# Reversible Data Hiding in Encrypted Image with Difference Expansion and Shifting

Dan Wu
Department of Mathematics, China Jiliang University
Hangzhou, China
e-mail: wudan@cjlu.edu.cn

Jiao Wu
Department of Mathematics, China Jiliang University
Hangzhou, China
e-mail: wuj@cjlu.edu.cn

Ruxing Xu
Department of Mathematics, China Jiliang University
Hangzhou, China
e-mail: xrxing@cjlu.edu.cn

**Abstract—A method of reversible data hiding in encrypted images is proposed, in which either data-extraction or image-recovery is applicable to an encrypted image. The proposed method is a reversible data hiding in encrypted image with improved performance. A content owner first encrypts the image by permutation using an encryption key. Then a data-hider may embed data into the encrypted image by difference expansion and shifting. If the receiver has the data-hiding key, he can extract the hiding data. If the receiver has the encryption key, he can decrypt the received image, and get an image similar to the original one. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error. Experimental results demonstrate that the proposed scheme can embed a larger payload into the encrypted image while keeping the same PSNR (peak signal-to-noise ratio).**

***Keywords- reversible data hiding; encrypt; difference expansion; difference shifting; recovery***

## I. INTRODUCTION

Data hiding has been widely used in areas such as ownership protection, content authentication, distribution tracking, and broadcast monitoring. However, in some applications, especially in the medical, military and legal domain, even the imperceptible distortion introduced in the embedding process is unacceptable. Under these circumstances, reversible data hiding [1-4] is desired, which not only extracts the hiding data, but also perfectly reconstructs the original host signal from the embedded work. Tian [1] proposed a high capacity reversible data embedding algorithms, which was based on difference expansion, and the method had been extended by [2-4]. Ni[5] proposed an algorithm based on histogram shifting, which utilized the zero or the minimum points of the histogram of an image and slightly modified the pixel grayscale values to embed data into the image. Thodi [6] proposed a reversible watermarking technique called prediction error expansion, which better exploited the correlation inherent in the neighborhood of a pixel than the difference expansion scheme. The rapid development of communication technology has given rise to a huge increase. To protect the information, encryption technique is often used. In that case both data hiding and encryption are desired. There are different schemes to perform data hiding techniques in encrypted image [7-11]. Zhang [8] proposed a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. Fujiyoshi [9] proposed a new method of separable reversible data hiding (RDH) for encrypted images in which hidden data can be extracted from an encrypted image conveying hidden data without image decryption. By histogram and spatial permutation, the proposed method firstly encrypts an image and simultaneously prepares room for RDH. Mohan [10] proposed A novel reversible data hiding algorithm with improved security, which can recover the original image in separable manner without any distortion from the marked image after the hidden data have been extracted, is presented in this paper. In the content owner side image is encrypted by key derived chaotic based transposition algorithm. The data hider then hides some data into the encrypted image by histogram modification based data hiding, making use of data hiding key. At the receiver side, if the receiver has only encryption key, then the decrypted image with high similarity with cover image can be obtained, but cannot read the hidden data.

This paper proposed a method of reversible data hiding in encrypted images, in which the owner can use the secret key either to extract the hiding data or to recover the image in an encrypted image. The proposed method is a reversible data hiding in encrypted image with improved performance. First the image is encrypted by permutation using an encryption key. Then the encrypted image hides data by the content owner, which is based on difference expansion and shifting. If the receiver has the data-hiding key, he can extract the hiding data. If the receiver has the encryption key, he can roughly recover the image. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error.

The structure of this paper is given as follows: In Section II, we provide the detailed description of our algorithm. Experimental results are presented in Section III,

## II. Proposed System

### A. Image Encryption

Assume we are considering a grayscale image of size m×n (m and n are even numbers). Each pixel of a grayscale image is represented by 8 bits. We get a sequence of pixels by scanning the image, which is denoted by $A = \{a_1, a_2, \cdots, a_{mn-1}, a_{mn}\}$, divide $A$ into m×n/2 blocks $\overline{A} = \{(a_1, a_2), \cdots, (a_{mn-1}, a_{mn})\}$, disturb the blocks by a secret key $k_1$, and get $\overline{\overline{A}} = \{(b_1, b_2), \cdots, (b_{mn-1}, b_{mn})\}$.

