Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **4**, July **2017**

A Multiple Image Based Reversible Data Hiding Scheme with High Embedding Capacity

Ying-Hsuan Huang[1] and Ching-Chun Chang[2,*]

[1]Aeronautical Systems Research Division
National Chung-Shan Institute of Science and Technology, Taichung 40722, Taiwan, R.O.C.
ying.hsuan0909@gmail.com

[2]Department of Computer Science, University of Warwick
Conventry CV4 7AL, UK
yinghsuan740909@gmail.com

Received October, 2016; revised March, 2017

Abstract. *In recent years, reversible data hiding methods using dual stego images have been proposed extensively. In order to embed more secret data, we proposed a reversible data hiding method that can embed secret data into M stego images, where $M \geq 2$. The pixel in M stego images can be used to embed N secret bits. The embedding capacity becomes greater as N and M increase, where N means the number of bits embedded in a pixel. However, directly embedding N secret bits into one pixel always causes serious distortion. In order to avoid this issue, we proposed an effective and efficient method that can encode a set of N secret bits as one smaller decimal number. Embedding the decimal number into the pixel does not cause serious distortion, and our experimental results showed that the proposed method can embed more secret bits than other methods. For the same embedding rate, the proposed method provides better image quality than other methods. In addition, the execution time of the proposed method is less than that of other methods.*
Keywords: Stego images, Reversible data hiding, Embedding rate, Image quality.

1. **Introduction.** The rapid development of communication technology has made the activities of daily life more and more convenient. However, hackers may be able to intercept and steal digital data when they are being transmitted. Thus, reversible data hiding, which embeds secret data into a cover image, was proposed as a means of thwarting hackers. Only the legal receiver can extract the secret data correctly and recover the original image losslessly.

The data embedding domains are classified, i.e., the frequency domain [1, 20] and the spatial domain [2-7, 9-19, 21, 22]. In the frequency domain, the cover pixels are transformed into coefficients. The coefficients in the low-frequency domain remain unchanged to avoid serious distortion of the image. Only the coefficients in the high-frequency domain can be used to embed secret data. In addition, the transformation of pixels increases the computational cost.

Reversible data hiding methods can be classified into four types, i.e., difference expansion [16], prediction error expansion [17-18], histogram shifting [12] and dual stego images [2, 3, 4, 13]. In 2003, Tian [16] proposed the difference expansion method, which expanded the difference between two adjacent pixels to embed one secret bit. However, there are

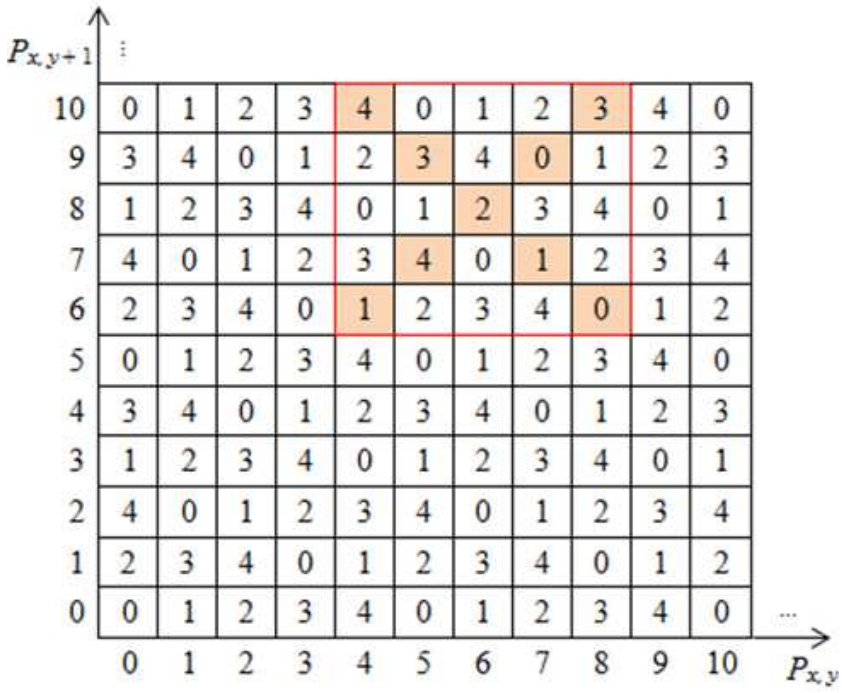

FIGURE 1. A portion of the modulus function matrix

some larger differences in the complex region of the cover image. Expanding these differences causes serious distortion of the image. To solve this problem, Thodi and Rodriguez [17] used inherent edge-detection predictor to generate the prediction value of the cover pixel, the prediction error of which is significantly smaller than the difference between two adjacent pixels. Consequently, expanding the prediction errors only generates slight distortion of the image.

