Multimed Tools Appl (2014) 69:569–584
DOI 10.1007/s11042-012-1114-0

Data hiding by an improved exploiting modification direction

Cheonshik Kim

Published online: 15 May 2012

Abstract This paper represents an improved data hiding scheme, CIE, which uses a codebook to improve the Exploiting Modification Direction (EMD) embedding scheme. In our scheme, one secret $(2^{n+x}-1)$-*ary* digit is hidden in a group of pixels in an image as a modified secret digit. Our proposed scheme has an embedding rate $R = \log_2(2^{n+x}-1)/n$, which is greater than the rate of the EMD scheme, which is $R = \log_2(2n+1)/n$ for $n \geq 2$. Embedding rate R is the number of secret bits embedded in each cover pixel. Our experimental results demonstrate that our scheme is able to embed 3 times as many secret bits in an image compared to the original EMD embedding scheme when $n = 2$ and $x = 5$. Our scheme has low time complexity and achieves this higher embedding performance while retaining reasonable perceptual quality for the image. An experiment verifies these features of our proposed data hiding scheme.

Keywords Steganography · Data hiding · EMD · CIE · Steganalysis

1 Introduction

In recent decades, data hiding has interested in many researchers, where many approaches to information hiding have been proposed for different applications such as copyright protection [1], secure communication [24], and image authentication [16]. Steganography techniques [7–9, 17] are used for digital rights management, information protection, and secret hiding. Data hiding techniques provide a

C. Kim (✉)
Computer Science and Engineering Faculty, Sejong University, 98 Gunja-Dong, Gwangin-Gu, Seoul, 143-747, Republic of Korea
e-mail: mipsan@sejong.ac.kr, database.lab@gmail.com

challenge for digital forensic research, as data can easily move through the Internet unnoticed. Steganalysis [10, 20, 22] has been developed as a technique for finding concealed information, and has led researchers to search for improved schemes for concealing data. In data hiding, the crucial factors are the embedding capacity and invisibility. The embedding capacity of a data hiding scheme is the amount of secret data that can be embedded into an image, and the invisibility measures of how unnoticeable the information is to dishonest users when the image has been manipulated.

Steganography techniques for hiding information use two different schemes: the spatial domain and the frequency domain scheme [24]. In the first scheme, messages are hidden in the spatial domain of a host image by embedding the messages directly into the pixels of the host image. Generally, this scheme hides messages with an LSB replacement scheme that replaces the four least significant bits (LSBs) of each pixel [3, 14, 15]. In the frequency domain scheme [4], images are first transformed using the discrete cosine transform (DCT) [4], the discrete wavelet transform (DWT) [18], or a similar mechanism, after which the secret messages are combined with the coefficients in the frequency forms of the images to accomplish the embedding. The data hiding based on frequency domain can reasonably resist attacks such as compression, noise addition, and filtering. On the other hand, spatial domain-based schemes show higher capacity compared to that produced by a frequency-based scheme. In addition, they provide good image quality.

A few schemes have been proposed to provide high embedding capacity in an image. Chang et al. [5] proposed a steganographic scheme that produces a high embedding payload with a Hamming code. The embedding rate for a secret message is $R = \log_2(1.99)$, which is approximately 0.99 bits per pixel (bpp). Zhang et al. [25] proposed the Exploiting Modification Direction (EMD) steganographic scheme. This scheme uses a $(2n+1)$-*ary* notational system, where n denotes the size of each group. The embedding rate for a secret message is $R = (\log_2(2n+1))/n$, which is approximately 1.161 bpp when $n = 2$ and there are $2n$ possible ways of modification. The EMD scheme has the best embedding rate, when $n = 2$. This scheme produces a steganographic data hiding scheme providing high capacity, and good image quality. Researchers have proposed various schemes to improve the EMD scheme such as those discussed by Chao et al. [6], Lee et al. [12], Jung et al. [8], Wang et al. [21], and Kim et al. [11].

In this paper we herein propose an improved data hiding scheme that uses a codebook to improve the EMD scheme, and is therefore called the CIE (Codebook to Improve the EMD) embedding for short. We use a $(2^{n+x}-1)$-*ary* notational system in this scheme, which encodes a stream of bits with a cover pixel. The embedding rate of our scheme is 3 times greater than the EMD scheme when $n = 2$ and $x = 5$. Moreover, the quality of the stego image is very high and security is not a problem, because it is not easy to detect whether or not there is a hidden message in an image, since the human visual system is less sensitive to signals embedded in noisy image regions containing high spatial frequencies.

The rest of this paper is organized as follows. In Section 2, we review current and related work. In Section 3, we introduce our proposed embedding and extracting procedures for grayscale images. In Section 4, we compare the embedding rates and stego image qualities for CIE and previous schemes. Section 5 presents our conclusions.

