Multimedia Tools and Applications (2019) 78:17995–18015
https://doi.org/10.1007/s11042-018-7101-3

Generalizing Hamming+k data hiding by overlapped pixels

Cheonshik Kim[1] · Dongkyoo Shin[1] · Ching-Nung Yang[2] · Yung-Shun Chou[2]

Received: 13 June 2018 / Revised: 21 November 2018 / Accepted: 18 December 2018 /
Published online: 16 January 2019

Abstract
Matrix coding based data hiding (MCDH) using linear codes (syndrome coding) is an efficient coding method for steganographic schemes to improve their embedding efficiency. Hamming code data hiding (HDH) is a well-known MCDH using a covering function $COV(1, n = 2^k - 1, k)$. Afterwards, Hamming+1 DH (H1DH) was proposed with good embedding efficiency. However, these two previous approaches, HDH and H1DH, are not efficient for a large amount of messages. To tackle this problem, Yang et al.'s proposed Hamming+k DH (HkDH), which enhance the extra one embedded bit in H1DH to k embedded bits in the HkDH. In this paper, we extended the HkDH to the Hamming+k with m overlapped pixels (Hk_mDH). The proposed Hk_mDH adopted pixel overlapping approach, optimal pixel adjustment process (OPAP), and Least Significant Bit (LSB) substitution. Experimental results demonstrate that our Hk_mDH has better embedding rate (ER) compared with previous schemes. In addition, we have proved that our Hk_mDH has excellent theoretical estimation of average mean square error.

Keywords Data hiding · Steganography · Hamming code · LSB · OPAP

1 Introduction

Data hiding (DH) is a technique of embedding secret data in an innocuous cover media such as image, audio, or text, and meanwhile may maintain the quality of cover media. For DH

A preliminary conference version of this paper appeared under the title "Capacity Enhancement of Hamming+k Data Hiding By Pixel Overlapping Approach," in IEEE Proc. of 17th IEEE International Conference on Communication Technology (ICCT 2017), Chengdu, China, 2017.

✉ Cheonshik Kim
mipsan@paran.com

✉ Dongkyoo Shin
shindk@sejong.ac.kr

Ching-Nung Yang
cnyang@gms.ndhu.edu.tw

[1] Department of Computer Science and Engineering, Sejong University, Seoul, Republic of Korea

[2] Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan

schemes, the cover media should not be improperly degraded, and the embedded data should not be recognized by the human visual system. That is, even if a cover image includes a lot of message, its existence should not be detected by the observer [1, 8, 16]. But in reality, most stego images may be detected by statistical analysis [12, 14]. To avoid the detection of steganalysis, we should reduce the number of modified pixels for embedding a message, such that these modifications will not seriously change the original features of the cover image.

The method of least significant (LSB) substitution is one of DH schemes. The technique of LSB replacement was widely researched in DH fields as well as achieving high embedding capacity is a merit of it [11, 20]. The LSB approach is easy and simple, but it has a critical issue that there is a statistical difference between modified and unmodified pixels in stego image. It is possible for MCDH to scatter secret message embedded in stego image to address this difference.

Unlike the naive LSB approache, the optimal pixels adjustment process (OPAP) [3] is widely used for achieving imperceptibility, because OPAP significantly improves peak signal to noise ratio (PSNR) of simple LSB. Recently, Yang et al. [15] also adopted LSB and OPAP to improve the visual quality of a cover image which was generated by neighbor mean interpolation.

For MCDH adopting covering function $COV(r, n, k)$, it had been possible to improve embedding efficiency by decreasing the number of changes [4]. F5 algorithm [13] is a kind of MCDH using $HC(n, n-k)$ Hamming code with minimum Hamming distance $d_{\min} = 3$ with $COV(1, n = 2^k - 1, k)$ [2]. Zhang and Wang [19] introduced exploit modification direction (EMD), which is ternary HC for fully exploiting LSBs. Fridrich et al. [6] also proposed a simple one-dimensional ternary code suitable for embedding large payloads. Previously MCDHs are based on the cover coding like Hamming code, Golay code, BCH and code [17, 18]. For instance, the Hamming+1 DH (H1DH) [18] used OPAP to improve stego image quality. The high capacity of information hiding (HCIH) [21] was introduced for high ER using H1DH and LSB replacement.

Kim and Yang [10] introduced a scheme to improve embedding capacity by overlapping two consecutive blocks based on HC(7, 4) DH (HDH). That is, it is possible to embed 6 bits in 11 pixels (note: $7 + 7 - 3 = 11$). But, for exploitation of the overlapped pixels, they only simply used second LSB. Recently, Kim et al. [9] proposed a Hamming+k data hiding (HkDH) scheme to hide $2k$ bits in a block with overlapped LSB and 2LSB using matrix encoding by adding or subtracting by two. These coarse approaches will lead to reducing somewhat the quality of cover image.

To tackle this problem, we extend this pixel overlapping approach on HkDH with m overlapped pixels (referred to as Hk_mDH) in this paper. We use the syndrome function of HC and OPAP simultaneously of overlapped pixels. The proposed Hk_mDH may conceal $2k$ secret bits to $(2^{k+1} - 1 - m)$ pixels, by changing two LSBs in a block with large probability, and at most no more than 3 modifications.

The rest of this paper is organized as follows. Section 2 briefly reviews Hamming code, HDH, and Kim and Yang's DH, and HkDH. In Section 3, we present Hk_mDH. In addition, some theoretical analyses are given. In Section 4, the proposed Hk_mDH is tested using some images. A comparison with the HDH, H1DH, HCIH, Kim and Yang's DH, and HkDH is also provided. Finally, this paper concludes in Section 5.

2 Related works

2.1 Hamming code

We first introduce a few basic concepts of Hamming code theory for cover coding. Hamming code HC$(n, n-k)$ of $d_{\min} = 3$ is a single error correction linear block code with, where k is the number of parity bits and $(n-k)$ is the number of information bits. Let $\mathbb{F}_2^n$ denotes the space of all n-bit column vectors $y = (y^1, \ldots, y^n)^T$. Let $y \in \mathbb{F}_2^n (n = 2^k - 1)$ be a codeword obtained from an information word $x \in \mathbb{F}_2^{(n-k)}$ via a $(n-k) \times n$ generator matrix G, where $y = x \cdot G$. Suppose that $\mathbf{H}$ is a $k \times n$ parity matrix with $G \cdot H^T = [0]_{(n-k)\times k}$.

For any $y \in \mathbb{F}_2^n$, the vector $S = Hy \in \mathbb{F}_2^k$ is called the syndrome of y. For each syndrome $S \in \mathbb{F}_2^n$, the set $C(S) = \{y \in \mathbb{F}_2^n | Hy = S\}$ is called a coset. We can figure out a one-bit error pattern to correctly decode the codeword with one-bit error. Suppose that the received codeword is $\hat{y}$ with an error pattern $e = (y \oplus \hat{y})$.

The position of e can be obtained from (1).

$$\begin{cases} \hat{y} \cdot H^T = (e \oplus y) \cdot H^T = e \cdot H^T + y \cdot H^T \\ (cf., y = (x \cdot G) \cdot H^T = 0) \\ = e \cdot H^T + 0 = e \cdot H^T \end{cases} \tag{1}$$

For example, the parity check matrix $\mathbf{H}$ of HC(7, 4) code is shown in (2).

