A Double Layered "Plus-Minus One" Data Embedding Scheme

Weiming Zhang, Xinpeng Zhang, and Shuozhong Wang

***Abstract*—In image steganography, a pixel can carry secret bits by choosing adding/subtracting one to/from the gray value. This kind of "± 1 steganography" can hide a longer message than simple LSB embedding. We propose a double-layered embedding method for implementing "± 1 steganography," in which binary covering codes and wet paper codes are used to hide messages in the LSB plane and the second LSB plane, respectively. We show that this method can achieve the upper bound on the embedding efficiency of "± 1 steganography" when the employed binary covering codes reach the upper bound on that of LSB steganography. Applications using random and structured covering codes show that the new method outperforms previous ones and can approach the upper bound.**

***Index Terms*—Covering codes, embedding efficiency, steganography, wet paper codes.**

I. Introduction

STEGANOGRAPHY is used to convey secret messages under the cover of digital media such as images. Although only the most insignificant components are altered, many analytical techniques can reveal existence of the hidden message by detecting statistical difference between the cover and stego objects. The following two measures may be taken in developing steganographic schemes to combat steganalysis:

1) avoid conspicuous parts when embedding messages into the cover;
2) improve embedding efficiency, i.e., embed more information per modification to the cover data.

The first can be achieved by, for example, using the "wet paper codes" [1], [2]. In this letter, we consider the second measure, which can also be done based on various coding mechanisms such as those described in [3]–[9]. All these are essentially binary covering codes with syndrome coding [5], [6] applicable to LSB steganography. In LSB embedding, stego-coding methods are used in the LSB plane, in which adding 1 to a pixel value is equivalent to subtracting 1 from the pixel value for carrying one secret bit.

In fact, by choosing adding/subtracting one (± 1 for short), every pixel can carry not just one bit but $\log_2 3$ bits of information, that is, a ternary digit, with the pixel gray value modulo 3. In other words, ternary covering codes in "± 1 steganography" can produce better embedding efficiency than binary covering codes. To take this advantage, Willems *et al.* [10] propose to use the ternary Hamming and Golay codes. Zhang *et al.* [11] and Fridrich *et al.* [12] independently introduce the same method that includes ternary Hamming coding as a subset. Mielikainen [13] presents a different solution in which the choice of whether to add or subtract one to/from a pixel value depends both on the original gray values and a pair of two consecutive secret bits.

In the present letter, we propose a double-layered embedding method to further improve the embedding efficiency of "± 1 steganography," which embeds the secret message in the LSB plane and the second LSB plane by using binary covering codes and wet paper codes, respectively. We prove that this new method can achieve the upper bound on the embedding efficiency of "± 1 steganography" when the selected binary covering codes reach the upper bound on that of LSB steganography. Applications using random and structured covering codes also indicate that this double-layered embedding mechanism outperforms previous methods and can approach the upper bound on the embedding efficiency of "± 1 steganography."

II. Preliminaries

An (R, n, k) embedding scheme F consists of an embedding function and an extraction function. The sender can embed k bits into n pixels with at most R changes using the embedding function, and the receiver can extract the embedded message using the extraction function. We limit ourselves to the ± 1 embedding in which a pixel is modified by at most one and measure the distortion energy with the average number of embedding changes R_a that is the expected number of changes over uniform distributed messages. Define average distortion $D = R_a/n$, embedding rate $\alpha = k/n$, and embedding efficiency $e = k/R_a = \alpha/D$. Using syndrome coding for a covering code can lead to such an embedding scheme [5], [6]. For example, the (7,4) Hamming code means a (1, 7, 3) embedding scheme, which can embed 3 secret bits into 7 pixels by changing one LSB with probability 7/8, and therefore, $R_a = 7/8$, $D = 1/8$, $\alpha = 3/7$, and $e = 24/7$. To apply an (R, n, k) scheme to an image with N pixel, we can divide the image into N/n blocks each having n pixels, assuming N is an integer multiple of n.

