ICIC Express Letters
Part B: Applications
Volume **8**, Number **12**, December **2017**

 ISSN 2185-2766
pp. **1559–1566**

DIAMOND SHAPE DIVISION REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

Chuan-Kuei Huang, Dyi-Cheng Chen, Wei-Liang Liu*
and Sung-Chin Huang

Department of Industrial Education and Technology
National Changhua University of Education
No. 2, Shi-Da Road, Changhua City 500, Taiwan
{ ckhuang; dcchen }@cc.ncue.edu.tw; d0431004@gm.ncue.edu.tw
*Corresponding author: d0231004@gm.ncue.edu.tw

Received July 2017; accepted September 2017

Abstract. *Visible data hiding embeds secret messages in media to reduce distortion such that an unintended observer will not be aware of the existence of the hidden messages. The conventional reversible data hiding (RDH) embedding capacity is so low. This study focuses on the need for higher embedding capacity, and then proposes an improving reversible data hiding method in encrypted images. Natural images contain strong correlations among adjacent pixels. Generally statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical, and also diagonal directions. In this study, a diamond shape division contains 13 pixels in a block, meets the characteristics of natural images. The experimental results show the proposed method not only enhances the embedding capacity but also remains high security.*
Keywords: Diamond shape division, Reversible data hiding, Embedding capacity

1. **Introduction.** The rapid development of network and information technology has the issues of privacy and information security being gradually emphasized. Secret messages delivered in the Internet could be hacked. For this reason, it becomes common to encrypt messages.

Symmetric encryption is used in traditional cryptography to encrypt the original media with a public-key. The encrypted message is then transmitted to the receiver, who would apply a private-key to decrypting the encrypted media and extracting the original information (Figure 1).

Data embedding could be divided into reversible and irreversible. Different from traditional cryptography, data embedding embeds secret messages in cover media to reduce distortion such that an unintended observer will not be aware of the existence of the hidden messages. Cover-media with the secret messages embedded is called stego media. The most common irreversible data hiding technique is the least significant bit (LSB) replacement method [1]. The human vision cannot easily identify slight adjustments to the digital media.

In many applications, they are not allowed any distortion such as legal judgment medical diagnosis, medical image, and military media documents. Therefore, the reversible data hiding method is explored. Many reversible data hiding (RDH) methods have been proposed in recent years, for example, the methods based on lossless compression [2,3]. Difference expansion (DE) was proposed by Tian [4] in 2003, who divided the neighboring pixels of a host image into non-overlapping pairs. In 2004, Alattar [5] extended Tian's method using four neighboring pixels as a set and enhanced the embedding capacity with

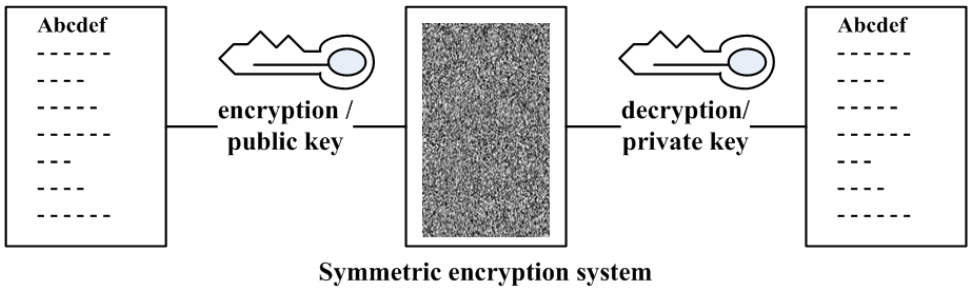


FIGURE 1. Symmetric encryption in traditional cryptography

function transfer. A lossless compression method for encrypted gray image using progressive decomposition and rate-compatible turbo codes is developed in [6]. In recent decade many researchers are more enthusiastic to improve the embedding capacity.

Histogram shifting (HS) was proposed by Ni et al. [7] in 2006, which calculated the pixels of the entire image to draw the histogram, extracted the peak point (the most) and the zero point (null or the least), vacated room for data embedding, shifted all pixels between the peak point and the zero point, and embedded all pixels at the peak point in the secret message with 0 or 1. HS utilized the pixel peak point to embed the secret message. In the process to extract secret messages, it simply extracted the secret message with 0 or 1 at such peak point and neighboring point sequentially, and the pixels between the peak point and the zero point were shifted back for restoring to the original values.