Different from the above method, Ni *et al.* [12] proposed a histogram-shifting method. In the histogram, the cover pixel that occurred most frequently is denoted as the peak point, and the cover pixel with zero frequency is denoted as the zero point. The cover pixels in the range from the peak point through the zero point are modified to embed secret data.

In 2007, Chang *et al.* proposed a modulus function matrix method to embed secret data into two stego images. In their method, the modulus function matrix was established by $M(P_{x,y}, P_{x,y+1}) = (P_{x,y} + 2P_{x,y+1}) \bmod 5$, where $P_{x,y}$ and $P_{x,y+1}$ denote a pair of cover pixels, and $0 \leq P_{x,y}, P_{x,y+1} \leq 255$. Fig. 1 shows part of the modulus function matrix. According to $M(P_{x,y}, P_{x,y+1})$ and the left and right diagonals of the modulus function matrix, two based-5 secret digits were embedded into two pairs of stego pixels. For example, a pair of cover pixels $\{P_{x,y}, P_{x,y+1}\}$ is $\{6, 8\}$, and the two secret digits are 3 and 1, respectively. The first secret digit, 3, was matched from the left diagonal of $M(6, 8)$, and its corresponding pixels $\{5, 9\}$ are used as the stego pixels of the first image. Afterwards, the second secret digit, 1, was matched from the right diagonal, and its corresponding pixels $\{4, 6\}$ are used as the stego pixels of the second image. We find that the maximum modification level of a pair of cover pixels is 4. In order to reduce the modification level, Chang *et al.* changed the embedding method from the left and right diagonals to the horizontal and vertical lines. The method only modified one of two cover pixels and reduced the modification level from 4 to 2.

The above two methods only embedded a based-5 secret digit into a pair of pixels. In order to embed more secret data, Chang *et al.* applied a magic matrix method to embed

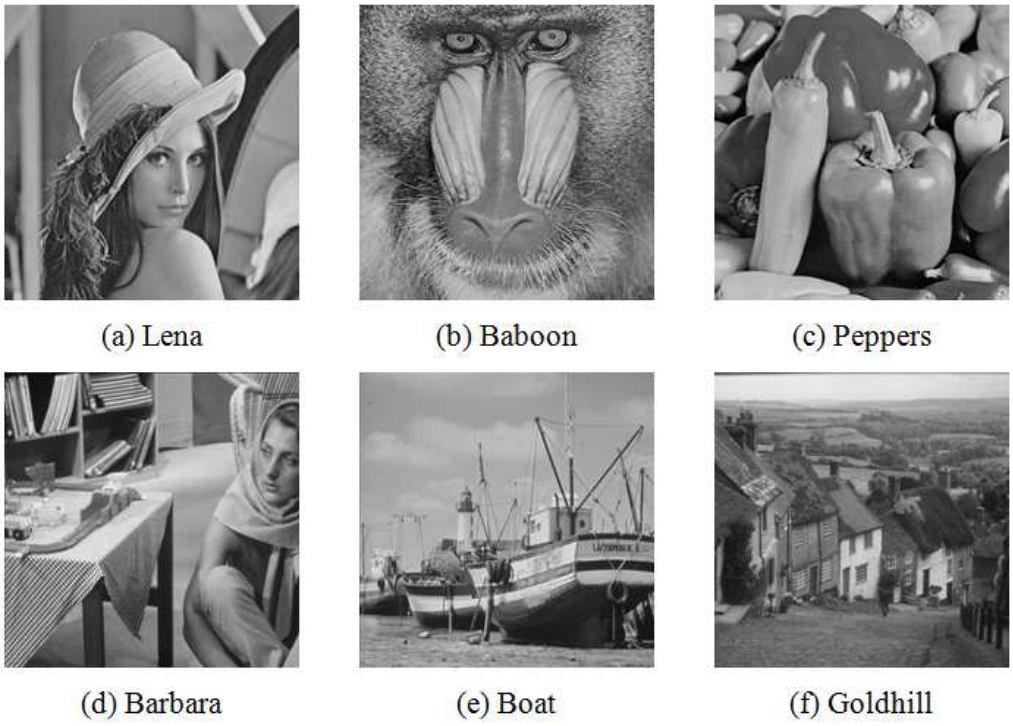

FIGURE 2. Six grayscale images, each of which consists of 512×512

based-9 secret digits into two stego images. The magic matrix was established by $M(P_{x,y}, P_{x,y}) = (P_{x,y} + 3P_{x,y}) \bmod 9$. The secret digits were embedded into two stego images by the right diagonal of the magic matrix.

