A High-Capacity Image Data Hiding Based on Extended EMD-2 Reference Matrix

Xue-Jing Li, Yu-Qi Feng, and Wan-Li Lyu(✉)

Key Laboratory of Intelligent Computing and Signal Processing
of Ministry of Education, School of Computer Science and Technology,
Anhui University, Hefei 230039, China
xjalcatraz@outlook.com, luckymonicafe@gmail.com,
wanly_lv@163.com

Abstract. Numerous steganography algorithms have been proposed to protect messages put into images. LSB, which is an exceedingly prominent means in this field, has been proven to work if the least significant bit of the cover image is replaced with the binary secrets stream. Inspired by LSB, a series of simple but effective methods were proposed, such as LSB-MR, EMD (exploiting modification direction), Sudoku, EMD-2, Turtle Shell, and so on. Nonetheless, an image steganography with larger payload is tremendously needed nowadays. A novel high capacity image data hiding algorithm based on extended EMD-2 and Sudoku hybrid reference matrix is proposed in this study. In this method, each cover pixel pair carries two secret 9-ary notational system numbers. The experiment result shows the embedding rate of the method is up to 3.16 *bpp*, which is higher than the related schemes and the visual quality desired.

Keywords: Data hiding · Image steganography · Modification direction · Embedding capacity

1 Introduction

Generally, the carriers of digital steganography include character, still image, dynamic video, voice, and so on. In addition, the data hiding of digital images has been more popular in recent years due to the increasing transmission of pictures [1, 2]. The technology was increasingly used to protect military information, but now is applied to most areas of people's life, especially to messages transmitted via the Internet [3]. The basic criteria to evaluate an image data hiding algorithm are ER (embedding rate) and PSNR (peak signal-to-noise ratio). Embedding capacity is estimated by ER while PSNR evaluates the visual quality of steganographic images. Furthermore, image quality interacts with the embedding payload [4]. A high capacity image steganography algorithm tends to gain a relatively poor image visual quality; hence it is a main focus where researchers seek new schemes, such as [5–7].

The classic algorithm LSB (the least significant bit replacement method) [8] was proposed by Turner in 1989, replacing the least significant bits to hide secret bits simply and efficiently. Nevertheless, the substitution bits can be detected through uncomplicated analysis. Then, a series of schemes are put forward, which are motivated

T. Tan et al. (Eds.): IGTA 2016, CCIS 634, pp. 51–61, 2016.
DOI: 10.1007/978-981-10-2260-9_7

by LSB substitution. Mielikainen proposed the LSB-MR (LSB matching revisited) algorithm in 2006 [9]. Although the hiding capacity in LSB-MR is as much as LSB, the modification equation $f(p_1, p_2) = LSB(p_1/2 + p_2)$ is changed, aiming to enhance security. In this method, two pixels (p_1, p_2) act as an embedding unit to hide two bits of secret messages, only one pixel of the embedding unit needs to be modified.

Subsequently, Zhang and Wang brought up an improved scheme named EMD (exploiting modification direction) [10], where each digit in the $(2n + 1)$-ary notational system is embedded by modifying, at most, one in the group of n cover pixels to obtain a higher embedding efficiency. The embedding payload is up to $\log_2(2n + 1)/n$ *bpp*. Chang et al. proposed put forward a novel Turtle Shell based method for image data hiding [11] whose embedding capacity is proved to be 1.50 *bpp*. In 2008, a new data hiding algorithm was proposed by Chang et al., named Sudoku [12]. The directions of modification have more selections compared to EMD, in order to obtain high embedding payload with minimal distortion. This method can hide a digit in the base-9 numeral system using two cover pixels, so the ER is up to $\log_2 9/2$ *bpp*. Soon after this algorithm became well-known, in 2010, Kim et al. put forward the EMD-2 method [13] allowed to modify at most two of n pixels in a base-$(10n - 13)$ $(n > 2)$ numeral system; namely, there are two values of pixels that can be increased or decreased by 1. So the embedding capacity increases to $\log_2(10n - 13)/n$ *bpp* $(n > 2)$. Later, a mass of algorithms come forward, but the embedding rate is limited to 1.58 *bpp*.