In addition, there are many methods [8-11] combining both of the DE and HS to residuals of the image, e.g., the expected errors, to achieve better performance. In some applications, we wish the cover media have been encrypted first in order to protect the privacy, and then embed secret messages into the encrypted media. In 2011, Zhang [12] proposed a novel reversible data hiding scheme for encrypted image by modifying a part of encrypted data. Lai and Tsai [13] proposed a new technique using mosaic image encryption. In 2009, Chao et al. [14] proposed a diamond encoding (DE) method to enhance the capacity. Li et al. [15] proposed a scheme of reversible data hiding in encrypted images by using cross division and additive homomorphism. They first established a non-overlapping cross division mask for cover image, and then encrypted the cover image by RC4 cryptosystem and additive homomorphism.

Many previous papers are enthusiastic to enhance the embedding capacity in encryption domain. This study majorly focuses on improving the embedding capacity in encrypted images and remains high security. The remainder of this study is organized as follows. Section 2 provides a brief literature review, while Section 3 describes the proposed method. The experimental results and discussion are shown in Section 4, and then the conclusion of the research at the end.

2. **Related Works.** Based on the homomorphic properties of the cryptosystem, a cross mask of encrypted images was developed with non-overlapping cross division (Figure 2) by Li et al. [15] in 2015. The difference between the central pixels in each cross block (Figure 2, pixel number 3, 7, 12, 16, 20, 29, and 33) and four neighboring pixels (up, down, left, and right) is used for developing the difference histogram to embed secret information with histogram shifting. Such an approach remains the same difference among neighboring pixels to effectively enhance the embedding capacity.

The approach proposed by Li et al. [15] is explained as follows.

Step 1: The cover image is established a cross mask with non-overlapping cross division (Figure 2). Assuming the central pixels of the divided cover image in the cross division block as $P_{a,b}$ (the a_{th} row, the b_{th} column), the neighboring pixels are $P_{a,b-1}$, $P_{a,b+1}$, $P_{a-1,b}$,

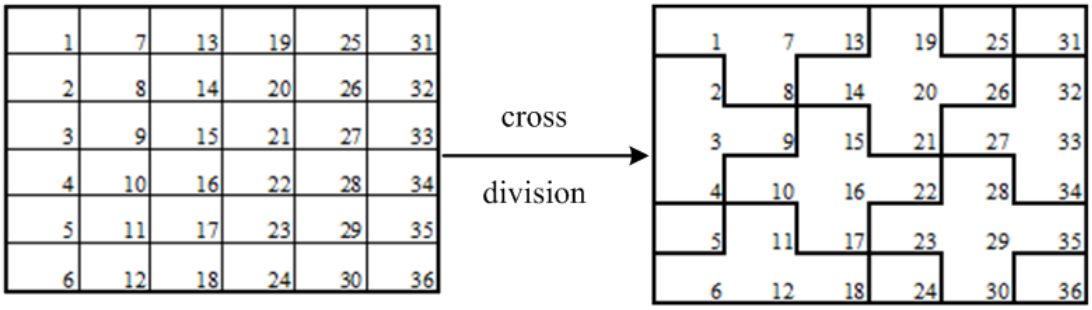


FIGURE 2. Li et al.'s cross division scheme (for example 6×6)

and $P_{a+1,b}$. Equation (1) is used for expressing the relationship among pixels.

$$\begin{cases} a = a \\ b = (2 \times a) \bmod 5 + 5 \times k \end{cases} \quad \forall a = 1, 2, \ldots, h, \quad k = 0, 1, \ldots, \left\lfloor \frac{w - (2 \times a) \bmod 5}{5} \right\rfloor \tag{1}$$

where h and w represent the image height and width.

Step 2: The RC4 cryptosystem generates a random sequence, sequentially filling the mask matrix. The outer pixels of cross division are replaced by the central pixel.

In order to encrypt the pixels M of the gray image, we choose K, a randomly generated key-stream using RC4 cryptosystem. The security of the cryptosystem lies on the underlying stream cipher used. The RC4 cryptosystem is secure after first few hundred bytes are discarded.

Step 3: Step 1 is combined with Step 2 to calculate the pixel of the encrypted image.

$$E_{a,b} = (P_{a,b} + M_{a,b}) \bmod 256 \tag{2}$$

where $E_{a,b}$, $P_{a,b}$, and $M_{a,b}$ represent encrypted pixel, original cover image pixel, and mask value respectively.