2 Related works

2.1 Exploiting Modification Direction (EMD)

In the EMD scheme, all pixels in a cover image are pseudo-randomly permuted using a secret key to partition the pixels into a series of groups. A pixel group will be denoted as $(g_1, g_2, ..., g_n)$, where $n \geq 2$. In order to hide secret digits, digits for hiding need to be converted into a sequence of digits of a $(2n+1)$-*ary* notational system. A secret binary message can be divided into $L = \lfloor K \cdot \log_2(2n+1) \rfloor$ bits, and the decimal value of each part of the secret will be represented by K digits in the $(2n+1)$-*ary* notational system. In this scheme, only one pixel in each pixel group is incremented or decremented by 1. A vector $(g_1, g_2, ..., g_n)$ in n-dimensional space is represented by its f value, which is calculated using (1):

$$f(g_1, g_2, ..., g_n) = (g_1 \times 1 + g_2 \times 2 + ... + g_n \times n) \; mod \; (2n+1) \tag{1}$$

No modification of a pixel g is needed if a secret digit d equals the extraction function of the original pixel group. If the secret digit $d \neq f$, we must calculate $s = d - f \; mod \; (2n+1)$. If s is no more than n, the value of g_s is increased by 1; otherwise, the value of g_{2n+1-s} is decreased by 1. The merit of the EMD scheme is that it provides good stego image quality with a peak signal-to-noise ratio (PSNR) of more than 52 dB, because at most one cover pixel needs to be increased or decreased by 1 in each pixel group. Thus, the stego image has the advantage of resisting various steganalysis techniques. However, the EMD scheme has room for further improvement of its embedding capacity, because the embedding rate is $R = (\log_2(2n+1))/n$.

2.2 The scheme of Lee et al.

The scheme proposed by Lee et al. [12] keeps the $(16 - p_m)$ most significant bits (MSBs) of a pixel-pair (two pixel group) unchanged, and alters the p_m LSBs to create virtual modifications of m-dimensional pseudo-random vectors for carrying the secret data, where $p_m = (8 - PV_1) + (8 - PV_2)$; PV_1 is the most significant bits of the first cover pixels, PV_2 is the most significant bit of the second cover pixels and, $m = 2^{p_m - 1} - 1$. In this scheme the embedding capacity steadily increases as m increases while the dB value decreases as m increases significantly. The embedding rate for this scheme is $R = (\log_2(2m+1))/2$. This scheme uses a virtual hypercube (virtual grayscale pixels), which is structured by a random number and the EMD embedding algorithm is applied into the hypercube. The number of bits per pixel (bpp) embedded by this scheme is $\log_2(15)/2 = 1.9534$ when there are 2 groups of pixels and the 2 LSBs of the pixels are modified. The embedding rate of Lee et al.'s scheme is therefore better than that of the EMD scheme.

2.3 The scheme of Chao et al.

Chao et al.'s scheme [6] (called the diamond scheme) hides a secret message by adjusting the pixel values in pixel groups. In this scheme, the neighborhood set $D_k(i, j)$ of 4 pixel value x, y, i, and j is constructed by

$$D_k(i, j) = \{(x, h)||i - x| + |j - y| \leq k\}. \tag{2}$$

where k is a positive integer. The neighborhood set D_k contains all of the vectors (x, y) with the distance to vector(i, j) smaller than k. The number of elements of the set D_k, l, is computed by $l = 2k^2 + 2k + 1$. This scheme's bpp is $\log_2(2k^2 + 2k + 1)$. The diamond encoding scheme provides an easy way to produce a more acceptable result than that yielded by simple LSB substitution schemes. Chao et al.'s diamond encoding scheme uses a diamond function f to compute the diamond characteristic value (DCV) in embedding and extraction procedures. The DCV of two pixel values i and j is calculated by

$$f(i, j) = ((2k + 1) \times i + j) \; mod \; l \tag{3}$$

where l is the number of elements of the set D_k. From the definition of the DCV, it is easy to find that DCV of the vector (i, j).

2.4 The scheme of Jung et al.

Jung et al. [8] and Byun et al. [2] proposed a data hiding scheme where each secret digit in a $(2n + 1)$-ary notational system can be carried by one cover pixel. By using one pixel for cover data, the scheme achieves a capacity, $R = 2.321$ bpp, double that of the EMD scheme, $R = (\log_2(2n + 1))/n$. In Jung et al.'s scheme, the size of the group pixels does not change as n is increased. When n is increased, the PSNR of images is reduced. For each cover pixel value, g_i, the function value f is calculated by

$$f = (g_i + x) \; mod \; (2n + 1). \tag{4}$$

where $|x| \leq n$. A stego pixel value, g_i', is obtained by

$$g_i' = g_i + x. \tag{5}$$

where x satisfies the condition $f = d$, where d is an n-ary secret digit.

2.5 The scheme of Wang et al.

The data hiding capacity of Wang et al.'s scheme [21] is analogous to the EMD scheme. The binary secret message S is first converted into the secret digits in the 5-*ary* notational system. Wang et al.'s scheme embeds a $2K$ secret digit into a group of $(2K + 1)$ cover pixels in $X \in \{x_1, x_2, \ldots, x_{H \times W}\}$, X sized $H \times W$ at a time. The embedding rate of this scheme is $(4 \times K)/(2 \times K + 1) = 1.99$ bpp. When K equals 1, 2, and 3, this scheme conceals 2, 4, and 6 secret digits in the base-5 notational system, into the groups of 3, 5, and 7 cover pixels, respectively.

$$y = f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} (x_i \times i) \; mod \; (2n + 1). \tag{6}$$

According to (6), when $n = 2$ we have $M(x_1, x_2) = f(x_1, x_2) = (x_1 + 2 \times x_2)$ *mod* 5. This means that each cover pixel pair (x_j, x_{K+1}) can be mapped to an element (x_j, x_{K+1}) in the reference matrix M, where x_j and x_{K+1} play the roles of x_1 and x_2, respectively, in (6) for $n = 2$. From the located element $M(x_j, x_{K+1})$, vertically identify the set of candidate elements VCE as follows:

$$VCE = \{M(x_j - 2, x_{K+1}), M(x_j - 1, x_{K+1}), M(x_j, x_{K+1}), M(x_j + 1, x_{K+1}), M(x_j + 2, x_{K+1})\}.$$

2.6 The scheme of Kim et al.

Kim et al. [11] proposed a data hiding scheme that was based on codeword. The codeword needs to be a shared sender and receiver for communicating with each other. This concept improved the embedding rate as much as that observed by Wang et al.'s scheme. The embedding rate of this scheme shows a higher embedding capacity, i.e., $R = (\log_2(2^{n+2} - 1)/n$ and also a good quality image. However, this scheme shows a lower capacity compared to Lee et al.'s and Jung et al.'s schemes.