If $b_{i1}$ and $b_{i2}$ are the gray values of a pixel-pair, then the integer-mean $m_i$ and the difference $d_i$ are defined as

$$\begin{cases} m_i = floor((b_{i1} + b_{i2}) / 2) \\ d_i = b_{i1} - b_{i2} \end{cases} \tag{1}$$

Denote the bits of a pixel as $h_{i,0}, h_{i,1}, \cdots, h_{i,7}$ where $1 \le i \le mn/4$, the gray value as $m_i$. That implies

$$h_{i,j} = \lfloor m_i / 2^j \rfloor \bmod 2, j = 0, 1, \ldots, 7 \tag{2}$$

And

$$m_i = \sum_{j=0}^{7} h_{i,j} 2^j \tag{3}$$

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated

$$H_{i,j} = h_{i,j} \oplus r_{i,j}, j = 0, 1, 2 \tag{4}$$

Where $r_{i,j}$ are determined by an encryption key using a standard stream cipher.

$$M_i = \sum_{j=0}^{7} H_{i,j} 2^j \tag{5}$$

Since this transformation is invertible, the encrypted gray values $eb_{i1}$ and $eb_{i2}$ can be given

$$\begin{cases} eb'_{i1} = M_i + floor((d_i + 1) / 2) \\ eb'_{i2} = M_i - floor(d_i / 2) \end{cases} \tag{6}$$

The encrypted pixel $eb_{i1}$ and $eb_{i2}$ are concatenated orderly as the encrypted data. We get the encrypted pixel sequence $EA = \{(eb_1, eb_2), \cdots, (eb_{mn-1}, eb_{mn})\}$, and obtain the encrypted image EI.

### B. Data embedding

The data-hider scans the encrypted image, get the sequence of encrypted pixels $EA = \{ea_1, ea_2, \cdots, ea_{mn-1}, ea_{mn}\}$, and divide $EA$ into m×n/2 blocks $\overline{EA} = \{(ea_1, ea_2), \cdots, (ea_{mn-1}, ea_{mn})\}$.

If $ea_1$ and $ea_2$ are the gray values of a pixel-pair, then the integer-mean $em$ and the difference $d$ are defined as

$$\begin{cases} em = floor((ea_1 + ea_2) / 2) \\ d = ea_1 - ea_2 \end{cases} . \tag{7}$$

Using the difference $d$, we can hide the bit $b$ via the following equations

$$\begin{cases} d' = 2d + b & -K \le d \le K - 1 \\ d' = d + K & d \ge K \\ d' = d - K & d < -K \end{cases} , \tag{8}$$

where $K$ is the threshold controlled by the user.

The watermarked pixel $ea'_1$ and $ea'_2$ can be calculated by $d'$ and $em$ via (7). When $d \ge K$ or $d < -K$, we shift the difference $d$ further away from the zero point, which is called the difference shifting, and leave $[K,\ 2K-1]$ and $[-2K-1,\ -K-1]$ empty for difference expansion. When $-K \le d \le K-1$, we expand the difference $d$ to embed the watermark bit $b$. As a result, the location map is unnecessary when extracting the information, which improves the embedding capacity.

### C. Data extracting and image recovery

With an encrypted image $EA'$ containing embedded data, if the receiver has only the data-hiding key, he may scan the image, get the sequence of pixels denoted as $\overline{EA}' = \{(ea'_1, ea'_2), \cdots, (ea'_{mn-1}, ea'_{mn})\}$, and calculate the difference $d'$ and the integer-mean $M$ of the pair $(ea'_{2i}, ea'_{2i+1})$.

When $-2K \le d' \le 2K - 1$, the hiding data can be obtained by extracting the lowest bits of difference $d'$.