The above-mentioned embedding schemes based on covering codes are used to improve the embedding efficiency. On the other hand, the wet paper codes as described in [1] and [2] are

Manuscript received April 25, 2007; revised May 29, 2007. This work was supported in part by the National Natural Science Foundation of China under Grants 60473022, 60372090, and 60502039, in part by the Shanghai Rising-Star Program under Grants 06QA14022, and in part by the Key Project of Shanghai Municipality for Basic Research under Grant 04JC14037. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. James E. Fowler.

W. Zhang is with the School of Communication and Information Engineering, Shanghai University, Shanghai 200076, China, and also with the Department of Information Research, Information Engineering Institute, Zhengzhou 450002, China (e-mail: nlxd_990@yahoo.com.cn).

X. Zhang and S. Wang are with the School of Communication and Information Engineering, Shanghai University, Shanghai 200076, China.

Digital Object Identifier 10.1109/LSP.2007.903255

1070-9908/$25.00 © 2007 IEEE

designed for the case in which the cover image has some constrained (wet) pixels. If, for example, k pixels are changeable (dry) and the other $N-k$ pixels are constrained (wet), a total of k bits can be embedded and received successfully using a wet paper code without sharing the knowledge about the positions of constraints between the sender and the receiver. We denote a wet paper coding scheme by W.

III. Proposed Method

We introduce the following double-layered embedding (DLE) method to fully exploit the information capacity of "±1 steganography." Suppose we want to embed a sequence of secret bits into a gray scale image with N pixels $(x_1,\ldots,x_N)$. For a pixel value x_i, denote its LSB by $L(x_i)$ and its second LSB by $S(x_i)$.

In the first layer embedding, select an embedding scheme F with embedding rate α, embedding efficiency e, and average distortion D, and embed αN bits $(m_1,\ldots,m_{\alpha N})$ into the LSB plane

$$(m_1,\ldots,m_{\alpha N}) = F[L(x_1),\ldots,L(x_N)]. \qquad (1)$$

Since the average distortion of F is D, we need, on average, to modify DN pixels to satisfy (1). Without loss of generality, assume both αN and DN are integers and exactly DN pixels need to be changed. In case $L(x_i)$ is changed, the pixel value x_i can either be increased or decreased by one. Note that, by choosing addition or subtraction, we have the control on the second LSB $S(x_i)$. Specifically, for an odd x_i, adding/subtracting one flips/keeps $S(x_i)$. If x_i is even, a contrary effect on $S(x_i)$ results.

By appropriately selecting addition or subtraction in the first layer embedding, we can freely alter the second LSBs at DN positions, i.e., exploit the second layer for embedding. The remaining $(1-D)N$ second LSBs are not changeable. Borrowing the terms of wet paper coding, we may say that these are DN dry positions and $(1-D)N$ wet positions. Note that, if the pixel value x_i is saturated, e.g., $x_i = 0$ or 255 in an 8-bit gray scale image, it can only be changed in one direction. In this case, the second LSB of x_i will always be labelled as a wet position. Nonetheless, the effect of this situation on the overall performance is neglected if saturated pixels are rare. Therefore, we assume that there are exactly DN dry positions and $(1-D)N$ wet positions after the first layer embedding. We can embed DN extra-bits $(m_{\alpha N+1},\ldots,m_{(\alpha+D)N})$ into the second LSB plane with a wet paper coding scheme W

$$(m_{\alpha N+1},\ldots,m_{(\alpha+D)N}) = W[S(x_1),\ldots,S(x_N)]. \qquad (2)$$

Thus, the embedding rate becomes $\alpha + D$, while the average distortion remains D since no additional modifications to the cover data are needed to satisfy (2). As a consequence, the embedding efficiency is increased by one, which is the ratio between embedding rate and average distortion. Performance of the described DLE method is stated in the following theorem.

Theorem 1: Let F be an embedding scheme with an embedding rate α, embedding efficiency e, and average distortion D. The DLE method using F has the embedding rate $\alpha + D$ and embedding efficiency $e+1$ and keeps the same average distortion D.

We now prove that the DLE method can exploit the information capacity of "±1 steganography" with the highest efficiency if F is the most efficient for LSB steganography.

