Maximizing Steganographic Embedding Efficiency by Combining Hamming Codes and Wet Paper Codes

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

[1] School of Communication and Information Engineering, Shanghai University,
Shanghai 200072, China
[2] Department of Information Research, Information Engineering University,
Zhengzhou 450002, China
zwmshu@gmai.com

Abstract. For good security and large payload in steganography, it is desired to embed as many messages as possible per change of the cover-object, i.e., to have high embedding efficiency. Steganographic codes derived from covering codes can improve embedding efficiency. In this paper, we propose a new method to construct stego-codes, showing that not just one but a family of stego-codes can be generated from one covering code by combining Hamming codes and wet paper codes. This method can enormously expand the set of embedding schemes as applied in steganography. Performances of stego-code families of structured codes and random codes are analyzed. By using the stego-code families of LDGM codes, we obtain a family of near optimal embedding schemes for binary steganography and ±1 steganography, respectively, which can approach the upper bound of embedding efficiency for various chosen embedding rate.

Keywords: steganography, stego-codes, covering codes, wet paper codes, Hamming codes, embedding efficiency, embedding rate.

1 Introduction

Steganography, the art of conveying information confidentially, is realized by embedding secret messages into innocuous cover-objects such as digital images, audios and videos. The very existence of the communication itself is hidden since the stego-object appears the same as the cover. However, as the cover-object is inevitably changed, the covert communication can still be detected by some statistical means. Given a payload, the steganographer should embed as many messages as possible per change of the cover-object, in other words, seek high embedding efficiency so that possibility of being detected is reduced. Crandall first pointed out that embedding efficiency could be improved by coding methods, and proposed the matrix coding [1]. The relation between steganographic codes (stego-codes for short) and covering codes was studied in [2,3]. It turned out that the stego-code could be defined by the covering

K. Solanki, K. Sullivan, and U. Madhow (Eds.): IH 2008, LNCS 5284, pp. 60–71, 2008.

code [3]. For instance, using an $[N, N - n]$ code with the covering radius R, one gets an (R, N, n) stego-code which can embed n bits of messages into a length-N binary cover block by changing at most R bits. Many binary stego-codes have been constructed using structured codes [3,4,5,6] or random codes [7,8].

Binary stego-codes can be used in binary steganography such as binary value image steganography and least significant bit (LSB) steganography. In LSB embedding, the stego-coding methods may be used in the LSB plane of an image, and adding 1 to a pixel is equivalent to subtracting 1 from the pixel for carrying one secret bit. In fact, the choice of addition or subtraction can also be used to carry information. Therefore each pixel can carry $\log_2 3$ bits of data, that is, a ternary digit, with the pixel gray value modulo 3, which is called "±1 steganography" and provides higher embedding efficiency than binary steganography. The ±1 steganography essentially involves a ternary coding problem which can be treated by ternary covering codes. Willems et al. [9] proposed ternary Hamming and Golay codes to improve embedding efficiency of ±1 steganography. A more efficient method appeared independently in [10] and [11], which introduce a family of stego-codes including the ternary Hamming as a subset. In a revisit of the LSB matching method, Mielikainen [12] proposed to choose addition and subtraction depending both on the original gray values and on a pair of consecutive secret bits. Generalization of the revisited LSB matching method is reported in [13].

The upper bounds of the embedding efficiency, with respect to the embedding rate, for binary and ±1 steganography have been obtained in [7] and [9], respectively. A main purpose of stego-coding is to design stego-codes in order to approach these upper bounds. Zhang et al. [14] recently presented a double layered embedding method which can employ any binary stego-codes to ±1 steganography to embed one more bit per change. Moreover it has been shown that, if a binary stego-code can reach the upper bound of embedding efficiency for binary steganography, the corresponding double layered embedding based on this binary stego-code can reach the upper bound of ±1 steganography [14]. Therefore, constructing good binary stego-codes can solve the problems for both binary steganography and ±1 steganography.

In this paper we propose a novel method to design stego-codes by exploiting Hamming codes and wet paper codes [15], which can introduce a family of stego-codes from any given binary stego-code. We call it a stego-code (SC) family of the given stego-code. With the proposed method, we can construct stego-codes approaching the upper bound of embedding efficiency for binary steganography and ±1 steganography at various embedding rates.

The organization of the paper is as follows. Section 2 introduces some notational conventions. Section 3 describes the construction and performance of stego-code families. In Section 4, the stego-code families are modified for applications in ±1 steganography. The paper is concluded following a discussion in Section 5.

