ICIC Express Letters
Part B: Applications
Volume **9**, Number **7**, July **2018**

ICIC International ©2018 ISSN 2185-2766
pp. **707–713**

DEVELOPMENT OF LOW-COMPLEXITY MATRIX EMBEDDING WITH AN EFFICIENT ITERATIVE STRATEGY

Hsi-Yuan Chang[1,2], Jyun-Jie Wang[3], Chi-Yuan Lin[3,*] and Chin-Hsing Chen[1,2]

[1]Institute of Computer and Communication Engineering
[2]Department of Electrical Engineering
National Cheng Kung University
No. 1, University Road, Tainan City 701, Taiwan
hsiyuan2017@gmail.com; chench@eembox.ncku.edu.tw

[3]Department of Computer Science and Information Engineering
National Chin-Yi University of Technology
No. 57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan
jjwang@ncut.edu.tw; *Corresponding author: chiyuan@ncut.edu.tw

Received November 2017; accepted February 2018

Abstract. *A novel suboptimal embedding algorithm for binary logos based on a weight approach embedding (WAE) is proposed. An optimal embedding algorithm, developed on the basis of the maximal likelihood algorithm, is aimed at locating the coset leader as an approach to the minimum embedding distortion. By contrast, there is no need to locate the coset leader; instead, a target vector is required. The corresponding weight of the target vector is close to that of the coset leader; the target vector's weight is discovered in an efficiently iterative manner. In case of a highest operating complexity, in contrast to that of the optimal maximal likelihood (ML) algorithm, the operating complexity of the suboptimal WAE is linearly proportional to the number of code dimensions, because a full search (which would be necessary in an ML algorithm) is not required. The lower embedding efficiency of the proposed algorithm is superior to those of algorithms proposed in previous works, when the logo message length is small.*
Keywords: Embedding algorithm, Maximal likelihood algorithm, Operation complexity

1. **Introduction.** Because of the numerous Internet and public communication network applications, steganography has been attracting increasing interest and has played crucial role in multimedia technology [1]. The encoding process of syndrome codes, also known as matrix embedding (ME) codes, is to embed a logo into a different image, such as a photograph, music, video, or text. Crandall [2] and Bierbrauer [3] have proposed a scheme called ME; in ME, matrices are derived from covering codes [3] and this approach a high embedding efficiency. Several researchers have implemented steganographic scheme using the suboptimal embedding algorithm [4-6]. However, as proposed by [6], the binary embedding algorithm is of an embedding capacity that is dependent on the size of the partitioned cover sequence, into which some number of 1s can be embedded; a maximum of 2 bits can be altered. As Li et al. [4] proposed in 2007, the tree-based parity check (TBPC) is a binary data embedding algorithm with an embedding capacity of up to $1 - pt(N)/0.5$, where N is an integer larger than 2. The TBPC provides a high embedding capacity and a fast computational time, up to approximately half the cover sequence length, with a maximal embedding distortion of up to 0.36 change/bit. Li et al. proposed a second version of the binary image-embedding algorithm, called the block-overlapping parity check (BOPC) [5], in 2007. The BOPC algorithm uses the properties of block-overlapping parity check to reduce toggling required in [5]. These methods [4-6]

