Near-Optimal Codes for Information Embedding in Gray-Scale Signals

Weiming Zhang, Xinpeng Zhang, and Shuozhong Wang

***Abstract*—High-performance steganography requires large embedding rate and small distortion, i.e., high embedding efficiency. Steganographic codes (stego-codes) derived from covering codes can improve embedding efficiency. In this paper, a new method is proposed to construct binary stego-codes for LSB embedding in gray-scale signals, which shows that not just one but a family of stego-codes can be generated from a covering code by combining Hamming codes and wet paper codes. This method can greatly expand the set of embedding schemes as applied to steganography. Performances of stego-code families (SCF) of structured codes and random codes are analyzed. SCFs of random codes can approach the rate-distortion bound on LSB embedding for any chosen embedding rate. Furthermore, SCFs are modified for applications in ± 1 embedding, and a treble layered embedding method for ± 2 embedding is obtained. By combining the modified SCFs and the treble layered method, a near-optimal scheme for ± 2 embedding is presented.**

***Index Terms*—Average distortion, covering codes, embedding efficiency, embedding rate, information embedding, LDGM codes, steganography, wet paper codes.**

I. Introduction

STEGANOGRAPHY, the art of conveying information confidentially, is realized by embedding information into innocuous cover-objects such as digital image, audio and video. 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. To resist the detection, the steganographer wants to minimize the impact of data embedding (distortion) on the cover-object for a given payload (embedding rate), which can be formulated as a rate-distortion problem. The rate-distortion bounds on least significant bit (LSB) embedding [1] and the general embedding manner in gray-scale signals [2] have been obtained. We call coding methods on this rate-distortion problem steganographic codes (stego-codes) in this paper. It turns out that the stego-code could be defined by the covering code [1], [3], and many binary stego-codes have been constructed using structured codes [3]–[7] or random codes [8], [9].

Binary stego-codes can be used for LSB embedding, in which coding methods are used in the LSB plane of gray-scale symbols, and messages are embedded with LSB flipping. In LSB embedding, the maximum change of each gray-scale symbol is one and each symbol can carry at most one bit of information. In fact, by choosing adding or subtracting one to/from the gray-scale value, each symbol can carry $\log_2 3$ bits of data, that is, a ternary digit, with the gray value modulo 3, called "± 1 embedding." The ± 1 embedding essentially involves a ternary coding problem that can be treated with ternary covering codes. Willems *et al.* [2] proposed ternary Hamming and Golay codes to improve the performance of ± 1 embedding. A more efficient method appeared independently in [10] and [11], which introduces a family of stego-codes including the ternary Hamming as a subset. Generally, we can limit the maximum modification as f, which is called "$\pm f$ embedding". For example, in "± 2 embedding," the allowable modifications include $\{-2, -1, 0, +1, +2\}$. Because stego-objects become detectable rather quickly with the increasing maximum embedding-caused changes, f must be small for steganographic applications.

A main goal of stego-coding is to approach the rate-distortion bounds [1], [2]. Binary stego-codes based on random linear codes [8] and low-density generator matrix (LDGM) codes [9] can approach the rate-distortion bound of LSB embedding for large embedding rates. Practically, however, the steganographer needs good codes at various embedding rates for different applications. For instance, Hamming stego-codes used in the F5 algorithm [12] are the most popular stego-coding methods because they are a family of variable-rate codes. Although the Golay stego-code seems to have better performance than the Hamming codes, it is only an isolated point providing a fixed embedding rate, as shown in Fig. 2. An interesting question is whether we can generate a family of stego-codes from the Golay code outperforming the Hamming codes.

By exploiting wet paper codes [13], we in this paper propose a novel method to design stego-codes, which can generate a family of variable-rate binary stego-codes from any given binary stego-code. We call it stego-code family associated with the given stego-code. With the proposed method, we can construct stego-codes approaching the rate-distortion bound on LSB embedding, ± 1 and ± 2 embedding at various embedding rates.

The organization of this paper is as follows. Section II introduces some notational conventions. Section III describes the construction and performance of stego-code families. In

Manuscript received May 29, 2008; revised October 31, 2009. Current version published March 10, 2010. This work was supported by the Natural Science Foundation of China (60803155), and by the High-Tech Research and Development Program of China (2007AA01Z477). The material in this paper was presented in part at the 10th Information Hiding Conference (IH'08), Santa Barbara, CA, May 2008.

W. Zhang is with the School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, P. R. China (e-mail: zwmshu@gmail.com).

X. Zhang and S. Wang are with the School of Communication and Information Engineering, Shanghai University, Shanghai 200076, China (e-mail: xzhang@shu.edu.cn; shuowang@shu.edu.cn).

Communicated by T. Fujiwara, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2009.2039087

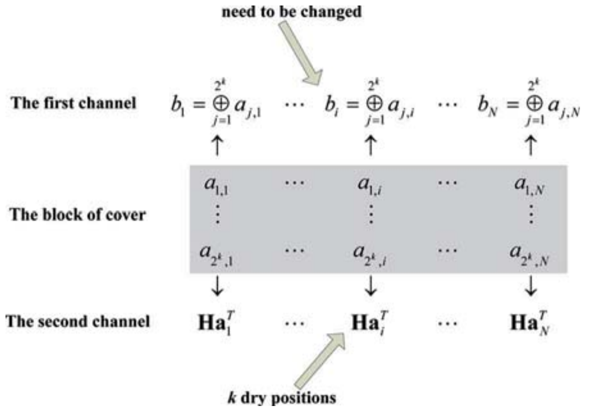
need to be changed
The first channel
$b_1 = \bigoplus_{j=1}^{2^k} a_{j,1}$ ⋯ $b_i = \bigoplus_{j=1}^{2^k} a_{j,i}$ ⋯ $b_N = \bigoplus_{j=1}^{2^k} a_{j,N}$
The block of cover
$a_{1,1}$ ⋯ $a_{1,i}$ ⋯ $a_{1,N}$
$a_{2^k,1}$ ⋯ $a_{2^k,i}$ ⋯ $a_{2^k,N}$
The second channel
$\mathbf{Ha}_1^T$ ⋯ $\mathbf{Ha}_i^T$ ⋯ $\mathbf{Ha}_N^T$
k dry positions

Fig. 1. Illustration on the general framework of the proposed method, in which $\mathbf{H}$ is the parity check matrix of the $[2^k-1, 2^k-k-1]$ Hamming code and $\mathbf{a}_i = (a_{1,i}, \ldots, a_{2^k-1,i}), 1 \leq i \leq N$.