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{2}$$

Suppose that there is one error bit occurred in $\hat{y}$ (say the 6-th bit from left), i.e., $e = (e_1, e_2, \ldots, e_7) = (0000010)$. The syndrome $S = (110)$ is extracted. It means that the error position is the 6-th from left. In order to embed message bits in each subset by making at most one embedding change, we divide the cover image into N/n subsets, each consisting of n pixels, where n is the length of the code. Given that a codeword with code length n, an error can occur in any of the n positions or no error has occurred. Thus, we have $2^k \geq n + 1$ for (n, k) code. If this bound is achieved with equality, $n = 2^k - 1$, then the code is a perfect code. Every binary HC is a perfect code.

The decoding procedure for HC is demonstrated as follows.

Step 1: Compute the syndrome $S(\hat{y}) = b(\hat{y}) \cdot H^T$, where $b(i) = i \bmod 2$ and $\hat{y}$ is received codeword.
Step 2: Find the error pattern e from the syndrome.
Step 3: Modify the cover object so that $y = (\hat{y} \oplus e)$, and then decode $x = y \cdot G^{-1}$.

2.2 HDH scheme

For simplicity, we adopt HC (7, 4) to describe HDH. This HDH may hide 3 secret bits δ for in 7 cover bits by using the covering function $COV(1, 7, 3)$. For pixel-domain DH, these 7 cover bits are selected from 7 LSBs of 7 pixels. For embedding procedure, we have to know the error e in between δ and the syndrome, i.e., $S' = (S \oplus \delta)$. The number of

cosets on HC (7,4) is eight and it is possible to embed δ through the changing one bit in all codewords in other cosets. For $COV(1, n, k)$, the codewords have the length $n = 2^k - 1$, change density is $d = 1/2^k$, ER is $\varphi = k/n = k/(2^k - 1)$, and embedding efficiency is $EE = \varphi/d = (2^k/(2^k - 1)) \cdot k$. That is, the embedding efficiency is defined as the expected number of bits embedded per one embedding change.

2.3 Kim and Yang's DH scheme

Kim and Yang's DH is a scheme based on HC(7,4) with 3 overlapped pixels in 11 consecutive pixels. In this case, it is possible to embed 6 secret bits into 11 pixels (i.e., $7+7-3 = 11$) $(x_1, \ldots, x_{11})$, as shown in Fig. 1. That is, one 11-pixel block is regarded as two HDHs using HC(7, 4) with 3 overlapped pixels. The first 3 secret bits $(\delta_1, \delta_2, \delta_3)$ are embedded into the LSBs $(c_1, \cdots, c_7)$ of the first 7 pixels $(x_1, \cdots, x_7)$ in the block by $COV(1, 7, 3)$ (see (3)), where $b(x_i) = c_i$ for $1 \le i \le 7$ and the $b(\cdot)$ is a function to extract the 1st LSB of a pixel. The other three secret bits $(\delta_4, \delta_5, \delta_6)$ are embedded into 7 bits $(c'_1, \ldots, c'_7)$ by $COV(1, 7, 3)$ (see (4)). These 7 bits $(c'_1, \cdots, c'_7)$ will be constructed from $c'_i = b(\lfloor x_{i+4}/2 \rfloor)$, $1 \le i \le 3$ and $c'_i = b(x_{i+4})$, $4 \le i \le 7$.

$$(\delta_1, \delta_2, \delta_3)^T = H \cdot (c_1, \ldots, c_7)^T = H \cdot (b(x_1), \ldots, b(x_7))^T \tag{3}$$

$$\begin{cases} (\delta_4, \delta_5, \delta_6)^T = H \cdot (c'_1, \cdots, c'_7)^T \\ = H \cdot (b(\lfloor x_5/2 \rfloor), \cdots, b(\lfloor x_7/2 \rfloor), b(x_8), \cdots, b(x_{11}))^T \end{cases} \tag{4}$$

2.4 H*k*DH scheme

In H*k*DH, the number of overlapping pixels was set to $2^k - 1$ and it was possible to embed $2k$ bits $(\delta_1, \cdots, \delta_{2k})$ in a block composed of $2^k - 1$ pixels by exploiting 2LSB and LSB. For $k = 3$, H*k*DH is based on HC (7,4), which is the same as Kim and Yang's DH but uses seven overlapping pixels. Moreover, the quality of a stego image was maintained by using manipulation skill of OPAP and HC. H*k*DH is briefly described as follows. The first k secret bits are embedded into the XOR-ed result of the 1st LSB and 2nd LSB of all the $2^k - 1$ pixel values using the syndrome of HC, and the other k bits are embedded with the 2nd LSB using HC. When compared with HDH, H1DH, and HCIH, the capacity of H*k*DH is improved, and meanwhile the PSNR is not seriously degraded.

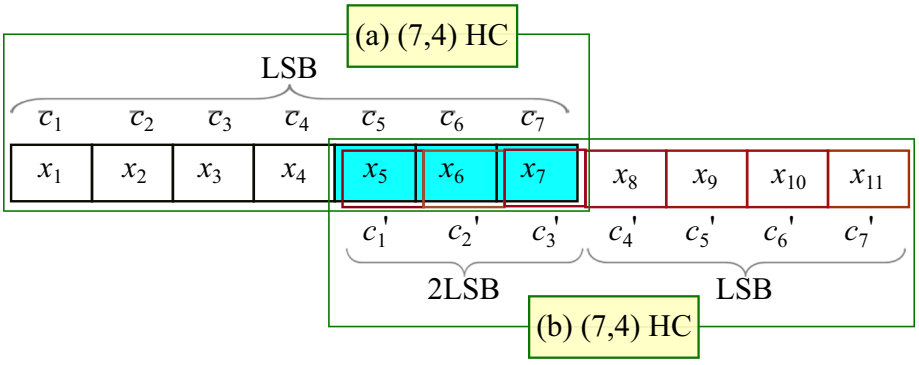


Fig. 1 A block with three overlapped pixels for Kim and Yang's DH

Embedding algorithm of H*k*DH

Step 1: Read 1-block and generate a codeword, $C_1 \in \mathbb{F}_2^{2^k-1}$, by performing an XOR operation between the 1st LSB and 2nd LSB with a sequence of pixels $(x_1, \ldots, x_{2^k-1})$ using (5),

$$C_1 = \sum_{i=1}^{2^k-1} \left[b\left(\left\lfloor \frac{x_i}{2} \right\rfloor \right) \oplus b(x_i) \right] \tag{5}$$

Step 2: Compute the syndrome S_1 (see (6) with the C_1 using parity check matrix $\mathbf{H}$. Compute a new syndrome as $S_1' = S_1 \oplus \delta_1^k$, in which δ is secret bits. If $S_1' \neq 0$, {if (LSB($x_{S_1'}$)=([00] or [10])), $x_{S_1'} + 1$, else $x_{S_1'} - 1$.}

$$S_1 = ([H \cdot C_1^T] \bmod 2)^T \tag{6}$$

Step 3: Compute a syndrome S_2 with only the second LSB, C_2 (see (7), of the x using (8). If ($S_2' \neq 0$), {if (LSB($x_{S_2'}$)=([00] or [10])), $x_{S_2'} - 1$, else $x_{S_2'} + 1$.}

$$C_2 = \sum_{i=1}^{2^k-1} \left[b\left(\left\lfloor \frac{x_1}{2} \right\rfloor \right), \ldots, b\left(\left\lfloor \frac{x_{2^k-1}}{2} \right\rfloor \right) \right] \tag{7}$$

$$S_2 = ([H \cdot C_2^T] \bmod 2)^T \tag{8}$$

3 The proposed Hamming+*k* scheme with *m* overlapped pixels

In Kim and Yang's DH using HC(7, 4), one modified bit of (c_1', c_2', c_3') causes a mean square error $2^2 = 4$ because these three bits (c_1', c_2', c_3') are the 2nd LSB of the pixels (x_5, x_6, x_7). This degrades the stego image quality seriously. To solve the problem, we extend this pixel overlapping approach and adopt OPAP and LSB simultaneously to reduce the average mean square error. In fact, the proposed Hk_mDH is an extension of HkDH, which use m overlapped pixels, where $0 \leq m \leq k$. In fact, our scheme is the HDH for $m = 0$, and the HkDH for $m = k$.