2.7 Steganalysis

Steganalysis, from an opponent's perspective, is an art of deterring covert communications while avoiding affecting the innocent communications. Its basic requirement is to determine accurately whether a secret message is hidden in the testing medium. Further requirements may include judging the type of the steganography, estimating the rough length of the message, or even extracting the hidden message. Ker's [10] experimental results showed that the HCF-COM-based steganalytic scheme performed quite well for color images, but it turned out to have very poor performance for gray-scale images. Ker found that the reason was due to the high variability of the cover images' HCF. Therefore, a down-sampled image by a factor of 2 in both dimensions and processed by a straightforward averaging filter was employed to calibrate the HCF-COM [13] of the full-sized image [10]. In view of the variation between the magnitudes of the HCF-COM of a cover image, denoted by $C(H[k])$, and that of the down-sampled image, denoted by $C(H'[k])$, the ratio $C(H[k]) = C(H'[k])$ is then proposed as a dimensionless discriminator. Another way of applying the HCF-COM is also introduced by computing the adjacency histogram. The HCF-COM detector based on $C(H[k]) = C(H'[k])$, and that based on the adjacency histogram are proven by extensive experimental data indicating that both of them produce reliable detectors for the LSB matching steganography in gray-scale images.

3 Our proposed CIE scheme

In this section, we present our proposed CIE scheme based on a $(2^{n+x} - 1)$-*ary* notational system for a group of pixels. CIE is a steganographic embedding scheme, where our scheme achieves a higher embedding efficiency and resonably good quality.

3.1 The embedding procedure

When a secret message is concealed in a series of pixel-groups in the EMD scheme, only one bit is increased or decreased in each pixel group. In this scheme, modifications in different directions are used to represent different secret data, leading to a higher embedding efficiency. In CIE, we utilize (7) to hide more secret bits than are hidden by the EMD scheme. In (7), a group of pixel values is represented as a vector $([g_1, g_2, \ldots, g_n])$. A vector $([g_1, g_2, \ldots, g_n])$ in an n-dimensional space is mapped to value f, which is computed by (7) as a weighted sum modulo $(2^{n+x} - 1)$. Each basis element 1 and 2 in Table 1 is used as an input to the extraction function f as weighted sum modulo $(2^{n+x} - 1)$ where $n = 2$ and $x = 3$. The parameter n is proportional to the number of pixels in a particular group; one expects a decrease in the embedding rate of an image when $n \geq 3$. Thus, CIE scheme is a maximum when $n = 2$. There is an inherent trade-off between embedding rate and image quality. The parameter x characterizes the trade-off, as increasing x increases the $(2^{n+x} - 1)$-*ary* notational system. Thus, it is proportional to the embedding rate of an image. When $n \geq 2$ and $x = 3$, it is formulated as $(n - 1) \times 6$. Table 1 is the codebook for a $(2^{n+3} - 1)$-*ary* system. In the case $n \geq 2$ and $x = 2$, it is formulated as $(n - 1) \times 3$ in (8). Table 2 is the codebook for a $(2^{n+2} - 1)$-*ary* system. The basis vector is chosen based on the value x.

The codebook can be constructed by basis vectors, therefore it is possible to increase or decrease the noise of an image by the combination of basis vectors. In EMD, the basis vector is [1, 2, ..., n], so it is possible to reduce noise in a stego image. However, the CIE scheme aspires toward a higher embedding rate and reasonable image quality. For this reason, we devised the basis vector as (8). In EMD, modulo $(2n + 1)$ is slowly increased, whereas modulo $(2^{n+x} - 1)$ of the CIE scheme is steeply increased when n is increased. Therefore, it is not appropriate to represent the value f with the basis vector of the EMD, because this causes the noises to increase. Thus, we chose a basis vector [1, 6], because it is possible to represent value f, and it yields reasonable noise levels.

Table 1 A basis vector [1, 6] when $n = 2$ and $x = 3$

Index	1	6	Index	1	6
0	0	0	16	−3	−2
1	1	0	17	−2	−2
2	2	0	18	−1	−2
3	3	0	19	0	−2
4	−2	1	20	1	−2
5	−1	1	21	−2	−2
6	0	1	22	−3	−1
7	1	1	23	−2	−1
8	2	1	24	−1	−1
9	3	1	25	0	−1
10	−2	2	26	1	−1
11	−1	2	27	2	−1
12	0	2	28	−3	0
13	1	2	29	−2	0
14	2	2	30	−1	0
15	3	2	–	–	–

Table 2 A basis vector [1, 3] when $n = 2$ and $x = 2$

Index	1	3	Index	1	3
0	0	0	8	−1	−2
1	1	0	9	0	−2
2	−1	1	10	−2	−1
3	0	1	11	−1	−1
4	1	1	12	0	−1
5	2	1	13	1	−1
6	0	2	14	−1	0
7	1	2	–	–	–