In this paper, a novel high-capacity image data hiding scheme called E-EMD2 (Extended EMD-2), which has the desired visual quality is discussed. This algorithm is based on an extended EMD-2 and Sudoku hybrid reference matrix $\boldsymbol{M}^*$, more momentously, the embedding capacity is much higher than anyone mentioned. The hybrid key matrix $\boldsymbol{M}^*$, whose abscissa and ordinate values range from 0 to 255, is generated by several unique Sudoku grids, which will be expounded on in Sect. 3 at great length. Every paired pixel can locate an appropriate element by guiding two 9-ary notational system digits to be embedded into matrix in the $\boldsymbol{M}^*$ meanwhile. Therefore, we can utilize a pair of cover image pixels to hide the secret image data twice to enhance the embedding payload, which increases up to $\log_2 9$ *bpp*. To exemplify our point, numerous experiments have been performed and corresponding results show the merits of this algorithm compared with others, which concretely reflect the high capacity with the desired visual quality.

The rest of the paper is organized as follows. Section 2 briefly introduces the related schemes including EMD, Sudoku and EMD-2, and Sect. 3 is the proposed method described in detail. The experiment results and conclusion will be stated in Sects. 4 and 5, respectively.

2 Related Work

2.1 EMD Method

A novel steganography method EMD, put forward by Zhang and Wang [10], converts secret messages into a sequence of digits in a $(2n + 1)$-ary notational system before the embedding procedure. In addition, every base-$(2n + 1)$ digit is carried by n pixels.

In this method, at most one pixel needs to alter its value by increasing or decreasing 1. So there are $(2n+1)$ possible ways to modify each cover pixel pair, including one way without modification. Additionally, the embedding and extraction formula f_1 is described by Eq. (1).

$$y = f_1(p_1, p_2, \cdots, p_n) = \left[\sum_{i=1}^{n} p_i \times i\right] mod(2n+1) \tag{1}$$

In Eq. (1), y is calculated by the sum of weights module $(2n+1)$, and pixels in the cover image are divided into a series of groups where $(p_1, p_2, \cdots, p_n)$ are gray values of pixels in a group, i.e., p_i is the i - th pixel.

The embedding procedure is described as follows. If a $(2n+1)$-ary numeral system secret digit $d = y$, then there is no embedding modification of directions that needs to be done, else compute $t = (d-y)mod(2n+1)$. Afterwards, increase the value of p_t by 1 while t is no more than n, otherwise, decrease the value of p_{2n+1-t} by 1.

By means of formula f_1, the receiver can easily retrieve the secret digit d. In the extraction procedure, when all of the secret digits have been calculated, they will be combined into a base-$(2n+1)$ notational system embedding sequence, which is converted from the original secret messages.

Experiment results prove the ER of the EMD method is up to 1.59 *bpp* when $n = 1$ and 1.16 *bpp* when $n = 2$. In a nutshell, the embedding payload and security have great improvement when compared with the LSB method.

2.2 Sudoku Method

Sudoku, another image data hiding algorithm proposed by Chang et al. [12], improves the EMD method in embedding capacity. This scheme's reference matrix is generated by a logic-based number placement Sudoku puzzle where every 9×9 grid is filled with the digits from 0 to 8. In a nutshell, the principal idea of this proposed method is to modify a pair of cover pixels according to the secret digit's candidate positions in a key matrix with minimum distortion.

The concrete embedding and extraction procedures are exhibited as follows. First and foremost, we calculate three sets of candidate elements CE_H, CE_V and CE_B, which are separately defined as the following regulations. For each cover pixel pair (p_i, p_{i+1}), the corresponding row and column elements in the Sudoku matrix, whose center digit is $M(p_i, p_{i+1})$, are unrepeated digits from 0 to 8. $M(p_i, p_{i+1})$ is the location of the two contiguous cover pixels, p_i and p_{i+1}, in the Sudoku reference matrix. Therefore, they compose the element sets CE_H and CE_V, which is presented in Eq. (2), where k is selected from $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.

$$\begin{cases} CE_H = \{M(p_i, p_{i+1} + k)\} \\ CE_V = \{M(p_i + k, p_{i+1})\} \end{cases} \tag{2}$$

$$CE_B = \begin{bmatrix} M(x_b, y_b) & M(x_b, y_b+1) & M(x_b, y_b+2) \\ M(x_b+1, y_b) & M(x_b+1, y_b+1) & M(x_b+1, y_b+2) \\ M(x_b+2, y_b) & M(x_b+2, y_b+1) & M(x_b+2, y_b+2) \end{bmatrix} \tag{3}$$

Ultimately, CE_B is defined as the surrounding elements set shown as Eq. (3), in the center of which is digit $M(p_i, p_{i+1})$. In Eq. (3), $x_b = 3 \times p_i/3$ while $y_b = 3 \times p_{i+1}/3$. Then, we will select three candidate elements from CE_H, CE_V, and CE_B, whose values equal the secret digit. After comparison, the ultimate modified location with minimum distortion is confirmed.