LSB steganography has the following upper bound [7] on the embedding efficiency e with respect to a given embedding rate α:

$$e(\alpha) \le \frac{\alpha}{H^{-1}(\alpha)}, \quad 0 \le \alpha \le 1 \qquad (3)$$

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. In [10], Willems *et al.* give the upper bound on the embedding rate of "±1 steganography" subject to the constraint of an average distortion D

$$C(D) = \begin{cases} G(D), & D \le \frac{2}{3} \\ \log_2 3, & D > \frac{2}{3} \end{cases} \qquad (4)$$

where $G(D) = H(D) + D$. To evaluate the embedding efficiency, we rewrite (4) as an upper bound on the embedding efficiency e depending on a given embedding rate α

$$e(\alpha) \le \frac{\alpha}{G^{-1}(\alpha)}, \quad 0 \le \alpha \le \log_2 3 \qquad (5)$$

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

Summarizing these results, we have the following theorem.

Theorem 2: If an embedding scheme F reaches the upper bound (3), the DLE method using F achieves the upper bound (5).

Proof: Assume that the embedding rate of F is α. Since F can achieve the bound (3), its embedding efficiency is $\alpha/H^{-1}(\alpha)$. Average distortion of F is $H^{-1}(\alpha)$ because embedding efficiency is the ratio between the embedding rate and average distortion. According to Theorem 1, the average distortion of DLE using F is also $H^{-1}(\alpha)$, and the embedding rate is $\alpha + H^{-1}(\alpha)$. Therefore, its embedding efficiency is

$$e = \frac{\alpha + H^{-1}(\alpha)}{H^{-1}(\alpha)}.$$

Moreover, because $G^{-1}(\alpha + H^{-1}(\alpha)) = H^{-1}(\alpha)$, the DLE with F achieves the upper bound (5).

Theorem 2 establishes that the DLE is optimal for "±1 steganography" provided the binary embedding scheme used is optimal for LSB steganography. For instance, the plain LSB embedding scheme inserts one secret bit into each host pixel and needs to modify on average half of them. It has an embedding rate 1 and embedding efficiency 2, which is a trivial case achieving the bound (3). By Theorem 2, employing the plain LSB embedding scheme in the DLE can achieve the bound (5) with an embedding rate 1.5 and embedding efficiency 3.

Moreover, since binary random linear codes achieve the bound (3) asymptotically [5], [7], Theorem 2 leads to the following theorem.

Theorem 3: DLE methods using binary random linear codes can asymptotically achieve the bound (5).

A drawback of random codes is the unavailability of fast algorithm for encoding. However, Fridrich [7] provides a feasible embedding method with random codes for large embedding rates with $\alpha \to 1$. In [7], a random parity check matrix in a systematic form $\mathbf{H}_{(n-k)\times n} = \mathbf{I}_{n-k} \times \mathbf{D}$ is used for syndrome

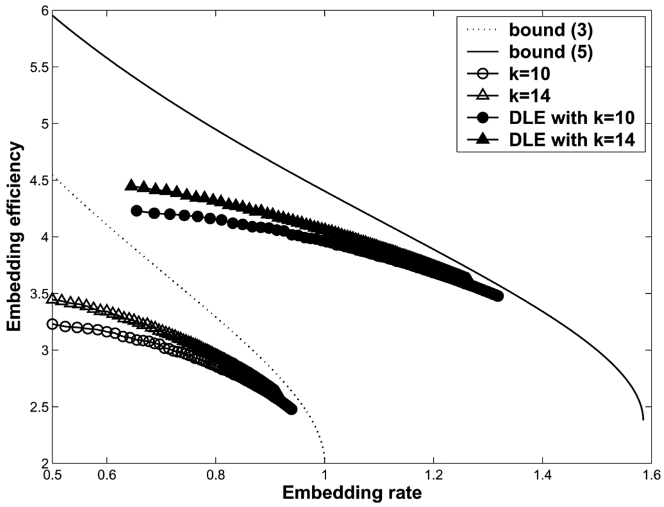

Fig. 1. Performance comparisons between random linear codes and the corresponding DLE methods for $k = 10$ and $k = 4$ with $n \leq 165$.