Equation (7) can be represented as an inner product between an image pixel value vector $([g_1, g_2, \ldots, g_n])$ and a basis vector $([1, 6, 12, ..., (n-1) \times 6])$, i.e., $f(g_1, g_2, \ldots, g_n) = ([g_1, g_2, \ldots, g_n] \cdot [1, 6, 12, ..., (n-1) \times 6])\ mod\ (2^{n+x} - 1)$ when $x \geq 3$. As d is a secret value, which are $d \in \{0, 1, ..., (2^{n+x} - 1) - 1\}$, it is possibly generated from the function of the random number generator of MATLAB. Equations (7)–(9) show the structure of the CIE scheme.

$$f(g_1, g_2, ..., g_n) = \left[\sum_{i=1}^{n} (g_i \cdot \pi_i) \right] mod\ (2^{n+x} - 1) \tag{7}$$

where

$$[\pi_1, \pi_2, ..., \pi_n] = \begin{cases} 1, 6, ..., (n-1) \times 6, & if\ \ (x \geq 3\ and\ n \geq 2) \\ 1, 3, ..., (n-1) \times 3, & if\ \ (1 \leq x \leq 2\ and\ n \geq 2) \end{cases} \tag{8}$$

The EMD and CIE are similar to a syndrome coding of Hamming code, so s is used for the syndrome value in the CIE scheme. The value is computed by (9). s is used in encoding secret digit d to make $d = f$, and it is defined with two cases: if $d \geq f$, s is $d - f$, and if $d < f$ and $n \geq 2$, s is $(2^{n+x} - 1) - |d - f|$.

$$s = \begin{cases} d - f & if\ \ (d \geq f) \\ (2^{n+x} - 1) - |d - f| & if\ \ (d < f\ and\ n \geq 2) \end{cases} \tag{9}$$

After computing the value s with (9), the modified pixel value vector g_i' can be computed by (10).

$$g_i' = g_i + codebook[s] \tag{10}$$

For the CIE embedding scheme, the codebook should be generated first. Since one more pixel value is changed compared to the EMD, which changes at most one pixel value, the numbers generated by the codebook should be larger than that of the EMD. The best choice of the codebook is to set $n = 2$ and $x = 3$. The basis vector for CIE can be derived as, at most, 4 pixel values changed. Consider a case where $n = 2$ and $x = 3$. The basis vector is given as [1, 6]. Note that the number of 0 can be generated by nullifying the basis vector (see Table 1) such as $0 = (0) \cdot 1 + (0) \cdot 6$. The number 1 is generated by setting the associated element 1 in the basis vector by 1 and also nullifying the basis vector element 2 such as $1 = (1) \cdot 1 + (0) \cdot 6$. In this way, numbers 2 and 3 can be generated. In order to generate number 4, setting the

element 1 in the basis vector by -2 and setting the second element by 1 and taking modulus 31 is based on (7). Thus, $(-2) \cdot 1 + (1) \cdot 6$ is 4. The number 16 generated by setting the associated element 1 in the basis vector by -3 and also setting the second element by -2 such as $-15 = (-3) \cdot 1 + (-2) \cdot 6$. Negative numbers are turned into positive numbers by the modulus operation,i.e., $(-15 \bmod 31) = 16$. It is certain that all numbers from 0 to 30 can be generated according to (7) by the combination of the basis elements with their associated coefficients. $(-2) \cdot 1 + (1) \cdot 6$ is not represented only by the number 4. It does not matter if it is calculated as $(4) \cdot 1 + (0) \cdot 6$. Therefore, it is possibly important to make an optimal basic vector, otherwise noise of the stego image can be increased. According to the theory of basis vectors ([1, 6]), a basis vector ([1, 6, 12]) can be constructed. Therefore, as a generalization, [1, 6, 12, 18, ..., $(n-1) \times 6$], where $n \geq 2$ and $x \geq 3$. Thus, it is possible to hide secret bits in an image by increasing or decreasing a maximum of 4 bits if there are more than two pixel groups. Table 1 is the codebook used for embedding and extracting secret messages with (7). The codebook is required for the CIE scheme. For this reason, both the sender and the receivers should have the codebook.

Example 1 We illustrate the embedding procedure with an example using a group of pixels with vector $g_i = [128, 130]$. In this case, $n = 2$ and $x = 3$. We can use Table 1 and (7)–(9). The variable to hide is d.

Step 1: First, use (7) to calculate the f value using the pixel pair g_i and the basis vector [1, 6]. $f = (128 \times 1 + 130 \times 6)\ mod\ 31$, that is, $f = 9$.

Step 2: To hide the decimal digit 4 in g_i, use (9) to calculate s. In this case, d is less than or equal to f, so $s = (2^{n+x} - 1) - |d - f|$, that is, $s = 26$.

Step 3: Look up the codebook and find the row for the number 26. The basis vector in this row is [1, -1], so g_i becomes [129, 129]. In the case of an overflow or underflow, $[g_1, g_2]$ has to be adjusted to the appropriate values. The rules are in (11) and (12):

$$\textbf{if } (g > 255), \quad g' = g - (2^{n+x} - 1) \tag{11}$$

$$\textbf{if } (g < 0), \quad g' = g + (2^{n+x} - 1) \tag{12}$$

3.2 The extraction procedure

The extraction procedure for recovering the message from a stego image is very simple, since you only have to know the f value for a group of pixels as calculated by (7).