In 2015, Lu *et al.* applied an LSB matching method to embed a large amount of secret bits into two stego images. In their method, only one of two pixels was increased or decreased by 1. However, some modified pixels cannot be recovered to the original pixel. In order to solve this problem, these pixels were modified further, which decreases the quality of the stego image.

In contrast to the above-mentioned methods, Lu *et al.* proposed a center-folding strategy to reduce the value of the secret message. The reduced values are embedded uniformly into two stego images, thus the visual quality of each stego image is satisfactory. However, the center-folding strategy increases the computation cost, and two stego images limit the hiding capacity. In this paper, we proposed an efficient method for encoding the secret bits and a reversible data hiding method to embed secret data into M stego images.

2. Proposed Method.

Although the center-folding strategy can reduce the distortion of the stego image, its computational cost is greater. The maximum hiding capacity of Lu *et al.*'s method is only $2 \times N \times W \times H$ bits. In order to reduce the computational cost and embed more secret bits, we proposed a novel and efficient method for encoding the secret data and a reversible data hiding method that can embed $(M-1) \times N \times W \times H$ secret bits into M stego images.

2.1. Secret Data Encoding.

In the proposed method, one pixel can be used to embed N secret bits. However, directly embedding N secret bits into the pixel may cause serious distortion of the image. Consequently, we proposed a novel method for encoding data that effectively can encode the small value of N secret bits to reduce the distortion of the image. The encoding method is described below.