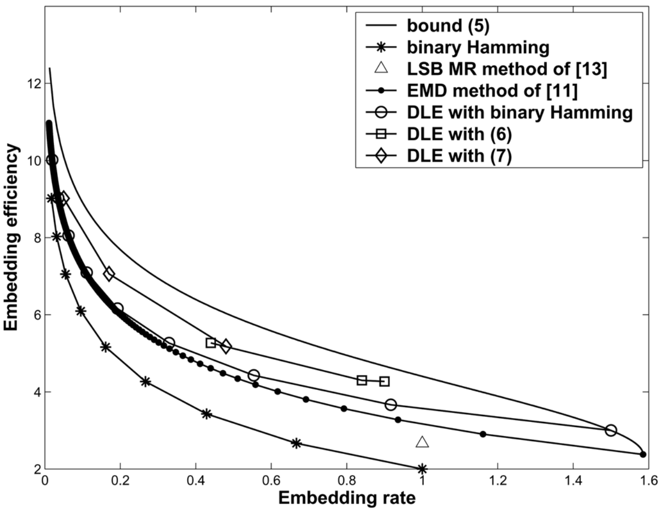

Fig. 2. Performance comparisons between the binary Hamming coding, the LSB MR method of [13], the EMD method of [11], and the DLE method using (6), (7), and binary Hamming codes.

coding, where $\mathbf{I}_{n-k}$ is an $(n-k) \times (n-k)$ identity matrix, and only the sub-matrix $\mathbf{D}$ is randomly generated. $\mathbf{H}_{(n-k)\times n}$ can embed $n-k$ secret bits into n pixels with a computation load $O(n2^k)$. The code dimension k should be small to keep low complexity. In other words, the embedding rate $\alpha = (n-k)/n$ must be large enough.

Fig. 1 illustrates the performances of random linear codes and the corresponding DLE methods for $k = 10$ and $k = 14$ with $n \leq 165$. It is observed that, by increasing k and n, the embedding efficiency of random linear codes becomes close to the bound (3) and the corresponding embedding efficiency of DLE methods close to the bound (5), justifying Theorem 3.

Theorem 2 also implies that we only need to search for good binary covering codes rather than ternary ones to efficiently use the information capacity of "±1 steganography." There are many efficient binary covering codes suitable for steganographic applications such as those described in [3]–[9], which can be employed in this DLE method. Another advantage of this new method over ternary coding [10] and the methods in [11] and [12] is that it can embed binary messages directly, while those in [10]–[12] require conversion of the messages to ternary or d-ary digits. In Section IV, we shall show that the proposed method can outperform previous ones.

IV. Applications Using Structured Covering Codes

The well-known matrix coding used in [4] is essentially an application of the binary Hamming code. It can embed k secret bits into $2^k - 1$ pixels by changing only one LSB with probability $(2^k-1)/2^k$, therefore incurring average distortion $1/2^k$ with an embedding rate $k/(2^k-1)$ and embedding efficiency $k2^k/(2^k-1)$. According to Theorem 1, the corresponding embedding rate and embedding efficiency in DLE are $k/(2^k-1) + 1/2^k$ and $k2^k/(2^k-1)+1$, respectively. When $k = 1$, it is just the case of DLE using the plain LSB embedding as described in the preceding section. Fig. 2 shows that the embedding rate and embedding efficiency of binary Hamming codes are both significantly improved by using the DLE mechanism that also outperforms the LSB MR method in [13].

Other structured binary covering codes, such as those discussed in [3]–[9], can also be used in the DLE method for constructing more efficient schemes. For example, the following are a family of embedding schemes presented in [6]:

$$(3,31,12) \quad (3,127,18) \quad (3,511,24) \tag{6}$$

and a set of BCH codes proposed in [8]

$$[31,11] \quad [35,11] \quad [45,29]. \tag{7}$$

With the method of [8], we estimate the average number of embedding changes R_a for the (3, 31, 12) embedding scheme by

$$\frac{C_{31}^1}{2^{12}} + \frac{C_{31}^2}{2^{12}} \times 2 + \left(1 - \frac{C_{31}^0 + C_{31}^1 + C_{31}^2}{2^{12}}\right) \times 3 = 2.97. \tag{8}$$

Therefore, its average distortion $D = 2.97/31 = 0.10$, embedding rate $\alpha = 12/31 = 0.48$, and embedding efficiency $e = 12/2.97 = 4.18$. The parameters of the other two schemes in (6) and the BCH codes in (7) can also be estimated in a similar manner [8]. With these parameters and Theorem 1, we can obtain the performances of DLE methods using (6) and (7).

