REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE BASED ON BLOCK HISTOGRAM SHIFTING

Zhaoxia Yin[1,2], Andrew Abel[3], Xinpeng Zhang[1,], Bin Luo[2]*

1. School of Communication and Information Engineering, Shanghai University, Shanghai 200072, P.R. China. xzhang@shu.edu.cn
2. Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, Hefei 230601, P.R. China. yinzhaoxia@ahu.edu.cn
3. Computing Science and Mathematics, University of Stirling. aka@cs.stir.ac.uk

[*] Corresponding author

ABSTRACT

Since there is good potential for practical applications such as encrypted image authentication, content owner identification and privacy protection, reversible data hiding in encrypted image (RDHEI) has attracted increasing attention in recent years. In this paper, we propose and evaluate a new separable RDHEI framework. Additional data can be embedded into a cipher image previously encrypted using Josephus traversal and a stream cipher. A block histogram shifting (BHS) approach using self-hidden peak pixels is adopted to perform reversible data embedding. Depending on the keys held, legal receivers can extract only the embedded data with the data hiding key, or, they can decrypt an image very similar to the original with the decryption key. They can extract both the embedded data and recover the original image error-free if both keys are available. The results demonstrate that higher embedding payload, better quality of decrypted-marked image and error-free image recovery are achieved.

Index Terms—Signal processing in encrypted domain (SPED), Reversible data hiding in encrypted images (RDHEI), Privacy protection

1. INTRODUCTION

Data hiding in digital images is very common, and can be divided into non-reversible [1,2] and reversible [3-10] categories, with the aim of reversible data hiding being to recover the original image error-free, which is of key interest in this paper. Reversible data hiding can be achieved mainly based on difference expansion [3-5] and histogram shifting [6-11]. All of these methods have good embedding efficacy for plaintext images. This means that the data hider must have access to and see the original cover image during the embedding process.

In many applications such as cloud computing and delegated calculation, multimedia owners need to transmit data to a remote server for further processing. Considering the needs of content security and privacy protection, the content owner needs to encrypt the data before uploading. Thus, signal processing in the encrypted domain (SPED) has become a very relevant issue in recent times. As a typical SPED topic, RDHEI can be used in many applications such as encrypted image authentication, content owner identification and privacy protection. Consequently, a number of RDHEI methods have been proposed [12-19].

In [12], an image is encrypted using a simple Exclusive-OR (EOR) operation and a data hider can embed additional data by flipping the three LSB (least significant bits) of pixels within data blocks. Hong et al. [13] improved on this with side block matching and smoothness sorting. Furthermore, Liao et al. proposed an improved method [19], in which multiple neighboring pixels are considered to reduce the average extracted-bit error rate. However, in these three methods, data can only be extracted after image decryption. This means that the data extraction is inseparable from the image recovery procedure.

To overcome the drawbacks, a separable RDHEI is proposed [14]. Legal receivers can choose three different options depending on the different keys held. Image decryption and data extraction is separable. While this approach was found to be successful, as the embedded payload increases, errors also increase, and the parameters make this approach somewhat complex for implementation. Recently, Wu and Sun [15] proposed another separable method based on pixel prediction. In the data hiding phase, a number of individual pixels are selected using a pseudo-random key, and additional bits are hidden in the two most significant bits. However, as the payload increases, the error rate also increases.

Apart from these methods, some RDHEI based on vacating room before encryption have also been proposed [16-18], where the reserved space is used to accommodate the additional data. However, making space for data embedding by the content owner might be impractical, because RDHEI methods always require the content owner to do nothing except image encryption, and data embedding is supposed to be accomplished by the data hider.

In summary, reversible data hiding in encrypted multimedia is an emerging technology, especially separable

RDHEI. There are four important evaluation criteria [12-15, 19]: the pure payload, the quality of the decrypted-marked-image, the error rate of the extracted data, and the error rate of the recovered image (i.e. the reversibility of the original image). This paper presents a new separable RDHEI method with higher embedding payload, better image quality and error-free data extraction and image reconstruction.

2. PROPOSED APPROACH

The framework of our proposed method can be seen in Figure 1.