In summary, the embedding payload (i.e., 1.58 *bpp*) and security are both significantly improved due to the various Sudoku matrixes, while the visual quality of steganographic images is also satisfying with nearly 45 *db* on average.

2.3 EMD-2 Method

To enhance the embedding capacity and to relatively improve image quality, Kim et al. put forward an exceedingly efficient information hiding scheme named EMD-2 scheme [13] in 2010. It allows for modification, at most, of two pixels' value by increasing or decreasing 1 in order to embed every secret digit transformed into $(2w+1)$-ary notational system. In addition, w equals 4 when n = 2, otherwise, the w value is $8+5(n-3)$ while $n > 2$. Equation (4) is used to describe the embedding and extraction formula f_2.

$$y = f_2(p_1, p_2, \cdots, p_n) = \left[\sum_{i=1}^{n} p_i \times b_i\right] mod(2w+1) \tag{4}$$

In Eq. (4), $(p_1, p_2, \cdots, p_n)$ is an n-dimension vector P_n composed of n pixels in a cover image, while b_i is defined as following Eq. (5).

$$[b_1, b_2, \cdots, b_i, \cdots, b_n] = \begin{cases} [1,3] & n = 2 \\ [1, 2, \cdots, 6+5(n-3)] & n > 2 \end{cases} \tag{5}$$

If secret digit $d = y$, then none of the pixel value modifications need to be done. Else, we need to compute $t = (d-y) mod(2w+1)$ and then select appropriate $t's$ n-dimension basis vector $P_t = (t_1, t_2, \cdots, t_i, \cdots, t_n)$ which makes Eq. (6) hold, where the conceivable options of t_i are selected from $\{1, 0, -1\}$. Eventually, the n-dimension pixels modified vector P'_n can be obtained by calculating the sum of P_n and P_t.

$$t = \left[\sum_{i=1}^{n} t_i \times b_i\right] mod(2w+1) \tag{6}$$

The receiver can expediently figure out the formula f_2 with the modified pixels' value and combine them into the original secret message. To summarize, this method has great amelioration in carrying payload compared with EMD. Nevertheless, the embedding rate is limited to 1.58 *bpp* while n = 2.

3 Proposed Scheme

As there are limited modification directions in previous reference matrixes, the payload of embedding secrets is not satisfied. Here, we present a novel high capacity image steganography method at great length, which is based on an extended EMD-2 and Sudoku hybrid reference matrix $\boldsymbol{M}^*$. Aiming at obtaining the higher embedding payload with a desired image visual quality, we make full use of the proposed matrix $\boldsymbol{M}^*$ generated by 9-ary notational system via modifying paired pixels twice. Namely, this two-dimensional key matrix $\boldsymbol{M}^*$ needs to guide two base-9 numeral digits to be embedded into the paired pixels.

3.1 Reference Matrix

The high-capacity proposed algorithm utilizes an extended EMD-2 and Sudoku hybrid two-dimensional reference matrix $\boldsymbol{M}^*$ whose abscissa and ordinate values range from 0 to 255. The entire matrix consists of several 9-ary digital system 27×9 grids, where every 3×3 sub-grid encompasses all base-9 digits from 0 to 8 and any nine adjacent sub-grids can constitute a 9×9 Sudoku puzzle. More momentously, the middle digits of the 3×3 sub-grids in every Sudoku puzzle are nine unrepeated continuous base-9 numeral digits. All of the 3×3 sub-grids' middle figures compose the EMD-2 two-dimensional key matrix once again. The formative 256×256 reference matrix $\boldsymbol{M}^*$ is shown in Fig. 1.