Step 4: To calculate the difference $(d_{a-1,b}, d_{a+1,b}, d_{a,b-1}, d_{a,b+1})$ between the central pixel $(P_{a,b})$ and the neighboring pixels $(P_{a-1,b}, P_{a+1,b}, P_{a,b-1}, P_{a,b+1})$ in the non-overlapping cross division block, for example, $d_{a-1,b} = \bmod (P_{a-1,b} - P_{a,b}, 256)$, then, a difference-histogram is generated by counting the frequency of the differences' value.

Step 5: Histogram shifting is utilized for embedding secret messages into the non-central pixels in each non-overlapping cross division according to the RC4 cryptosystem generated in Step 2. That is, at most 4 secret messages could be embedded in the cross division.

3. **Proposed Method.** This paper proposes an improving method. Natural images contain strong correlations among adjacent pixels. Generally statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical, and also diagonal directions. The diamond shape block division adequately increases the number of pixels in each non-overlapping block, so to effectively improve the embedding capacity.

3.1. **Division method.** This work applies diamond shape division (Figures 3(c)-3(f)). The diamond shape block contains more pixels, efficiently achieving much higher capacity and remaining high security compared to Li et al.'s [15].

3.2. **Encryption.** The initial value x_0 $(0 \leq x_0 < 1)$ and u (bifurcation parameter, $3.569945 < u \leq 4$ comes into chaos state) are given to correspond to the logistic map sequence $x_{n+1} = ux_n(1 - x_n)$ in nonlinear chaos system generated by each pixel of the original image, which is further transferred into the range of grey-level pixels (e.g., the