2 Notation

We take images as covers to describe the proposed method. To embed data, the cover image is divided into disjoint segments of N pixels, denoted by $\mathbf{g} = (g_1, \ldots, g_N)$, and let $\mathbf{x} = (x_1, \ldots, x_N)$ be their LSBs which is used as carriers. Because the message is usually encrypted before embedding, it can be considered a binary random sequence, and the message block $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{F}_2^n$. A stego-code $\mathrm{SC}(R, N, n)$ can embed n bits of messages into N pixels with at most R modifications. The equivalence between stego-codes and covering codes is shown in [3]. Let $\mathcal{C}$ be an $[N, N-n]$ binary code with a covering radius R, then we can construct a stego-code $\mathrm{SC}(R, N, n)$ by syndrome coding of $\mathcal{C}$ [5,7]. An example of stego-code based on the Hamming codes will be given in Subsection 3.1.

Note that the covering radius R is the largest number of possible changes while the purpose of stego-coding is to minimize the average number of embedding changes R_a [5,7]. Therefore in the following we will replace R with R_a to denote the stego-code, i.e., when we use the notation $\mathrm{SC}(R_a, N, n)$, the first parameter means the average number of changes which is equal to the average distance to the code $\mathcal{C}$ [7]. For perfect codes such as Hamming and Golay codes, the average number of changes can be calculated by $R_a = \frac{1}{2^n} \sum_{i=0}^{R} i \binom{N}{i}$.

For a stego-code $\mathrm{SC}(R_a, N, n)$, we define the embedding rate $\alpha = n/N$, which is the number of bits carried by each pixel; define the average distortion $D = R_a/N$, which is the average changing rate of the cover image; and define the embedding efficiency $e = n/R_a = \alpha/D$, which is the average number of embedded bits per change. We use embedding rate α and embedding efficiency e to evaluate the performance of stego-codes.

3 Stego-Code Families

3.1 Basic Hamming Wet Paper Channel

The covering radius of $[2^k - 1, 2^k - k - 1]$ Hamming codes is one for all integers $k \geq 1$, which can be used to construct a stego-code and embed k bits of messages into $2^k - 1$ pixels by changing at most one of them. Taking $[7, 4]$ Hamming code as an example, we explain how to embed and extract 3 bits of messages into 7 pixels. Let $\mathbf{H}$ be the parity check matrix of the $[7, 4]$ Hamming code

$$\mathbf{H} = \begin{pmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{pmatrix} . \tag{1}$$

Here we make the columns in the natural order of increasing binary numbers. Given a length-7 block of cover $\mathbf{x}$ and a 3 bits message block $\mathbf{m}$, for instance $\mathbf{x} = (1\,0\,0\,1\,0\,0\,0)$ and $\mathbf{m} = (1\,1\,0)$, compute

$$\mathbf{H} \cdot \mathbf{x}^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} . \tag{2}$$

Note that the obtained result $(0\,1\,1)$ is the binary representation of three, that is, the third column of $\mathbf{H}$. By changing the third bit of $\mathbf{x}$ and to get $\mathbf{x}' = (1\,0\,1\,1\,0\,0\,0)$, the embedding process is completed. To extract the messages, we only need to compute

$$\mathbf{H} \cdot \mathbf{x}'^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \mathbf{m}^T \ . \qquad (3)$$

In the above embedding process, no change is needed if $\mathbf{H} \cdot \mathbf{x}^T = \mathbf{m}^T$. This occurs with probability $1/2^3$ because the message is a random sequence of cipher text; otherwise we make $\mathbf{H} \cdot \mathbf{x}^T = \mathbf{m}^T$ by changing only one bit of $\mathbf{x}$, with probability $7/2^3$. Therefore the average number of changes made is $7/2^3$, meaning that we have constructed a stego-code $\mathrm{SC}(7/2^3, 7, 3)$. In general, with the same method we can get stego-code $\mathrm{SC}\left((2^k-1)/2^k, 2^k-1, k\right)$ using $[2^k-1, 2^k-k-1]$ Hamming code for any integer $k \geq 1$. When $k = 1$ the Hamming stego-code $\mathrm{SC}(1/2, 1, 1)$ is just the simple LSB steganography which can embed one bit of message into each pixel and modifies its LSB with probability 1/2.

