Twice Grid Colorings in Steganography

Weiming Zhang[1, 2], Xinpeng Zhang[1], Shuozhong Wang[1]

1- School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China

2- Information Engineering University, Zhengzhou 450002, China

E-mail: zwmshu@gmail.com

Abstract

A novel method of steganographic embedding is described based on vertex colorings in the grid graph, in which rainbow coloring is repeated in every block of cover signals to increase embedding efficiency. This is an improvement of the previous grid coloring method in steganography. It also outperforms LSB matching revisited method and direct sums of ternary Hamming codes. The proposed method can generate more embedding schemes which cover the range of change rates and information rates more densely.

1. Introduction

Steganography is a science of secret communication by data hiding. The message sender usually selects a digital multimedia file as a cover-object, and embeds secret message in it. The embedding process is controlled by a key which is shared by the sender and the receiver who can retrieve the message. In data embedding, only slight distortion of the cover-object is allowed so that it is difficult for any third party to detect the existence of the hidden message.

To resist detection, a steganographic scheme should seek high embedding efficiency. In other words, one needs to embed as many data as possible per change of the cover-object. It has been shown that embedding efficiency can be increased by covering codes with syndrome coding [1].

We assume the cover-object is a sequence of grayscale signals $x_1, \ldots, x_N$, and $x_i \in \{0,1,2,\ldots,2^B-1\}$, where typically $B = 8$, 12, or 16. For example, $B = 8$ for grayscale images. If information is only carried by the least significant bits (LSBs) of x_i's, one can use binary covering codes. If the largest magnitude of changes is limited to 1, by x_i+c, $c \in \{0,1,-1\}$, $x_i \bmod 3$ can represent any ternary digit. In this case, one signal of the cover-object can carry $\log_2 3$ bits of information, which is called "±1 steganography".

It has been proven that the smallest embedding impact can be achieved by "±1 steganography" which essentially involves a ternary coding problem. Willems et al. [2] proposed ternary Hamming codes to increase embedding efficiency of ±1 steganography. A more efficient method appeared independently in [3] and [4], which can be viewed as an application of vertex colorings in the grid graph.

In this paper, we propose a new method for "±1 steganography" based on repeating rainbow colorings, which can generate more embedding schemes with better performance than previous methods.

2. Embedding based on ternary Hamming codes

We take 8 bits grayscale images as an example to describe the embedding methods. To use $[(3^r-1)/2, (3^r-1)/2 - r]$, $r \geq 1$, ternary Hamming code, we first divide the cover-object $x_1, \ldots, x_N$ into disjoint segments of n pixels, where $n=(3^r-1)/2$. By syndrome coding, the sender can communicate r ternary digits in $n=(3^r-1)/2$ pixels with $R_a=(3^r-1)/3^r$ modifications on average [2]. We say that this embedding scheme has change rate

$$\rho = \frac{R_a}{n} = \frac{2}{3^r},\ r \geq 1, \tag{1}$$

and information rate

$$\alpha = \frac{r \log_2 3}{n} = \frac{2r \log_2 3}{3^r - 1},\quad r \geq 1. \tag{2}$$

The pair (ρ, α) is called CI rate[1] in [4]. Embedding efficiency is equal to α/ρ. The purpose of steganographer is to seek high information rate and

[1] Here we define the change rate with average number of modifications, while it is defined by the largest number of possible modifications in [4].

978-0-7695-3278-3/08 $25.00 © 2008 IEEE
DOI 10.1109/IIH-MSP.2008.36

low change rate. Ternary Hamming codes can provide a family of embedding schemes with CI rates

$$\left(\rho(r), \alpha(r)\right) = \left(\frac{2}{3^r}, \frac{2r\log_2 3}{3^r - 1}\right), \quad r \geq 1. \tag{3}$$

For steganographic applications, we need embedding methods with various kinds of CI rates, which can be obtained by direct sum of Hamming codes. For instance, from two Hamming codes with CI rates ($\rho(r_1)$, $\alpha(r_1)$) and ($\rho(r_2)$, $\alpha(r_2)$), we can get new embedding schemes with CI rates

$$u\left(\rho(r_1), \alpha(r_1)\right) + (1-u)\left(\rho(r_2), \alpha(r_2)\right),\ 0 \leq u \leq 1. \tag{4}$$