DOI: 10.24507/icicelb.09.07.707

are highly efficient and fast for steganography. They utilize a simple matrix strategy to further improve the computational complexity of embedding. [7] proposed a method for increasing the embedding speed of matrix embedding by extending the matrix with some referential columns. Compared with the original matrix embedding, the proposed method can exponentially reduce the computational complexity for an equal increment of embedding efficiency. However, in most cases, such as linear block codes of sufficiently large dimension, the main common disadvantage is that maximum likelihood decoding cannot be performed because of the high complexity required in matrix embedding codes of long length. The researchers in [8] proposed an improved embedding method based on BCH codes. The complexity of [8] is linear, whereas that of optimal embedding with maximum likelihood decoding is exponential. The researchers in [9] offered a novel family of embedding codes, generated by the systematic convolutional codes. This family of methods, along with Vitrebi decoding, has high embedding efficiency in targets of sufficiently long length. For security, [10] concealed a large amount of information in a binary image by using a steganographic scheme, which uses a secret key and a weight matrix to increase security; the weight matrix increases the embedding rate, and an XOR operator reduces the time complexity. Another important secure steganographic method was proposed in [11]; it proposed a game-theoretic framework for examining adaptive steganography while taking the knowledge of the analysis into account. Recent developments have contributed toward achieving the application of multimedia communications. [12] devised a novel steganography algorithm that has a high capacity while still retaining the ability of adjusting the embedding distortion. A shifting strategy is explored to embed the secret data into a given 3-D model effectively. In [13], the algorithm of embedding a 2.4Kbps low-bit-rate Mixexcitation linear prediction (MELP) speech into G.729 coding speech was presented by adapting the techniques of covering code and the interleaving and [14] presented an algorithm based on a secret sharing scheme and an error-correcting code (ECC), which combines grey relational analysis (GRA) with a partition mode in video compression standard H.264/AVC. Authors in [15] proposed a framework for nonadditive distortion steganography by defining joint distortion on pixel blocks. Moreover, [16] proposed a novel low-complexity embedding algorithm that uses a modified majority-logic algorithm to decode RM codes, in which a message passing algorithm is performed on the highest order of information bits in the RM codes.

The current study focused on the ME method, in which the stego is a function of the logo and the cover to achieve excellent embedding efficiency with low complexity. This study proposes a steganographic scheme in which the toggle is found by using ME, attempting to attain a suboptimal toggle trade-off between embedding efficiency and computational complexity. By using an iterative method, weight approach embedding (WAE) adds a row vector of a generator matrix to a toggle object in an attempt to obtain a new toggle object where the weight is less than the old weight. Finally, we developed practical embedding algorithms by analyzing the trade-off, distortion, embedding efficiency and complexity.

The remainder of this paper is organized as follows. In Section 2, we review several elementary concepts from coding theory and introduce the optimal embedding algorithm. Section 3 provides a description of our major work for suboptimal embedding strategy. Section 4 presents experimental results and their discussion. Finally, Section 5 offers conclusions.

2. **Bound on Embedding Efficiency.** In this section, we focus on the coding theorem for the case of ME in a binary sequence. Binary data hiding refers to an issue where the average level of distortion d of embedding strategy can be determined by a binary linear embedding code (n, k) at a given embedding rate $R_e = (n-k)/n$. The lower bound of distortion $d_{\min}$ is thus bounded using the rate-distortion function. Coding theory is discussed here.

An introduction to embedding algorithms for linear codes is presented, as follows. For an embedding scheme using linear codes, an (n, k) linear code C at an embedding rate $R_e = (n-k)/n = m/n$. Under the assumption that a logo sequence $s \in \{0,1\}^m$ embedded into a cover sequence $u \in \{0,1\}^n$ by using the linear code C is transmitted to the receiver, the optimal stego sequence $l' = u - e_{opt}$, where e_{opt} is provided by an embedder (i.e., a stego l') modified from u and corresponding to the logo message s. This can be formulated as a rate-distortion problem. Assume that the linear code C at embedding rate R_e corresponds to an embedding average distortion $d = E[d(l', u)]/n = E[w(e_{opt})]/n$. The theoretically achievable bound is derived as $k/n \geq 1-h(d)$, where $h(d) = \delta \log_2(1/d)+(1-d)\log_2(1/(1-d))$ denotes a binary entropy function. Thus, we can obtain a bound of embedding rate as $h(d) \geq R_e$ and the minimal average distortion d is

$$d \geq h^{-1}(R_e), \tag{1}$$

where $0 \leq d \leq 0.5$ and $h^{-1}(\cdot)$ is the inverse binary entropy function. Without loss of generality, the embedding efficiency is defined as follows:

$$\eta = \frac{R_e}{d} = \frac{m}{D}, \tag{2}$$

where $D = nd$ is the average embedding distortion per block. By using (1), one can prove that (2) is an asymptotic upper bound as follows:

$$\eta \leq \frac{R_e}{h^{-1}(R_e)} = \eta_\delta.$$

This η_δ is the upper bound of embedding efficiency.