We now improve the embedding efficiency of Hamming stego-codes by splitting the LSB embedding channel into two different channels. Without loss of generality, assume that the length of the cover is $L2^k$, and divide it into L disjoint blocks. The corresponding LSB blocks are denoted by

$$(x_1, \cdots, x_{2^k}), \quad \ldots, \quad \left(x_{(L-1)2^k+1}, \cdots, x_{L2^k}\right) \ . \qquad (4)$$

First, compress each block into one bit with an exclusive-or operation:

$$y_i = \bigoplus_{j=1}^{2^k} x_{i2^k+j}, \quad i = 0, 1, \cdots, L-1 \ . \qquad (5)$$

We take $(y_0, \cdots, y_{L-1})$ as the first embedding channel, and apply the simple LSB steganography, i.e., $\mathrm{SC}(1/2, 1, 1)$, to it. Therefore each y_i can carry one bit of message and needs to be changed with probability 1/2.

Second, take the first $2^k - 1$ elements from every cover block, and write

$$\mathbf{x}_1 = (x_1, \cdots, x_{2^k-1}), \quad \ldots, \quad \mathbf{x}_L = \left(x_{(L-1)2^k+1}, \cdots, x_{L2^k-1}\right) \ . \qquad (6)$$

Let $\mathbf{H}$ be the parity check matrix of the $[2^k-1, 2^k-k-1]$ Hamming code having a form like (1). In the embedding process of the first channel, if some y_i, for example y_1, needs to be modified, we can flip any one of the 2^k bits in the first block to change y_1, and therefore we can map the first block into any k bits that we need by $\mathbf{H}\mathbf{x}_1^T$. In fact, if $\mathbf{H}\mathbf{x}_1^T$ is just the k bits we want, we can flip x_{2^k} to change y_1, otherwise we make $\mathbf{H}\mathbf{x}_1^T$ equal to any other vector of k bits by changing one of the first 2^k-1 bits in this block. With this in mind, we construct the second embedding channel as follows:

$$\mathbf{H}\mathbf{x}_1^T, \quad \mathbf{H}\mathbf{x}_2^T, \quad \cdots, \quad \mathbf{H}\mathbf{x}_L^T \ . \qquad (7)$$

This channel consists of Lk bits. Because in the embedding process of the first channel there are on average $L/2$ y_i's to be changed, with these changes the corresponding $Lk/2$ bits in the second embedding channel (7) can be modified freely as analyzed in the above. Forbidding any change to the rest $Lk/2$ bits, we get a typical wet paper channel with $Lk/2$ dry positions and $Lk/2$ wet positions [15]. With the binary wet paper coding method in [15] we can embed about $Lk/2$ bits of messages on average, and the receiver can extract these messages without any knowledge about the dry positions. For this reason, we call the second embedding channel as the basic Hamming wet paper channel. A detailed method of binary wet paper coding can be found in [15].

In fact, we embed messages using the above channels in two steps. In the first step, we embed L bits into the channel (5), and label the indices of y_i's which need to be changed, but no change is actually made in this step. In the second step, construct Hamming wet paper channel (7) and embed messages with an embedding rate 1/2 using wet paper coding. In the process of wet paper coding, one bit is flipped in every block with the labelled index i, $1 \leq i \leq L$, which also completes the changes needed by the first step. Combining the two steps, we on average embed $1 + k/2$ bits of messages into a length-2^k block of covers by 1/2 changes, meaning that we obtain the stego-code $\mathrm{SC}(1/2, 2^k, 1 + k/2), k \geq 1$.

3.2 General Framework

To generalize the method described in Subsection 3.1 to any stego-code SC $(R_a, N,\ n)$, we divide the cover image into disjoint blocks of $N2^k$ pixels and, without loss of generality, assume the cover image consists of $LN2^k$ pixels. Write the LSBs of each block as a matrix as follows:

$$\begin{array}{l} x_{1,1}, \cdots,\ x_{1,N} \\ x_{2,1}, \cdots,\ x_{2,N} \\ \cdots \\ x_{2^k,1}, \cdots, x_{2^k,N} \end{array} \quad . \tag{8}$$

In the first step, compress each column into one bit as

$$y_i = \bigoplus_{j=1}^{2^k} x_{j,i} \quad i = 1, 2, \cdots, N \ . \tag{9}$$

Applying $\mathrm{SC}(R_a, N, n)$ to $(y_1, \cdots, y_N)$, we can embed n bits of messages with R_a changes on average. In the second step, let

$$\mathbf{x}_1 = \left(x_{1,1}, \cdots, x_{2^k-1,1}\right), \quad \cdots, \quad \mathbf{x}_N = \left(x_{1,N}, \cdots, x_{2^k-1,N}\right) \ . \tag{10}$$