Definition 1. The concrete location of a cover pixel pair $\left(\mathrm{p_x}, \mathrm{p_y}\right)$ in key matrix $\boldsymbol{M}^*$ can be computed according to Eq. (7), where formulas F and R are defined as $F(x) = x/3$ and $R(x, y) = xmody$, respectively.

$$M\left(p_x, p_y\right) = R\left(\left[F\left(R\left(p_y, 27\right), 3\right) + R(p_x, 9) + 3R\left(p_y, 3\right) - 1\right], 9\right) \tag{7}$$

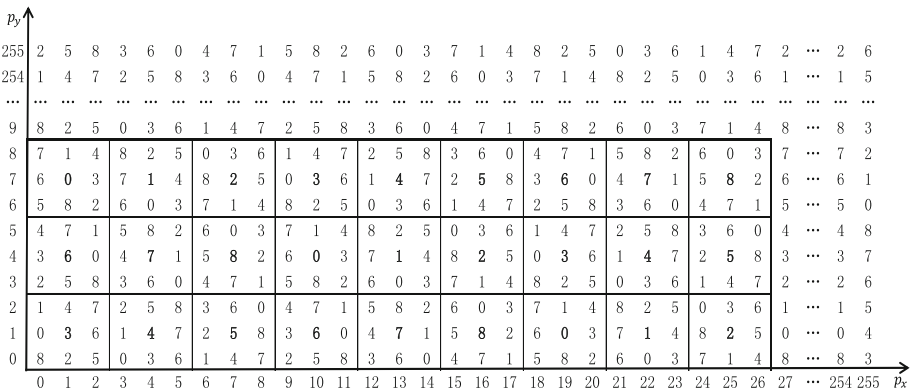

Fig. 1. The 256×256 reference matrix $\boldsymbol{M}^*$

Definition 2. Every 3×3 sub-grid can be regarded as a box denoted by $B(b_x, b_y)$, which contains nine $M(p_x, p_y)$ elements and $p_x \in \{3b_x, 3b_x + 1, 3b_x + 2\}$ and $p_y \in \{3b_y, 3b_y + 1, 3b_y + 2\}$. We utilize the center digit of each box to indicate its value, i.e., $B(b_x, b_y) = M(3b_x + 1, 3b_y + 1)$, as the overstriking character shown in Fig. 1. For instance, $B(0,0) = M(1,1) = 3$ while $B(1,2) = M(4,7) = 8$. To summarize, every cover pixel pair (p_x, p_y) pertains to a 3×3 box named $B(b_x, b_y)$ where b_x and b_y can be computed as Eq. (8).

$$\begin{cases} b_x = p_x/3 \\ b_y = p_y/3 \end{cases} \tag{8}$$

Definition 3. All center elements in the boxes constitute a two-dimensional EMD-2 reference matrix $\boldsymbol{R}^*$, as indicated in Fig. 2. Hence, the circumambient boxes for each $B(b_x, b_y)$ compose a new 3×3 cell defined as Eq. (9), where b_x and b_y are calculated anteriorly by Eq. (8).

$$C(b_x, b_y) = \begin{bmatrix} B(b_x - 1, b_y - 1) & B(b_x - 1, b_y) & B(b_x - 1, b_y + 1) \\ B(b_x, b_y - 1) & B(b_x, b_y) & B(b_x, b_y + 1) \\ B(b_x + 1, b_y - 1) & B(b_x + 1, b_y) & B(b_x + 1, b_y + 1) \end{bmatrix} \tag{9}$$

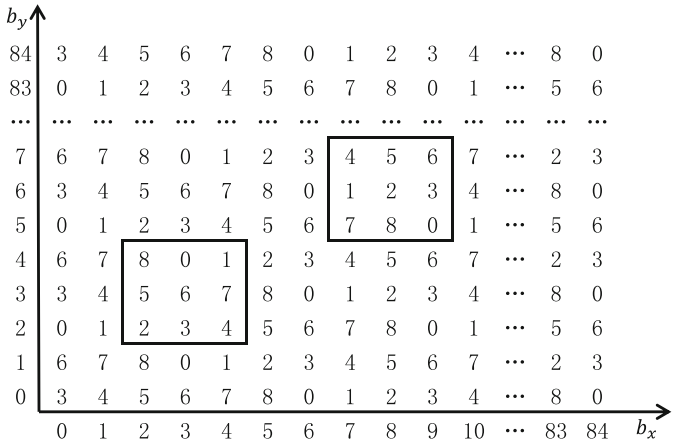

Fig. 2. The 85×85 sub-matrix $\boldsymbol{R}^*$

For each cell $C(b_x, b_y)$, the element boxes are all 9-ary notational system digits that are unrepeated and continuous; additionally, the range is from 0 to 8.