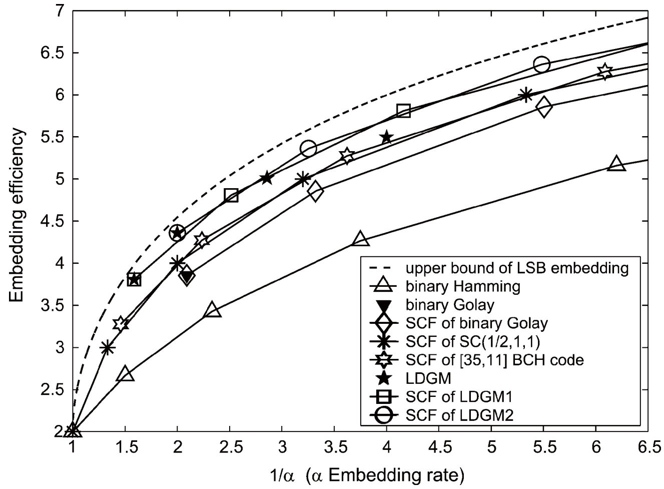

Fig. 2. Performance of stego-code families. The abscissa represents $1/\alpha$ where α is embedding rate.

Section IV, the stego-code families are modified for applications in ±1 embedding. In Section V, a treble-layered scheme for ±2 embedding is given. The paper is concluded following a discussion in Section VI.

II. Notations

We assume that the cover-object is a sequence of gray-scale signals $\mathbf{x} = (x_1, \ldots, x_N)$, and $x_i \in \mathcal{G} = \{0, 1, 2, \ldots, 2^B - 1\}$, $1 \leq i \leq N$, where typically $B = 8, 12$, or 16. For example, $B = 8$ for gray-scale images. Because the message is usually encrypted before being embedded, it can be considered a binary random sequence. The message block is denoted by $\mathbf{m} = (m_1, \ldots, m_n) \in \mathcal{F}_2^n$, which is independent of the cover $\mathbf{x}$. After embedding $\mathbf{m}$ into $\mathbf{x}$, we get a stego-object $\mathbf{y} = (y_1, \ldots, y_N)$, where $y_i \in \mathcal{G}$, $1 \leq i \leq N$. We use squared-error distortion as did in [2]: if a gray-scale symbol x_i is changed into y_i, the resulting distortion is $D(y_i - x_i) = (y_i - x_i)^2$. If the maximum modification is f, the set of allowable modifications is $\mathcal{Z} = \{-f, -f+1, \ldots, +f\}$. Assuming $p_z = P(z)$, $z \in \mathcal{Z}$, is the probability distribution over $\mathcal{Z}$, the average distortion is

$$d = \sum_{z \in \mathcal{Z}} p_z D(z) = \sum_{z \in \mathcal{Z}} p_z z^2. \tag{1}$$

Specifically, if $f = 1$, the average distortion equals to the changing probability, i.e., the ratio between the average number of changes and the length of the cover block.

The embedding rate is defined as $\alpha = n/N$, which is the number of bits carried by each gray-scale signal. Rate-distortion functions for $f = 1, 2, \ldots, \infty$ were obtained in [2]

$$r_f(\Delta) = \max_{\{P_z : \sum_z P_z z^2 \leq \Delta\}} H(Z) \tag{2}$$

where $H(Z) = -\sum_{z \in \mathcal{Z}} P(z) \log_2 P(z)$ is the entropy determined by the distribution $\{P(z), z \in \mathcal{Z}\}$. Equation (2) is a tight upper bound on the embedding rate α subject to the constraint of average distortion Δ for maximum allowable modification f.

Embedding efficiency e is defined as the ratio between embedding rate and average distortion: $e = \alpha/d$. For applications in steganography, *embedding rate-embedding efficiency* is generally used to evaluate performance, which is equivalent to the rate-distortion measurement. The rate-distortion bound (2) can be recognized in its equivalent form as an upper bound on embedding efficiency e with respect to a given embedding rate α

$$e(\alpha) \leq \frac{\alpha}{r_f^{-1}(\alpha)} \tag{3}$$

where $r_f^{-1}(\alpha)$ is inverse of the rate-distortion function $r_f(\Delta)$.

For LSB embedding, the manner of modification is LSB flipping, and the maximum amplitude of modification is one. Thus the average distortion is determined by the average number of changes. The efficiency of LSB embedding can be improved with a binary stego-code, and equivalence between stego-codes and covering codes have been shown in [1], [3], [6], and [8]. Let $\mathcal{C}$ be an $[N, N-n]$ binary code with an covering radius R. We can use $\mathcal{C}$ to embed n bits of messages into the LSBs of N gray-scale symbols with at most R changes by syndrome coding [6], [8]. The average number of changes R_a is equal to the average distance to the code $\mathcal{C}$. For perfect codes such as Hamming and Golay codes, $R_a = \frac{1}{2^n} \sum_{i=0}^{R} i \binom{N}{i}$. We denote such a stego-code as $\mathrm{SC}(R_a, N, n)$. Note that the notation $\mathrm{SC}(R_a, N, n)$ in this paper only denotes a binary stego-code. An example of binary stego-codes based on binary Hamming codes will be given in Section III-A.