3. Grid coloring method

Fridrich et al. proposed a more efficient method for ±1 steganography based on rainbow colorings as follows [4]. Let $\mathbb{Z}$ and $\mathbb{Z}_n$ denote integer and integer modulo n, respectively. Let d be a positive integer and (e_1, ..., e_d) be the standard basis of $\mathbb{Z}^d$, that is, $(e_i)_j$ equals 1 if $i = j$, otherwise it is 0. The d-dimensional grid graph G_d is defined by the vertex set $V(G_d) = \mathbb{Z}^d$ and the edge set $E(G_d)$ as follows. $\{u, v\} \in E(G_d)$ if and only if $u - v$ equals e_i or $-e_i$ for some $i \in \{1, ..., d\}$.

Define coloring c of G_d by

$$c : \mathbb{Z}^d \to \mathbb{Z}_{2d+1}$$

$$c(x_1, x_2, \cdots, x_d) \equiv \sum_{i=1}^{d} i x_i \bmod (2d+1) \tag{5}$$

G_d is $2d$-regular and c is rainbow $(2d+1)$-coloring of G_d, which means every vertex v of G_d has $2d$ neighborhoods and all these $2d+1$ vertexes can be assigned different colors by c.

We can embed a $(2d+1)$-ary digit m into d pixels (x_1, ..., x_d) by using coloring $c(x_1, ..., x_d)$ to represent message m. No modification is needed if m is equal to the color. When $m \neq c(x_1, ..., x_d)$, calculate $h \equiv m - c(x_1, ..., x_d) \bmod (2d+1)$. If h is no more than d, increase the value of x_h by one, otherwise, decrease the value of x_{2d+1-h} by one. Therefore m is embedded into (x_1, ..., x_d) by at most one change. The average number of changes $R_a = 2d/(2d+1)$ because m equals $c(x_1, ..., x_d)$ with probability $1/(2d+1)$. This embedding method has CI rates

$$\left(\rho(d), \alpha(d)\right) = \left(\frac{2}{2d+1}, \frac{\log_2(2d+1)}{d}\right), \quad d \geq 1. \tag{6}$$

The above method is also reported in [3], while Fridrich et al. used Eq. (5) in a different way. They combined the rainbow coloring with q-ary Hamming codes in [4], which can embed $r\log_2 q$ bits into $(q^r-1)d/(q-1) = (q^r-1)/2$ pixels by $(q^r-1)/q^r$ changes on average, where $q = 2d+1$ is a prime power, which leads to CI rates

$$\left(\rho(r), \alpha(r)\right) = \left(\frac{2}{q^r}, \frac{2r\log_2 q}{q^r - 1}\right),\ r \geq 1. \tag{7}$$

When $q=3$, Eq. (7) becomes the same as Eq. (3), therefore ternary Hamming embedding is a subset of the schemes in [4]. It is also proven that the information rate in (7) is greater than or equal to the information rate of the corresponding direct sum of ternary Hamming codes with the very same change rate. Note that, by letting $d = (q^r-1)/2$ in Eq. (6) where q is a prime power, we get Eq. (7), meaning that the method in [4] can be obtained by directly applying rainbow colorings.

4. Twice Grid colorings method

In this section, we improve the grid coloring method by repeating rainbow colorings on a block of pixels. Divide the cover-object into disjoint segments of mn pixels, $m \geq 3$, $n \geq 3$, and arrange every segment as a matrix such as $(x_{i,j})$, $1 \leq i \leq m$, $1 \leq j \leq n$.

The embedding process consists of two steps. In the first step, apply rainbow coloring (5) to each row with $d = n$,

$$c(x_{i,1}, x_{i,2}, \cdots, x_{i,n}) \equiv \sum_{j=1}^{n} j x_{i,j} \bmod (2n+1),\ 1 \leq i \leq m. \tag{8}$$

Thus we embed $\log_2(2n+1)$ bits of messages in every row by changing one pixel with probability $2n/(2n+1)$, therefore embeds a total of $m\log_2(2n+1)$ bits with $2mn/(2n+1)$ modifications on average. After the first embedding step, we denote the *modified cover-object* as $\{y_{i,j}\}$, $1 \leq i \leq m$, $1 \leq j \leq n$.