For an (n, k) linear code C, the embedding efficiency between the optimal (i.e., maximum likelihood decoding) and the suboptimal algorithms can be formalized as

$$\frac{m}{nh^{-1}(R_e)} \geq \frac{m}{D_{opt}} \geq \frac{m}{D_{sub}},$$

where D_{opt} and D_{sub} represent the average distortion estimated for each block in the optimal algorithm and the suboptimal algorithm, respectively. The aforementioned equation can be expressed in an alternative form as $\eta_\delta \geq \eta_{opt} \geq \eta_{sub}$. The intervals between the efficiency bound and the realization can be defined as

$$\varepsilon_{opt} = \eta_\delta - \eta_{opt}$$

and

$$\varepsilon_{sub} = \eta_\delta - \eta_{sub},$$

where η_{opt} and η_{sub} are the bound obtained using optimal embedding algorithm (maximum likelihood decoding) and the bound obtained using a suboptimal embedding algorithm, respectively. For an efficient linear code, the value ε should be sufficiently low.

3. **Suboptimal Embedding Algorithm: WAE Algorithm.** We present an efficient algorithm for performing binary hiding. As described in the preceding section, performing ML decoding corresponding to an arbitrarily large linear block code is unrealistic. Here, the coset leader is found in an alternative approach to the conventional ML decoding. A simple method is applied to locating a toggle sequence with low weight during the search for a coset leader sequence e_{opt}. This search is aimed at locating a sequence e_{sub}, and $w(e_{sub}) \geq w(e_{opt})$, in lieu of the optimal coset leader $w(e_{opt})$. Ensuring that $w(e_{sub})$ remains sufficiently close to $w(e_{opt})$ is required. Certainly, $w(e_{sub})$ is a sequence defined in C^x. Obtained by the addition of $w(e_{sub})$ to the cover sequence u, the stego sequence l' cannot be proven to be the optimal sequence.

We describe the framework for constructing a low-complexity embedding scheme using a generator matrix. Assume that an embedding scheme using linear codes, with an (n, k) linear code C being specified by the $k \times n$ generator matrix G at an embedding rate

$R_e = (n-k)/n = m/n$, can embed m bits of message sequences $s \in \{0,1\}^m$ into cover sequences $u \in \{0,1\}^n$ of length n. The following embedding scheme carries m bits of message s_l in a cover sequence u as

$$l_{opt} = \arg\min_{l \in C_l} d(u, l).$$

It is used to locate the optimal stego sequence $l_{opt} \in C^l$, which is the sequence closest to u; the minimal error between l_{opt} and u is represented as

$$\min_{l \in C^l} d(u, l) = \min_{x \in C^x} ||u - (x - c)|| = \min_{v \in \{0,1\}^k} ||u - (x - vG)||. \tag{3}$$

Equation (3) must be used to find vG such that $x' = x - vG$ is closest to u. In fact, in the case of a sufficiently large code finding x' using (3) is difficult because the complexity of finding the codeword increases as 2^k. Assume that there exists an efficient algorithm for determining x'; the suboptimal stego object l' is

$$l' = u - x' = u - x + vG = u - x + c. \tag{4}$$

Equation (4) can offer a low computational complexity in finding suboptimal stego. According to (4), a suboptimal algorithm (i.e., the WAE algorithm) is used for finding suboptimal stego. In the optimal embedding algorithm, $f(s_x)$ is decoded to gain the codeword c, and the coset leader sequence e is obtained by adding c to x (i.e., $x + c$). Here, $f(s_x)$ is not directly decoded through ML decoding; instead, the syndrome s_x of the toggle x is intended to remain invariant. The simplest means of achieving this is to add the codeword c, which is a subset of the linear code C, to the toggle x as x' (i.e., $x' = x + c$). Therefore, the weight of x' is altered through the codeword c, but x' still falls within the coset C^x. Although a total of 2^k codewords exist in the linear code C, testing them all would be unrealistic. Only k codewords are selected from 2^k codewords for testing, which form the row sequences g_i of a systematic generator matrix G_s as follows.