Construct a Hamming wet paper channel using the same method as in Subsection 3.1

$$\mathbf{H}\mathbf{x}_1^T, \quad \mathbf{H}\mathbf{x}_2^T, \quad \cdots, \quad \mathbf{H}\mathbf{x}_N^T \ . \tag{11}$$

The length of this embedding channel is Nk, including $R_a k$ dry positions and $(N - R_a)k$ wet positions on average. Because there are L blocks in total, each of which can introduce such a Hamming wet paper channel. We can cascade them to employ wet paper coding, and finally embed on average $n + R_a k$ bits of messages into every length-$N2^k$ block with R_a changes. Thus we get a stego-code $\mathrm{SC}(R_a, N2^k, n + R_a k)$, $k \geq 0$. In the second step we use only the R_a columns corresponding to the modified positions in the first step to carry extra messages with no additional modification. If any other column is also used to carry k bits of messages, two additional changes are needed with probability $(2^k - 1)/2^k$, which will lead to low embedding efficiency.

The above construction implies that, for any stego-code $\mathrm{SC}(R_a, N, n)$, there are a family of stego-codes $\mathrm{SC}(R_a, N2^k, n + R_a k)$, $k \geq 0$, associated with it. We denote $\mathrm{SC}(R_a, N2^k, n + R_a k)$ with $S(k)$, $k \geq 0$, and $S(0)$ is just $\mathrm{SC}(R_a, N, n)$.

Definition 1. *Call $S(k)$, $k \geq 0$, the stego-code family* (SCF) *associated with* SC (R_a, N, n)*. Because stego-codes and covering codes are equivalent, if* $\mathrm{SC}(R_a, N, n)$ *can be obtained from the covering code $\mathcal{C}$, we also call $S(k)$, $k \geq 0$, as the* SCF *of $\mathcal{C}$.*

For a stego-code $\mathrm{SC}(R_a, N, n)$, its embedding rate $\alpha = n/N$, embedding efficiency $e = n/R_a$ and average distortion $D = R_a/N$. Then the SCF of SC (R_a, N, n), $S(k)$, $k \geq 0$, has embedding rate $\alpha(k)$, embedding efficiency $e(k)$ and average distortion $D(k)$ as follows:

$$\alpha(k) = \frac{n + R_a k}{N2^k} = \frac{\alpha + Dk}{2^k},\ e(k) = \frac{n + R_a k}{R_a} = e + k,\ D(k) = \frac{R_a}{N2^k} = \frac{D}{2^k} \quad (12)$$

For example, the $[23, 12]$ Golay code, whose covering radius is 3, has the average number of embedding changes

$$R_a = \frac{\binom{23}{1}}{2^{11}} + \frac{\binom{23}{2}}{2^{11}} \times 2 + \frac{\binom{23}{3}}{2^{11}} \times 3 = 2.853 \quad (13)$$

Golay code implies the stego-code $\mathrm{SC}(2.853, 23, 11)$, and therefore the stego-code family $\mathrm{SC}(2.853, 23 \times 2^k, 11 + 2.85k)$, $k \geq 0$. As shown in Fig.1, the SCF of binary Golay provides a family of stego-coding schemes with embedding efficiency better than the binary Hamming.

The stego-code family $\mathrm{SC}(1/2, 2^k, 1 + k/2)$, $k \geq 0$, obtained in Subsection 3.1 is the SCF of $\mathrm{SC}(1/2, 1, 1)$, i.e., Hamming code with $k = 1$. Furthermore, every stego-code in [3-6] leads to a family of stego-codes which enormously enlarges the set of coding methods for applications in steganography. However, we found that almost all stego-codes in [3,4,5,6] are below the embedding efficiency curve of SCF of binary Hamming ($k = 1$), except for a few with large embedding rate such as the $[35, 11]$ non-primitive BCH code proposed in the literature [5]. In Fig.1, it is shown that we can get points exceeding the curve of SCF of binary Hamming ($k = 1$) with the SCF of $[35, 11]$ BCH code. Note that the codes used in [3,4,5,6] are structured codes, and we can employ random codes to construct stego-code families even closer to the upper bound of embedding efficiency.