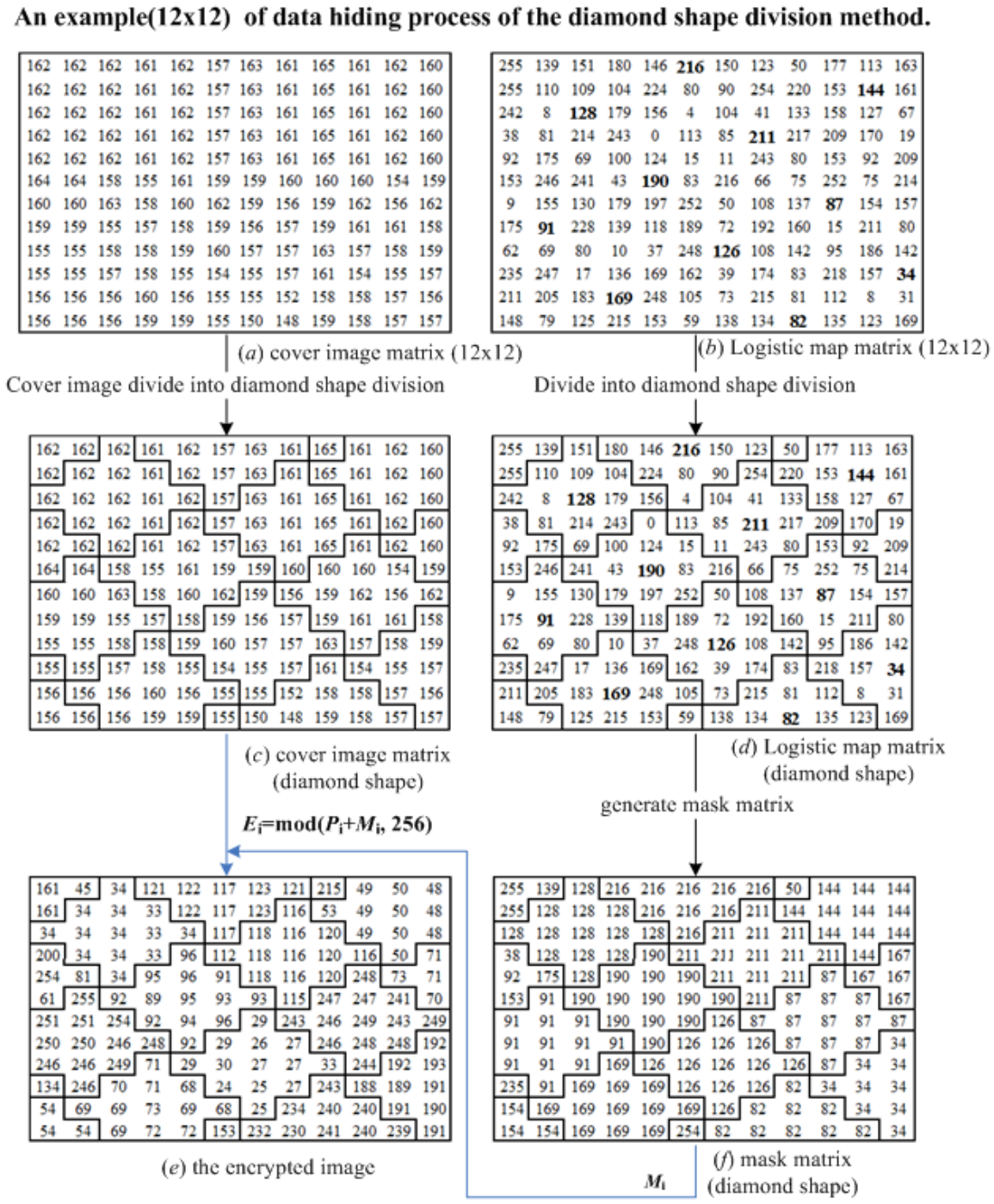


FIGURE 3. Encrypting image in diamond shape division procedure

remainder of x_i multiplying by 10^{14} and then modulo 256 (Figure 3(b)) and develop the diamond shape mask (Figure 3(f)). The encryptor sorts the central value of diamond shape based block of chaos matrix. It is impossible to figure out the permutation to get the original image since there exist a huge number of ways of performing the permutation especially for large sized images.

3.3. **Embedding and extraction.** The embedding and extraction schemes are the same as Li et al.'s [15], refer to step 3 to 5. Every block mostly embeds 12 secret message bits.

The number of block in 512×512 image is larger than 20000. The block permutation is 20000! Since permutation based transposition algorithms for image confused the original image, it efficiently increases security.

TABLE 1. Comparison of experimental results between Li et al.'s and proposed method

Li et al.'s

	PSNR (dB)	Entropy	Correlation	Capacity (bits)
Tiffany	6.932845	7.998900	0.002810	45068
Baboon	9.515770	7.999253	0.000549	12772
Lena	9.233206	7.999269	0.000222	38170
Jet	8.027540	7.999040	−0.000617	57025
Scene	8.227566	7.999108	0.000121	24371
Peppers	8.863232	7.999107	−0.002970	28033

proposed method

	PSNR (dB)	Entropy	Correlation	Capacity (bits)
Tiffany	**6.897437**	**7.999097**	**0.002433**	**46253**
Baboon	**9.494631**	7.998953	−0.005089	**12805**
Lena	9.204670	7.999017	−0.009564	**38901**
Jet	**8.015495**	7.998600	−0.004550	**57584**
Scene	8.244126	7.999043	−0.002716	**27805**
Peppers	**8.853779**	7.998777	−0.005803	**32739**

Table 1 shows the compared results of Li et al.'s [15] and proposed method, including peak signal-to-noise ratio (PSNR), entropy, correlation coefficient and capacity (bits).

PSNR is defined as follows.

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{Peak^2}{\mathrm{MSE}} \tag{3}$$

where $Peak = 255$ (in gray-level image), and MSE is defined as

$$\mathrm{MSE} = \frac{1}{w \times h} \sum_{a=1}^{w} \sum_{b=1}^{h} \left(P_{a,b} - P'_{a,b}\right)^2 \tag{4}$$

w and h stand for the dimension of images, $P_{a,b}$ and $P'_{a,b}$ represent the pixel at the a_{th} row and the b_{th} column of the cover image and the stego image, respectively.

The entropy equation of a gray-level image s is defined as follows.

$$H(s) = N(x_i) \log_2 \frac{1}{N(x_i)} \tag{5}$$

where $N(x_i)$ stands for the gray-level pixel equal to the appearance probability of i.