Example 2 Consider the stego pixel group ([129, 129]) with $n = 2$ and $x = 3$. In Example 1, secret digit 4 was concealed in the pixel group. Before the secret digit was concealed in the pixel group, the original pixel group was ([128, 130]). It is possible to find the secret value as compute f using (7).

Step 1: Calculate f value with a pixel group ([129, 129]) and the associated basis vector [1 6]. In this case, $f = 1 \times 129 + 6 \times 129 = 903\ \%\ 31 = 4$.

Step 2: The receiver simply finds out the hidden value, i.e., it is $f = d = 4$.

4 Experimental results

The purpose of our CIE scheme is to embed secret digits into a cover image. Our scheme maintains secrecy as it will guarantee a higher embedding capacity and good image quality. We experimented with some grayscale images, and compared the results to the schemes of EMD [25], Lee et al.'s scheme [12], Chao et al.'s scheme [6], Jung et al.'s scheme [9], Wang et al.'s scheme [21], and Kim et al.'s scheme [11]. Our experiment used MATLAB. The rand() function of MATLAB was used to generate a pseudo-random number, which was rounded to a $(2^{n+x}-1)$-*ary* number to generate a payload. We then applied the previous scheme and CIE schemes to test images taken from the University of Southern California database [19]. Two main factors were used to evaluate the performance of our CIE data hiding scheme: visual quality, and the data hiding capacity of the stego image.

Our CIE scheme has a good embedding capacity rate, $R = \log_2(2^{n+x}-1)/n$, which is $\log_2(31)/2$ or 2.4771 when $n = 2$ and $x = 3$. In case $n = 2$ and $x = 5$, the embedding capacity rate of CIE is $\log_2(127)/2$ or $R = 3.4943$. The embedding rate of Kim et al.'s scheme is $R = \log_2(2^{n+2}-1)/n = 1.9534$ bpp, which is the maximum embedding rate, when $n = 2$. As can be seen in Fig. 1, the embedding rate is gradually decreased as the number of pixels is increased. Moreover, the embedding rate of CIE scheme is greater than 3 times that of the EMD scheme. The experiment (see Fig. 1) shows that the capacity of our CIE scheme is better than that of the EMD scheme. Furthermore, our CIE scheme is an improvement compared to Lee et al.'s scheme because it does not always flip four bits in a group of pixels. For instance, if $s = \{1–3, 28–30\}$, the second pixel is not changed when $n = 2$ and $x = 3$. Neither the CIE scheme nor the EMD scheme flips any bits in a group of pixels, when d is equal to f. In comparison, Lee et al.'s scheme always flips three bits when p_m is three. Thus, Lee et al.'s scheme is a not a complete scheme in the aspect of optimization of algorithm. In the case of less optimization, a statistical analysis attack is possible, in which case this scheme will not provide a good quality stego image. Therefore, Lee

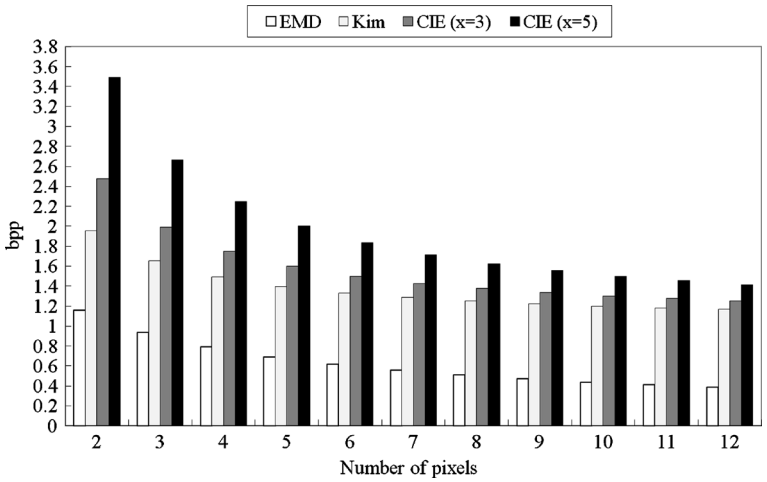


Fig. 1 Comparison of embedding capacity rates between CIE and EMD

et al.'s scheme does not conceal the secret message in a stego image in a way that protects it from steganographic techniques [7]. We used nine grayscale images, Lena, Baboon, Elaine, Airplane, Pepper, Goldhill, Barbara, Boat and Zelda, as cover-images in our experiment.

Each image is 512 × 512 pixels. The average PSNR value for our CIE scheme is about 43.9088 dB (see Table 3). The PSNR value for the EMD scheme averages around 52 dB, since the bpp embedding capacity is 1.16, and not many pixels are flipped. When the encoding scheme of EMD is used in the LSB plane of an image, adding 1 to a pixel is equivalent to subtracting 1 from the pixel to flip its LSB for carrying the secret message. Therefore, the CIE scheme provides lower image quality than the EMD scheme, because CIE is fully exploited to hide many secret messages. On the other hand, the human visual system cannot discriminate between the original image and the stego image, which has more than 35 dB of the original image quality. Thus, the CIE can resist steganalysis detection using a human visual system. For this reason, it is acceptable to use as a carrier for secret messages. Table 3 shows the comparisons of PSNR between the CIE scheme and previous schemes. The PSNR is the most widely used metric for measuring the distortion between the cover image and the stego image [6]. The PSNR of a grayscale image is defined as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{13}$$

The mean square error (MSE) for an $M \times N$ of gray-level image is defined as follows:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{k=1}^{M} \sum_{k=1}^{N} (x_{ij} - x'_{ij})^2 \tag{14}$$

Here x_{ij} denotes the original pixel value and x'_{ij} denotes the noisy pixel value.