In the second step, we embed $\log_2(2m+1)$ bits into the first column ($y_{1,1}$, ..., $y_{m,1}$) using rainbow coloring

$$c(y_{1,1}, y_{2,1}, \cdots, y_{m,1}) \equiv \sum_{i=1}^{m} i x_{i,1} \bmod (2m+1). \tag{9}$$

In this embedding, at most one pixel in ($y_{1,1}$, ..., $y_{m,1}$) needs to be modified with probability $2m/(2m+1)$, which will influence the result of row embeddings in the first step. Therefore we should adjust the values of pixels in the corresponding row. There are several possible cases as described in the following.

We denote the final *stego-object* after two embedding steps by $\{z_{i,j}\}$, $1 \leq i \leq m$, $1 \leq j \leq n$. Without loss of generality, assume that $y_{1,1}$ should be changed in the second step. Because the possible cases are in pairs, we only describe one for each pair, and the other as indicated by the number in brackets can be solved

using a similar method with the same cost of modifications

Case 1(2): When embedding messages in the first row, one pixel $x_{1,k}$, $2<k\le n$, is *increased* (*decreased*) by one, i.e. $y_{1,k}=x_{1,k}+1$, and in the second step, $y_{1,1}$ should be *increased* (*decreased*) by one. Then let $z_{1,1}=y_{1,1}+1=x_{1,1}+1$, $z_{1,k}=y_{1,k}-1=x_{1,k}$ and $z_{1,k-1}=y_{1,k-1}+1=x_{1,k-1}+1$. The final influence on the embedding result of the first row is $1-k+(k-1)=0$. We introduce one change on $x_{1,1}$ and $x_{1,k-1}$, respectively, but restore the change on $x_{1,k}$. Therefore we can keep the result in the first row and satisfy the embedding in the second step with only one additional change.

Case 3(4): One pixel $x_{1,k}$, $2\le k<n$, is *increased* (*decreased*) by one i.e. $y_{1,k}=x_{1,k}+1$, and $y_{1,1}$ should be *decreased* (*increased*) by one. Let $z_{1,1}=y_{1,1}-1=x_{1,1}-1$, and let $z_{1,k}=y_{1,k}-1=x_{1,k}$ and $z_{1,k+1}=y_{1,k+1}+1=x_{1,k+1}+1$. One additional change is needed.

Case 5(6): The pixel value $x_{1,n}$, is *increased* (*decreased*) by one, i.e. $y_{1,n}=x_{1,n}+1$ and $y_{1,1}$ should be *decreased* (*increased*) by one. Then let $z_{1,1}=y_{1,1}-1=x_{1,1}-1$, and $z_{1,n}=y_{1,n}-2=x_{1,n}-1$. The final influence on the embedding in the first row is $-1-2n\equiv 0 \mod (2n+1)$. The modification on $x_{1,n}$ is still one, therefore we only introduce one additional change to $x_{1,1}$.

Case 7(8): The pixel value $x_{1,1}$ is *increased* (*decreased*) by one, i.e. $y_{1,1}=x_{1,1}+1$ and $y_{1,1}$ should be *decreased* (*increased*) by one. Let $z_{1,1}=y_{1,1}-1=x_{1,1}$, $z_{1,2}=y_{1,2}-1=x_{1,2}-1$, and $z_{1,3}=y_{1,3}+1=x_{1,3}+1$. The final influence on the embedding in the first row is $-1-2+3=0$. We introduce one change to $x_{1,1}$ and $x_{1,3}$, respectively, but restore the change to $x_{1,1}$, therefore the number of additional changes is one.