$$G_s = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}. \tag{5}$$

This row sequence set is defined as $\Gamma = \{g_1, g_2, \ldots, g_k\}$. For an arbitrary $g_i \in \Gamma$, the toggle syndrome s_x is expressed as

$$s_x = H(u + l) = Hx = Hx + Hg_i = H(x + g_i) = Hx', \tag{6}$$

where x, u, and l are the toggle sequence, cover sequence, and logo sequence, respectively. Although the syndrome s_x remains invariant with g_i added to x, the toggle sequence x, along with the corresponding weight does change. The distortion can be reduced if a modified toggle sequence x' of lower weight than the original toggle sequence x can be found. Eventually, the distortion can be improved through a small amount of weight variation. Certainly, the dimension of a candidate Γ can be extended, and k row sequences can be selected from G_s, or $\Gamma_N = \{g_i | i = 1, \ldots, N, N = \binom{k}{l}\}$ can be formed as a combination of two arbitrary sequences within G_s. However, the cost associated with an increment in N is a higher operational complexity. The case for $\binom{k}{l}$ is addressed in this paper. In this case, the modified toggle sequence $x' = x + g_i$ is gained through an appropriate weight variation of toggle x with the main goal of changing the weight of x' to approximate that of the coset leader e. Assume that $w(x) = \lambda$ and λ is a constant; the sequence x', approaching e, can be expressed as

$$x' = \arg\min_{g_i \in \Gamma} w(g_i + x), \tag{7}$$

where the sequence x' represents the sequence with the minimum weight after k rounds of testing. In the case that

$$w(e_{opt}) \leq w(x') \leq \lambda, \tag{8}$$

the sequence x' remains closer to the coset leader e_{opt} than the sequence x does. The aforementioned algorithm, designated as WAE, sufficiently reduce the toggle weight iteratively. Finally, (2) can be used to determine the embedding efficiency as $\eta = m/D$.

4. **Simulation Results.** The aforementioned algorithms were simulated in terms of operational time and embedding efficiency. The programs were developed in MATLAB and executed on a computer with an Intel E8300 2.83-GHz CPU and 2G DRAM. In these simulations, the cover and logo sequence were selected randomly.

1) Computational complexity
Figure 1 illustrates a comparison of various suboptimal algorithms in terms of CPU time required in a case involving 10^5 embedded bits. TBPC required the least amount of CPU time. The WAE algorithm based on a TBPC parity check matrix came in second place, and the BOPC algorithm came in third place. The algorithms can be arranged (in ascending order) as follows in terms of the CPU time required: [4] < WAE < [5] < ex_Random WAE < [6]. As shown in Figure 1, a long code provides improved embedding efficiency at the cost of requiring a greater amount of CPU time.

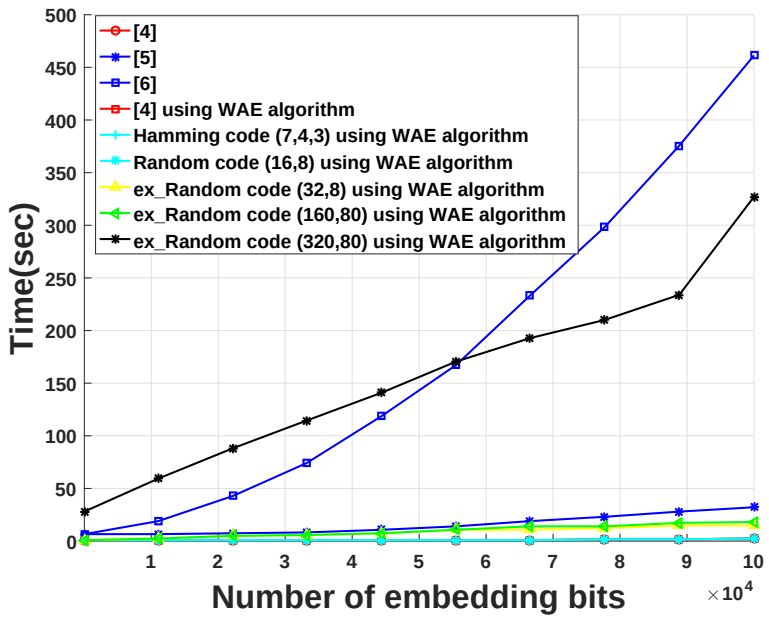

FIGURE 1. Time versus embedding capacity for different algorithms. (ex: expanded strategy)