3.1 Design concept

We introduce design concept about the proposed Hk_mDH using $COV(1, 2^k - 1, k)$. The Hk_mDH embeds k secret bits (δ_1^k) into the first $(2^k - 1)$ pixels using $COV(1, 2^k - 1, k)$ and then embeds the other k secret bits (δ_{k+1}^{2k}) into the last $(2^k - 1)$ pixels. The size of one block is $2^{k+1} - m - 2$ and the block is composed of pixels $(x_1, \ldots, x_{2^{k+1}-m-2})$ with m overlapped pixels in our DH. With the pixel overlapping approach, one stego block is divided into two 7-pixel subblocks. The first $(2^k - 1)$ pixels are composed of $(x_1, \ldots, x_{2^k-1})$, and the last 7 pixels are $(x_{2^k-m}, \ldots, x_{2^{k+1}-m-2})$. As shown in (9) and (10), the secret bits (δ_1^k) and (δ_{k+1}^{2k}) are, respectively, embedded in the block.

$$\begin{cases} (\delta_1, \ldots, \delta_k)^T = H \cdot (b(x_1), \ldots, b(x_{2^k-m-1}), \\ b(x_{2^k-m}) \oplus b\left(\left\lfloor \frac{x_{2^k-m}}{2} \right\rfloor \right), \ldots, b(x_{2^k-1}) \oplus b\left(\left\lfloor \frac{x_{2^k-1}}{2} \right\rfloor \right)) \end{cases} \tag{9}$$

$$\begin{cases} (\delta_{k+1}, \ldots, \delta_{2k})^T = H \cdot (b\left(\left\lfloor \frac{x_{2^k-m}}{2} \right\rfloor \right), \ldots, b\left(\left\lfloor \frac{x_{2^k-1}}{2} \right\rfloor \right), \\ b(x_{2^k}), \ldots, b(x_{2^k-m-2})) \end{cases} \tag{10}$$

Here, the design concept (Fig. 2) of Hk_mDH are briefly described using (9) and (10). For one cover block, the first k secret bits are embedded into the 7-bits acquired from the right hand side (RHS), (c_1^7), of (9) and then the other k secret bits are embedded the other 7-bits obtained from RHS, ($c_1^{7\prime}$), of (10). The overlapped pixels in (9) and (10) are to be XOR-ed of 1st LSB and 2nd LSB, respectively.

The proposed method applies the different procedure to each of the following three cases:

Case 1 When S_1 and S_2 ((9) and (10)) are different values, the two formula apply to only 1st LSBs of the blocks. In this case, OPAP is not necessary (see Fig. 3a).

Case 2 When (S_1 and S_2) $\in \{5, 6, 7\}$, i.e., $S_1 \neq S_2$, the optimization method by OPAP and LSB is required (see Fig. 3b).

Case 3 When $S_1 = S_2$, perform $x_i \pm 1$ where $i (= 8 \ldots 11)$ is randomly selected in Fig. 3c. After then, S_2 may point to non-overlapped pixels. Afterward, apply HC to the pixel pointed by S_2.

The proposed method leads to a mean square error (i.e., $2^2 = 4$) if the collision of two syndromes happens (e.g., when $S_1 = S_2$). In this case, the method of (Case 3) may remove the cause of the error.

For example, given a pixel x with grayscale value 244 (11110100), the XOR-ed value of 1st LSB and 2nd LSB is $0 \oplus 0 = 0$. If $x' = x - 1$, then $x' = 243$ (11110011) and the 2nd LSB is changed from "0" to "1", and but the XOR-ed value of 1st LSB and 2nd LSB is unchanged, because of $0 \oplus 0 = 1 \oplus 1$. Thus, the changed value is only 1. When the changed pixels in (9) and (10) are within the same overlapped pixel, we should change the modified position to other two positions in (10) so that the mean square error will be reduced.

Example 1 Consider an example that we embed the first k secret bits by (9), and modify the LSB in one overlapped pixel from $x = 10 = (00001010)_2$ to $x' = 11 = (00001011)_2$. In

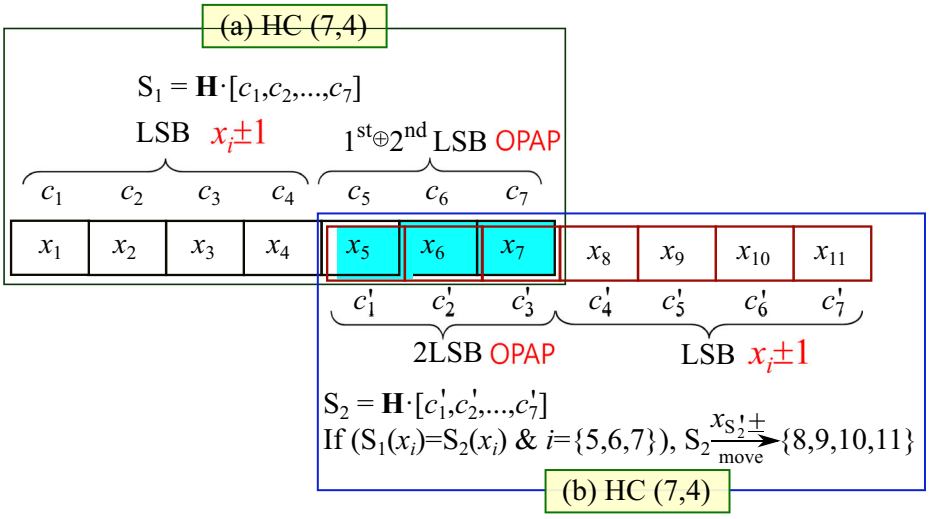


Fig. 2 A conceptual diagram of the proposed Hk_mDH, m=3

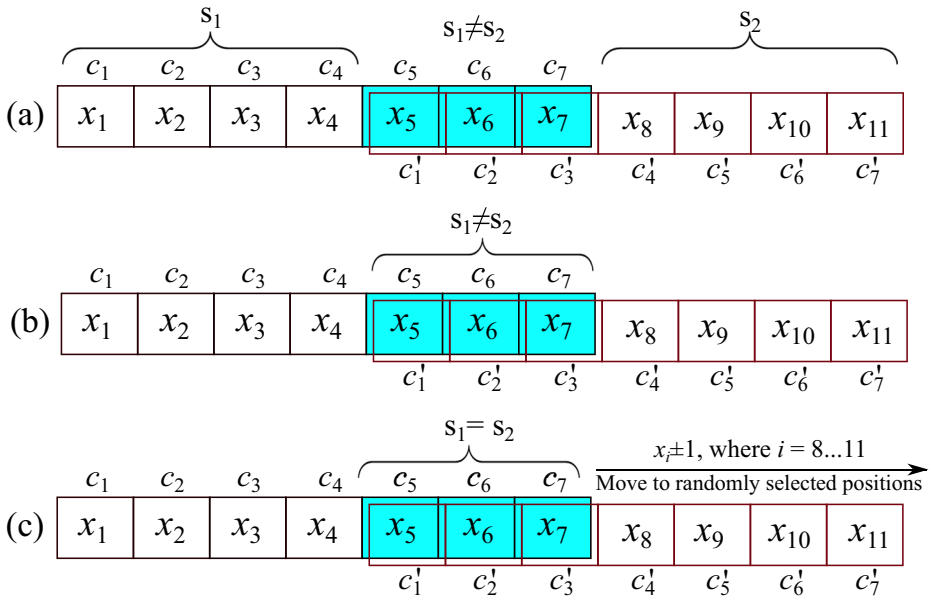


Fig. 3 Sketchy diagram for the proposed concept (assuming $m = 3$)