For a stego-code $\mathrm{SC}(R_a, N, n)$, the embedding rate $\alpha = n/N$, average distortion $d = R_a/N$, and embedding efficiency $e = n/R_a = \alpha/d$. The rate-distortion function for LSB embedding is as follows [1]:

$$r(\Delta) = \begin{cases} H(\Delta) & \Delta \leq \frac{1}{2} \\ 1 & \Delta > \frac{1}{2} \end{cases} \tag{4}$$

where $H(\Delta) = -\Delta \log_2 \Delta - (1 - \Delta) \log_2 (1 - \Delta)$ is the binary entropy function. Similar to (3), (4) can be rewritten as the upper bound of embedding efficiency e with respect to a given embedding rate α [8]

$$e(\alpha) \leq \frac{\alpha}{H^{-1}(\alpha)}, \quad 0 \leq \alpha \leq 1 \tag{5}$$

where $H^{-1}(\alpha)$ is inverse of $H(\Delta)$.

III. Stego-Code Families

A. Basic Hamming Wet Paper Channel

For a gray-scale signal $(x_1, \dots, x_N)$, let $(a_1, \dots, a_N)$ be its LSB, which is used as carriers of binary stego-coding. Now we describe how to construct binary stego-codes with Hamming codes. To use $[2^k-1, 2^k-k-1], k \geq 1$, Hamming codes, first divide the LSB $(a_1, \dots, a_N)$ into disjoint segments of 2^k-1 bits. The message is associated with the coset of the Hamming code. There are 2^k cosets for $[2^k-1, 2^k-k-1]$ Hamming code, which can represent k bits of messages, and the message is denoted as the syndrome with respect to a fixed parity check matrix $\mathbf{H}$. For instance, assume the first block of LSB is $\mathbf{a} = (a_1, \dots, a_{2^k-1})$, and the corresponding message block is $\mathbf{m} = (m_1, \dots, m_k)$. To embed $\mathbf{m}$ into $\mathbf{a}$, compute syndrome $\mathbf{Ha}^T$. If $\mathbf{Ha}^T = \mathbf{m}^T$, $\mathbf{m}$ is embedded into $\mathbf{a}$ without any change, otherwise we only need to flip one $a_i, 1 \leq i \leq 2^k-1$, to make $\mathbf{Ha}^T = \mathbf{m}^T$ hold because the covering radius of Hamming code is one. When embedding $\mathbf{m}$, one change is needed with probability $(2^k-1)/2^k$, therefore, the average number of changes $R_a = (2^k-1)/2^k$.

Taking [7, 4] Hamming code as an example, we explain how to embed and extract 3 bits of messages into 7 gray-scale symbols. Let $\mathbf{H}$ be the parity check matrix of the [7, 4] Hamming code

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{6}$$

Here we make the columns in an ascending order of binary numbers. Given a length-7 block of cover $\mathbf{a}$ and a three bit message block $\mathbf{m}$, for instance $\mathbf{a} = (1\ 0\ 0\ 1\ 0\ 0\ 0)$ and $\mathbf{m} = (1\ 1\ 0)$, compute

$$\mathbf{Ha}^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}. \tag{7}$$

Note that the obtained result $(0\ 1\ 1)$ is the binary representation of 3, meaning the third column of $\mathbf{H}$. By changing the third bit of $\mathbf{a}$ to get $\mathbf{a}' = (1\ 0\ 1\ 1\ 0\ 0\ 0)$, the embedding process is completed. To extract the message, we only need to compute

$$\mathbf{Ha}'^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \mathbf{m}^T. \tag{8}$$

In the above embedding process, no change is needed if $\mathbf{H} \cdot \mathbf{a}^T = \mathbf{m}^T$. This occurs with probability $1/2^3$ because the message is a random sequence of encrypted text; otherwise we make $\mathbf{H} \cdot \mathbf{a}^T = \mathbf{m}^T$ by changing only one bit of $\mathbf{a}$ with probability $7/2^3$. Therefore, the average number of changes is $7/2^3$, indicating that we have constructed a stego-code $\mathrm{SC}(7/2^3, 7, 3)$. In general, using the same method we can get stego-code $\mathrm{SC}\left((2^k-1)/2^k, 2^k-1, k\right)$ with $[2^k-1, 2^k-k-1]$ 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 replacement which embeds one bit of message into each gray-scale symbol 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 cover is $L2^k$ which can be divided into L disjoint blocks. The corresponding LSB blocks are denoted by

$$(a_1, \dots, a_{2^k}), \quad \dots, \quad \left(a_{(L-1)2^k+1}, \dots, a_{L2^k}\right). \tag{9}$$

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

$$b_i = \bigoplus_{j=1}^{2^k} a_{i2^k+j}, \quad i = 0, 1, \dots, L-1. \tag{10}$$

We take $(b_0, \dots, b_{L-1})$ as the first embedding channel, and apply the simple LSB replacement, namely $\mathrm{SC}(1/2, 1, 1)$, to it. Therefore, each b_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

$$\begin{aligned} \mathbf{a}_1 &= (a_1, \dots, a_{2^k-1}), \dots, \\ \mathbf{a}_L &= \left(a_{(L-1)2^k+1}, \dots, a_{L2^k-1}\right). \end{aligned} \tag{11}$$

Let $\mathbf{H}$ be the parity check matrix of the $[2^k-1, 2^k-k-1]$ Hamming code, having a form like (6). In the embedding process of the first channel, if some b_i needs to be modified, we can flip any one of the 2^k bits in the ith block to change b_i, and simultaneously map the ith block to any k bits $\mathbf{Ha}_i^T$ that we need. In fact, if $\mathbf{Ha}_i^T$ is the k bits we want, we flip a_{i2^k} to change b_i, otherwise we can make $\mathbf{Ha}_i^T$ 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:

$$\mathbf{Ha}_1^T, \mathbf{Ha}_2^T, \dots, \mathbf{Ha}_L^T. \tag{12}$$

This channel contains Lk bits. Because in the embedding process of the first channel there are on average $L/2$ b_i's to be changed, with these changes the corresponding $Lk/2$ bits in the second embedding channel (12) 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 [13]. With the binary wet paper coding method as described in [13] 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 [13].

In fact, we embed messages using the above channels in two steps. In the first step, we embed L bits into the channel (10), and label the indices of b_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 (12) and embed messages using wet paper codes. In the process of wet paper coding, one bit is flipped in every block with the labeled index i, $1 \leq i \leq L$, which also completes the changes needed in the first step. Combining the two steps, we embed $1 + k/2$ bits of messages on average into a length-2^k block of covers by $1/2$ changes, meaning that we obtain the stego-code $\mathrm{SC}(1/2, 2^k, 1 + k/2)$.