We now make performance comparisons between the DLE using (6), (7) and binary Hamming codes, the ternary Hamming coding of [10], the EMD method of [11], and the Rainbow Coloring method of [12]. Both the EMD and Rainbow Coloring methods provide the same family of schemes, which can embed $\log_2(2d+1)$ bits of messages into d pixels with $2d/(2d+1)$ changes on average. Therefore, the corresponding embedding rate and embedding efficiency are as follows:

$$\alpha_d = \frac{\log_2(2d+1)}{d} \quad e_d = \frac{(2d+1)\log_2(2d+1)}{2d} \tag{9}$$

where d is a positive integer. Note that, when $d = (3^r-1)/2$, $r \geq 1$, (9) just yields the performance parameters of ternary Hamming coding of [10]. Hence, we only need to compare the DLE method with the EMD method of [11]. The comparison results in Fig. 2 show that the DLE with binary Hamming codes is slightly more efficient than the EMD method, while the DLE with (6) and (7) significantly exceed the EMD and are close to the bound (5). Nonetheless, advantage of the DLE over the EMD is most pronounced for large payloads but negligible for small payloads because the EMD also approaches the upper bound when the payload is small.

V. Discussions

In this letter, we propose a DLE mechanism and prove that, if the binary coding method for the LSB plane embedding is optimal, the corresponding DLE method is optimal for “± 1 steganography.” Fridrich *et al.* [14] recently proposed a new stego-coding method based on the low-density generator matrices (LDGM) codes with performance very closed to the bound (3). According to Theorem 2, application of this method to the DLE will lead to performance approaching the bound (5). Further studies on combining DLE method with LDGM codes will be carried out.

Moreover, the DLE method can also be used to improve the embedding efficiency of wet paper codes with a “double wet paper coding” scheme, i.e., applying the wet paper coding to DLE in both the first layer and the second layer embedding. In [2], the random linear codes are adopted to increase embedding efficiency of wet paper codes, called “block minimal method.” Obviously, applying the block minimal method in DLE will yield more efficient wet paper codes.

References

[1] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, “Writing on wet paper,” *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3923–3935, Oct. 2005.

[2] J. Fridrich, M. Goljan, and D. Soukal, “Efficient wet paper codes,” in *Proc. 7th Int. Workshop Information Hiding, LNCS 3727*, 2005, pp. 204–218.

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

[4] A. Westfeld, “F5: A steganographic algorithm,” in *Proc. 4th Int. Workshop Information Hiding, LNCS 2137*, 2001, pp. 289–302.

[5] F. Galand and G. Kabatiansky, “Information hiding by coverings,” in *Proc. IEEE Information Theory Workshop*, 2004, pp. 151–154.

[6] J. Bierbrauer and J. Fridrich, Constructing Good Covering Codes for Applications in Steganography, 2006. [Online]. Available: http://www.math.mtu.edu/~jbierbra/.

[7] J. Fridrich and D. Soukal, “Matrix embedding for large payloads,” *IEEE Trans. Inf. Foren. Sec.*, vol. 1, no. 3, pp. 390–394, Sep. 2006.

[8] D. Schönfeld and A. Winkler, “Embedding with syndrome coding based on BCH codes,” in *Proc. 8th ACM Workshop Multimedia and Security*, 2006, pp. 214–223.

[9] 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.

[10] F. Willems and M. Dijk, “Capacity and codes for embedding information in gray-scale signals,” *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1209–1214, Mar. 2005.

[11] X. Zhang and S. Wang, “Efficient steganographic embedding by exploiting modification direction,” *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.

[12] J. Fridrich and P. Lisoněk, “Grid coloring in steganography,” *IEEE Trans. Information. Theory*, vol. 53, no. 4, pp. 1547–1549, Apr. 2007.

[13] J. Mielikainen, “LSB matching revisited,” *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[14] J. Fridrich and T. Filler, “Practical methods for minimizing embedding impact in steganography,” in *Proc. SPIE Electronic Imaging*, Jan. 2007, vol. 6050.