS-based ME using cubic numbers, one can get an efficiency of 3.08 for $M=4096$. With the CS-based ME using powers of 3, one can get an efficiency of 3.65 when $N=26$. And, for the CS-based ME of Example 10 with $(q, a, b, k) = (3, 5, 8, 2^{10})$, one can get an efficiency as large as 4.10. Moreover, one can also observe that the CS-based ME of Example 10 can approach the theoretical upper bound of ± 1 embedding, and for a sufficient large embedding rate (see the red rectangle between the embedding rates 1.5 and 1.6), it can provide an even larger efficiency. For the latter case, $q=5$ and the maximum modification to cover pixels is 2.

Table 2
Optimal CS of $\mathbb{Z}_M$ for $N=2$ and $M \in \{2, \ldots, 2^4\}$.

M	optimal CS	ER	EE
2	(1,1)	0.5000	2.0000
3	(1,1)	0.7924	2.3774
4	(1,2)	1.0000	2.6666
5	(1,2)	1.1609	2.9024
6	(1,2)	1.2924	2.5849
7	(1,2)	1.4036	2.4564
8	(1,3)	1.5000	2.4000
9	(1,3)	1.5849	2.3774
10	(1,3)	1.6609	1.9540
11	(1,3)	1.7297	1.9026
12	(2,3)	1.7924	1.7924
13	(1,5)	1.8502	1.7180
14	(1,4)	1.9036	1.6152
15	(1,4)	1.9534	1.5421
16	(1,6)	2.0000	1.4883

Table 3
Optimal CS of $\mathbb{Z}_M$ for $N=3$ and $M \in \{2, \ldots, 2^6\}$.

M	Optimal CS	ER	EE
2	(1,1,1)	0.3333	2.0000
3	(1,1,1)	0.5283	2.3774
4	(1,1,2)	0.6666	2.6666
5	(1,1,2)	0.7739	2.9024
6	(1,2,3)	0.8616	3.1019
7	(1,2,3)	0.9357	3.2752
8	(1,2,3)	1.0000	3.0000
9	(1,2,3)	1.0566	2.8529
10	(1,2,3)	1.1073	2.7682
11	(1,2,3)	1.1531	2.7181
12	(1,2,4)	1.1949	2.6887
13	(1,2,4)	1.2334	2.6725
14	(1,2,5)	1.2691	2.6651
15	(1,2,5)	1.3022	2.6637
16	(1,2,6)	1.3333	2.6666
17	(1,2,6)	1.3624	2.6725
18	(1,2,6)	1.3899	2.5882
19	(1,2,6)	1.4159	2.5222
20	(2,5,6)	1.4406	2.5423
21	(1,3,8)	1.4641	2.5621
22	(1,3,8)	1.4864	2.4526
23	(1,3,8)	1.5078	2.4771
24	(1,3,8)	1.5283	2.4453
25	(1,3,8)	1.5479	2.4186
26	(1,3,9)	1.5668	2.3963
27	(1,3,9)	1.5849	2.3774
28	(1,3,9)	1.6024	2.2434
29	(1,3,9)	1.6193	2.2012
30	(3,5,9)	1.6356	2.1971
31	(1,3,11)	1.6513	2.1330
32	(1,4,10)	1.6666	2.0779
33	(1,6,15)	1.6814	2.0808
34	(1,3,13)	1.6958	1.9882
35	(1,11,16)	1.7097	2.0400
36	(4,6,9)	1.7233	1.9799
37	(1,3,14)	1.7364	1.9274
38	(1,6,9)	1.7493	1.8992
39	(1,12,18)	1.7618	1.9086
40	(1,4,14)	1.7739	1.8673
41	(1,5,13)	1.7858	1.8615
42	(2,15,18)	1.7974	1.8412
43	(1,3,17)	1.8087	1.7948
44	(1,14,20)	1.8198	1.8061
45	(1,4,17)	1.8306	1.7908
46	(1,8,12)	1.8411	1.7768
47	(1,4,18)	1.8515	1.7639
48	(1,4,18)	1.8616	1.7407
49	(1,4,14)	1.8715	1.7195
50	(1,8,12)	1.8812	1.7312
51	(1,4,15)	1.8908	1.7017
52	(2,10,13)	1.9001	1.7035
53	(1,4,21)	1.9093	1.6865
54	(1,4,20)	1.9182	1.6707
55	(1,5,21)	1.9271	1.6913
56	(1,5,18)	1.9357	1.6508
57	(1,5,22)	1.9442	1.6459
58	(1,4,16)	1.9526	1.6334
59	(1,5,17)	1.9608	1.6218
60	(1,22,26)	1.9689	1.6183
61	(1,4,17)	1.9769	1.6007
62	(1,5,18)	1.9847	1.6120
63	(1,5,25)	1.9924	1.6092
64	(1,7,18)	2.0000	1.5802

In summary, with these primary constructions of CS, the CS-based ME can provide high embedding efficiency and lead to secure steganography.