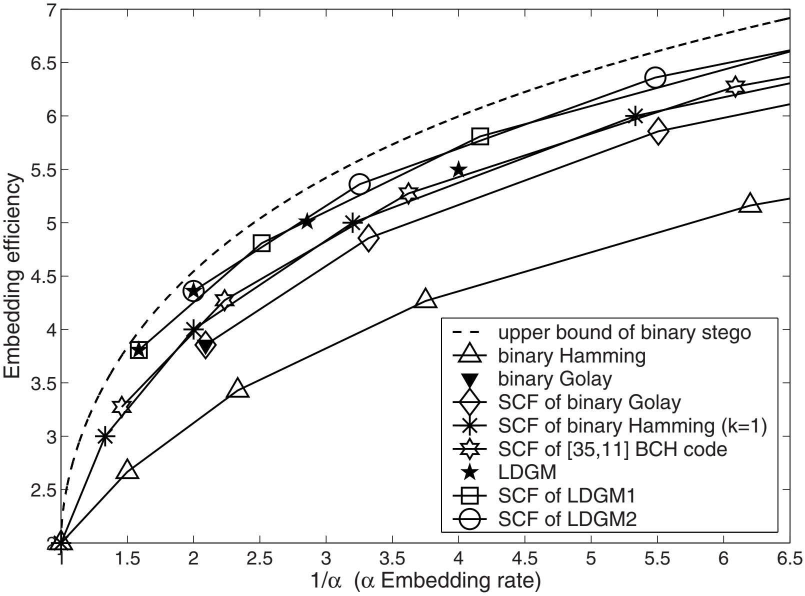

Fig. 1. Performance of stego-code families. The abscissa represents $1/\alpha$ where α is embedding rate.

3.3 SCFs of Random Codes

Binary steganography has the following upper bound [7] of embedding efficiency e with respect to a given embedding rate α.

$$e(\alpha) \leq \frac{\alpha}{H^{-1}(\alpha)}, \quad 0 \leq \alpha \leq 1 \ , \tag{14}$$

where $H(y) = -y \log_2 y - (1-y) \log_2(1-y)$ is the binary-entropy function, and H^{-1} is the inverse function of H.

It has been shown [2,7] that binary random linear codes can achieve the bound (14) asymptotically with the code length $N \to \infty$. The drawback of random codes is high computational complexity for encoding. However, Fridrich et al. presented an embedding scheme with random linear codes in [7] and they also proposed a more efficient method using LDGM codes in [8] recently, which can achieve embedding efficiency very close to the bound (14) with reasonable complexity when the embedding rate α is relatively large.

For instance, by taking LDGM code with length $N = 10000$, Fridrich et al. reported four stego-codes in [8] with embedding rate and embedding efficiency (α, e) as follows:

$$(0.63, 3.808),\ (0.50, 4.360),\ (0.35, 5.010),\ (0.25, 5.495)\ . \tag{15}$$

The four stego-codes are labelled as LDGM in Fig.1, indicating that when the embedding rate is larger than or equal to 0.5, embedding efficiency of LDGM can almost achieve the upper bound. Therefore we use the first two codes in (15) to generate two SCFs. Calculating average distortions by $D = \alpha/e$ and applying (12), we can obtain the following performance of the two SCFs:

$$\alpha_1(k) = \frac{0.63 + 0.165k}{2^k}, \quad e_1(k) = 3.808 + k, \quad k \geq 0 \ ; \tag{16}$$

$$\alpha_2(k) = \frac{0.50 + 0.115k}{2^k}, \quad e_2(k) = 4.360 + k, \quad k \geq 0 \ . \tag{17}$$

These two SCFs are labelled “SCF of LDGM1” and “SCF of LDGM2” in Fig.1, respectively. It is observed that the SCFs of LDGM codes are closer to the upper bound than SCFs of structured codes.

We find that SCFs is still close to the upper bound (14) even when the embedding rate drops, i.e., the k value increases. As an example, the distance between “SCF of LDGM2” (17), for $0 \leq k \leq 10$, and the upper bound (14) is listed in Table 1. All new generated codes, i.e., codes for $1 \leq k \leq 10$, keep small distances from the upper bound, i.e., less than 0.25, only with slight fluctuation. This implies that SCF can provide embedding efficiency close to the upper bound for even very small embedding rate α. One merit of random codes in [7,8] is that they can provide a continuous family of stego-codes dependent on the embedding rate α. Thus, if we generate stego-codes using random codes for all large embedding rates, e.g., $\alpha \geq 0.5$, and collect all their SCFs, then we can get a family of near optimal stego-codes for arbitrarily chosen embedding rates, be it large or small.

Table 1. Distance between “SCF of LDGM2” (17) and the upper bound (14)

k	0	1	2	3	4	5	6	7	8	9	10
$\alpha_2(k)\%$	50.00	30.75	18.25	10.56	6.00	3.36	1.86	1.02	0.55	0.33	0.16
Distance	0.184	0.226	0.240	0.244	0.243	0.241	0.239	0.236	0.234	0.231	0.230

3.4 Computational Complexity

The proposed method increases embedding efficiency by combining previous stego-codes with wet paper codes, which costs more computational complexity, and the additional computational complexity comes from the wet paper coding.