As can be seen in Table 3, the embedding capacity of our the CIE scheme is 2.4771 bpp while that of other previous schemes is equal to or less than that of CIE scheme. Although CIE's embedding rate is the same as that of Lee et al.'s scheme, the PSNR of the CIE scheme shows a higher quality of an image. Jung et al.'s scheme show 45.1239 dB on average of the PSNR when bpp is equal to 2.32 bpp and this scheme presents good visual quality against capacity of an image, but the CIE scheme shows higher capacity under the same conditions, i.e., $n = 2$ and $x = 3$. Wang et al.'s scheme is a reasonably good scheme in the aspect of the high PSNR of an image. The PSNR of the CIE scheme is higher than that of Lee et al.'s scheme when embedding rate $(\log_2(31)/2) = 2.4771$ bpp. Chao et al.'s scheme shows a good PSNR in compared to that of Lee et al.'s scheme.

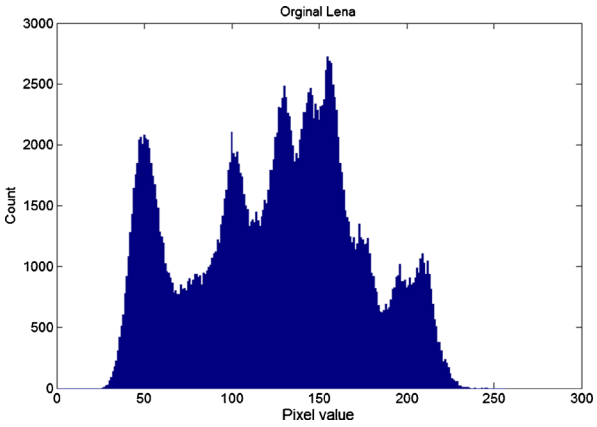
But most of apparent is that the CIE scheme is slightly better than the PSNR of Chao et al.'s scheme. Steganalysis [23] is a technique for detecting whether or not an image is a stego image. Steganalysis usually uses statistical tools to analyze the pixel value distribution in a suspicious image, for the purpose of cracking the secret messages. Therefore, if a stego image is created by significantly modifying the cover image, it is possible for steganalysis tools to detect the distortion in the stego image. For this reason, we analyzed the histogram of the original image, and compared the data to the stego images.

Figure 2 shows the histograms for the Lena image which were generated by Lee et al.'s scheme, and the CIE scheme. In Fig. 2, the stego image generated by Lee

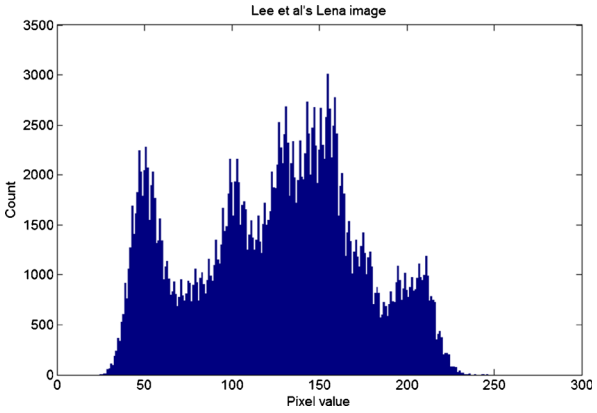
Table 3 Comparison of embedding capacity between previous schemes and our scheme

Name	CIE scheme	Chao et al.'s scheme	Lee et al.'s scheme		Kim et al.'s scheme	Jung et al.'s scheme	Wang et al.'s scheme
	$\log_2(31)/2 =$ 2.4771 (bpp)	$\log_2(2k^2+2k+1)/2 =$ 2.32 (bpp), $k=3$	$\log_2(15)/2 =$ 1.9534 (bpp)	$\log_2(31)/2 =$ 2.4771 (bpp)	$\log_2(15)/2 =$ 1.9534 (bpp)	$\log_2(2n+1)\times 2 =$ 2.32 (bpp), $n=2$	$(4\times K)/(2\times K+1) =$ 1.99 (bpp), $K=70$
Lena	43.9166 dB	41.3204 dB	44.3121 dB	37.4860 dB	46.8855 dB	45.1192 dB	45.1653 dB
Baboon	43.9106 dB	41.4178 dB	44.2792 dB	37.8913 dB	46.8884 dB	45.1240 dB	45.1564 dB
Tiffany	43.9284 dB	41.5460 dB	44.5052 dB	37.7621 dB	46.9051 dB	45.1488 dB	45.1698 dB
Airplane	43.9074 dB	41.4306 dB	44.4518 dB	37.4565 dB	46.8770 dB	45.1236 dB	45.1695 dB
Pepper	43.9079 dB	41.3547 dB	44.3180 dB	37.8214 dB	46.8869 dB	45.1225 dB	45.1642 dB
Goldhill	43.9079 dB	41.4132 dB	44.2786 dB	37.4447 dB	46.8846 dB	45.1164 dB	45.1537 dB
Barbara	43.8969 dB	41.4137 dB	44.2835 dB	37.6154 dB	46.8815 dB	45.1217 dB	45.1545 dB
Boat	43.9003 dB	41.3648 dB	44.3305 dB	37.7919 dB	46.8756 dB	45.1168 dB	45.1625 dB
Zelda	43.8950 dB	41.4569 dB	44.2220 dB	37.9218 dB	46.9004 dB	45.1224 dB	45.1658 dB
Average	43.9088 dB	41.4076 dB	44.3448 dB	37.6586 dB	46.8872 dB	45.1239 dB	45.1624 dB