this case, if the modification position in (10) is the same, $x'' = 12 = (00001100)_2$ by OPAP. Thus, the difference value, $|x - x''|$ is "2" and mean square is $2^2 = 4$. But, if the modified position moves to other two position, the mean square error is reduced from $2^2 = 4$ to $(1^2 + 1^2) = 2$. Through the procedure of this optimization process, it will be able to reduce a lot of errors that may happen when we hide messages by using Hk_mDH.

In the final analysis, it is certain that modifying two 1st LSBs may obtain good PSNR than modifying one 2nd LSB theoretically. Assume that the k-tuple secret δ is embedded by $\delta = y' \cdot H^T$, where y' is changing one bit (or no change) in the $(2^k - 1)$-tuple y, where $S = y \cdot H^T$. Suppose that $S = (S_1 \oplus S_2)$, and then we have $S = (S_1 \oplus S_2) = (y_1 \cdot H^T \oplus y_2 \cdot H^T)$, where y_1 and y_2 are two $(2^k - 1)$-tuples via changing one bit in y, respectively. Finally, we may embed k bits by changing two positions in one block.

3.2 Embedding procedure

For brief explanation, we here assume that $k = 3$ (i.e., by $COV(1, 7, 3)$ covering function) and $m = 3$ for the proposed Hk_mDH, which can embed 6 secret bits into 11 cover pixels. Moreover, the extraction procedure is just a reverse procedure of the embedding procedure, so we skip the extraction procedure. The detailed procedure of the embedding is as follow.

Step 1: Read the next one block $(2^{k+1} - m - 2)$ bits x from the cover object and generate a codeword, $p \in \mathbb{F}_2^{2^k-1}$, by (11).

$$p = \left(b(x_1), \ldots, b(x_4), \left(b(x_5) \oplus b\left(\left\lfloor \frac{x_5}{2} \right\rfloor\right)\right), \ldots, \left(b(x_7) \oplus b\left(\left\lfloor \frac{x_7}{2} \right\rfloor\right)\right)\right) \tag{11}$$

Step 2: Calculate the syndrome $S_1 = H \cdot p^T$ and $S_1' = S_1 \oplus (\delta_1^3)$.

Step 3: If $(S_1' \leq (7-m+1)-1)$, $(x_{S_1'})\pm$, else if $(S_1' \in \{7-m+1,\ldots,7\})$, when $(LSB(x_{S_1'}) = ([00]\text{or}[10])) : x_{S_1'} + 1$ or when $(\text{LSB}(x_{S_1'}) = ([01]\text{or}[11])) : x_{S_1'} - 1$.

Step 4: Generate another codeword, $q \in \mathbb{F}_2^{2^k-1}$, by (12).

$$q = \left(b\left(\left\lfloor \frac{x_5}{2} \right\rfloor\right), \ldots, b\left(\left\lfloor \frac{x_7}{2} \right\rfloor\right), b(x_8), \ldots, b(x_{11})\right) \tag{12}$$

Step 5: Calculate the syndrome $S_2 = H \cdot q^T$ and $S_2' = S_2 \oplus (\delta_4^6)$.

Step 6: If $(S_1' = S_2')$, $\{(x_i)\pm$, where $i = 8\ldots11$ and choose one from $i\}$, else if $(S_1' \neq S_2')$, {If $(S_2' \geq 8)$, $(x_{S_2'})\pm$, else if $(S_2' \in \{7-m+1,\ldots,7\})$, when $(\text{LSB}(x_{S_2'}) = ([00\text{or}[10])) : x_{S_2'} - 1$ and when $(\text{LSB}(x_{S_2'}) = ([01]\text{or}[11])) : x_{S_2'} + 1.\}$

Step 7: Go to Step 1 until not end of block.

3.3 Theoretical estimation of average mean square error

The HDH has i, 0 or 1, where the LSBs need to be modified with probability $\binom{2^k-1}{i}/2^k$ over every $2^k - 1$ pixels. Obviously, the ER of HDH is $\varphi_{HDH} = k/(2^k-1)$, and the average mean square error of HDH $AMSE_{\text{HDH}}$ is derived in (13). For $k = 3$, we have $\varphi_{HDH} = 3/7 = 0.428$ and $AMSE_{\text{HDH}} = 1/8 = 0.125$.

$$AMSE_H = \left(0^2 \times \binom{2^k-1}{0}/2^k + 1^2 \times \binom{2^k-1}{1}/2^k\right)/(2^k-1) = \frac{1}{2^k} \tag{13}$$

The H1DH [18] extended from HDH may embed $(k+1)$ secret bits into 2^k pixels. Thus, the ER is $\varphi_{H1DH} = (k+1)/2^k$. The $AMSE_{\text{H1DH}}$ is given as follows [18]. For $k = 3$, we have $\varphi_{H1DH} = 4/8 = 0.5$ and $AMSE_{\text{H1DH}}$ $1/8 - 1/128 = 0.117$.

$$AMSE_{H1} = \begin{cases} (0^2 \times \binom{2^k-1}{0}/2^k + 1^2 \times \left(\binom{2^k-1}{0}/2^k \times 1/2\right) \\ +1^2 \times \binom{2^k-1}{1}/2^k)/2^k = \frac{1}{2^k} - \frac{1}{2^{2k+1}} \end{cases} \tag{14}$$

From the encoding algorithm of HkDH, it is observed that $S_1' \neq S_2'$ has three cases: (6) and (8) hold with probability $1/2^{2k}$, one of these equations holds and the other does not with the probability $(2^k-1)/2^{2k}$, and neither equation holds but the positions of the changed pixels are different with probability $(2^k-1)\cdot(2^k-2)/2^{2k}$. The case where neither equation holds but the positions of the changed pixels are the same (i.e., $S_1' = S_2'$) has probability $(2^k-1)/2^{2k}$. Therefore, $AMSE_{\text{Hk}}$ is directly derived from (15).

$$AMSE_{Hk} = \begin{cases} (0^2 \times \frac{1}{2^{2k}} + 1^2 \times \frac{(2^k-1)}{2^{2k}} + 1^2 \times \frac{(2^k-1)}{2^{2k}} + (1^2+1^2)\times \\ (((2^k-1)\times(2^k-2)/2^{2k})) \\ \frac{(S_1'\neq S_2')+(1^2+1^2+1^2)\times\left(\frac{(2^k-1)}{2^{2k}}\right)(S_1'=S_2'))}{2^k} - 1 \\ = \frac{(2^{k+1}+1)}{2^{2k}} = \frac{1}{2^{k-1}} + \frac{1}{2^{2k}} \end{cases} \tag{15}$$

For the proposed Hk_mDH, by using LSB and OPAP, we may embed these $2k$ secret bits into $(2^{k+1}-2-m)$ pixels with only two modifications (grayscale value differs with only one like changing two LSBs) with large probability, and at most no more than 3 modifications.