B. General Framework

To generalize the method described in Section III-A to any stego-code $\mathrm{SC}(R_a, N, n)$, we divide the cover-object into disjoint blocks of $N2^k$ symbols and, without loss of generality, assume that the cover-object consists of $LN2^k$ symbols. Write LSBs of each block as a matrix as follows:

$$\begin{matrix} a_{1,1}, \ \ldots, \ a_{1,N} \\ a_{2,1}, \ \ldots, \ a_{2,N} \\ \cdots \\ a_{2^k,1}, \ \ldots, \ a_{2^k,N}. \end{matrix} \tag{13}$$

From the cover block, two channels will be constructed as shown in Fig. 1.

In the first step, compress each column of (13) into one bit as

$$b_i = \bigoplus_{j=1}^{2^k} a_{j,i} \quad i = 1, 2, \ldots, N. \tag{14}$$

Applying $\mathrm{SC}(R_a, N, n)$ to $(b_1, \ldots, b_N)$, we can embed n bits of messages with R_a changes on average.

In the second step, let

$$\begin{aligned} \mathbf{a}_1 &= \left(a_{1,1}, \ldots, a_{2^k-1,1}\right), \ldots, \\ \mathbf{a}_N &= \left(a_{1,N}, \ldots, a_{2^k-1,N}\right). \end{aligned} \tag{15}$$

Construct a Hamming wet paper channel using the same method as in Section III-A

$$\mathbf{Ha}_1^T, \mathbf{Ha}_2^T, \ldots, \mathbf{Ha}_N^T. \tag{16}$$

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 $\mathrm{SC}(R_a, N2^k, n + R_a k)$.

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. When taking $k = 0$ in this code family, we get $\mathrm{SC}(R_a, N, n)$ itself.

Definition 1: Call $\mathrm{SC}(R_a, N2^k, n + R_a k)$, $k \geq 0$, the stego-code family (SCF) associated with $\mathrm{SC}(R_a, N, n)$. Because stego-codes and covering codes are equivalent, we also call $\mathrm{SC}(R_a, N2^k, n + R_a k)$, $k \geq 0$, as the SCF of $\mathcal{C}$ if $\mathrm{SC}(R_a, N, n)$ can be obtained from the covering code $\mathcal{C}$.

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 $d = R_a/N$. The SCF associated with it, $\mathrm{SC}(R_a, N2^k, n + R_a k)$, $k \geq 0$, has an embedding rate $\alpha(k)$, embedding efficiency $e(k)$ and average distortion $d(k)$ as follows:

$$\begin{aligned} \alpha(k) &= \frac{n + R_a k}{N2^k} = \frac{\alpha + dk}{2^k}, \\ e(k) &= \frac{n + R_a k}{R_a} = e + k, \\ d(k) &= \frac{R_a}{N2^k} = \frac{d}{2^k}, \quad k \geq 0. \end{aligned} \tag{17}$$

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

$$R_a = \frac{\binom{23}{1}}{2^{11}} + \frac{\binom{23}{2}}{2^{11}} \times 2 + \frac{\binom{23}{3}}{2^{11}} \times 3 \approx 2.85. \tag{18}$$

Golay code implies the stego-code $\mathrm{SC}(2.85, 23, 11)$, and therefore the stego-code family $\mathrm{SC}(2.85, 23 \times 2^k, 11 + 2.85k)$, $k \geq 0$. As shown in Fig. 2, 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 Section III-A is the SCF of simple LSB replacement $\mathrm{SC}(1/2, 1, 1)$. Furthermore, every stego-code in [3]–[7] leads to a family of stego-codes which enormously enlarges the set of coding methods for applications in steganography. Surprisingly, we find that almost all stego-codes in [3]–[7] are below the embedding efficiency curve of the SCF of $\mathrm{SC}(1/2, 1, 1)$, except for a few with large embedding rate such as the $[35, 11]$ nonprimitive BCH code proposed in [6]. Fig. 2 shows that we can get points exceeding the curve of SCF of $\mathrm{SC}(1/2, 1, 1)$ with SCF of $[35, 11]$ BCH code. Note that the codes used in [3]–[7] are structured codes, and we can employ random codes to generate stego-code families even closer to the upper bound on embedding efficiency.

C. SCFs of Random Codes

It has been shown [1], [8] that binary random linear codes can reach the upper bound of embedding efficiency (5) 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 [8]. They also proposed a more efficient method using LDGM codes in [9], which can achieve embedding efficiency very close to the bound (5) 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 4 stego-codes in [9] with embedding rate and embedding efficiency (α, e) as follows:

$$(0.63, 3.808), \ (0.50, 4.360), \ (0.35, 5.010), \ (0.25, 5.495). \tag{19}$$

The 4 stego-codes are labeled as LDGM in Fig. 2, indicating that when the embedding rate is greater than or equal to 0.5, embedding efficiency of LDGM can almost reach the upper bound. Therefore we use the first two codes in (19) to generate two SCFs. Calculating average distortions by $d = \alpha/e$ and applying (17), we can obtain the following performance of the two SCFs:

$$\begin{aligned} \alpha_1(k) &= \frac{0.63 + 0.165k}{2^k} \\ e_1(k) &= 3.808 + k, \quad k \geq 0; \end{aligned} \tag{20}$$

$$\begin{aligned} \alpha_2(k) &= \frac{0.50 + 0.115k}{2^k} \\ e_2(k) &= 4.360 + k, \quad k \geq 0. \end{aligned} \tag{21}$$

TABLE I
DISTANCE BETWEEN "SCF OF LDGM2" (21) AND THE UPPER BOUND (5)

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

These two SCFs are labeled "SCF of LDGM1" and "SCF of LDGM2" in Fig. 2, respectively. It is observed that 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 (5) even when the embedding rate drops, i.e., the k value increases. As an example, the distance between "SCF of LDGM2" (21), for $0 \leq k \leq 10$, and the upper bound (5) is listed in Table I. All new generated codes, codes for $1 \leq k \leq 10$, keep small distances from the upper bound, that is, less than 0.25, only with a slight fluctuation. This implies that SCF can provide embedding efficiency close to the upper bound even for very small embedding rate α. One merit of random codes in [8] and [9] is that they can provide a continuous family of stego-codes depending 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.