3.2 The Embedding Phase

In the reference hybrid matrix $\boldsymbol{M}^*$, each 3×3 box is constituted of base-9 digits and the nine adjacent boxes can compose a Sudoku puzzle. Furthermore, all of the middle numbers of the boxes generate a new sub-matrix $\boldsymbol{R}^*$, which is a EMD-2 two-dimension key matrix. Initially, the size of the designated gray-level cover image I and stego image I' are similarly $H \times W$, which are the height and width of I, respectively. The embedding algorithm is indicated as following steps.

Input: Cover grayscale image I, secret digit stream S, and reference matrix $\boldsymbol{M}^*$.
Output: Steganographic grayscale image I'.
Step 1. Convert the binary secret stream $S = (b_1, b_2, \cdots, b_L)$ into 9-ary notational system digits, i.e., $(b_1, b_2, \cdots, b_L)_2 = (s_1, s_2, \cdots, s_{H\times W})_9$ where $L = H \times W \times \log_2 9$. Then carry out Step 2.
Step 2. Initialize $i = 1$ and then proceed to Step 3.
Step 3. Locate the specific element $M(p_i, p_{i+1})$ in the reference matrix $\boldsymbol{M}^*$ for each cover pixel pair (p_i, p_{i+1}), which computing method is in accordance with Eq. (7). Moreover, according to Definition 2, the located element $M(p_i, p_{i+1})$ pertains to a box $B(b_x, b_y)$ where $b_x = p_i/3$ and $b_y = p_{i+1}/3$. Afterwards, move to Step 4.
Step 4. Read the converted secret digit stream $(s_i, s_{i+1})_9$. If $s_i = B(b_x, b_y)$, no modification of directions is required; else, select the appropriate box $B\left(b'_x, b'_y\right)$ whose value equals s_i, according to Eq. (9). Continue to Step 5.
Step 5. Judge the value of s_{i+1}, if $B\left(b'_x, b'_y\right) = s_{i+1}$, maintain the status quo. Otherwise, choose the applicable element $M\left(p'_i, p'_{i+1}\right)$ in the 3×3 box $B\left(b'_x, b'_y\right)$, where $s_{i+1} = M\left(p'_i, p'_{i+1}\right)$. Ultimately, $(s_i, s_{i+1})_9$ is embedded into the cover pixel pair (p_i, p_{i+1}) simultaneously, which satisfies Eq. (10). Next, move to Step 6.

$$\begin{cases} s_i = B\left(b'_x, b'_y\right) \\ s_{i+1} = M\left(p'_i, p'_{i+1}\right) \end{cases} \tag{10}$$

Step 6. Set $i = i + 2$ and repeat Steps 3 to 5 through the end of the secret stream.

Instance 1. Embedding the secret stream

Presume the original binary secret stream S is $(1111)_2$ and the cover grayscale pixel pair (p_i, p_{i+1}) is $(6, 7)$. First and foremost, the binary secret messages S need to be converted into base-9 numeral system digits, i.e. $(s_i, s_{i+1}) = (16)_9$. Ultimately, we locate an accurate point $M(6, 7) = 1$ in the reference matrix $\boldsymbol{M}^*$ according to Eq. (7). In addition, $M(6, 7)$ belongs to box $B(2, 2)$, which can be computed by Eq. (8). Because the value of $B(2, 2)$ is equal to $M(7, 7) = 2 \neq s_i$, we thus seek through the 3×3 cell $C(2, 2)$ in sub-matrix $\boldsymbol{R}^*$ to obtain the proper box element, which is $B(2, 1) = M(7, 4) = 1 = s_i$. After modifying the cover pixels for the first time, the current location in the key matrix $\boldsymbol{M}^*$ is $M(7, 4) = 1$, which isn't identical to s_{i+1}. Therefore, check the other eight elements around $M(7, 4)$ in box $B(2, 1)$ to seek out a

final position $M(p'_i, p'_{i+1})$ that satisfies equality $s_{i+1} = M(p'_i, p'_{i+1}) = 6$. Ultimately, the stego image I' is obtained by recomposing the cover pixels' value to $M(6,3)$ in order to conceal the secret digits $(16)_9$.