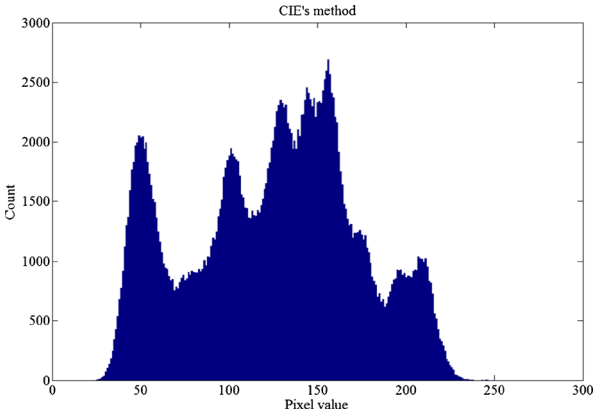
Fig. 2 The histogram analysis of the Lena stego image generated by two schemes



(a) The histogram of original Lena image



(b) The histogram of the stego image generated by Lee et al.'s scheme.



(c) The histogram of the stego image generated by the CIE scheme.

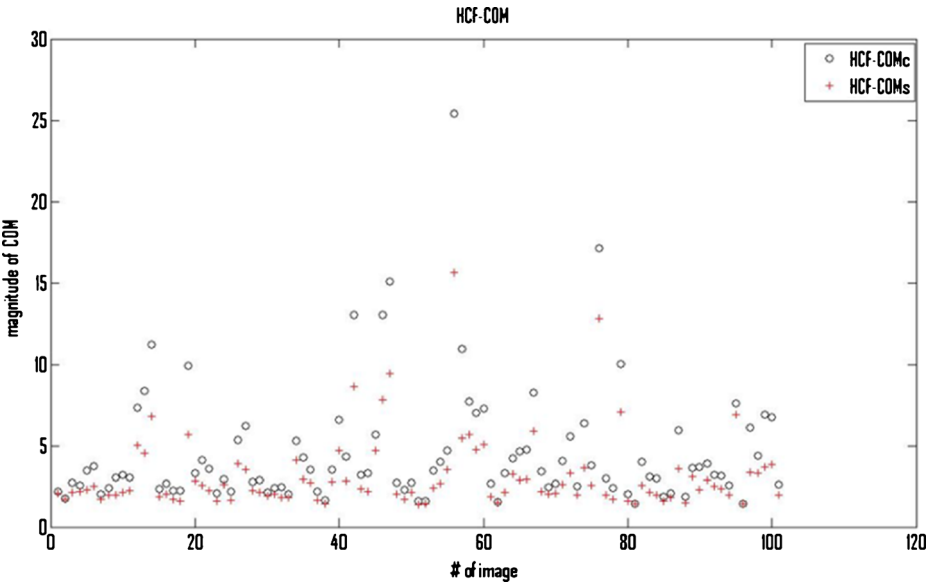


Fig. 3 Original Lena image (*circles*) and Stego image (*crosses*) after embedding for 200 images

et al.'s scheme causes an irregular modification. In this case, it is easily detected by the steganalysis technique. On the other hand, the stego image generated by the CIE scheme is more effective that of Lee et al.'s scheme, so the CIE scheme's secret hiding scheme has less possibility of being detected, than the scheme used by Lee et al.'s scheme.

Figure 3 shows the result based on the steganalysis [10], with a database of 200 grayscale images. The circle is the original grayscale Lena image, and crosses are

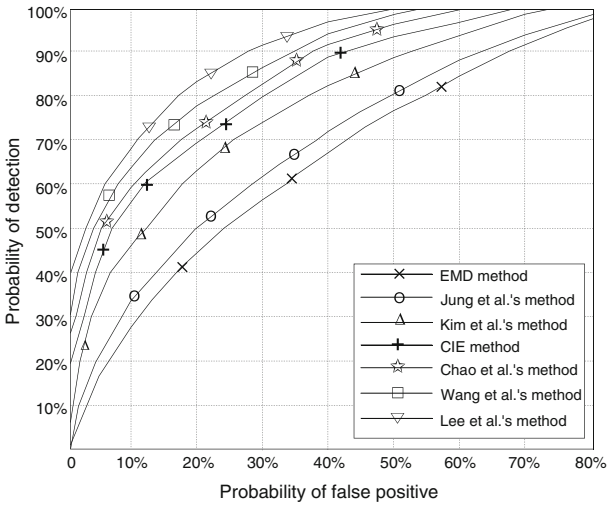


Fig. 4 ROC curves with a 100% payload

stego images. The crosses are located around the circles, so it is difficult to detect our proposed scheme from this steganalysis tool. Therefore, the CIE scheme is very strong against steganalysis. In Fig. 4, we provide receiver operating characteristic (ROC) curves, showing how false-positive and false-negative errors tradeoff as the detection threshold is varied, for stego images from cover images embedded with maximal-length random messages. For steganalysis, we use a calibrated adjacency HCF-COM detector. The curves show how the probabilities of detection and false positives vary as the detection threshold is adjusted.