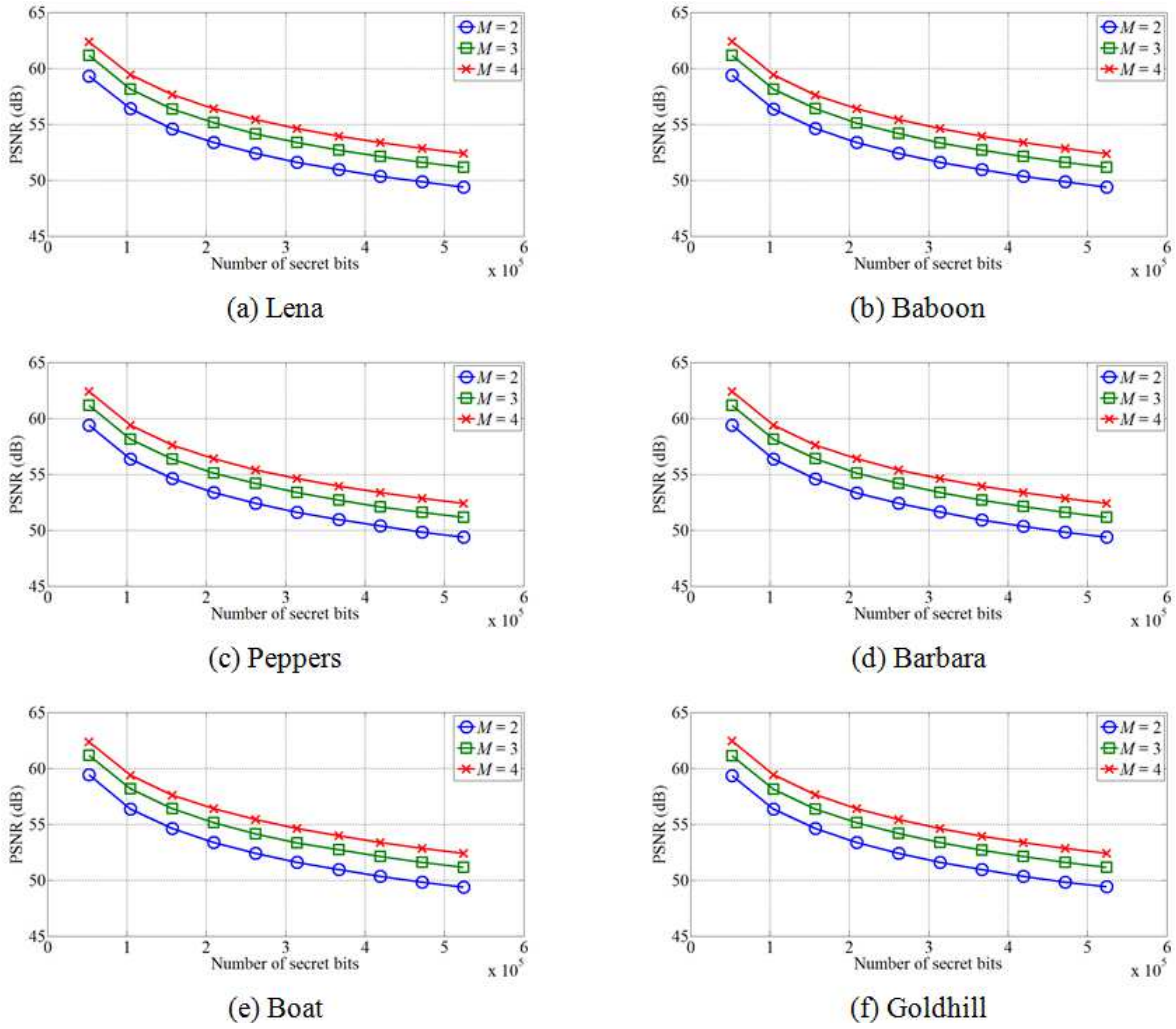

FIGURE 3. Comparison of PSNR values for various values of M

Let $B_k = \{b_1, b_2, ..., b_N\}$ be a set of N secret bits, where k denotes its identification (ID) number. The first bit b_1 in B_k is used as the signal value of the encoded secret digit s_k. If $b_1 = 0$, then s_k is set to be a positive integer; otherwise, s_k is set to be a negative integer. Afterwards, s_k can be derived by

$$s_k = \begin{cases} -2^{N-1}, & \text{if } b_1 = 1 \text{ and } b_t = 0, \\ \sum_{t=2}^{N} 2^{N-t} \times b_t, & \text{if } b_1 = 0, \\ -\sum_{t=2}^{N} 2^{N-t} \times b_t, & \text{otherwise.} \end{cases}$$

2.2. **Data Embedding.** Before the data hiding, the random seed RS is generated by the private keys of M participants, i.e., $RS = \sum_{l=1}^{M} PK_l$, where $M > 1$, and PK_l denotes the private key. The RS can be used to generate a random sequence $R = \{r_1, r_2, ..., r_{H \times W}\}$, where $0 \leq r_i \leq 1$, and H and W denote the height and the width of the cover image, respectively. The random value r_i in R is normalized to determine the embedding position, i.e., $\hat{r_i} = \lfloor 10 \times r_i \rfloor mod M + 1$, where $\hat{r_i}$ denotes the normalized value and $\hat{r_i} \in [1, M]$.

The normalized random value $\hat{r_i}$ makes the cover pixel $P_{x,y}$ become the pixel of the $\hat{r}_i^{th}$ stego image. According to $P_{x,y}$, the secret digit s_k is embedded by

$$P_{x,y,z} = \begin{cases} P_{x,y} + s_k, & \text{if } 2^{N-1} \leq P_{x,y} \leq 255 - 2^{N-1} - 1, \\ P_{x,y}, & \text{otherwise,} \end{cases}$$