D. Computational Complexity

The proposed method improves embedding efficiency by combining previous stego-codes with wet paper codes, which has higher computational complexity. The additional complexity comes from the wet paper coding.

For the SCF of $\mathrm{SC}(R_a, N, n)$, computational complexity is determined by the complexity of implementing $\mathrm{SC}(R_a, N, n)$ and coding on the Hamming wet paper channel. Usually implementation of stego-codes based on constructed covering codes is very simple. For random codes, fast algorithms were proposed in [8] and [9]. To construct a Hamming wet paper channel, we only need to perform XOR of some binary vectors of length k to get the changing positions, as shown in the example on $[7,4]$ Hamming code in Section III-A, which has negligible complexity.

A fast algorithm for binary wet paper coding has been presented in [13]. For a length-M wet paper channel with m dry positions, we can embed messages with an embedding rate m/M and computational complexity $O(M\ln(m/\lambda))$ where λ is a constant [13]. For embedding messages in a Hamming wet paper channel, computational complexity is mainly determined by length of the channel. As shown in Section III-B, if the cover image consists of $LN2^k$ symbols, 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 $M = 10^5$.

IV. MODIFIED SCFS FOR ±1 EMBEDDING

The rate-distortion function (2) for ±1 embedding, i.e., $f = 1$, has the following equivalent form [2]:

$$r_1(\Delta) = \begin{cases} H(\Delta) + \Delta & \Delta \leq \frac{2}{3} \\ \log_2 3 & \Delta > \frac{2}{3}. \end{cases} \tag{22}$$

The corresponding upper bound on embedding efficiency e depending on a given embedding rate α is

$$e(\alpha) \leq \frac{\alpha}{r_1^{-1}(\alpha)}, \quad 0 \leq \alpha \leq \log_2 3. \tag{23}$$

To approach the bound (23) by using SCFs of binary codes, we only need to slightly modify the construction of Hamming wet paper channel in Section III-B. To use a stego-code $\mathrm{SC}(R_a, N, n)$, we also assume that the cover consists of L disjoint blocks of length $N2^k$. Each block is arranged as a matrix with a form of (13). For simplicity, we only use the first column to explain the modification made to the Hamming wet paper channel.

The first column of LSBs in (13) is $(a_{1,1}, \ldots, a_{2^k,1})$ and the corresponding column of gray value is $(x_{1,1}, \ldots, x_{2^k,1})$. $b_1 = a_{1,1} \oplus \cdots \oplus a_{2^k,1}$ is the first bit of the first embedding channel, and this column is mapped into k bits by

$$\mathbf{Ha}_1^T = \mathbf{H}(a_{1,1}, \ldots, a_{2^k-1,1})^T. \tag{24}$$

Let

$$c_1 = \left(\left\lfloor \frac{x_{11}}{2} \right\rfloor + \cdots + \left\lfloor \frac{x_{2^k,1}}{2} \right\rfloor \right) \bmod 2. \tag{25}$$

If b_1 needs to be flipped, we can change any one component in $(a_{1,1}, \ldots, a_{2^k,1})$. Which one should be changed is determined by the k bits $\mathbf{Ha}_1^T$ that we want. For example, suppose that $a_{i,1}$, $1 \leq i \leq 2^k$, should be changed. This can be achieved by $x_{i,1}+1$ or $x_{i,1}-1$. The choice of adding or subtracting one can be used to control the value of $\lfloor x_{i,1}/2 \rfloor \bmod 2$, and therefore control the value of c_1. This means that, when flipping b_1, we get a free bit c_1, or a dry position in terms of wet paper codes, by the same change. In other words, when changing b_1, we can map $(x_{1,1}, \ldots, x_{2^k,1})$ to any $k+1$ bits $(\mathbf{Ha}_1^T, c_1)$ by one change. Doing this to every column of (13), the Hamming wet paper channel (16) can be modified as

$$\mathbf{Ha}_1^T, c_1, \mathbf{Ha}_2^T, c_2, \ldots, \mathbf{Ha}_N^T, c_N. \tag{26}$$

This is an embedding channel of length $N(k+1)$ with $R_a(k+1)$ dry positions. Therefore we get stego-codes embedding $n + R_a(k+1)$ bits of messages into $N2^k$ cover symbols with R_a changes on average, $k \geq 0$, which we call the modified SCF of $\mathrm{SC}(R_a, N, n)$.

Note that the above embedding process may fail when a gray value x is saturated, i.e., $x = 0$ or $2^B - 1$. In this case, change in only one direction is allowed. When $x = 0$ but $x - 1$ is required, we use $x + 3$ instead. Similarly, if $x = 2^B - 1$ but $x + 1$ is required, we use $x - 3$ instead. This of course will introduce larger distortion. However, if the probability of gray value saturation is small, 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:

$$\alpha(k) = \frac{\alpha + d(k+1)}{2^k}, \quad e(k) = e + k + 1,$$
$$d(k) = \frac{d}{2^k}, \quad k \geq 0. \tag{27}$$

Comparing (27) and (17), we conclud that both the embedding rate and embedding efficiency of SCF are improved by the modified SCF with keeping the same average distortion.

The stego-code $\mathrm{SC}(1/2, 1, 1)$ can reach the rate-distortion bound of LSB embedding at the maximum embedding rate 1 for LSB embedding. The first code in the modified SCF of $\mathrm{SC}(1/2, 1, 1)$ achieves the rate-distortion bound of ± 1 embedding at embedding rate 1.5. Note that the maximum embedding rate achieved by modified SCFs is just 1.5 which is smaller than the maximum embedding rate, $\log_2 3 \approx 1.585$, of the ± 1 embedding.