2) Embedding efficiency
According to the preceding results, the WAE algorithm, compared with the optimal embedding algorithms, requires a lower operating complexity, but also has degraded embedding efficiency, namely $\eta = m/D$. As presented in Figure 2 and Table 1, the embedding efficiency η, corresponding to various systematic linear block codes, was compared between both the WAE and optimal embedding algorithms. When applied to an $(2^m - 1, m, 3)$ Hamming linear code, WAE exhibited an identical efficiency to that of the optimal embedding algorithms, because WAE requires only one iteration to successfully locate the toggle coset leader. The parameter ε_δ represents the difference between the bound and the optimal embedding efficiency limits in a case involving an

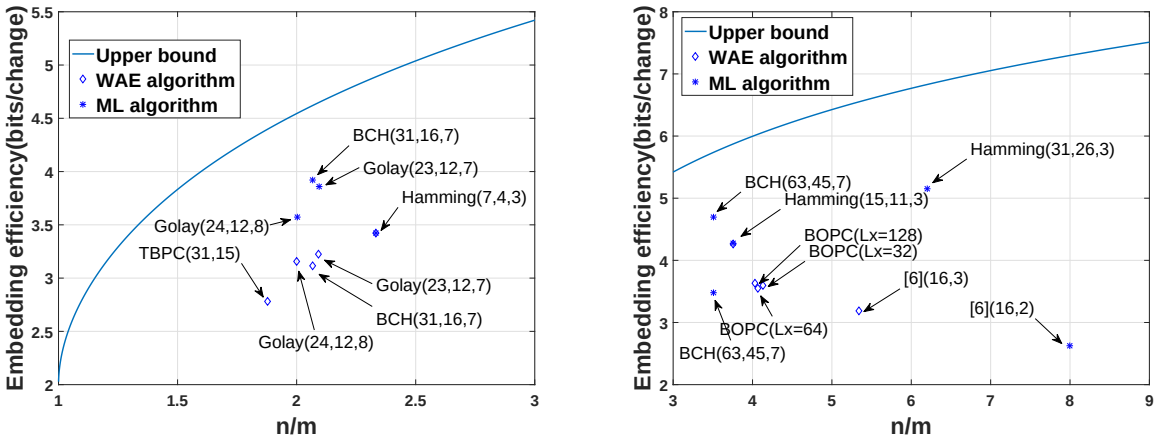

FIGURE 2. Embedding efficiency of various algorithms

TABLE 1. Performance comparisons of various embedding algorithms, including Hamming code, UWPC code, BCH code, and Golay code in WAE and optimal embedding algorithms ("W-" = using WAE algorithm, "/" = unachievable)

code (n, k)	rate (m/n)	n	ε_{opt}	ε_{sub}	time (sec)
[6] (16, 2)	0.125	16	/	4.616	14.313
[6] (64, 2)	0.031	64	/	6.708	44.434
[6] (16, 3)	0.187	16	/	3.327	7.964
[6] (64, 3)	0.046	64	/	5.443	24.035
W-Hamming (31, 5)	0.161	31	1.645	1.653	1.731
[5] (Lx = 32)	0.2424	4225	/	2.526	2.01
[5] (Lx = 64)	0.2461	16641	/	2.455	1.871
[5] (Lx = 128)	0.2481	66049	/	2.337	1.564
W-Random (16, 4)	0.25	16	/	2.803	0.48
W-Random_ex (160, 40)	0.25	160	/	2.693	4.45
W-Random_ex (15, 4)	0.2667	15	1.549	1.618	1.32
[4] (7, 4)	0.571	7	/	1.436	0.724
[4] (15, 8)	0.533	15	/	1.607	0.407
[4] (31, 16)	0.516	31	/	1.68	0.236
W-BCH (15, 8)	0.5333	15	1.388	1.366	0.657
W-Golay (24, 12)	0.5	24	0.962	1.487	0.87

invariant embedding rate R_e. A low value of ε_δ signifies that the embedding efficiency provided by the optimal embedding algorithm tends to the theoretical limit. Similarly, the parameter ε_{opt} denotes the difference between the embedding efficiencies of the suboptimal and optimal embedding algorithms. If the value of ε_{opt} is low, the embedding efficiency rendered by the suboptimal algorithm is close to that of the optimal embedding algorithm. Accordingly, through WAE, the operation time is as short as 1.38 sec at the cost of a degraded $\varepsilon_{opt} = 1.332$ and a 1.86% efficiency.