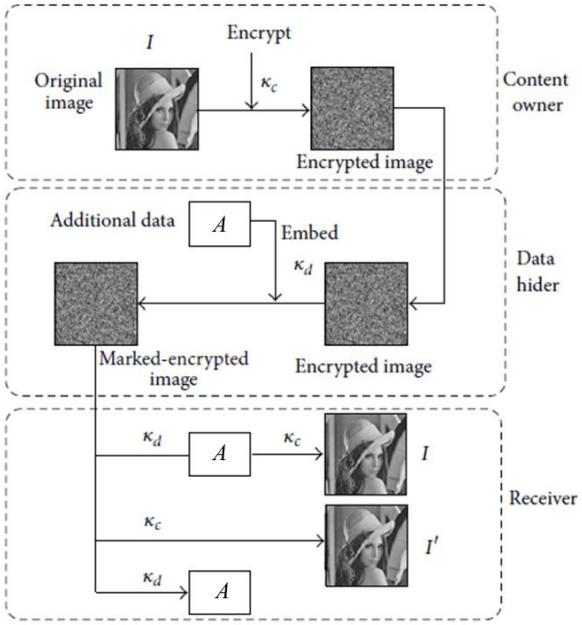

Fig. 1 Overall framework of RDHEI Approach

There are three main aspects of this approach, which can be divided into three main roles. Firstly, the content owner has the role of encrypting the original image, and generating the encrypted image. The content key K_c can be used both in image encryption and image decryption. The data hider then embeds additional data into the encrypted image by making use of BHS and generates a marked encrypted image $\bar{E}_X$ as well as a data hiding key K_d. Finally, $\bar{E}_X$ and one or both of the keys (K_c, K_d) can be sent to a legal receiver. As this is a fully reversible and separable method, $\bar{E}_X$ can be processed differently depending on the keys held by the receiver, returning either the additional embedded data A alone, a decrypted-marked-image I' (very similar to the original), or returning both A and the recovered image I.

2.1. Image Encryption

By adopting a permutation encryption based on Josephus traversing [20], an image I can be encrypted to create I_e. As a further additional level of security, a stream cipher is also adopted to encrypt the m Most Significant Bits (MSB) of I_e to produce a fully encrypted image E. Firstly, the original image I of dimensions $W_a \times W_b$ is divided into N non-overlapping blocks $\{B_i\}_{i=0}^{N-1}$, with each block B_i being composed of $u \times v$ pixels. Multi-granularity encryption is utilized using Josephus traversing to obtain the permuted blocks $\{\bar{B}_i\}_{i=0}^{N-1}$, and then further randomly permuting the pixels in each block. Thus, the encrypted image I_e can be decomposed into eight bit planes. Pseudo-random bits are then generated using a standard stream cipher and used to further encrypt m MSB of I_e by the Exclusive OR (EOR) processing operation, just as [12-14] and this produces the fully encrypted image E. The decryption K_c contains the block pixel dimensions u, v, as well as the seed value s_r needed for the stream cipher, and also the values required to implement the block level and pixel level Josephus traversal.

2.2. Location map marking

Conventionally, histogram contraction is commonly used to ensure that there are no saturated pixels present before histogram shifting techniques are utilized. This therefore means that we need to pre-process an image by modifying saturated pixels, which are noted in a location map H. In this paper, we present a location map marking approach that will allow for a much smaller location map to be created that significantly reduces the quantity of side information that has to be embedded. To perform the location map marking process, all pixels q in each block B are visited, i.e. all $\{B_i\}_{i=0}^{N-1} = \{\{q_{i,j}\}_{j=0}^{u\times v-1}\}_{i=0}^{N-1}$ are visited sequentially, assuming N blocks, with each block of dimension $u \times v$ pixels. Firstly, if a pixel is close to saturation, then $q_{i,j} \in \{1, 2^l - 1 - 1\}$, and accordingly the location map vector H has a value of '1' appended to it. If $q_{i,j} \in \{0, 2^l - 1\}$, this means a saturated pixel has been detected, and '0' is appended to H. The pixel $q_{i,j}$ is then modified as follows to produce the modified pixel $q'_{i,j}$

$$q'_{i,j} = \begin{cases} 2^l - 1 - 1, & q_{i,j} = 2^l - 1 \\ 1, & q_{i,j} = 0 \\ q_{i,j}, & \text{otherwise} \end{cases} \quad (1)$$

As a result, the location map H marks only values that are either saturated or within one bit of saturation. This means that the dimensionality of H can be significantly lower than using a full binary map, meaning that less side information has to be embedded.