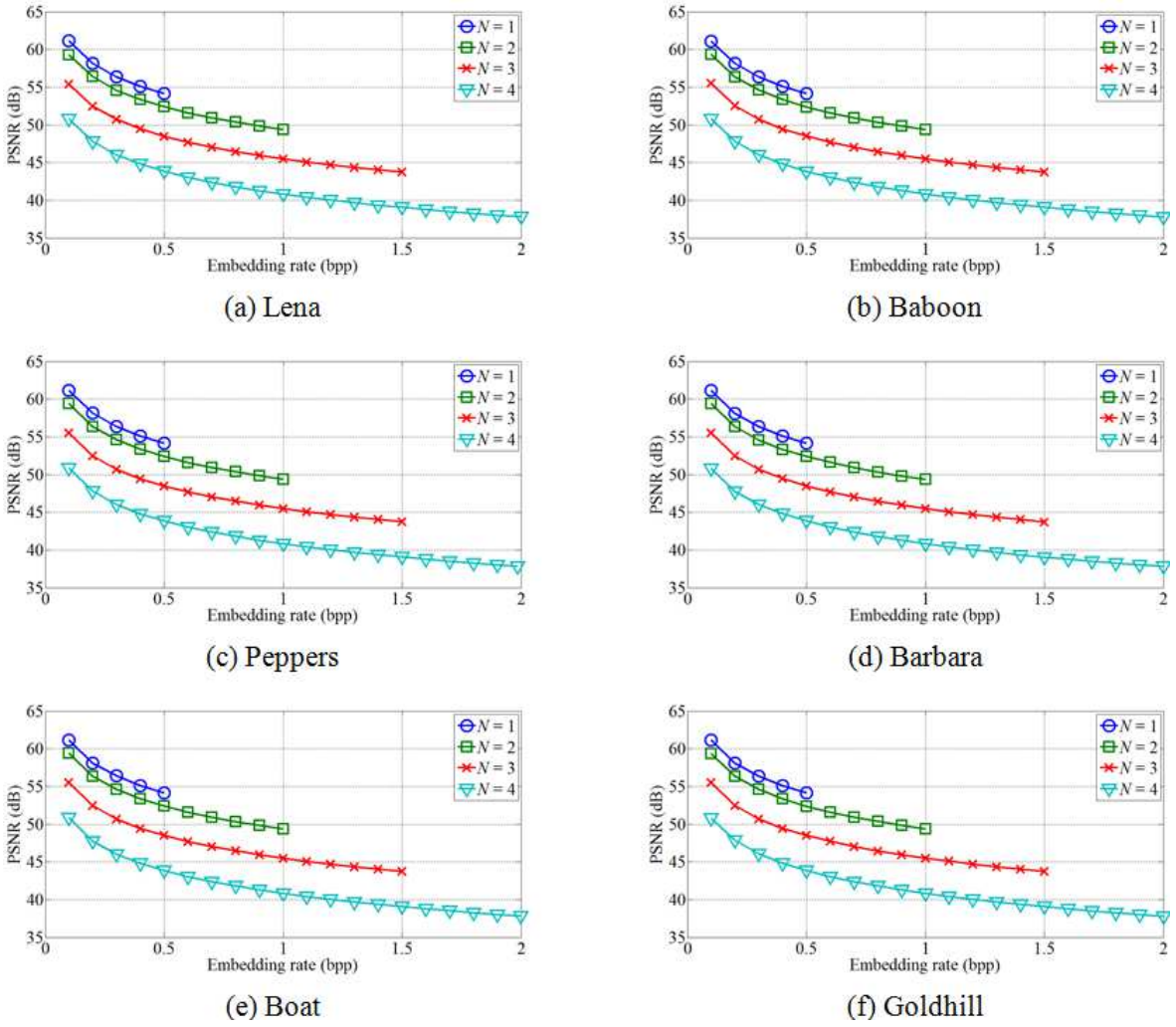

FIGURE 4. Comparison of embedding rates and the PSNR values for various N

where z denotes the ID number of the stego image and $z \notin r_i$. The boundary pixels, i.e., those greater than $(255 - 2^{N-1} - 1)$ or those smaller than 2^{N-1}, did not embed any secret digits to avoid the problems of overflow and underflow. However, there are a few boundary pixels in natural images. In other words, most cover pixels can be used to embed secret digits.

2.3. **Extraction and Recovery.** First, RS is generated by the same way as the embedding procedure. The random sequence $R = \{r_1, r_2, ..., r_{H\times W}\}$ is generated by RS and is normalized by $\hat{R} = \{\hat{r}_1, \hat{r}_2, ..., \hat{r}_{H\times W}\}$. The normalized sequence is the same as that of the embedding procedure, thus the cover pixel $P_{x,y}$ can be obtained from the $\hat{r}_i^{th}$ stego image. Afterwards, all of the secret digits are extracted correctly by $s_k = P_{x,y,z} - P_{x,y}$, where $4 \leq P_{x,y} \leq 252$ and $z \neq r_i$.

2.4. **Secret Data Decoding.** After extracting the secret digit s_k, it can be decoded as a set of original secret bits $B_k = \{b_1, b_2, ..., b_N\}$ by

$$b_1 = \begin{cases} 0, & \text{if } s_k \geq 0, \\ 1, & \text{otherwise,} \end{cases}$$