The correlation coefficient (Cor) is defined as

$$Cor_{uv} = \frac{\mathrm{cov}(u, v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{6}$$

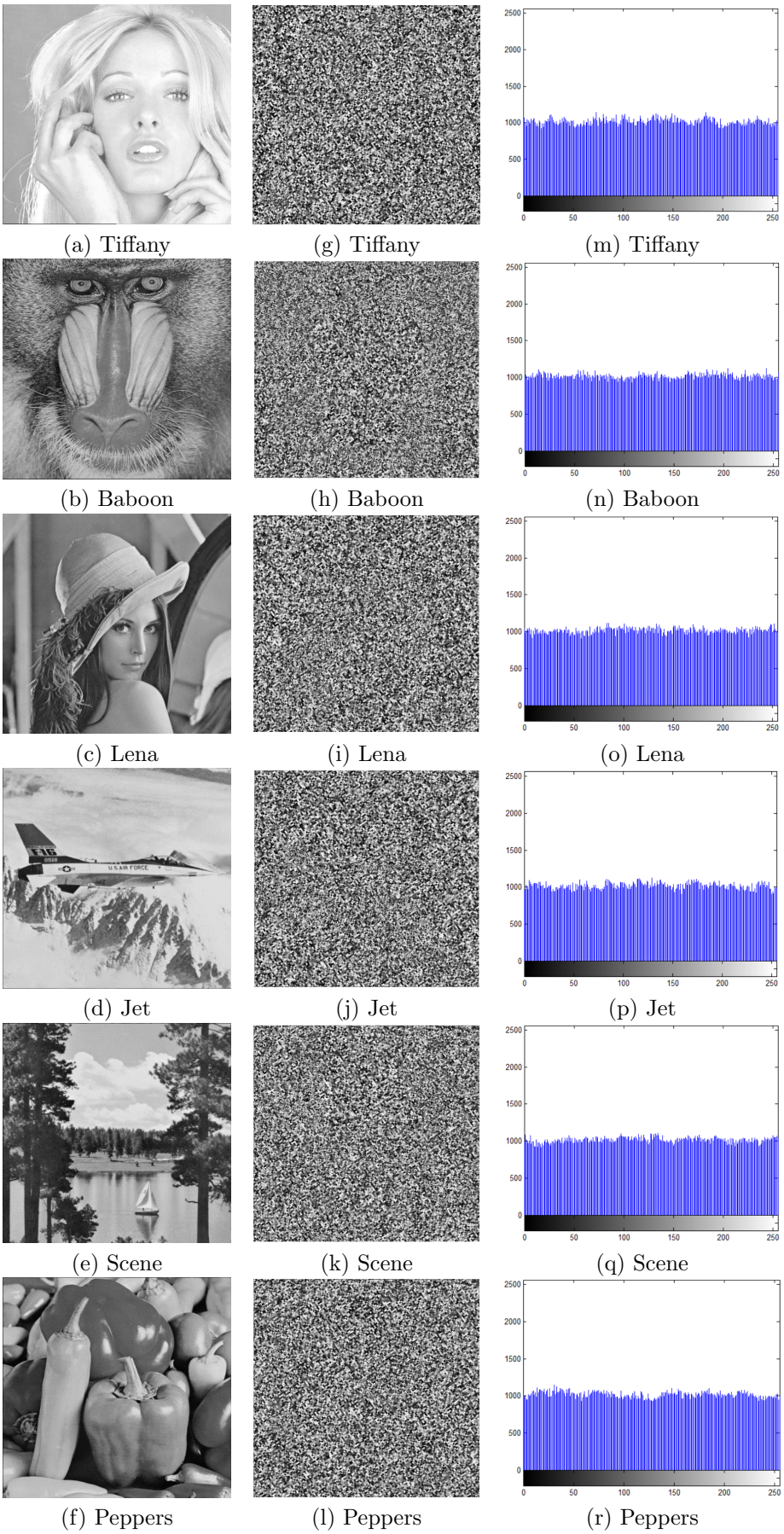
where u, v are the image values of gray-level images, and $D(u)$ and $D(v)$ are the variance of u, v.

The definition is shown as follows.

$$D(u) = \frac{1}{n} \sum_{i=1}^{n} \left(u_i - M(u)\right)^2 \tag{7}$$

where $M(u)$ and $M(v)$ are the average value (mean) of u and v, defined as follows.

$$M(u) = \frac{1}{n} \sum_{i=1}^{n} u_i \tag{8}$$



(a) Tiffany (g) Tiffany (m) Tiffany

(b) Baboon (h) Baboon (n) Baboon

(c) Lena (i) Lena (o) Lena

(d) Jet (j) Jet (p) Jet

(e) Scene (k) Scene (q) Scene

(f) Peppers (l) Peppers (r) Peppers

FIGURE 4. (a-f) Standard test images in SIPI database, (g-l) diamond shape division stego images and (m-r) histogram of the stego images