2.3 Data embedding of BHS

We choose two pixels of each block randomly to use as the basis pixels and indicate peak values, and then can pass the seed used to generate these locations as part of a data hiding key. The peak values are therefore hidden within the image data, and are known to be self-hidden.

To carry out this process, for each image block B_i, two basic pixels $\hat{q}_{i,L}$, $\hat{q}_{i,R}$ are randomly selected and the remaining $u\times v-2$ pixels are denoted by $\{\bar{q}_{i,j}\}_{j=0}^{u\times v-3}$. Using the basic pixels $\hat{q}_{i,L}$, $\hat{q}_{i,R}$, two peaks in each block are determined, with $g_{i,L}$ and $g_{i,R}$ identified as Eqs. (2) and (3):

$$g_{i,L}=\min(\hat{q}_{i,L},\hat{q}_{i,R}) \tag{2}$$

$$g_{i,R}=\max(\hat{q}_{i,L},\hat{q}_{i,R}) \tag{3}$$

The data hider then concatenates H and the additional data A to form a string of message bits X, and then scans the non-basic pixels $\{\{\bar{q}_{i,j}\}_{j=0}^{u\times v-3}\}_{i=0}^{N-1}$ (i.e. excluding the two pixels used to determine peak values) to conceal X.

To do this, if a scanned pixel ($\bar{q}_{i,j}$) is equal to the value of $g_{i,L}$ or $g_{i,R}$, a bit $x\in\{0,1\}$ extracted from X is embedded by modifying $\bar{q}_{i,j}$ to $q''_{i,j}$ according to Eq. (4).

$$q''_{i,j}=\begin{cases}\bar{q}_{i,j}-x, & \bar{q}_{i,j}=g_{i,L}\\ \bar{q}_{i,j}+x, & \bar{q}_{i,j}=g_{i,R}\end{cases} \tag{4}$$

If a bit of value 0 is to be embedded, the value of $q''_{i,j}$ remains unchanged from $\bar{q}_{i,j}$. However, if a value of 1 is to be embedded, then depending if the value of $\bar{q}_{i,j}$ matches that of $g_{i,L}$ or $g_{i,R}$, the value of $q''_{i,j}$ is shifted by ±1. Otherwise, pixels that do not match $g_{i,L}$ or $g_{i,R}$ are either maintained or shifted by one unit according to Eq. (5).

$$q''_{i,j}=\begin{cases}\bar{q}_{i,j}, & g_{i,L}<\bar{q}_{i,j}<g_{i,R}\\ \bar{q}_{i,j}-1, & \bar{q}_{i,j}<g_{i,L}\\ \bar{q}_{i,j}+1, & \bar{q}_{i,j}>g_{i,R}\end{cases} \tag{5}$$

The resulting embedded blocks, then make up the final marked image $\{B''_i\}_{i=0}^{N-1}$.

2.4 Data extraction & image recovery

To extract data from an image consisting of marked image blocks $\{B''_i\}_{i=0}^{N-1}$, we consider the pixels $\{q''_{i,j}\}_{j=0}^{u\times v-3}$ in each block. However, it is important to note that we already know the location of the self-hidden peak pixel values, and so these pixels are left untouched, and only the non-basic pixels are considered. Message bits x can be extracted from each block B'_i using Eq. (6).

$$x=\begin{cases}0, & q''_{i,j}=g_{i,L} \text{ or } q''_{i,j}=g_{i,R}\\ 1, & q''_{i,j}=g_{i,L}-1 \text{ or } q''_{i,j}=g_{i,R}+1\end{cases} \tag{6}$$