Consider the case that the receiver has the encryption key but does not know the data-hiding key. Clearly, he cannot extract the embedded data and recover the original image. However, the original image content can be roughly recovered. Denoting the bits of pixels in the encrypted image containing embedded data as $h'_{i,0}, h'_{i,1}, \cdots, h'_{i,7}$ ($1 \le i \le mn/4$), the receiver can decrypt the received data

$$M'_{i,j} = h'_{i,j} \oplus r_{i,j}, j = 0, 1, 2 \tag{9}$$

Where $r_{i,j}$ are derived from the encryption key. The integer mean of decrypted pixel pairs are

$$M'_i = \sum_{j=0}^{7} h'_{i,j} 2^j \tag{10}$$

The gray values of decrypted pixels are

$$\begin{cases} eb'_{i1} = M'_i + floor((d'_i + 1)/2) \\ eb'_{i2} = M'_i - floor(d'_i / 2) \end{cases} \tag{11}$$

where $d'_i$ is same as $d'_i$ in equation (8).

Since the data-embedding operation does not alter any MSB of encrypted image, the decrypted MSB must be same as the original MSB. So, the content of decrypted image is similar to that of original image.

## III. Experimental Result

The test image Lena sized 512×512 shown in Fig .1 was used as the original image in the experiment. After image encryption, the eight encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig .2. Then, we let $K = 1$ to embed 19368 additional bits into the encrypted image. The encrypted image containing the embedded data is shown in Fig .3, and the embedding rate is 0.074 bit per pixel (bpp). With an encrypted image containing embedded data, we could extract the additional data using the data-hiding key. If we directly decrypted the encrypted image containing embedded data using the encryption key, the value of PSNR in the decrypted image was 49.7166 dB. The directly decrypted image is given as Fig .4. By using both the data-hiding and the encryption keys, the embedded data could be successfully extracted and the original image could be perfectly recovered from the encrypted image containing embedded data.

Table 1 is the experimental results of our scheme which include the payload, and the peak-signal-noise-ratio (PSNR) of different thresholds. Then, we let $K = 4$ to embed 66998 additional bits into Fig.2. The encrypted image containing the embedded data is shown in Fig .5, and the embedding rate is 0.255 bit per pixel (bpp). If we directly decrypted the encrypted image containing embedded data using the encryption key, the value of PSNR in the decrypted image was 42.9281 dB. Fig .6 shows the directly decrypted image.

TABLE I. Payload and PSNR of different thresholds

| **Threshold (*K*)** | **payload** | **PSNR** |
|---|---|---|
| *K*=1 | 19368 | 49.7166 |
| *K*=2 | 37688 | 46.594 |
| *K*=3 | 53421 | 44.4728 |
| *K*=4 | 66998 | 42.9281 |