For the SCF of SC(R_a, N, n), computational complexity is determined by the complexity of implementing SC(R_a, N, n) and coding on the Hamming wet paper channel. Usually implementation of stego-codes based on constructed covering codes is very simple. For random codes, a fast algorithm is proposed in [8]. To construct the Hamming wet paper channel, we only need an XOR of some binary vectors of length k to get the changing position, as shown in the example on $[7, 4]$ Hamming code in Subsection 3.1, which has negligible complexity.

A fast algorithm on binary wet paper coding has been presented in [15]. For length-M wet paper channel with m dry positions, we can embed messages with embedding rate m/M and computational complexity $O(M \ln(m/\delta))$ where δ is a constant [15]. For Hamming wet paper channel, computational complexity is mainly influenced by the length of the channel. As shown in Subsection 3.2, if the cover image consists of $LN2^k$ pixels, we can get a Hamming wet paper channel of length LNk. When using wet paper codes, we can divide this channel into disjoint segments with appropriate length M such as $M = 10^5$.

4 Modified SCFs for ±1 Steganography

Coding for ±1 steganography can be viewed as a problem of ternary codes. Ternary Hamming and Golay codes were proposed by Willems, who also obtained the upper bound at the embedding rate α of ±1 steganography subject to the constraint of an average distortion D [9]:

$$C(D) = \begin{cases} G(D) & D \leq \frac{2}{3} \\ \log_2 3 & D > \frac{2}{3} \end{cases} , \tag{18}$$

where $G(D) = H(D)+D$. To evaluate embedding efficiency, we rewrite Equation (18) as an upper bound of the embedding efficiency e depending on a given embedding rate α:

$$e(\alpha) \leq \frac{\alpha}{G^{-1}(\alpha)}, \quad 0 \leq \alpha \leq \log_2 3 \ , \tag{19}$$

where G^{-1} is the inverse function of G.

To employing SCFs of binary codes to approach the bound (19), we only need to slightly modify the construction of Hamming wet paper channel in Subsection 3.2. Assume that the cover is a gray scale image. Denote the gray value of a pixel by g_i, $0 \leq g_i \leq 255$, whose LSB is represented with x_i. For a stego-code SC(R_a, N, n), we still suppose that the image consists of L disjoint pixel blocks of length $N2^k$. Each block is arranged as a matrix with the form like (8). For simplicity, we only use the first column to explain the modification to the Hamming wet paper channel.

The first column of LSBs in (8) is $(x_{1,1}, \cdots, x_{2^k,1})$ and the corresponding column of gray value is $(g_{1,1}, \cdots, g_{2^k,1})$. $y_1 = x_{1,1} \oplus \cdots \oplus x_{2^k,1}$ is the first bit of the first embedding channel, and this column is mapped into k bits by

$$\mathbf{H}\mathbf{x}_1^T = \mathbf{H}(x_{1,1}, \cdots, x_{2^k-1,1})^T . \tag{20}$$

Let

$$z_1 = \left(\left\lfloor \frac{g_{11}}{2} \right\rfloor + \cdots + \left\lfloor \frac{g_{2^k,1}}{2} \right\rfloor \right) \bmod 2 \ . \tag{21}$$

If y_1 needs to be flipped, we can change any one component in $(x_{1,1}, \cdots, x_{2^k,1})$. Which one should be changed is determined by the k bits $\mathbf{H}\mathbf{x}_1^T$ that we want. For example, suppose that $x_{i,1}$, $1 \leq i \leq 2^k$, should be changed. This can be achieved by $g_{i,1} + 1$ or $g_{i,1} - 1$. The choice of adding or subtracting one can be used to control the value of $\lfloor g_{i,1}/2 \rfloor \bmod 2$, therefore control the value of z_1. This means that, when flipping y_1, we get a free bit z_1, or a dry position in terms