Case 9(10): The pixel value $x_{1,1}$ is *increased* (*decreased*) by one, i.e. $y_{1,1}=x_{1,1}+1$ and $y_{1,1}$ should be *increased* (*decreased*) by one. If only one additional modification is needed when making $z_{2,1}=y_{2,1}+1$ in the second row (similar to Case 1-8), we can let $z_{1,1}=y_{1,1}-1=x_{1,1}$, $z_{1,2}=y_{1,2}-1=x_{1,2}-1$, $z_{1,3}=y_{1,3}+1=x_{1,3}+1$, and $z_{2,1}=y_{2,1}+1$. Thus the influence on the first row is $-1-2+3=0$, on the first column is $-1+2=1$, and two additional changes are introduced. Or if only one additional modification is needed when making $z_{3,1}=y_{3,1}+1$ in the third row, we let $z_{1,1}=y_{1,1}-2=x_{1,1}-1$, $z_{1,2}=y_{1,2}+1=x_{1,2}+1$, and $z_{3,1}=y_{3,1}+1$, which also need two additional changes. If neither of the above two conditions is met, keep $z_{1,1}=y_{1,1}$, and select k, $2\le k\le m-1$, such that when making $z_{k,1}=y_{k,1}-1$ and $z_{k+1,1}=y_{k+1,1}+1$, only one additional modification is needed in the kth row and $(k+1)$th row, respectively. Let $z_{k,1}=y_{k,1}-1$ and $z_{k+1,1}=y_{k+1,1}+1$, introducing two additional changes. Otherwise, let $z_{1,1}=y_{1,1}+1=x_{1,1}+2$, $z_{1,2}=y_{1,2}+1=x_{1,2}+1$, $z_{1,3}=y_{1,3}-1=x_{1,3}-1$.

Case 11(12): The pixel value $x_{1,2}$ is *increased* (*decreased*) by one, i.e. $y_{1,2}=x_{1,2}+1$, and $y_{1,1}$ should be *increased* (*decreased*) by one. Let $z_{1,1}=y_{1,1}+1=x_{1,1}+1$, $z_{1,2}=y_{1,2}-2=x_{1,2}-1$, and $z_{1,3}=y_{1,3}+1=x_{1,3}+1$. The final influence on the embedding in the first row is $1-2\times 2+3=0$. The modification on $x_{1,2}$ is still one, and two additional changes are introduced.

Case 13(14): No pixel is modified in the embedding of the first row, and $y_{1,1}$ should be *increased* (*decreased*) by one. Keep $z_{1,1}=y_{1,1}$, and select k, $2\le k\le m-1$, such that only one additional modification is needed in the kth row and $(k+1)$th row, respectively when making $z_{k,1}=y_{k,1}-1$ and $z_{k+1,1}=y_{k+1,1}+1$. Let $z_{k,1}=y_{k,1}-1$ and $z_{k+1,1}=y_{k+1,1}+1$, introducing two additional changes. If no such kind of k's exists, let $z_{1,1}=y_{1,1}+1$, $z_{1,2}=y_{1,2}+1=x_{1,2}+1$, $z_{1,3}=y_{1,3}-1=x_{1,3}-1$, introducing three changes.

From the above analysis, it is obvious that at most one change is needed with probability $(2n-2)/(2n+1)$ in step 2. Therefore in Case 9(10), probability of more than two modifications is less than $9/(2n+1)^2$. Note that Case 9 or 10 occurs with probability $1/(4n+2)$. Therefore the effect of a change of magnitude 2 in Case 9(10) can be neglected. In Case 13(14), the number of changes is less than 3 on average. For simplicity, we estimate the average number of changes in step 2 by

$$\frac{2m}{2m+1}\left(\frac{4n-4}{2(2n+1)}+\frac{4\times 2}{2(2n+1)}+\frac{2\times 3}{2(2n+1)}\right)=\frac{2m(2n+5)}{(2m+1)(2n+1)} \quad . \tag{10}$$

The average number of changes for the entire embedding process is

$$R_a(m,n)=\frac{2nm}{2n+1}+\frac{2m(2n+5)}{(2m+1)(2n+1)} \ , \tag{11}$$

and the change rate

$$\rho(m,n)=\frac{R_a(m,n)}{mn}=\frac{4mn+6n+10}{(2m+1)(2n+1)n} \quad . \tag{12}$$

The information rate

$$\alpha(m,n)=\frac{m\log_2(2n+1)+\log_2(2m+1)}{mn} \quad . \tag{13}$$

5. Performance comparisons

For ±1 steganography, there is an upper bound on the information rate α subject to the constraint of an changing rate ρ such that $\alpha\le H(\rho)+\rho$, $0\le\rho\le 2/3$ [2],

where $H(\rho) = -\rho\log_2\rho-(1-\rho)\log_2(1-\rho)$ is the binary-entropy function.