3.3 The Extraction Phase

Similarly, the secret messages S can be exactly retrieved from the received steganographic image I' by means of the following extraction algorithm. Since the size of the stego grayscale image I' is also $H \times W$ defined as above, the extracted secret stream S is no more than $H \times W \times \log_2 9$.

Obtain stego pixel pair (p'_i, p'_{i+1}) from grayscale steganographic image I' and calculate current location $M(p'_i, p'_{i+1})$ by using Eq. (7) to identify the hidden secret digit s_{i+1}. Compute the box $B(b'_x, b'_y)$ that $M(p'_i, p'_{i+1})$ pertains to, in accordance with $b'_x = p'_i/3$ and $b'_y = p'_{i+1}/3$, so that $s_i = B(b'_x, b'_y)$. Hence, the two embedded base-9 secrets are extracted similarly as in Eq. (10). Until all the stego pixels have been traversed and the extraction tasks are finished, we convert the extracted 9-ary numeral system digits into the original binary secret stream S, i.e., $(s_1, s_2, \cdots, s_{H\times W})_9 = (b_1, b_2, \cdots, b_L)_2$ in which L is equal to $H \times W \times \log_2 9$.

Instance 2. Extracting the secret stream

Assume the obtained pair of stego pixels (p'_i, p'_{i+1}) is $(6,3)$, and the values of $M(p'_i, p'_{i+1})$ and corresponding $B(b'_x, b'_y)$, where $b'_x = 2$ and $b'_y = 1$, both can be simply calculated according to Eqs. (7) and (8), i.e., $M(6,3) = 6$ while $B(2,1) = 1$. We extract the embedded secret 9-ary digits satisfied by Eq. (10), so $(s_i, s_{i+1})_9 = (16)_9$. After converting this into a binary numeral stream, the original secret messages are presented as $(b_i, b_{i+1})_2 = (s_i, s_{i+1})_9 = (16)_9 = (1111)_2$.

4 Experimental Results

To certify the performance of the proposed method, we used eight grayscale cover images of the common size 512×512, and all experiments were performed using MATLAB R2014a software.

In this experiment, the embedding payload rate (ER) and the peak signal to noise ratio (PSNR) are two criteria used to evaluate the implementation result, which represents the payload capability and image visual quality, respectively. The PSNR of an $H \times W$ grayscale image is calculated by Eq. (11), where x_{ij} indicates the value of cover image's pixel and $\bar{x}_{ij}$ denotes the steganographic image pixel's value.

$$PSNR = 10 \times log_{10} \frac{255^2}{\frac{1}{H\times W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} \left(x_{ij} - \bar{x}_{ij}\right)^2} \tag{11}$$

Additionally, the ER of an $H \times W$ cover image is described as Eq. (12) at length. Here, $\|S\|$ is a statistical value denoting the total sum of the embedded secret digits.

$$ER = \frac{\|S\|}{H \times W} \tag{12}$$

As a result, the ER of all hiding methods above can be simply computed using Eq. (12). Because the EMD method can hide a base-$(2n+1)$ numeral system digit in n pixels, $ER_{EMD} = log_2(2n+1)/n\ bpp$, i.e., while $n = 2$, the ER of EMD is merely equal to 1.16 *bpp*. The Turtle Shell Method enhances the hiding capacity compared to EMD since $ER_{Turtle\ Shell} = log_2 8/2 = 1.50\ bpp$. $ER_{Sudoku} = log_2 3\ bpp$, which is nearly up to 1.58 *bpp*. The hiding capacity of proposed algorithm is greater than the former, as it can embed two digits in base-9 into two pixels simultaneously. Therefore, $ER_{E-EMD2} = log_2 9\ bpp$, which is approximately equal to 3.16 *bpp*. It is obvious that our method has been proven to provide the best results.

The visual quality of the experimental images implemented by this proposed algorithm is shown as in Fig. 3. In summary, there are eight steganographic grayscale images to exemplify the ER and the corresponding PSNR of the proposed method in this study. The following Table 1 shows the PSNR and the corresponding embedding rate of different steganography algorithms. Experiment results show the ER of our proposed method is up to 3.16 *bpp*, while the PSNR average approaches 39.62 *db*.

The above experiment results indicate that the embedding payload capability of this proposed scheme is much higher than other related works. Meanwhile, it still offers an acceptable visual quality. On account of the concession we made in image quality, the novel method stands out in obtaining a much higher payload in the embedding rate when compared to other published works previously mentioned.