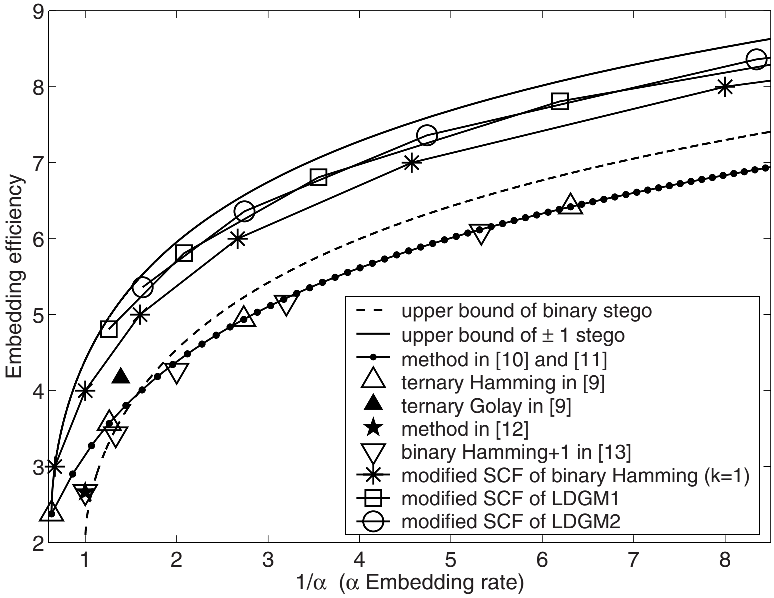

Fig. 2. Performance comparisons among modified SCFs and methods in [9,10,11,12,13]

of wet paper codes, by the same change. In other words, when changing y_1, we can map $(g_{1,1}, \cdots, g_{2^k,1})$ to any $k+1$ bits $(\mathbf{Hx}_1^T, z_1)$ by one change. Doing this to every column of (8), the Hamming wet paper channel (11) can be modified as follows:

$$\mathbf{Hx}_1^T, z_1, \mathbf{Hx}_2^T, z_2, \ldots, \mathbf{Hx}_N^T, z_N \quad . \tag{22}$$

This is an embedding channel of length $N(k+1)$ with $R_a(k+1)$ dry positions. Therefore we can get stego-codes $\mathrm{SC}(R_a, N2^k, n + R_a(k+1)), k \geq 0$. We call them the modified SCF of $\mathrm{SC}(R_a, N, n)$.

Note that the above embedding process may fail when the pixel value $g_{i,1}$ is saturated, i.e., $g_{i,1} = 0$ or 255. In this case, change in only one direction is allowed. When $g_{i,1} = 0$, $g_{i,1} - 1$ is not allowed. We can use $g_{i,1} + 3$ instead to satisfy z_1. Similarly, when $g_{i,1} = 255$ while $g_{i,1} + 1$ is required to satisfy z_1, we use $g_{i,1} - 3$ instead. This of course will introduce larger distortion. But if the probability of gray value saturation is not too large, the effect on the overall performance is negligible.

For a stego-code $\mathrm{SC}(R_a, N, n)$ with embedding rate $\alpha = n/N$, embedding efficiency $e = n/R_a$ and average distortion $D = R_a/N$, the modified SCF has the following performance:

$$\alpha(k) = \frac{\alpha + D(k+1)}{2^k}, \quad e(k) = e + k + 1, \quad D(k) = \frac{D}{2^k}, \quad k \geq 0 \ . \tag{23}$$

Comparing (23) and (12), it can be concluded that both embedding rate and embedding efficiency are improved with the modified SCF at the same average distortion.

Performance comparisons have been made between the modified SCFs and the previous methods. The EMD method in [10] and grid coloring method in [11] can provide the same family of schemes, embedding $\log_2(2d+1)$ bits into d pixels with $2d/(2d+1)$ changes on average, which includes the ternary Hamming stego-codes. The method in [13] applied binary covering codes to ±1 steganography by extending the length of codes and the method in [12] is a special case of the "binary Hamming +1" scheme in [13]. Fig.2 shows that the modified SCF of binary Hamming ($k = 1$) significantly exceeds the methods in [9,10,11,12,13]. Moreover, the modified SCFs of LDGM codes are very close to the upper bound (19). In other words, they provide near optimal embedding schemes for ±1 steganography.

5 Conclusions

In this paper, we have proposed a new method to construct embedding schemes for applications in steganography, which can generate a family of stego-codes from one covering code. By combining this method with random codes such as LDGM codes, we can get a family of near optimal stego-codes for arbitrarily chosen embedding rates.