Performance comparisons have been made between the modified SCFs and the previous methods in terms of the metric *embedding rate-embedding efficiency*. The EMD method in [10] and Grid Coloring method in [11] can provide the same family of schemes, embedding $\log_2(2n + 1)$ bits into n host symbols with $2n/(2n + 1)$ changes on average, which includes the ternary Hamming stego-codes. The method in [14] applied binary covering codes to ± 1 embedding by extending the length of codes. The "binary Hamming +1" scheme in [14] can embed $k + 1$ bits into 2^k host symbols with $(2^{k+1} - 1)/2^{k+1}$ changes on average, which includes the LSB Matching Revisited method [15] as a special case. Fig. 3 shows that the modified SCF of $\mathrm{SC}(1/2, 1, 1)$ significantly exceeds the methods in [2], [10], [11], [14], and [15]. Moreover, performance of the modified SCFs of LDGM codes are very close to the upper bound (23). In other words, they provide near-optimal codes for ± 1 embedding.

V. Treble-Layered Scheme for ± 2 Embedding

In Section IV, additional messages are embedded into $\lfloor x/2 \rfloor \bmod 2$, which is the second LSB of gray-scale symbol x. Therefore messages are carried by LSB plane and the second LSB plane in the ± 1 embedding. In this section, we propose a treble-layered scheme for ± 2 embedding by exploiting the first three LSB planes of gray-scale symbols.

Because we have obtained binary stego-codes approaching rate-distortion bound for various embedding rates in Section III, for simplicity in the discussion, we assume the binary stego-codes used in this section are optimal, i.e., for average distortion Δ, $0 < \Delta \leq 0.5$, we can achieve an embedding rate $H(\Delta)$.

For ± 2 embedding, the set of possible modifications $\mathcal{Z} = \{-2, -1, 0, +1, +2\}$. Assume the probability distribution over $\mathcal{Z}$ is p_z, $z \in \mathcal{Z}$. Let $p_1 = p_{-1} + p_{+1}$ be the probability of changes with an amplitude one, and $p_2 = p_{-2} + p_{+2}$ be the probability of changing two. Thus $p_0 + p_1 + p_2 = 1$. Assume the cover-object consists of N gray-scale symbols $x_1, \ldots, x_N$. The embedding process includes the following three steps.

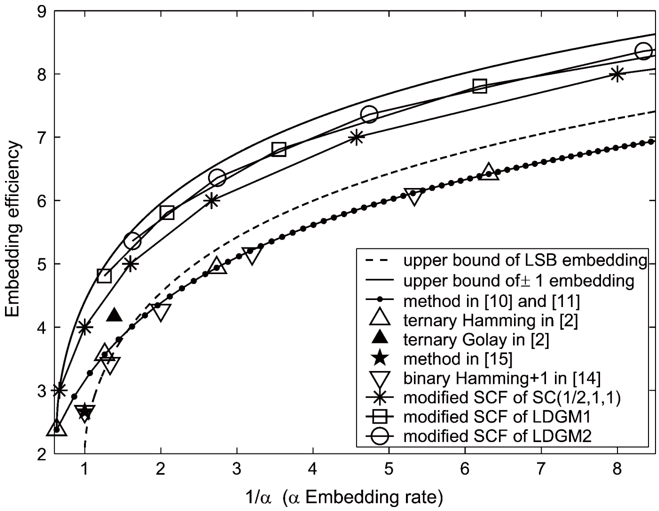

Fig. 3. Performance comparisons among the modified SCFs and the methods described in [2], [10], [11], [14], and [15].

First, we use binary stego-codes to embed messages in the LSB plane by ± 1. The changing probability is p_1, which is also the average distortion of the LSB embedding, so we can almost reach the embedding rate $H(p_1)$.

Next, we embed messages in the second LSB layer with binary stego-codes. All the second LSBs are allowed to be modified in the following manner: p_1 fraction of them can be modified by ± 1 introduced in the first step, and the rest can be modified by ± 2. The change rate of the second LSB layer is $p_2/(1 - p_1)$ because we need to have $p_2 N$ changes with amplitude two when constrained to $(1 - p_1)$ fraction of the cover. Thus, the embedding rate is $H(p_2/(1 - p_1))$.

Finally, we embed messages in the third LSB plane with wet paper codes. Because $p_2 N$ bits in the second LSB plane need to be changed using ± 2, by choosing $+2$ or -2, we can freely control the third LSBs of the corresponding gray-scale symbols. Label these $p_2 N$ positions in the third LSB plane as dry positions and the other $(1 - p_2)N$ positions as wet positions. By wet paper coding, we can embed information with an embedding rate p_2.

Similar to the ± 1 embedding, some cover symbols may cause problems in the above scheme. If a gray value $x = 0$ while $x - 1$ is required according to the rules in the first and second steps, we should use $x + 3$ instead; If $x = 2^B - 1$ while $x + 1$ is needed, we use $x - 3$ instead. If $x = 0, 1, 2^B - 1$, or $2^B - 2$, only one modification direction in $x \pm 2$ is permitted in the second step, for which the third LSB of x will always be labeled as a wet position. These cases will introduce extra distortion, or decrease the embedding rate. Nevertheless, if they rarely occur, the effect on the overall performance can be neglected.

Combining the above three embedding steps, we get an embedding rate $\alpha = H(p_1) + H(p_2/(1 - p_1)) + p_2$ with average distortion $d = p_1 \times 1 + p_2 \times 2^2 = p_1 + 4p_2$. If constrain the average distortion to no more than Δ, the treble-layered scheme can achieve an embedding rate

$$\max_{\{(p_1,p_2):p_1+4p_2\le\Delta\}} H(p_1)+H\left(\frac{p_2}{1-p_1}\right)+p_2. \tag{28}$$

Let us find the distance between (28) and the rate-distortion bound (2). When $f=2$, (2) is equivalent to

$$\max_{\{p_z:(p_{-1}+p_{+1})+4(p_{-2}+p_{+2})\le\Delta\}} H(p_0,p_{-1},p_{+1},p_{-2},p_{+2}) \tag{29}$$

where $H(p_0,p_{-1},p_{+1},p_{-2},p_{+2})=-\sum_{z=-2}^{+2}p_z\log_2 p_z$.