The values of φ_{Hk_mDH} can be easily from (16). About the AMSE_{Hk_mDH}, if both equations (9) and (10) are satisafied, then the MSE is $(0^2 \times 1/2^{2k})$, while the MSE will be $(1^2\times(2^k-1)/2^{2k} + 1^2\times(2^k-1)/2^{2k})$ for any one equation is satisfied (9) or (10). Consider the cases one change in (9). The MSE is $(1^2+1^2)\times(2^k-1)/2^k \times (((2^k-1-m)/(2^k-1))\times(2^k-1)/2^k)$ for the case that the change is in the first (2^k-1-m) bits, and the MSE

is $(1^2+1^2)\times(2^k-1)/2^k\times((m/(2^k-1))\times(2^k-2)/2^k)$ for the change is in the last m bits. On the other hand, for the case two changes in the last m bits for (9), the MSE is $(1^2+1^2+1^2)\times(2^k-1)/2^k((m/2(2^k-1))\times 1/2^k)$. Finally, the average AMSE_{Hk_mDH} is derived in (17). For $k=3$ and $m=3$, we have $\varphi_{Hk\_mDH}=6/(16-2-3)=0.545$ and $\mathrm{AMSE}_{Hk\_mDH}=0.256$.

$$\begin{cases}\varphi_{Hk\_mDH}=2k/((2^k-1)+(2^k-1)-m)\\ =2k/(2^{k+1}-2-m)\end{cases} \tag{16}$$

$$\begin{cases} AMSE_{Hk\_m}=\{(0^2\times 1/2^{2k}+1^2\times(2^k-1)/2^{2k}+1^2\times(2^k-1)/2^{2k})\\ \text{(note: both equations are satisfied, or any one equation satisfied)}\\ +(1^2+1^2)\times(2^k-1)/2^k\times\\ \left(\overbrace{\left(((2^k-1-m)/(2^k-1))\times(2^k-1)/2^k\right)}^{\text{one change in the first } (2^k-1-m) \text{ bits for (9)}}+\overbrace{\left((m/(2^k-1))\times(2^k-2)/2^k\right)}^{\text{one change in the last } m \text{ bits for (9)}}\right)\\ +(1^2+1^2+1^2)\times(2^k-1)/2^k\times\ \overbrace{\left((m/(2^k-1))\times 1/2^k\right)}^{\text{two changes in the last } m \text{ bits for (9)}}\ \}/(2^k-1)\\ =\{(2\times(2^k-1)/2^{2k})+(2\times((2^k-1)^2-m)/2^{2k})+(3\times m/2^{2k})\}/(2^k-1)\\ =(2^{k+1}+m/(2^k-1))/(2^{2k})=\frac{1}{2^{k-1}}+\frac{m/(2^k-1)}{2^{2k}}\end{cases} \tag{17}$$

4 Experiment and comparison

4.1 Experimental results

We have proved by using the formula that Hk_mDH improves the performance of PSNR by reducing AMSE meanwhile, retain the embedding payload. To verify the proposed theory, we compare Hk_mDH with the previous scheme and prove the superiority of Hk_mDH as a result of the comparison. To evaluate performance, we experiment on the stego image quality for HDH ($k=3$), H1DH ($k=3$), HCIH ($n=7$), Kim and Yang's DH ($k=3$ with 3 overlapped pixels), HkDH, and the proposed Hk_mDH ($k=3, m=3$) using MATLAB with 512×512 original grayscale images [7] with cover images (see Fig. 4).

Generally, MSE (see (18)) and PSNR (see (19)) are widely used to measure the quality of an image. The value of MSE is used to measure average the squared intensity differences between a distorted image and reference image. If an image has a small MSE value, it has a relatively good visual quality. PSNR describes the ratio of the maximum possible power of a signal to the power of corrupting noise and is a clearly good instrument for evaluation about the quality of an image as objectively. MSE measures the energy of the signal using the L^2 - norm, which is energy preserving. The MSE between two image x and y is

$$MSE(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-y_i)^2 \tag{18}$$

(a) Baboon (b) Barbara (c) Boats

(d) Goldhill (e) Airplane (f) Lena

(g) Peppers (h) Tiffany (i) Zelda

Fig. 4 Original images used in experiment.

The error signals, $e_i = x_i - y_i$, denotes the difference between the original and distorted signal. The MSE is usually expressed as the PSNR measure

$$PSNR = 10log_{10}\frac{L^2}{MSE}, \tag{19}$$

where L is the dynamic range of allowable pixel intensities. For example, for an 8-bit per pixel image, $L = 2^8 - 1 = 255$. The definition of capacity means how much information

can be hidden in the cover image. That is to say, it refers to the amount of information. This is used for important criteria about DH. For this reason, we tried to find algorithms to increase their capacity without degrading stego image. (20) means the ratio of the number of message bits ($||d||$), to the total number of pixels.

$$\varphi = \frac{||d||}{N \times N} \tag{20}$$

Table 1 demonstrates the comparison among HDH, H1DH, HCIH, Kim and Yang's DH, HkDH, and Hk_mDH, which are DH methods based on HC. It appears that each ERs of them are 0.43, 0.5, 0.75, 0.54, 0.86, and 0.54, respectively. The ER of HCIH is higher than HDH, H1DH, and Kim and Yang's DH. The maximum ER of both HkDH and the proposed Hk_mDH has the same. The Hk_mDH has good PSNR although the ER of Hk_mDH is higher ER than that of HDH, H1DH, HCIH, and Kim and Yang's DH.

H1DH is the best in the aspect of quality, and HkDH and Hk_mDH could have the highest ER with maintaining good PSNR. Especially, Hk_mDH can trade PSNR for ER using variable m. The two elements, PSNR and ERs, are the relation in inverse proportion to each other. In addition, in the proposed Hk_mDH, we can trade $AMSE_{\mathrm{H}k\_m\mathrm{DH}}$ for $\varphi_{\mathrm{H}k\_m\mathrm{DH}}$ by selecting m. For example, we may have $\varphi_{\mathrm{H}k\_m\mathrm{DH}} = 0.666$ and $AMSE_{\mathrm{H}k\_m\mathrm{DH}} = 0.261$ for $k = 3$ and $m = 5$.

Figure 5 represents the comparison among original and stego images such as (a) original (b) HDH, (c) H1DH, (d), HCIH, (e) Kim and Yang's DH, (f) HkDH, and (g) Hk_mDH, respectively. The PSNR of H1DH is the highest in this experiment and the difference of PSNR between H1DH and Hk_mDH is about 1.43 PSNR. That is to say, it has only slight errors.

Table 2 shows performance comparisons according to control variable m (when m = 1, 3, 5, and 7). At this time, the proposed Hk_mDH has ERs 0.46, 0.54, 0.67, and 0.86, respectively. We may adjust ER and PSNR by increasing/decreasing m. In the Hk_mDH, the value of m may be decreased or increased according to user's need. Users may embed a large amount of messages by increasing the value of m.

Figure 6 demonstrates the comparison among stego images derived from Hk_mDH when the variable $m = 1 \ldots 7$. Since the stego images are originated by the optimized DH, it is not easy to distinguish the original through the human visual system.