As can be seen in Fig. 4, the EMD scheme shows a good performance against the HCF-COM detector, because this scheme can distribute payload fairly. The size of data hiding capacity in the EMD scheme, Kim et al.'s scheme, and the CIE scheme is in inverse proportion to n, which is a number of group pixel. Therefore, this scheme will be strong against HCF-COM as one increases the number of group pixels. As can be seen in Fig. 5, the stego images produced by the CIE scheme are of good quality,

Fig. 5 CIE scheme based stego image, $R = \log_2(31)/2$

so it is difficult to distinguish between the original cover image and proposed stego image.

5 Conclusions

Data hiding is necessary for digital rights management, information protection, and concealing secrets, because it is not easy to protect a secret message from hackers and attackers. Our CIE scheme proposes a $(2^{n+x}-1)$-*ary* number system for data hiding. We have shown herein that this scheme has a better embedding capacity than that proposed by EMD or of the schemes of Lee et al., Chao et al., Wang et al., and Kim et al. when exploiting one and two LSB planes of pixels in the cover image, respectively. Our proposed scheme presented lower quality compared to that of Jung et al.'s scheme so, one way to improve the quality of an image is to reduce capacity in an image. Therefore, we improved on the steganography in previous proposed schemes. In the near future, we will further optimize our CIE scheme against various Internet attacks such as steganalysis.

References

1. Bender W, Gruhl D, Mormoto N, Lu A (1996) Techniques for data hiding. IBM Syst J 35:313–336
2. Byung JY, Jung KH, Yoo KY (2008) Improved data hiding method by exploiting modification direction. In: International symposium on ubiquitous multimedia computing, UMC '08, pp 264–266
3. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37(3):469–474
4. Chang CC, Chen TS, Chung LZ (2002) A steganographic method based upon JPEG and quantization table modification. Inf Sci-Inf Comput Sci 141(1–2):123–138
5. Chang C-C, Kieu TD, Chou Y-C (2008) A high payload steganographic scheme based on (7, 4) Hamming code for digital images. In: International symposium on electronic commerce and security, Guangzhou, China, pp 16–21
6. Chao RM, Wu HC, Lee C-C, Chu Y-P (2009) A novel image data hiding scheme with diamond encoding. EURASIP J Inf Secur 2009:1–9
7. Fridrich J, Goljan M, Du R (2001) Detecting LSB steganography in color, and gray-scale images. IEEE Trans Multimedia 8:22–28
8. Jung KH, Yoo KY (2009) Improved exploiting modification direction method by modulus operation. Int J Signal Process Image Process Pattern 2(1):79–87
9. Katzenbeisser S, Petitcolis FAP (2003) Higher-order statistical steganalysis of palette images. In: Proceedings of the SPIE, electronic imaging, security, steganography, watermarking of multimedia contents V, Santa Clara, California, pp 178–190
10. Ker AD (2005) Steganalysis of LSB matching in grayscale images. IEEE Signal Process Lett 12(6):441–444
11. Kim C, Shin DK, Shin DI, Zhang X (2011) Improved steganographic embedding exploiting modification direction in multimedia communications. Commun Comput Inf Sci 186:130–138
12. Lee CF, Chang CC, Wang KH (2008) Improvement of EMD embedding method for large payloads by pixel segmentation strategy. Image Vis Comput 26(12):1670–1676
13. Li X, Zeng T, Yang B (2008) Detecting LSB matching by applying calibration technique for difference image. In: Proc. of the 10th ACM workshop on multimedia and security. ACM Press, New York, pp 133–138
14. Lin PL, Hsieh C-K, Huang P-W (2005) A hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recogn 38(12):2519–2529
15. Mielikainen J (2006) LSB matching revisited. IEEE Signal Process Lett 13(5):285–287
16. Ni Z, Shi YQ, Ansari N, Su W, Sun Q, Lin X (2008) Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Trans Circuits Syst Video Technol 18(4):497–509

17. Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. IEEE Secur Privacy 1(3):32–44
18. Spaulding J, Noda H, Shirazi MN, Kawaguchi E (2002) BPCS steganography using EZW lossy compressed images. Pattern Recogn Lett 23(13):1579–1587
19. University of Southern California (2011) The USC-SIPI image database. Retrieved from http://sipi.usc.edu/database/ on 1 March 2011
20. Wang H, Wang S (2004) Cyber warfare: steganography vs. steganalysis. Commun ACM 47(10):76–82
21. Wang ZH, Kieu TD, Chang CC, Li MC (2010) A novel information concealing method based on exploiting modification direction. J Inf Hiding Multimedia Signal Process 1(1):1–9
22. Westfeld A (1999) Attacks on steganographic systems. In: Proceedings of the 3rd information hiding workshops, Dresden, Germany, 28 September–1 October, pp 61–75
23. Westfeld A (2004) F5: a steganographic algorithm. In: Proceedings of the 4th international workshop on information hiding 2001. Lecture notes in computer science, vol 2137, Pittsburgh, PA, USA, pp 289–302
24. Yu YH, Chang CC, Hu YC (2005) Hiding secret data in images via predictive coding. Pattern Recogn 38(5):691–705
25. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):781–783

Cheonshik Kim received his B.S. degree in computer engineering from Anyang University, Korea in 1995, and M.S. degree in information engineering from Hankuk University of Foreign Studies (HUFS), Korea in 1997 and Ph D. degree in computer engineering from HUFS in 2003. He joined the Faculty of Sejong University, Korea where he is currently a professor in Department of Computer Science and Engineering. His research interests include Multimedia systems, Distance learning, Databases, Data mining, and Information Security. He is a member of IEEE and IEEK (Institute of Electronics Engineers of Korea).