5. **Conclusions.** This study proposes a WAE suboptimal embedding algorithm, with low operating complexity, that is applicable to an arbitrary (n, k) linear block code with a parity check matrix. ML algorithm can be criticized for being extremely sensitive to the dimension k, because the operating complexity varies exponentially with k. For WAE, the complexity exhibits a linear dependence on k; therefore, WAE is making it applicable

to a linear block code of large dimension. WAE requires a complexity of only $O(\sigma k)$ when locating the toggle sequence, whereas the complexity of the ML algorithm is $O(2^k)$, an unacceptable figure for a large value of k. The considerably lower complexity in WAE is achieved at the cost of a small amount of embedding efficiency.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, Information hiding – A survey, *Proc. of IEEE*, vol.87, no.6, pp.1062-1078, 1999.

[2] R. Crandall, Some notes on steganography, *Steganography Mailing List*, http://os.inf.tu-dresden.de/westfeld/crandall.pdf, 1998.

[3] J. Bierbrauer, *Crandall's Problem*, 1998.

[4] R. Y. M. Li, O. C. Au, K. K. Lai, C. K. M. Yuk and S. Y. Lam, Data hiding with tree based parity check, *IEEE International Conference*, pp.635-638, 2007.

[5] R. Y. M. Li, O. C. Au, C. K. M. Yuk, S. K. Yip and S. Y. Lam, Halftone image data hiding with block-overlapping parity check, *Proc. of IEEE*, vol.2, pp.193-196, 2007.

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

[7] C. Wang, W. Zhang, J. Liu and N. Yu, Fast matrix embedding by matrix extending, *IEEE Trans. Inf. Theory*, vol.7, no.1, pp.346-350, 2012.

[8] R. Zhang, V. Sachnev, M. B. Botnan, H. J. Kim and J. Heo, An efficient embedder for BCH coding for steganography, *IEEE Trans. Inf. Theory*, vol.58, pp.7272-7279, 2012.

[9] J. J. Wang, H. Chen, C. Y. Lin and T. Y. Yang, An embedding strategy for large payload using convolutional embedding codes, *IEEE International Conference on ITS Telecommunications (ITST)*, pp.365-369, 2012.

[10] B. Feng, W. Lu and W. Sun, Secure binary image steganography based on minimizing the distortion on the texture, *IEEE Trans. Information Forensics & Security*, vol.10, pp.243-255, 2015.

[11] P. Schottle and R. Bohme, Game theory and adaptive steganography, *IEEE Trans. Information Forensics & Security*, vol.11, pp.760-773, 2016.

[12] N. Li, J. Hu, R. Sun, S. Wang and Z. Luo, A high-capacity 3D steganography algorithm with adjustable distortion, *IEEE Access*, vol.5, pp.24457-24466, 2017.

[13] Z. Wu, H. Cao and D. Li, An approach of steganography in G.729 bitstream based on matrix coding and interleaving, *Chinese Journal of Electronics*, vol.24, pp.157-165, 2015.

[14] Y. Zhang, M. Zhang, X. Yang, D. Guo and L. Liu, Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC, *Tsinghua Science and Technology*, vol.22, pp.198-209, 2017.

[15] W. Zhang, Z. Zhang, L. Zhang, H. Li and N. Yu, Decomposing joint distortion for adaptive steganography, *IEEE Trans. Circuits and Systems for Video Technology*, vol.27, pp.2274-2280, 2017.

[16] T. Yang and H. Chen, Matrix embedding in steganography with binary Reed-Muller codes, *IET Image Processing*, vol.11, no.7, pp.522-529, 2017.