To obtain an optimal solution of (29), consider for some $\delta>0$ the distribution $\{p_z^*, z\in\mathcal{Z}=\{-2,-1,0,+1,+2\}\}$

$$p_z^*=\frac{\exp\left(-\delta z^2\right)}{\beta} \tag{30}$$

having variance $\sum_{z=-2}^{+2}p_z^*z^2=\Delta$, where $\beta=\sum_{z=-2}^{+2}\exp(-\delta z^2)$. For any distribution $\{p_z, z\in\mathcal{Z}\}$ with variance $\sum_{z=-2}^{+2}p_z z^2\le\Delta$, we have

$$\begin{aligned}\sum_{z=-2}^{+2}p_z\ln\frac{1}{p_z^*}&=\sum_{z=-2}^{+2}p_z\ln\left(\beta\exp(\delta z^2)\right)\\&=\ln\beta+\delta\sum_{z=-2}^{+2}p_z z^2\\&\le\ln\beta+\delta\Delta.\end{aligned} \tag{31}$$

Note that the relative entropy $\sum_{z=-2}^{+2}p_z\ln(p_z/p_z^*)$ is nonnegative, therefore, $\sum_{z=-2}^{+2}p_z\ln(p_z^*/p_z)\le 0$ and the entropy

$$\sum_{z=-2}^{+2}p_z\ln\frac{1}{p_z}=\sum_{z=-2}^{+2}p_z\ln\frac{p_z^*}{p_z}+\sum_{z=-2}^{+2}p_z\ln\frac{1}{p_z^*}\le\ln\beta+\delta\Delta. \tag{32}$$

The equality holds only when $\{p_z, z\in\mathcal{Z}\}$ equal to $\{p_z^*, z\in\mathcal{Z}\}$, so $\{p_z^*, z\in\mathcal{Z}\}$ is an optimal distribution for (29).

Let

$$p_1^*=p_{+1}^*+p_{-1}^*,\quad p_2^*=p_{+2}^*+p_{-2}^*. \tag{33}$$

From (30), it is obvious that $p_{+1}^*=p_{-1}^*$ and $p_{+2}^*=p_{-2}^*$; therefore, $p_{+1}^*=p_{-1}^*=p_1^*/2$ and $p_{+2}^*=p_{-2}^*=p_2^*/2$. Thus the rate-distortion bound (29) can be rewritten as shown in (34) at the bottom of the page.

Taking $p_1=p_1^*$, $p_2=p_2^*$, and $p_0=p_0^*$ in the treble-layered scheme, we can achieve an embedding rate

$$H(p_1^*)+H\left(\frac{p_2^*}{1-p_1^*}\right)+p_2^* \tag{35}$$

with the same average distortion $\Delta=p_1^*+4p_2^*$. Therefore when using distribution $\{p_z^*, z\in\mathcal{Z}\}$, the distance between the treble-layered scheme and the rate-distortion bound (34) is

$$p_1^*\left[1-H\left(\frac{p_2^*}{1-p_1^*}\right)\right]. \tag{36}$$

When $1-p_1^*=2p_2^*$, (36) becomes zero, i.e., the treble-layered scheme reaches the upper bound. From (30) we can obtain distribution satisfying $1-p_1^*=2p_2^*$, and calculate the corresponding embedding rate $\alpha=2.27$ from (35). That implies that the treble-layered scheme is available for embedding rate $\alpha\in[0,2.27]$, which can not reach the maximum embedding rate, $\log_2 5\approx 2.322$, of the ±2 embedding.

Note that $\{p_z^*\}$ is not the optimal distribution for the treble-layered scheme. We have obtained a numerical solution of (28), with which the treble-layered scheme can perform somewhat better than with distribution $\{p_z^*, z\in\mathcal{Z}\}$ (see Fig. 4).

The performance comparison is also done by using *embedding rate-embedding efficiency*. Fig. 4 shows that, for small embedding rates, distance between the upper bound of ±1 and ±2 embedding is very small, but distance between the treble-layered scheme and the upper bound is large. Because ±2 embedding includes ±1 embedding and the upper bound of ±1 embedding can be approached by the modified SCFs for embedding rate $\alpha\le 1.5$, we propose the following combining scheme for ±2 embedding. For an embedding rate $\alpha\in[0,1.5]$, we only do ±1 changes by using the modified SCFs; for $\alpha\in(1.5,2.27]$, we use the treble-layered scheme. This way, we can realize near-optimal embedding in most cases. Since the treble-layered schemes using distribution $\{p_z^*, z\in\mathcal{Z}\}$ and the optimal distribution have close performance for $\alpha\in(1.5,2.27]$, we can use distribution $\{p_z^*, z\in\mathcal{Z}\}$ directly in the combining scheme.

VI. Conclusion

Information embedding methods have an increasingly wide range of applications, such as steganography, digital watermarking, and backward compatible communication systems. In this paper, we propose a new method for embedding data in

$$\begin{aligned}H(p_0^*,p_{-1}^*,p_{+1}^*,p_{-2}^*,p_{+2}^*)&=H\left(p_0^*,\frac{p_1^*}{2},\frac{p_1^*}{2},\frac{p_2^*}{2},\frac{p_2^*}{2}\right)\\&=H(p_0^*,p_1^*,p_2^*)+p_1^*+p_2^*\\&=H(p_1^*)+(1-p_1^*)H\left(\frac{p_2^*}{1-p_1^*}\right)+p_1^*+p_2^*\\&=H(p_1^*)+H\left(\frac{p_2^*}{1-p_1^*}\right)+p_2^*+p_1^*\left[1-H\left(\frac{p_2^*}{1-p_1^*}\right)\right].\end{aligned} \tag{34}$$