In Table 3, we measured PSNRs under the same condition (i.e., embedding capacity: 90000 random bits) using about Hamming-like schemes such as HDH, H1DH, HCIH, Kim and Yang's DH, HkDH, and Hk_mDH. Although the amount of embedding capacity is the same for the same cover images, the PSNRs of stego images are different because the embedding approaches (or algorithms) are different. In this experiment, Hk_mDH (when $COV(15, 4)$) had higher PSNRs than HDH, HCIH, Kim and Yang's DH, and HkDH and the PSNR of H1DH is slightly higher rather than Hk_mDH.

4.2 Steganlysis

Fridrich et al. [5] proposed a steganalysis based on statistical analysis with the object of the detection of stego image. This method define two mappings: F_1 for $0 \longleftrightarrow 1, 2 \longleftrightarrow 3, \ldots, 254 \longleftrightarrow 255$ and F_{-1} for $-1 \longleftrightarrow 0, 1 \longleftrightarrow 2, \ldots, 255 \longleftrightarrow 256$. When the

Table 1 Performance comparison of all Hamming-like DHs

Images	HDH ($n = 7, k = 3$)		H1DH ($n = 7, k = 3$)		HCIH ($n = 7$)		Kim & Yang's DH ($n = 7, k = 3$)		HkDH ($n = 7, k = 3$)		Hk_mDH ($n = 7, k = 3$)	
	dB	φ	dB	φ	dB	φ	dB	φ	dB	φ	dB	φ
Baboon	57.15	0.43	57.44	0.5	53.43	0.75	53.96	0.54	53.63	0.86	53.63	0.86
Barbara	57.16	0.43	57.44	0.5	53.43	0.75	53.93	0.54	53.65	0.86	53.64	0.86
Boats	57.15	0.43	57.44	0.5	53.43	0.75	53.94	0.54	53.64	0.86	53.65	0.86
Goldhill	57.16	0.43	57.44	0.5	53.44	0.75	53.95	0.54	53.62	0.86	53.65	0.86
Airplane	57.15	0.43	57.44	0.5	53.45	0.75	53.95	0.54	53.63	0.86	53.64	0.86
Lena	57.16	0.43	57.44	0.5	53.43	0.75	53.95	0.54	53.63	0.86	53.65	0.86
Peppers	57.16	0.43	57.44	0.5	53.46	0.75	53.95	0.54	53.64	0.86	53.64	0.86
Tiffany	57.16	0.43	57.46	0.5	53.43	0.75	53.96	0.54	53.64	0.86	53.63	0.86
Zelda	57.16	0.43	57.43	0.5	53.43	0.75	53.99	0.54	53.64	0.86	53.99	0.86
Average	57.16	0.43	57.44	0.5	53.44	0.75	53.95	0.54	53.63	0.86	53.64	0.86

Fig. 5 Comparison of Lena images derived from various schemes: **a** original **b** HDH (57.16dB), **c** H1DH (57.44 dB), **d** HCIH (53.43 dB) **e** Kim and Yang's DH (53.95 dB), **f** HkDH (53.63 dB), and **g** Hk_mDH ($m = 3$; 56.01 dB)

LSB of cover image is different from the hidden bit, F_1 is used. The method to measure the smoothness of a group $(x_1, x_2, \ldots, x_n)$ is as follows:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \tag{21}$$

Table 2 Performance comparisons for various m variations

Images	$m = 1, n = 13$		$m = 3, n = 11$		$m = 5, n = 9$		$m = 7, n = 7$	
	PSNR	φ	PSNR	φ	PSNR	φ	PSNR	φ
Baboon	56.7699	0.46	55.9999	0.54	54.9586	0.67	53.6301	0.86
Barbara	56.7603	0.46	56.0026	0.54	54.9581	0.67	53.6402	0.86
Boats	56.7552	0.46	56.0022	0.54	54.9475	0.67	53.6451	0.86
Goldhill	56.7628	0.46	56.0066	0.54	54.9187	0.67	53.6481	0.86
Airplane	56.7849	0.46	56.0024	0.54	54.9399	0.67	53.6353	0.86
Lena	56.7579	0.46	56.0019	0.54	54.9413	0.67	53.6450	0.86
Peppers	56.7718	0.46	56.0121	0.54	54.9390	0.67	53.6447	0.86
Tiffany	56.7718	0.46	56.0024	0.54	54.9571	0.67	53.6569	0.86
Zelda	56.7706	0.46	55.9987	0.54	54.9385	0.67	53.6348	0.86
Average	56.7695	0.46	56.0032	0.54	54.9443	0.67	53.6422	0.86

Fig. 6 PSNRs of Lena images when m=1,3,5,7; **a** m=1 (56.75 dB), **b** m=3 (55.87 dB), **c** m=5 (54.86 dB), **d** m=7 (53.64 dB)

R_m is referred to the ratio of blocks that f increases when F_1 is applied to a part of each block and S_m is referred to the ratio of blocks when f is decreased. R_{-m} and S_{-m} are referred to ratio of blocks when F_{-1} is applied to a part of each block. If cover image does not embed secret data, F_1 and F_{-1} may equally increase the f value of blocks, i.e., $R_m \approx R_{-m}$ and $S_m \approx S_{-m}$. When secret bits are embedded, the difference between R_m and S_m decreases whereas the difference between R_{-m} and S_{-m} increase, i.e., $R_{-m} - S_{-m} > R_m - S_m$. Figure 7 shows the RS analysis results for a stego image Lena and

Table 3 Performance comparison of proposed scheme and previous schemes (using 90000 embedding bits)

Images	HDH ($n = 7, k = 3$)	H1DH ($n = 7, k = 3$)	HCIH ($n = 7$)	Kim & Yang ($n = 7, k = 3$)	HkDH ($n = 7, k = 3$)	Hk_mDH ($n = 15, k = 4$)
	dB	dB	dB	dB	dB	dB
Baboon	58.1181	60.2399	56.8402	57.8956	57.6139	59.6822
Barbara	58.1161	60.2205	56.8220	57.8783	57.6251	59.6836
Boats	58.1181	60.2528	56.8193	57.8873	57.6295	59.6803
Goldhill	58.1342	60.2361	56.8145	57.8964	57.5826	59.7000
Airplane	58.1102	60.2666	56.8258	57.8823	57.6180	59.6950
Lena	58.1370	60.2013	56.8365	57.8967	57.6008	59.6730
Peppers	58.1332	60.2302	56.8314	57.9062	57.6243	59.6900
Tiffany	58.1443	60.2709	56.8477	57.9517	57.6274	59.7188
Zelda	58.1271	60.2302	56.8428	57.8952	57.5954	59.6893
Average	58.1264	60.2387	56.8311	57.8988	57.6130	59.6902

the x-axis denotes the ER and the y-axis the rate of regular and singular pixel groups with $m = [0110]$ and $-m = [0\ -1\ -1\ 0]$. From Fig. 7a, when LSB replacement is used simply, the larger the payload, the greater the difference between $(R_{-m} - S_{-m})$ and $(R_m - S_m)$. But, Fig. 7b shows that $R_m \approx R_{-m}$ and $S_m \approx S_{-m}$ hold when the payload is increased. Therefore, it is apparent that our proposed scheme is secure against the RS detection attack.