4. Conclusion

In this work, a general framework for ME based on CS in finite abelian group is proposed. It includes many previous works such as the conventional ME (binary and ternary) and SDCS-based steganography as special cases. The proposed CS-based ME formally extended these classical steganographic methods. This work is a summarization and extension of the previous works.

However, this paper is just a beginning work of CS-based ME, and only some specific examples and preliminary numerical results are presented. There are many subsequent works for the future research, for examples:

(1) Besides the presented CSs, how to construct specific (G, A) such that there exists a fast encoding method (i.e., finding an element of D_g) and meanwhile a high embedding efficiency can be achieved?

(2) For a given (M, N) (in this case, the embedding rate is fixed), how to determine the optimal (G, A) such that the embedding distortion is minimized?

(3) Consider a non-cyclic group G in Smith canonical form or a direct product of cyclic groups of prime power order, what is the necessary and sufficient condition that a sequence A is a CS of G?

(4) What is the impact of the group structure on the embedding performance? For example, for two non-isomorphic groups $\mathbb{Z}_{3^K}$ and $\mathbb{Z}_3^K$, do they have the same embedding distortion? Or, in a more general case, in what conditions, the two groups $\mathbb{Z}_{\prod_{i=1}^K q_i}$ and $\mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_K}$ have the same embedding distortion.

(5) How to construct good (G, A) such that $s_i \in \{0, \pm 1\}$ and $d_g \le T$ hold? Here, T is a given threshold. In this case, each pixel value is modified at most by 1 and the total distortion for N pixels is restrained by T. In particular, does there exist a (G, A) with $M = 1 + 2N^2$ such that for each $g \in G$, it can be written as $s_i a_i + s_j a_j$ with $i \ne j$ and $s_i, s_j \in \{0, \pm 1\}$?

More investigations on CS-based ME, including both theoretical analysis and numerical contribution for practically efficient steganography, are expected. The interesting theoretical problems related to CS-based ME are beyond the steganography scope.

Acknowledgements

This work was supported by National High-tech Technology R&D Program (863 Program) of China under Grant 2014AA015205 and National Natural Science Foundation of China under contract No. 61471272. The work of Weiming Zhang was supported by National Natural Science Foundation of China under contract No. 61170234.

Appendix A

We give the key points for the proof of (24).

For simplicity, we take $k = k_1 + k_2$ and the matrix defined in (22) as M_k. For a given $g = (g_1, \dots, g_k) \in \mathbb{Z}_q^{ka}$ with each $g_i \in \mathbb{Z}_q^a$, suppose that a vector $S = (s_1, \dots, s_k) \in \mathbb{Z}^{kb}$ satisfying $M_k S = g$ where each $s_i \in \mathbb{Z}^b$. Here, we use either row or column vectors depending on the choice for convenience. We then have, $M_{k_1} S' = g'$, where $S' = (s_1, \dots, s_{k_1})$ and $g' = (g_1, \dots, g_{k_1})$. Now, suppose that $S' \in D_{g'}$ (see (5)), i.e., S' is the solution having the minimal l^2-norm. In this case, we can derive that $M_{k_2} S'' = g''$, where $S'' = (s_{k_1+1}, \dots, s_k)$ and $g'' = (g_{k_1+1} - A_2 s_{k_1}, g_{k_1+2}, \dots, g_k)$. Then, by taking $S'' \in D_{g''}$, we have

$$d_g \le d_{g'} + d_{g''} \tag{26}$$

where d_g is defined in (4). Notice that in the above equation, d_g, $d_{g'}$ and $d_{g''}$ correspond to the CSs (the matrices) M_k, M_{k_1} and M_{k_2}, respectively. Next, in (26), fixing g' and summing up every $g_i \in \mathbb{Z}_q^a$ for each $i \in \{k_1 + 1, \dots, k\}$, we can get

$$\sum_{g'' \in \mathbb{Z}_q^{k_2 a}} d_{(g', g'')} \le \sum_{g'' \in \mathbb{Z}_q^{k_2 a}} (d_{g'} + d_{g''}) = q^{k_2 a} d_{g'} + \sum_{g'' \in \mathbb{Z}_q^{k_2 a}} d_{g''}. \tag{27}$$

It yields that

$$\sum_{g \in \mathbb{Z}_q^{ka}} d_g = \sum_{g' \in \mathbb{Z}_q^{k_1 a}, g'' \in \mathbb{Z}_q^{k_2 a}} d_{(g', g'')} \le q^{k_2 a} \sum_{g' \in \mathbb{Z}_q^{k_1 a}} d_{g'} + q^{k_1 a} \sum_{g'' \in \mathbb{Z}_q^{k_2 a}} d_{g''}. \tag{28}$$

This completes the proof of (24) according to the definition of embedding distortion in (9).