Figure 1. Original Lena

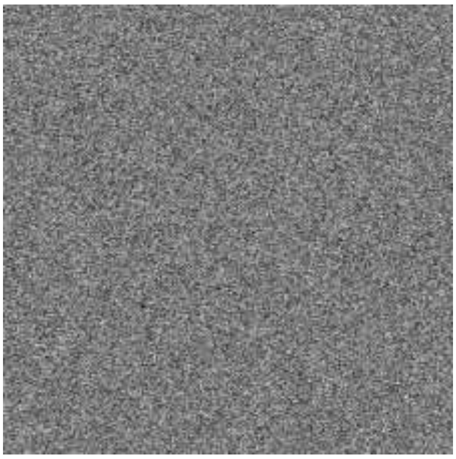

Figure 2. The encrypted version,

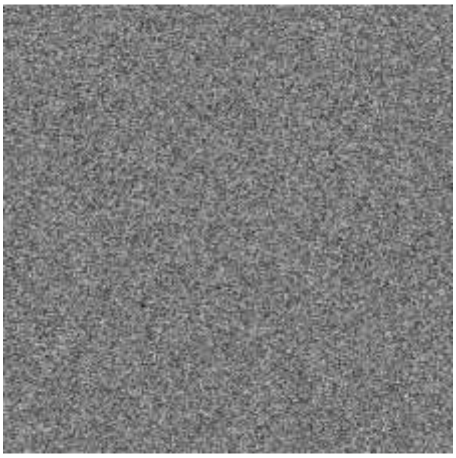

Figure 3. Encrypted image containing embedded data with embedding rate 0.074 bpp

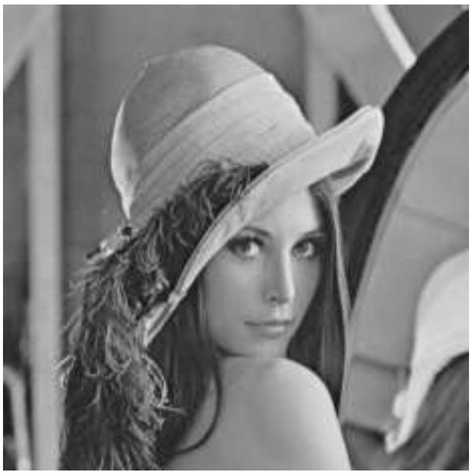

Figure 4. Directly decrypted (PSNR=49.7166)

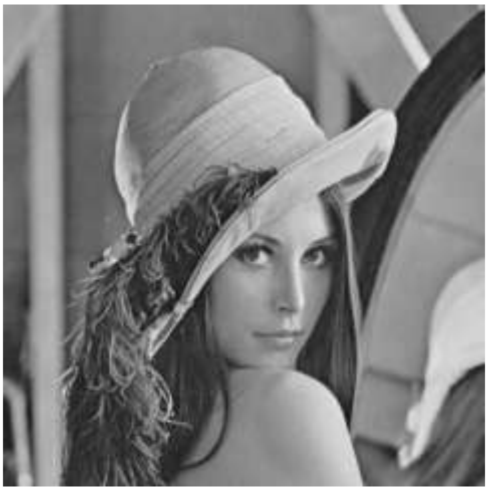

Figure 5. Directly decrypted (PSNR=42.9281)

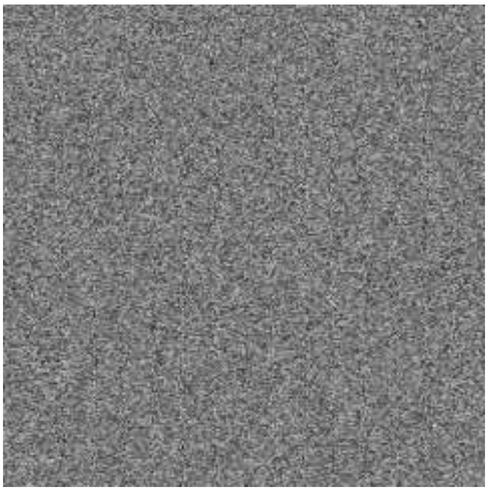

Figure 6. Encrypted image containing embedded data with embedding rate 0.255 bpp

## ACKNOWLEDGMENT

The authors would like to thank the National Natural Science Foundation of China (No. 61302190).

## REFERENCES

[1] J. Tian: Reversible data embedding using a difference expansion. J. IEEE Transactions on Circuits and Systems for Video Technology. 13(8), 890-896 (2003)

[2] A M. Alattar: Reversible watermark using the difference expansion of a generalized integer transform. J. IEEE transactions on image processing. 13(8), 1147-1156 (2004)

[3] C C Chang, T C.Lu: A difference expansion oriented data hiding scheme for restoring the original host images. J. The Journal of Systems & Software. 79(12), 1754-1766 (2006)

[4] D M Thodi, J J. Rodriguez: Expansion embedding techniques for reversible watermarking. J. IEEE transactions on image processing. 16(3), 721-730 (2007)

[5] Z Ni, Y Q Shi, N Ansari, W Su.: Reversible data hiding. J. IEEE Transactions on Circuits and Systems for Video Technology. 16(3): 354-362 (2006)

[6] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[7] W. Zhang, K. Ma, N. Yu, Reversibility improved data hiding in encrypted images, Signal Process. 94 (2014) 118–127.

[8] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[9] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol.7, pp.826–832, Apr. 2012.

[10] M.Fujiyoshi, Separable reversible data hiding in encrypted images with histogram permutation, 2013 IEEE International Conference on Information Communication and Embedded Systems (ICICES), ICMEW2013, Page(s):1-4.

[11] A.K. Mohan, ; M.R.Saranya, ; K Anusudha, An Algorithm for Enhanced Image Security with Reversible Data Hiding 2014 International Conference on Contemporary Computing and Informatics (IC3I) 1042-1045