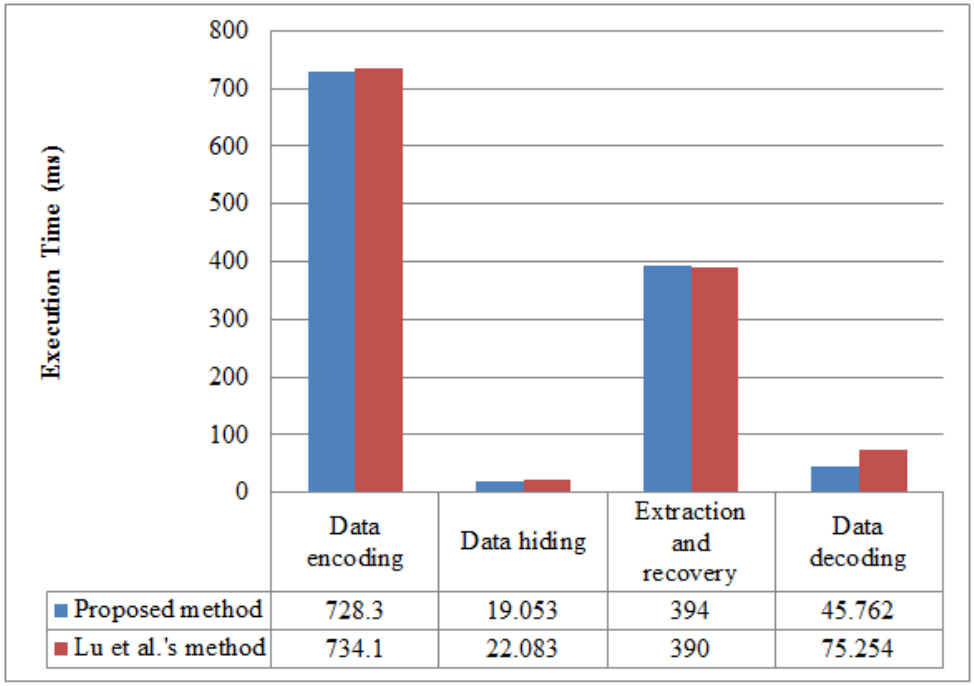

FIGURE 5. Comparison of the execution times of the proposed method and Lu *et al.*'s method

and $b_t = \lfloor s_k/2^{N-t} \rfloor \bmod 2$, where $t = 2, 3, ..., N$. In other words, s_k is decoded as one signal bit b_1 and the binary representation of $|s_k|$.

3. **Experimental Results.** In the experiments, we used MATLAB 7.6 for the pseudo-random generation of one binary sequence that was used as the secret sequence. Fig. 2 shows six grayscale images. These images were used as the cover images. In addition, the peak signal-to-noise ratio (PSNR) was calculated to measure the similarity between the cover image and the stego image, i.e., $\text{PSNR} = 10 \times \log_{10}(255^2/\text{MSE})$, where MSE is the mean square error between the cover image and the stego image. Higher values of PSNR mean that there is higher similarity between the cover image and the stego image. When the PSNR value is greater than 30 dB, the human eye cannot efficiently detect the difference between the cover image and the stego image.

The embedding rate is calculated by $R = EC/(M \times H \times W)$, where EC denotes the total embedding capacity of the M stego images. Larger values of R indicate that the cover pixel can be used to embed more secret bits.

We evaluated the performance of the proposed method by fixing N and changing M. In Fig. 3, N is fixed to 3 and M is variable, which means the same secret digits are embedded into M stego images. Obviously, the PSNR value becomes greater as M increases. Therefore, the proposed method can effectively maintain good quality of the stego image by increasing M. In the following experiments, M is fixed to 2 and N is variable, which means a set of N secret bits can be embedded into one of two stego pixels. Fig. 4 shows that the embedding rate R becomes greater as N increases. However, when $N > 6$, most PSNR values are smaller than 30 dB. Consequently, the appropriate range of N is [2, 5].

Since the proposed method can embed secret data into M stego images, the EC value of the proposed method is significantly greater than that of Lu *et al.*'s method. In addition, the execution time of the proposed method is less than that of Lu *et al.*'s method, as shown in Fig. 5. In the data encoding phase, Lu *et al.* converted a set of N secret bits into a decimal number and then reduced its value using the center-folding strategy.