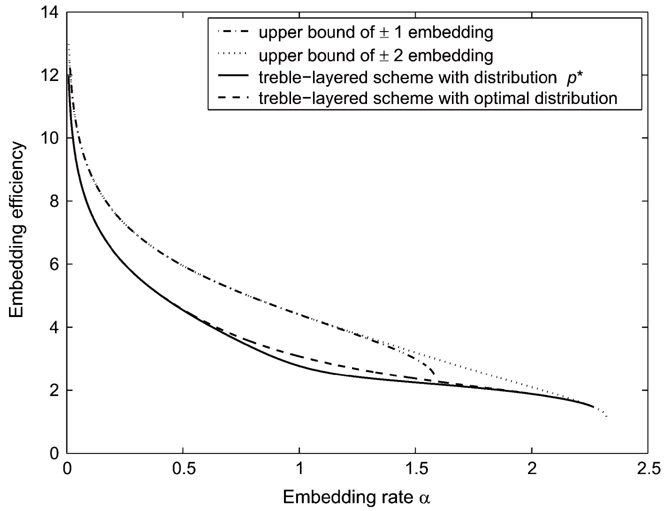

Fig. 4. Performance of the treble-layered scheme and the combining scheme.

gray-scale signals, which can generate a family of embedding codes from one covering code. By combining this method with random codes such as LDGM codes, we get a family of binary codes approaching the upper bound on embedding efficiency of LSB embedding at various embedding rates. Base on the binary codes, near-optimal schemes for ±1 and ±2 embedding are also proposed.

In steganographic applications, the message sender can always reduce changes to the cover signal by embedding fewer data, i.e., use low embedding rate to combat detection. However, advances in steganalysis have already made detecting LSB steganography of low embedding rates possible. For example, the method introduced in [16] can detect simple LSB replacement with an embedding rate as low as 2%. Since the embedding efficiency of simple LSB replacement is 2, detecting 2% embedding rate means detecting 1% of changes in the cover. The SCF of simple LSB replacement proposed in Section III-A can reach embedding efficiency 10 for the embedding rate of 2%, that is, the amount of changes is reduced to 0.2%. That is why SCFs can be used to resist steganalysis. Furthermore, it has been proved that ±1 embedding is more secure than LSB replacement because ±1 embedding can avoid the statistical imbalance caused by LSB replacement. As shown in Section IV, higher embedding efficiency for ±1 embedding can be obtained by using modified SCFs, which therefore will provide even better security.

On the other hand, the relations between the stego-codes and covering codes have been established in [1] and [3], and relations between stego-codes and error-correcting codes have been studied in [7] and [17]. Duality between data embedding and source coding is shown in [9] and [18]. For example, LDGM codes can be very close to the Shannon's limit, which is the very reason that schemes based on LDGM codes in [9] can almost achieve the bound on embedding efficiency. All these results imply that the method proposed in this paper is potentially applicable to other coding problems.

ACKNOWLEDGMENT

The authors would like to thank Professor J. Fridrich and Dr. T. Filler for providing the results of stego-coding based on LDGM codes.

REFERENCES

[1] F. Galand and G. Kabatiansky, "Information hiding by coverings," in *Proc. IEEE Inf. Theory Workshop*, 2003, pp. 151–154.

[2] F. Willems and M. Dijk, "Capacity and codes for embedding information in gray-scale signals," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1209–1214, Mar. 2005.

[3] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography," *LNCS Trans. Data Hiding and Multimed. Secur.*, vol. 4920, no. 3, pp. 1–22, 2008.

[4] R. Crandall, Some Notes on Steganography, Posted on Steganography Mailing List 1998 [Online]. Available: http://os.inf.tu-dresden.de/westfeld/crandall.pdf

[5] Y. C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1227–1231, Aug. 2002.

[6] D. Schönfeld and A. Winkler, "Embedding with syndrome coding based on BCH codes," in *Proc. ACM 8th Workshop on Multimed. Secur.*, 2006, pp. 214–223.

[7] C. Munuera, "Steganography and error-correcting codes," *Signal Process.*, vol. 87, pp. 1528–1533, 2007.

[8] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Trans. Inf. Secur. Forens.*, vol. 1, no. 3, pp. 390–394, Sep. 2006.

[9] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Proc. SPIE, Secur., Steganogr., Watermarking of Multimed. Contents IX*, San Jose, CA, 2007, vol. 6050, pp. 2–3.

[10] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, pp. 781–783, Nov. 2006.

[11] J. Fridrich and P. Lisoněk, "Grid coloring in steganography," *IEEE Trans. Inf. Theory*, vol. 53, pp. 1547–1549, Apr. 2007.

[12] A. Westfeld, "F5-a steganographic algorithm: High capacity despite better steganalysis," in *Proc. 4th Int. Workshop Inf. Hiding, 2001, LNCS 2137*, 2001, pp. 289–302.

[13] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Trans. Signal Process.*, vol. 53, pp. 3923–3935, Oct. 2005.

[14] W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," *IEEE Commun. Lett.*, vol. 11, pp. 680–682, Aug. 2007.

[15] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, pp. 285–287, May 2006.

[16] A. D. Ker, "A general framework for the structural steganalysis of LSB replacement," in *Proc. Int. Workshop 7th Inf. Hiding, 2005, LNCS 3727*, 2005, pp. 296–311.

[17] W. Zhang and S. Li, "A coding problem in steganography," *Designs, Codes and Cryptogr.*, vol. 46, no. 1, pp. 67–81, Jan. 2008.

[18] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1159–1180, May 2003.

Weiming Zhang received the M.S. and Ph.D. degrees in 2002 and 2005, respectively, from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China.

Currently, he is an Associate Professor with the School of Information Science and Technology, University of Science and Technology of China, Hefei. His research interests include information hiding and cryptography.

Xinpeng Zhang received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively.

Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a Professor. His research interests include information hiding, image processing, and digital forensics.

Shuozhong Wang received the B.S. degree in 1966 from Peking University, P.R. China, and the Ph.D. degree in 1982 from the University of Birmingham, England.

He was with the Institute of Acoustics, Chinese Academy of Sciences, from 1983 to 1985 as a Research Fellow. He joined the Shanghai University of Technology, China, in October 1985 as an Associate Professor. He is now a Professor with the School of Communication and Information Engineering, Shanghai University. He was a Visiting Associate Scientist with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, from March 1993 to August 1994. His research interests include acoustics, image processing, audio processing, and multimedia security.