Performance comparisons have been made between direct sums of ternary Hamming codes, grid coloring method in [3, 4], LSB matching revisited method in [5], and the method proposed in this paper. LSB matching revisited [5] provides only one CI rate (0.375, 1). For small information rate, since ternary Hamming, grid coloring method and twice grid coloring method have equal performance, we only draw the cases of information rates larger than 0.5 in Fig.1. It is observed that the information rates of grid coloring schemes are never worse than that of direct sums of ternary Hamming codes. However grid coloring method generates only a few embedding schemes with large information rates. The proposed method outperforms grid coloring method and provides more selectable CI rates.

Acknowledgments

This work was supported by the Natural Science Foundation of China (60502039, 60773079), the China Postdoctoral Science Foundation funded project (20070420096), the High-Tech Research and Development Program of China (2007AA01Z477), and Shanghai Rising-Star Program (06QA14022). We thank J. Rifà and H. Rifà-Pous for their interesting idea on stego-coding.

References

[1] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography," available at: http://www.math.mtu.edu/~jbierbra/ (2006)

[2] F. Willems and M. Dijk, "Capacity and codes for embedding information in gray-scale signals," IEEE Transactions on Information Theory, vol. 51, no. 3, pp. 1209-1214, Mar. 2005.

[3] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, Nov. 2006.

[4] J. Fridrich and P. Lisoněk, "Grid coloring in steganography," IEEE Transactions on Information Theory, vol. 53, no. 4, pp. 1547-1549, Apr. 2007.

[5] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, May 2006.

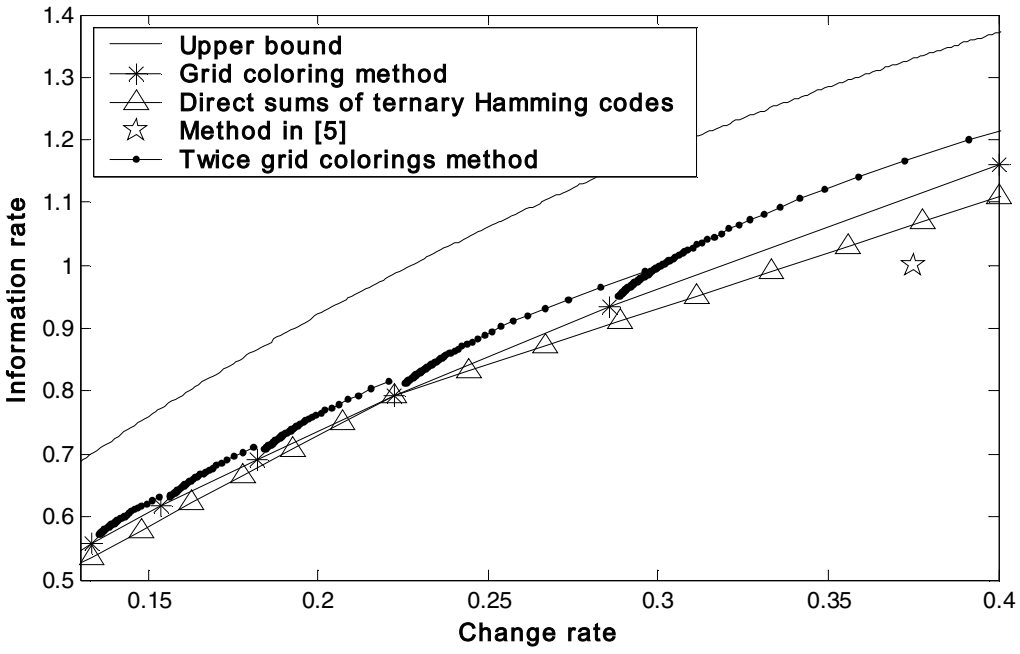

Fig.1 Performance comparison between the proposed method and previous approaches.