To resist detection, the sender can always reduce changes to the cover by embedding fewer messages into an image, i.e., use low embedding rate. However, recent advances in steganalysis have made LSB steganography with small embedding rates detectable. For example, the method in [16] can detect simple LSB steganography with embedding rate as low as 2%. Since embedding efficiency of simple LSB steganography is 2, detecting 2% embedding rate means detecting 1% changes. SCF of LDGM codes can provide embedding efficiency better than 10 for the embedding rate of 2%, that is, changes are reduced to 0.2%. That is why SCFs are used to resist steganalysis. Furthermore, it has been shown that ±1 steganography is more secure than LSB steganography because ±1 embedding can avoid the statistical imbalance introduced by LSB replacement. As shown in Section 4, larger embedding efficiency can be obtained with the modified SCFs, so ±1 steganography plus the modified SCFs will provide even better security.

On the other hand, relations between stego-coding and error-correcting codes have been studied in [6,17]. The duality between data embedding and source coding is shown in [8,18]. For example, LDGM codes can be very close to the rate-distortion bound of the source codes, which is just the reason that schemes based on LDGM codes in [8] can almost achieve the bound of embedding efficiency. All these results imply that the SCF is potentially applicable to both source coding and channel coding. Our further study will include applications of SCFs to other fields.

Acknowledgments. This work was supported by the Natural Science Foundation of China (60803155, 60502039), the China Postdoctoral Science

Foundation funded project (20070420096), the High-Tech Research and Development Program of China (2007AA01Z477), and Shanghai Rising-Star Program (06QA14022).

Special thanks go to Professor Jessica Fridrich and Dr. Tomáš Filler for the results of stego-coding based on LDGM codes. The authors would also like to sincerely thank the anonymous reviewers for their valuable comments.

References

1. Crandall, R.: Some notes on steganography. Posted on steganography mailing list (1998), `http://os.inf.tu-dresden.de/westfeld/crandall.pdf`
2. Galand, F., Kabatiansky, G.: Information hiding by coverings. In: Proceedings of the IEEE Information Theory Workshop 2004, pp. 151–154 (2004)
3. Bierbrauer, J., Fridrich, J.: Constructing good covering codes for applications in steganography. In: Transactions on Data Hiding and Multimedia Security. LNCS. Springer, Heidelberg (to appear, 2007), `http://www.math.mtu.edu/jbierbra/`
4. Tseng, Y.C., Chen, Y.-Y., Pan, H.-K.: A secure data hiding scheme for binary images. IEEE Transactions on Communications 50(8), 1227–1231 (2002)
5. Schönfeld, D., Winkler, A.: Embedding with syndrome coding based on BCH codes. In: Proc. ACM the 8th workshop on Multimedia and Security, pp. 214–223 (2006)
6. Munuera, C.: Steganography and error-correcting codes. Signal Processing 87, 1528–1533 (2007)
7. Fridrich, J., Soukal, D.: Matrix embedding for large payloads. IEEE Transactions on Information Security and Forensics 1(3), 390–394 (2006)
8. Fridrich, J., Filler, T.: Practical methods for minimizing embedding impact in steganography. In: Proc. SPIE Electronic Imaging, vol. 6050 (2007)
9. Willems, F., Dijk, M.: Capacity and codes for embedding information in gray-scale signals. IEEE Transactions on Information Theory 51(3), 1209–1214 (2005)
10. Zhang, X., Wang, S.: Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters 10(11), 781–783 (2006)
11. Fridrich, J., Lisoněk, P.: Grid coloring in steganography. IEEE Transactions on Information Theory 53(4), 1547–1549 (2007)
12. Mielikainen, J.: LSB matching revisited. IEEE Signal Processing Letters 13(5), 285–287 (2006)
13. Zhang, W., Wang, S., Zhang, X.: Improving embedding efficiency of covering codes for applications in steganography. IEEE Communications Letters 11(8), 680–682 (2007)
14. Zhang, W., Zhang, X., Wang, S.: A double layered "plus-minus one" data embedding scheme. IEEE Signal Processing Letters 14(11), 848–851 (2007)
15. Fridrich, J., Goljan, M., Lisonek, P., Soukal, D.: Writing on wet paper. IEEE Transactions on Signal Processing 53(10), 3923–3935 (2005)
16. Ker, A.D.: A General Framework for the Structural Steganalysis of LSB Replacement. In: Barni, M., Herrera-Joancomartí, J., Katzenbeisser, S., Pérez-González, F. (eds.) IH 2005. LNCS, vol. 3727, pp. 296–311. Springer, Heidelberg (2005)
17. Zhang, W., Li, S.: A coding problem in steganography. Designs, Codes and Cryptography 46(1), 67–81 (2008)
18. Barron, R.J., Chen, B., Wornell, G.W.: The duality between information embedding and source coding with side information and some applications. IEEE Transactions on Information Theory 49(5), 1159–1180 (2003)