References

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, Cambridge, UK, 2010.

[2] B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganalysis, J. Inf. Hiding Multimed. Signal Process. 2 (2) (2011) 142–172.

[3] R. Crandall, Some notes on steganography [online] ⟨http://www.di.unisa.it/~ads/corso-security/www/CORSO-0203/steganografia/LINKSLOCALI/matrix-encoding.pdf⟩, 1998.

[4] A. Westfeld, High capacity despite better steganalysis: F5 – a steganographic algorithm, in: Proceedings of IH, Springer Lecture Notes in Computer Science, vol. 2137, 2001, pp. 289–302.

[5] M. van Dijk, F. Willems, Embedding information in grayscale images, in: Proceedings of 22nd Symposium on Information Theory in the Benelux, 2001, pp. 147–154.

[6] F. Galand, G. Kabatiansky, Information hiding by coverings, in: Proceedings of IEEE ITW, 2003, pp. 151–154.

[7] J. Fridrich, D. Soukal, Matrix embedding for large payloads, IEEE Trans. Inf. Forensics Secur. 1 (3) (2006) 390–395.

[8] J. Fridrich, P. Lisoněk, D. Soukal, On steganographic embedding efficiency, in: Proceedings of IH, Springer Lecture Notes in Computer Science, vol. 4437, 2006, pp. 282–296.

[9] J. Bierbrauer, J. Fridrich, Constructing good covering codes for applications in steganography, in: Transactions on Data Hiding and Multimedia Security III, Springer Lecture Notes in Computer Science, vol. 4920, 2008, pp. 1–22.

[10] V. Sachnev, H.-J. Kim, Ternary data hiding technique for JPEG steganography, in: Proceedings of IWDW, Springer Lecture Notes in Computer Science, vol. 6526, 2010, pp. 202–210.

[11] Y. Qi, X. Li, B. Wang, B. Yang, A study of optimal matrix for efficient matrix embedding in $\mathbb{F}_3$, in: Proceedings of IWDW, Springer Lecture Notes in Computer Science, vol. 7809, 2012, pp. 8–18.

[12] J. Mielikainen, LSB matching revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285–287.

[13] X. Li, T. Zeng, B. Yang, Improvement of the embedding efficiency of LSB matching by sum and difference covering set, in: Proceedings of IEEE ICME, 2008, pp. 209–212.

[14] X. Li, B. Yang, D. Cheng, T. Zeng, A generalization of LSB matching, IEEE Signal Process. Lett. 16 (2) (2009) 69–72.

[15] C. Liu, X. Li, X. Lu, B. Yang, Improving embedding efficiency by incorporating SDCS and WPC, in: Proceedings of IEEE ICME, 2009, pp. 1018–1021.

[16] X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Commun. Lett. 10 (11) (2006) 781–783.

[17] R.-M. Chao, H.-C. Wu, C.-C. Lee, Y.-P. Chu, A novel image data hiding scheme with diamond encoding, EURASIP J. Inf. Secur. (2009) 1–9.

[18] H.J. Kim, C. Kim, Y. Choi, S. Wang, X. Zhang, Improved modification direction methods, Comput. Math. Appl. 60 (2) (2010) 319–325.

[19] T.D. Kieu, C.-C. Chang, A steganographic scheme by fully exploiting modification directions, Expert Syst. Appl. 38 (8) (2011) 10648–10657.

[20] J. Wang, Y. Sun, H. Xu, K. Chen, H.J. Kim, S.-H. Joo, An improved section-wise exploiting modification direction method, Signal Process. 90 (11) (2010) 2954–2964.

[21] X.-T. Wang, C.-C. Chang, C.-C. Lin, M.-C. Li, A novel multi-group exploiting modification direction method based on switch map, Signal Process. 92 (6) (2012) 1525–1535.

[22] W.-C. Kuo, Image hiding by square fully exploiting modification directions, J. Inf. Hiding Multimed. Signal Process. 4 (3) (2013) 128–137.

[23] W.-C. Kuo, S.-Y. Chang, Hybrid GEMD data hiding, J. Inf. Hiding Multimed. Signal Process. 5 (3) (2014) 420–430.

[24] D.-C. Wu, W.-H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognit. Lett. 24 (9–10) (2003) 1613–1626.

[25] X. Zhang, S. Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognit. Lett. 25 (3) (2004) 331–339.

[26] H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proc.-Vis. Image Signal Process. 152 (5) (2005) 611–615.

[27] C.H. Yang, C.Y. Weng, S.J. Wang, H.M. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems, IEEE Trans. Inf. Forensics Secur. 3 (3) (2008) 488–497.