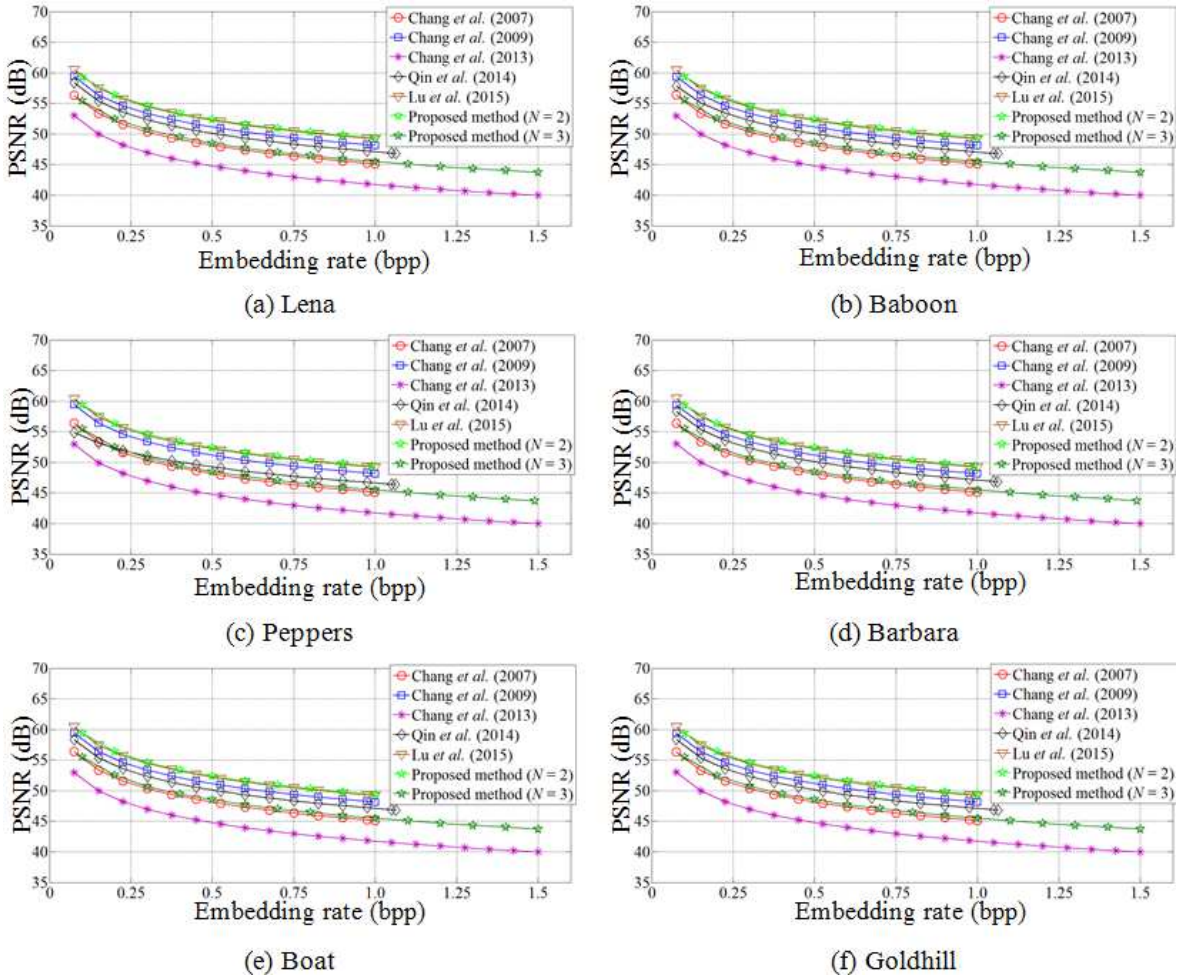

FIGURE 6. The embedding rates and PSNR values of the proposed method and five related methods

However, the set of N secret bits can be encoded directly by the proposed method; that is why the execution time of our encoding method is 5.8 microseconds less than that of Lu *et al.*'s method.

In the data embedding phase, Lu *et al.*'s method uniformly embeds one secret digit into two stego images, which takes more execution time. The proposed method can directly embed secret digits into M stego images. Consequently, the proposed method has a higher embedding efficiency than Lu *et al.*'s method.

In the extraction and recovery phase, the proposed method must discriminate between the cover pixel and the stego pixel, which increases the execution time. However, the extracted digits can be decoded efficiently as the secret bits. Different from the proposed method, Lu *et al.* increased the value of the extracted digits and converted it into a binary sequence, which requires more execution time.

Fig. 6 compares the proposed method with five related methods [2, 3, 4, 11, 13]. The proposed method achieves a greater PSNR value than the five related methods for the same R value. This is because the proposed method encodes secret bits as small digits to reduce distortion.