The covariance $\mathrm{cov}(u, v)$ between u and v is defined as follows.

$$\mathrm{cov}(u, v) = \frac{1}{n} \sum_{i=1}^{n} M(u_i - M(u))(v_i - M(v)) \tag{9}$$

From Table 1, low PSNR represents low readability, and most images of PSNR are lower than Li et al.'s [15]. The entropy shows the chaos degree, and correlation coefficient not only verifies the low correlation among neighboring pixels but also verifies that the encrypted image with diamond shape division still remains the embedding characteristics.

Theoretically, the ideal embedding capacity is 12/13 bpp (bit per pixel), which is higher than Li et al.'s [15] 4/5 bpp. Moreover, Table 1 shows the embedding capacity assumption. The proposed method outperforms Li et al.'s [15].

4. **Conclusion.** Aiming at Li et al.'s [15] approach, this study makes an improvement with diamond shape based division to effectively increase the embedding capacity of secret messages. The ideal embedding capacity is 12/13 bpp, which outperforms Li et al.'s 4/5 bpp. This study majorly focuses on improving the embedding capacity in encrypted images and remains high security. The experimental results show the actual embedding capacity is higher than Li et al.'s [15]. A diamond shape division contains more pixels (from 5 to 13). Although the entropy (approach to ideal value 8) and correlation coefficient (approach to ideal value 0) may be very little inferior to Li et al.'s [15], they are very close to ideal values. In the further research we endeavor to apply logical operation (like as exclusive OR) in bit-wise manners by using a chaotic mapping. This method most probably takes advantages of PSNR, entropy and correlation coefficient. Consequently, the experimental results show proposed method not only enhances the capacity but also remains high security.

REFERENCES

[1] C. K. Chan and L. M. Cheng, Hiding data in images by simple LSB substitution, *Pattern Recognit.*, vol.37, no.3, pp.469-474, 2004.

[2] T. Kalker and F. M. J. Willems, Capacity bounds and constructions for reversible data hiding, *Security Watermarking Multimedia Contents V*, vol.5020, pp.604-611, 2003.

[3] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, Lossless generalized-LSB data embedding, *IEEE Trans. Image Process.*, vol.14, no.2, pp.253-266, 2005.

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

[5] A. M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, *IEEE Trans. Image Process.*, vol.13, no.8, pp.1147-1156, 2004.

[6] W. Liu, W. Zeng, L. Dong and Q. Yao, Efficient compression of encrypted grayscale images, *IEEE Trans. Image Process.*, vol.19, no.4, pp.1097-1102, 2010.

[7] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, Reversible data hiding, *IEEE Trans. Circuits Syst. Video Technology*, vol.16, no.3, pp.354-362, 2006.

[8] W. Hong, T. S. Chen and C. W. Shiu, Reversible data hiding for high quality images using modification of prediction errors, *J. Syst. Softw.*, vol.82, no.11, pp.1833-1842, 2009.

[9] P. Tsai, Y. C. Hu and H. L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, *Signal Process.*, vol.89, pp.1129-1143, 2009.

[10] L. Luo et al., Reversible image watermarking using interpolation technique, *IEEE Trans. Inf. Forensics Security*, vol.5, no.1, pp.187-193, 2010.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh and Y.-Q. Shi, Reversible watermarking algorithm using sorting and prediction, *IEEE Trans. Circuits Syst. Video Technol.*, vol.19, no.7, pp.989-999, 2009.

[12] X. P. Zhang, Reversible data hiding in encrypted images, *IEEE Signal Processing Letters*, vol.18, no.4, pp.255-258, 2011.

[13] I. J. Lai and W. H. Tsai, Secret-fragment-visible mosaic image – A new computer art and its application to information hiding, *IEEE Trans. Inf. Forens. Secur.*, vol.6, no.3, pp.936-945, 2011.

[14] R. M. Chao, H. C. Wu, C. C. Lee and Y. P. Chu, A novel image data hiding scheme with diamond encoding, *EURASIP J. Inf. Security*, vol.2009, 2009.

[15] M. Li, D. Xiao, Y. Zhang and H. Nan, Reversible data hiding in encrypted images using cross division and additive homomorphism, *Signal Processing: Image Communication*, vol.39, pp.234-248, 2015.