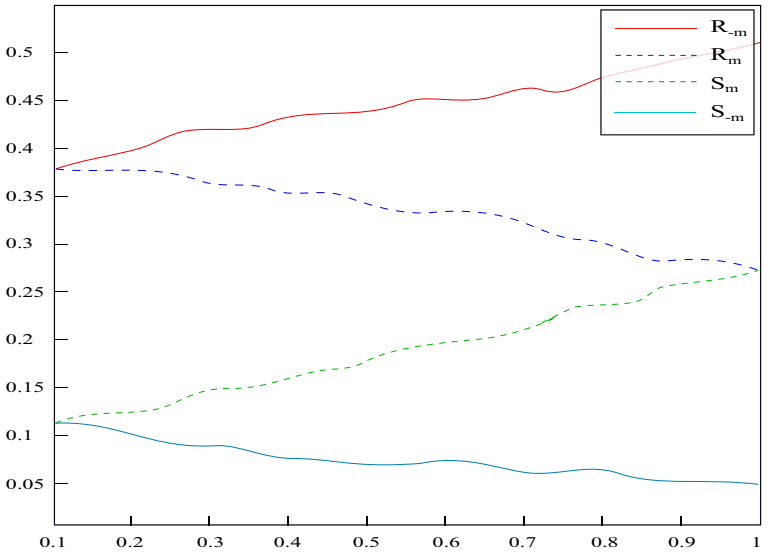
4.3 Performance evaluation

In the proposed Hk_mDH, m denotes the number of overlapped pixels. We can obtain the higher ER by increasing the value of m. For example, our Hk_mDH by $COV(1, 7, 3)$ covering function has $\varphi_{\mathrm{H}k\_m\mathrm{DH}} = 6/14$ and $AMSE_{\mathrm{H}k\_m\mathrm{DH}} = 0.252$ for $m = 1$.

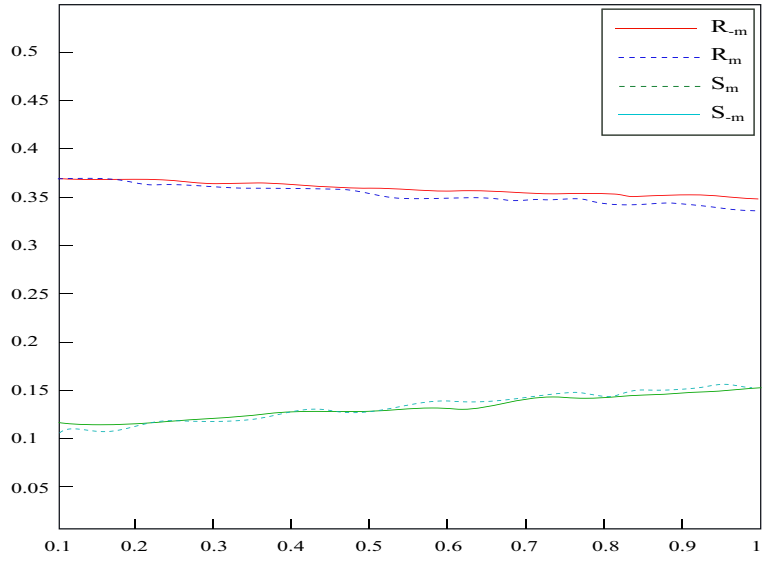
On the other hand, we could obtain $\varphi_{\mathrm{H}k\_m\mathrm{DH}}$=6/7 and $AMSE_{\mathrm{H}k\_m\mathrm{DH}} = 0.265$ for $m = 6$. Therefore, our Hk_mDH is possible to control stego image quality via the value of m. In another application, if we want a high ER we may use Hk_mDH using $COV(1, 7, 3)$ with $m = 7$, which has a very high capacity of 6/7. Even for this case, the $AMSE$ = 0.265 has a PSNR of approximately $53.8dB$.

In addition, we may control $AMSE$ by choosing the value of k, on which the large k decrease $AMSE$. Table 4 illustrates the ERs $\varphi_{\mathrm{H}k\_m\mathrm{DH}}$ and average mean square errors $AMSE_{\mathrm{H}k\_m\mathrm{DH}}$ of the proposed Hk_mDH for various values of m.

Figure 8 represented the histograms of the original Lena image and the stego image of the Hk_mDH. The bar chart and line plot are histograms of the original image and its modified image using Hk_mDH (when $m = 3$ and $COV(1, 15, 4)$, and$\varphi = 0.3$), respectively. This histogram only showed the frequency of the pixel values between 50 and 100 only to highlight the two differences values clearly. Figure 8 shows that it is not easy to find clues about the hidden secret message can be found with only the stego image. However, a blind test may hardly find such differences.



(a) Simple LSB scheme (Lena)



(b) Hk_mDH (Lena)

Fig. 7 Comparison of RS-diagrams between cover images produced by simple LSB-embedding DH and Hk_mDH

Table 4 Comparison of φ and AMSE for various values of m for the proposed Hk_mDH

$COV(1, 7, 3)$		$m = 1$	$m = 3$	$m = 5$	$m = 7$
	$\varphi_{\mathrm{H}k\_m\mathrm{DH}}$	6/13	6/11	6/9	6/7
	$AMSE_{\mathrm{H}k\_m\mathrm{DH}}$	0.252	0.256	0.261	0.265
$COV(1, 15, 4)$		$m = 1$	$m = 5$	$m = 10$	$m = 15$
	$\varphi_{\mathrm{H}k\_m\mathrm{DH}}$	8/29	8/25	8/20	8/15
	$AMSE_{\mathrm{H}k\_m\mathrm{DH}}$	0.125	0.126	0.127	0.128
$COV(1, 31, 5)$		$m = 1$	$m = 8$	$m = 16$	$m = 31$
	$\varphi_{\mathrm{H}k\_m\mathrm{DH}}$	10/61	10/54	10/46	10/31
	$AMSE_{\mathrm{H}k\_m\mathrm{DH}}$	0.062	0.0062	0.063	0.063
$COV(1, 63, 6)$		$m = 1$	$m = 18$	$m = 36$	$m = 63$
	$\varphi_{\mathrm{H}k\_m\mathrm{DH}}$	12/125	12/108	12/90	12/63
	$AMSE_{\mathrm{H}k\_m\mathrm{DH}}$	0.031	0.031	0.031	0.031
$COV(1, 127, 7)$		$m = 1$	$m = 40$	$m = 80$	$m = 127$
	$\varphi_{\mathrm{H}k\_m\mathrm{DH}}$	14/253	14/214	14/174	14/127
	$AMSE_{\mathrm{H}k\_m\mathrm{DH}}$	0.015	0.015	0.015	0.015