Group a. Tiffany, Baboon, Zelda and Barbara

Group b. Bridge, Goldhill, Lena and Pepper

Fig. 3. Steganographic images after embedding secrets with the proposed algorithm using Tiffany, Baboon, Zelda, Barbara, Bridge, Goldhill, Lena and Pepper grayscale images

Table 1. Comparisons of ER and corresponding PSNR of the proposed scheme and related reference-matrix-based schemes

Images	EMD [10]		Turtle Shell [11]		Sudoku [12]		Proposed	
	PSNR (*db*)	ER (*bpp*)	PSNR (*db*)	ER (*bpp*)	PSNR (*db*)	ER (*bpp*)	PSNR (*db*)	ER (*bpp*)
Tiffany	52.11	1.16	49.41	1.50	45.02	1.58	39.61	3.16
Baboon	52.11	1.16	49.39	1.50	44.68	1.58	39.63	3.16
Zelda	52.12	1.16	49.40	1.50	44.96	1.58	39.62	3.16
Barbara	52.11	1.16	49.40	1.50	44.77	1.58	39.61	3.16
Bridge	52.12	1.16	49.42	1.50	44.62	1.58	39.62	3.16
Goldhill	52.11	1.16	49.38	1.50	44.84	1.58	39.61	3.16
Lena	52.12	1.16	49.42	1.50	44.97	1.58	39.63	3.16
Pepper	52.12	1.16	49.40	1.50	44.67	1.58	39.62	3.16

5 Conclusions

A novel high-capacity image steganography based on the extended EMD-2 and Sudoku hybrid reference matrix is reviewed in this study, which concurrently embeds two base-9 notational system digits into paired pixels. From the above experiment results, we have concluded that the proposed method can obtain a large payload and a relatively desired image visual quality; more specifically, the ER and corresponding PSNR are 3.16 *bpp* and 39.62 *db*, respectively.

Acknowledgements. This research work is supported by Provincial Training Projects of Innovation and Entrepreneurship for Undergraduates of Anhui University, which is under Grant No. J1018515315. The corresponding experiment results is with the help of key laboratory of intelligent computing and signal processing of ministry of education.

References

1. Bender, W., Gruhl, D., Morimoto, N., Lu, A.: Techniques for data hiding. IBM Syst. J. **35**, 313–336 (1996)
2. Zielinska, E., Mazurczyk, W., Szczypiorski, K.: Trends in steganography. Commun. ACM **57**(3), 86–95 (2014)
3. Ker, A.D.: Improved detection of LSB steganography in grayscale images. In: Fridrich, J. (ed.) IH 2004. LNCS, vol. 3200, pp. 97–115. Springer, Heidelberg (2004)
4. Fridrich, J., Soukal, D.: Matrix embedding for large payloads. IEEE Trans. Inf. Forensics Secur. **1**(3), 390–394 (2006)
5. Chao, R.M., Wu, H.C., Lee, C.C.: A novel image data hiding scheme with diamond encoding. EURASIP J. Inf. Secur. **2009**, 1–9 (2009)
6. Hong, W., Chen, T.S.: A novel data embedding method using adaptive pixel pair matching. IEEE Trans. Inf. Forensics Secur. **7**(1), 176–184 (2012)

7. Hong, W.: Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique. Inf. Sci. **221**(1), 473–489 (2013)
8. Turner, L.F.: Digital data security system. Patent IPN, WO89/08915 (1989)
9. Mielikainen, J.: LSB matching revisited. IEEE Sig. Process. Lett. **13**(5), 285–287 (2006)
10. Zhang, X., Wang, S.: Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett. **10**(11), 781–783 (2006)
11. Chang, C.C., Liu, Y., Nguyen, T.: A novel turtle shell based scheme for data hiding. In: 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP-2014), Kitakyushu, Japan, pp. 89–93 (2014)
12. Chang, C.C., Chou, Y.C., Kieu., T.D.: An information hiding scheme using Sudoku. In: Proceedings of 3rd International Conference on Innovative Computing, Information and Control, pp. 17–21 (2008)
13. Kim, H.J., Kim, C., Choi, Y., Wang, S., Zhang, X.: Improved modification direction methods. Comput. Math Appl. **60**(2), 319–325 (2010)