4. **Conclusions.** In this paper, we successfully solve the two problems of Lu *et al.*'s method, i.e., high computational cost and low embedding capacity. In the proposed

method, the secret bits are encoded directly and embedded into M stego images. Experimental results show that the proposed method has greater embedding capacity, higher PSNR value and less execution time than the related methods. Consequently, the proposed method is superior to other methods.

REFERENCES

[1] Y. K. Chan, W. T. Chen, S. S. Yu, Y. A. Ho, C. S. Tsai, and Y. P. Chu, A HDWT-based reversible data hiding method, *Journal of Systems and Software*, vol. 82, no. 3, pp. 411-421, 2009.

[2] C. C. Chang, Y. C. Chou, and T. D. Kieu, Information hiding in dual images with reversibility, *in Proceedings of the Third International Conference on Multimedia and Ubiquitous Engineering*, pp. 145-152, 2009.

[3] C. C. Chang, T. D. Kieu, and Y. C. Chou, Reversible data hiding scheme using two steganographic images, *in Proceedings of IEEE Region 10 International Conference (TENCON)*, pp. 1-4, 2007.

[4] C. C. Chang, T. C. Lu, G. Horng, Y. H. Huang, and Y. M. Hsu, A high payload data embedding scheme using dual stego-images with reversibility, *in Proceedings of the Ninth International Conference on Information, Communications and Signal Processing*, pp. 1-5, 2013.

[5] M. Fallahpour, Reversible image data hiding based on gradient adjusted prediction, *IEICE Electronics Express*, vol. 5, no. 20, pp. 870-876, 2008.

[6] H. C. Huang and F. C. Chang, Multi-tier and multi-bit reversible data hiding with contents characteristics, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 1, pp. 11-20, 2016.

[7] C. F. Lee, H. L. Chen, and H. K. Tso, Embedding capacity raising in reversible data hiding based on prediction of difference expansion, *Journal of Systems and Software*, vol. 83, no. 10, pp. 1864-1872, 2010.

[8] T. C. Lu, C. M. Lu, and C. C. Chang, Multimedia Security Techniques, Taiwan: CHWA, 2007.

[9] T. C. Lu, C. Y. Tseng, and J. H. Wu, Asymmetric-histogram based reversible information hiding scheme using edge sensitivity detection, *Journal of Systems and Software*, vol. 116, no. 2-21, 2016.

[10] T. C. Lu, C. Y. Tseng, and J. H. Wu, Dual imaging-based reversible hiding technique using LSB matching, *Signal Processing*, vol. 108, pp. 77-89. 2015.

[11] T. C. Lu, J. H. Wu, and C. C. Huang, Dual-image-based reversible data hiding method using center folding strategy, *Signal Processing*, vol. 15, pp. 195-213, 2015.

[12] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, Reversible data hiding, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006.

[13] C. Qin, C. C. Chang, and T. J. Hsu, Reversible data hiding scheme based on exploiting modification direction with two steganographic images, *Multimedia Tools and Applications*, vol. 74, no. 15, pp. 5861-5872, 2015.

[14] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, An inpainting-assisted reversible steganographic scheme using histogram shifting mechanism, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 7, pp. 1109-1118, 2013.

[15] C. Qin, C. C. Chang, and L. T. Liao, An adaptive prediction-error expansion oriented reversible information hiding scheme, *Pattern Recognition Letters*, vol. 33, no. 16, pp. 2166-2172, 2012.

[16] J. Tian, Reversible data embedding using a difference expansion, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.

[17] D. M. Thodi and J. J. Rodriguez, Prediction-error based reversible watermarking, *in Proceedings of IEEE Conference on Image Processing*, vol. 3, pp. 1549-1552, 2004.

[18] D. M. Thodi and J. J. Rodriguez, Expansion embedding techniques for reversible watermarking, *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721-730, 2007.

[19] S. Y. Wang, C. Y. Li, and W. C. Kuo, Reversible data hiding based on two-dimensional prediction errors, *IET Image Processing*, vol. 7, no. 9, pp. 805-816, 2013.

[20] S. Weng and J. S. Pan, Integer transform based reversible watermarking incorporating block selection, *Journal of Visual Communication and Image Representation*, vol. 35, pp. 25-35, 2016.

[21] S. Weng, J. S. Pan, and J. Deng, Invariability of remainder based reversible watermarking, *Journal of Network Intelligence*, vol. 1, no. 1, pp. 16-22, 2016.

[22] S. Weng, J. S. Pan, and L. Li, Reversible data hiding on an adaptive pixel-embedding strategy and two-layer embedding, *Information Sciences*, vol. 369, pp. 144-159, 2016.