[28] C.H. Yang, S.J. Wang, C.Y. Weng, Analyses of pixel-value-differencing schemes with LSB replacement in stegonagraphy, in: Proceedings of IIH-MSP, 2007, pp. 445–448.

[29] L. Ji, X. Li, B. Yang, Z. Liu, A further study on a PVD-based steganography, in: Proceedings of MINES, 2010, pp. 686–690.

[30] S. Tan, B. Li, Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-spline fitting, IEEE Signal Process. Lett. 19 (6) (2012) 336–339.

[31] J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images, IEEE Trans. Inf. Forensics Secur. 7 (3) (2012) 868–882.

[32] X. Li, B. Li, X. Luo, B. Yang, R. Zhu, Steganalysis of a PVD-based content adaptive image steganography, Signal Process. 93 (9) (2013) 2529–2538.

[33] J. Fridrich, P. Lisoněk, D. Soukal, Writing on wet paper, IEEE Trans. Signal Process. 53 (10) (2005) 3923–3935.

[34] J. Fridrich, M. Goljan, D. Soukal, Wet paper codes with improved embedding efficiency, IEEE Trans. Inf. Forensics Secur. 1 (1) (2006) 102–110.

[35] J. Fridrich, T. Filler, Practical methods for minimizing embedding impact in steganography, in: Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, Proceedings of SPIE, 2007.

[36] W. Zhang, X. Zhang, S. Wang, Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes, in: Proceedings of IH, Springer Lecture Notes in Computer Science, vol. 5284, 2008, pp. 60–71.

[37] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forensics Secur. 5 (2) (2010) 201–214.

[38] T. Pevny, T. Filler, P. Bas, Using high-dimensional image models to perform highly undetectable steganography, in: Proceedings of IH, Springer Lecture Notes in Computer Science, vol. 6387, 2010, pp. 161–177.

[39] V. Holub, J. Fridrich, Designing steganographic distortion using directional filters, in: Proceedings of IEEE WIFS, 2012, pp. 234–239.

[40] V. Holub, J. Fridrich, Digital image steganography using universal distortion, in: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, 2013, pp. 59–68.

[41] W. Hong, Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique, Inf. Sci. 221 (2013) 473–489.

[42] T. Filler, J. Judas, J. Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, IEEE Trans. Inf. Forensics Secur. 6 (2011) 920–935.

[43] W. Hong, T.-S. Chen, A novel data embedding method using adaptive pixel pair matching, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 176–184.

[44] J. Fridrich, Minimizing the embedding impact in steganography, in: Proceedings of ACM MM&SEC, 2006, pp. 2–10.

[45] Y. Gao, X. Li, T. Zeng, B. Yang, Improving embedding efficiency via matrix embedding: a case study, in: Proceedings of IEEE ICIP, 2009, pp. 109–112.

[46] C. Wang, W. Zhang, J. Liu, N. Yu, Fast matrix embedding by matrix extending, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 346–350.

[47] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering Codes, Elsevier, Amsterdam, 1997.

[48] M. Khatirinejad, P. Lisoněk, Linear codes for high payload steganography, Discrete Appl. Math. 157 (5) (2009) 971–981.

[49] Y. Gao, X. Li, B. Yang, Employing optimal matrix for efficient matrix embedding, in: Proceedings of IIH-MSP, 2009, pp. 161–165.

[50] P. Lisoněk, Sum covers in steganography, in: Proceedings of ACCT, 2008, pp. 186–191.

[51] J. Fridrich, P. Lisoněk, Grid coloring in steganography, IEEE Trans. Inf. Theory 53 (4) (2007) 1547–1549.

[52] A. Mrose, Untere schranken für die reichweiten von extremalbasen fester ordnung, Abh. Math. Sem. Univ. Hambrug 48 (1979) 118–124.

[53] R.L. Graham, N.J.A. Sloane, On additive bases and harmonious graphs, SIAM J. Algebra Discrete Math. 1 (4) (1980) 382–404.

[54] M.A. Fitch, R.E. Jamison, Minimum sum covers of small cyclic groups, Congr. Numerantium 147 (2000) 65–81.

[55] H. Haanpää, Minimum sum and difference covers of abelian groups, J. Integer Sequences 7 (2) (2004). article 04.2.6.

[56] D.F. Hsu, X. Jia, Additive bases and extremal problems in groups, graphs and networks, Util. Math. 66 (2004) 61–91.

[57] V. Sidorenko, V. Zyablov, Decoding of convolutional codes using a syndrome trellis, IEEE Trans. Inf. Theory 40 (5) (1994) 1663–1666.

[58] F.M.J. Willems, M. van Dijk, Capacity and codes for embedding information in gray-scale signals, IEEE Trans. Inf. Theory 51 (3) (2005) 1209–1214.