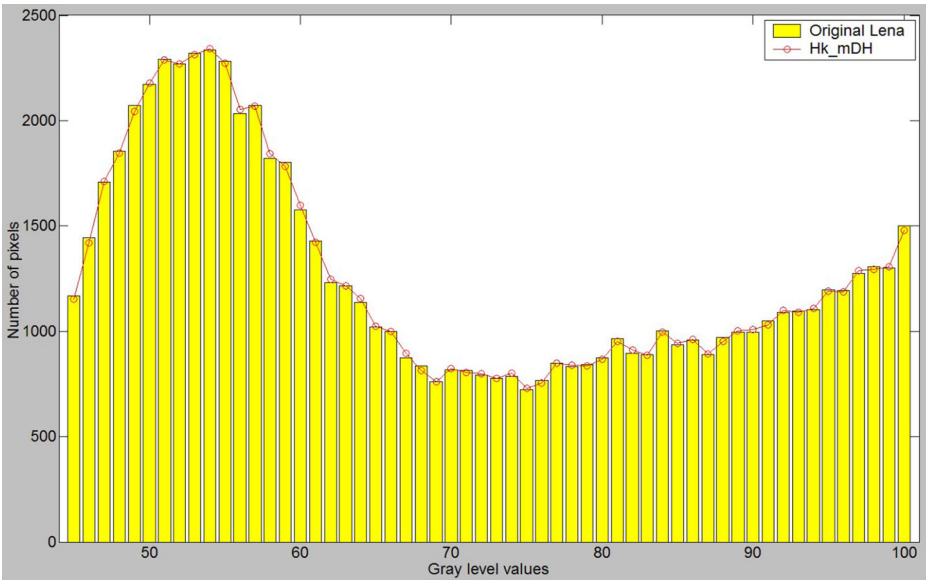


Fig. 8 Histogram of original Lena image (bars) and image modified using Hk_mDH (plots)

5 Conclusion

In this paper, we introduced Matrix coding based data hiding (MCDH) methods. Generally, the methods based on MCDH are superior in the aspect of efficiency. However, they are not higher ER than that of simple LSB method. To solve these problems, we proposed an optimization way to ER and image quality by OPAP and LSB. The proposed Hk_mDH was designed to trade ER off against the stego image quality by using the value of m. This property enabled that Hk_mDH can be used intended application for a specific purpose. For example, it may be secure communication. That is, it is possible to increase m when the size of the concealed data is large and to decrease m for the high PSNR. For example, if the value of m is reduced to a minimum, it can be used for secure communication applications. In the future, we will improve more performance both embedding capacity and PSNR for a cover image by upgrading Hk_mDH.

Acknowledgements This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by (2015R1D1A1A01059253), and was supported under the framework of international cooperation program managed by NRF (2016K2A9A2A05005255). Also, it was supported in part by Ministry of Science and Technology (MOST), under 105-2221-E-259-015-MY2.

References

1. Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. IBM Syst J 35(3-4):313–336
2. Bierbrauer J, Fridrich J (2008) Constructing good covering codes for applications in steganography. Transactions on Data Hiding and Multimedia Security III 4920:1–22
3. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37(3):469–474
4. Crandall R (1998) Some notes on steganography. http://dde.binghamton.edu/download/Crandall_matrix.pdf. Accessed 31 May 2018
5. Fridrich J, Goljan M (2002) Practical steganalysis of digital images - state of the art. In: Proceedings SPIE photonics west, electronic imaging , security and watermarking of multimedia contents. San Jose, California, January 1–13, vol 4675
6. Fridrich J, Lisoněk P, Soukal D (2007) On steganographic embedding efficiency. Lect Notes Comput Sci 4437:282–296
7. Image database ref., http://sipi.usc.edu/database/database.php? volume=misc. Accessed 31 May 2018
8. Kim C (2010) Data hiding based on compressed dithering images. Advances in Intelligent Information and Database Systems 283:89–98
9. Kim C, Shin D, Yang CN, Chou YS (2018) Improving capacity of Hamming (n, k)+1 stego-code by using optimized Hamming+k. Digital Signal Processing. https://doi.org/10.1016/j.dsp.2018.03.016, pp 1–9 (online 2 April)
10. Kim C, Yang CN (2016) Data hiding based on overlapped pixels using Hamming code. Multimed Tools Appl 75(23):15651–15663
11. Mielikainen J (2006) LSB matching revisited. IEEE Signal Proc Let 13(5):285–287
12. Stanley CA (2005) Pairs of values and the chi-squared attack. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.146.5017,1-45. Accessed 5 May 2018
13. Westfeld A (2001) F5 - a steganographic algorithm: high capacity despite better steganalysis. In: Proceedings of the 4th international workshop on information hiding, pp 289–302
14. Xia Z, Wang X, Sun X, Liu Q, Xiong N (2016) Steganalysis of LSB matching using differences between nonadjacent pixels. Multimed Tools Appl 75(4):1947–1962
15. Yang CN, Hsu SC, Kim C (2017) Improving stego image quality in image interpolation based data hiding. Computer Standards & Interfaces 50:209–215

16. Yang CN, Ye GC, Kim C (2011) Data hiding in halftone images by XOR block-wise operation with difference minimization. KSII Trans Internet Inf Syst 5(2):457–476
17. Zhang R, Sachnev V, Bakke BM, Kim HJ, Heo J (2012) An efficient embedder for BCH coding for steganography. IEEE T Inform Theory 58(12):7272–7279
18. Zhang W, Wang S, Zhang X (2007) Improving embedding efficiency of covering codes for applications in steganography. IEEE Commun Lett 11(8):680–682
19. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):781–783
20. Zhang X, Zhang W, Wang S (2007) Efficient double layered steganographic embedding. Electron Lett 43(8):482–483
21. Zhang Y, Jiang J, Zha Y, Zhang H, Zhao S (2013) Research on embedding capacity and efficiency of information hiding based on digital images. Int J Intell Sci 3:77–85

Cheonshik Kim received his B.S. degree in Computer Engineering from Anyang University, Korea, in 1995; his M.S. degree in Computer Engineering from Hankuk University of Foreign Studies (HUFS), Korea, in 1997; and his Ph.D. degree in Computer Engineering from HUFS in 2003. From March 2010, he was a professor of Department of Computer Science, Sejong University, Korea. From March 2013, he was a professor of Department of Digital Media Engineering, Anyang University, Korea. He won a research award from the IEEK in 2012. He has served as the Editor for ICACT Transaction on Advanced Communications Technology (TACT) since 2012. He served as program chair of the International conference, GPC 2013 and FutureTech 2014, IEEK Computer Society in various capacities, including Vice-President since 2010. He is a member of IEEE. His research interests include Multimedia Systems, Data Hiding, and Watermarking. His research is supported by NRF. He was a subject of biographical record in the marquis who's who in the world 2013 - 2018.

Dongkyoo Shin received a B.S. in Computer Science from Seoul National University, Korea, in 1986, an M.S. in Computer Science from Illinois Institute of Technology, Chicago, Illinois, in 1992, and a Ph.D. in Computer Science from Texas A&M University, College Station, Texas, in 1997. He is currently a Professor in the Department of Computer Engineering at Sejong University in Korea. From 1986 to 1991, he worked in Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he worked in the Multimedia Research Institute of Hyundai Electronics Co., Korea as a Principal Researcher. His research interests include XML based middleware, digital right management for multimedia, mobile Internet and ubiquitous computing.

Ching-Nung Yang obtained his Ph. D. degree in Electrical Engineering from National Cheng Kung University. His B.S. and M.S. degrees, both were awarded in Department of Telecommunication Engineering from National Chiao Tung University. Dr. Yang served in National Dong Hwa University since 1999. His current title is Professor in Department of Computer Science and Information Engineering. He had been Visiting Professor to University of Missouri Kansas City, University of Milan, and University of Tokyo. He is currently a Fellow of IET (IEE) and an IEEE senior member. Professor Yang has done extensive researches on visual cryptography and secret image sharing, and is the chief scientist in both areas. His areas of interest include error correcting code, multimedia security, cryptography, and information security. He has authored two books and has published over 200 (including more than 100 SCI-indexed papers) professional research papers in the areas of information security and coding theory.

Yung-Shun Chou is a graduate student at the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan. His research includes data hiding and coding theory.