In addition to extracting the message bits, the BHS process is also reversed to return the non-basic pixels $q''_{i,j}$ to their unmodified state $\bar{q}_{i,j}$ as follows.

$$\bar{q}_{i,j}=\begin{cases}q''_{i,j}, & g_{i,L}<q''_{i,j}<g_{i,R}\\ q''_{i,j}+1, & q''_{i,j}<g_{i,L}\\ q''_{i,j}-1, & q''_{i,j}>g_{i,R}\end{cases} \tag{7}$$

This then returns $B_i=\{\hat{q}_{i,L},\hat{q}_{i,R},\bar{q}_{i,j}\}_{j=0}^{u\times v-3}$, with all data removed and histogram shifting undone. Finally, the original image can be recovered using the location map H to undo the histogram contraction process. We consider all pixels $\{\hat{q}_{i,L},\hat{q}_{i,R},\bar{q}_{i,j}\}_{j=0}^{u\times v-3}$ in each block together to be $q'_{i,j}$ and then check all pixels $\{q'_{i,j}\}_{j=0}^{u\times v-1}$. If a pixel is close to saturation (i.e. $q'_{i,j}\in\{1,2^l-1-1\}$), then, h, the first non-processed value of location map H is extracted, and the pixel is modified using Eq. (8).

$$q_{i,j}=\begin{cases}2^l-1, & q'_{i,j}=(2^l-1-1) \quad AND \quad (h=0)\\ 0, & (q'_{i,j}=1) \quad AND \quad (h=0)\\ q'_{i,j}, & \text{otherwise}\end{cases} \tag{8}$$

3. EXPERIMENTS AND RESULTS

In this section, we firstly show the performance of multi-level encryption based on stream cipher and Josephus traversing. Furthermore, the performance of the proposed RDHEI is analyzed and compared with state-of-the-art alternative approaches [14-15] in terms of the pure payload, image quality and error rate with several commonly used test images and UCID datasets [21].

The histograms corresponding to the associated gray level pixel values before and after encryption are shown in Figure 2, showing the original image (top row), a previously used encryption approach [12-15] (middle row), and our approach (bottom row). Since the image encryption schemes introduced in [12-15] are the same, with a stream cipher adopted and applied to all bits of each pixel, the results are the same. It can be seen that with regard to histogram distribution, our encryption method has the same uniform appearance as the other approaches compared.

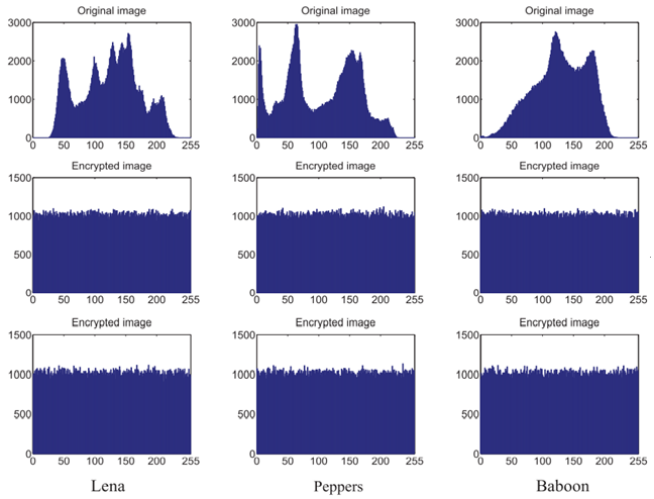

Fig. 2 The gray-level frequency histograms

The payload is the number of bits embedded in each pixel and the unit of measurement is bpp (bits per pixel). However, the reported small payload limits its potential for

practical applications. Take Lena as an example, the maximum payload of RDHEI proposed by [14] is 8596 bits, about 0.0328bpp. The pure payload of images from the UCID database using the proposed RDHEI method is shown in Figure 3. It can be seen that the pure payload varies depending on different cover images, and that most of the natural images have good performance. The mean pure payload of all of the 1338 images from UCID is 0.13bpp, with a peak value of 0.51bpp. It can also be seen that using an extra bit for embedding (and consequently one less for stream cipher encryption) can improve pixel payload.

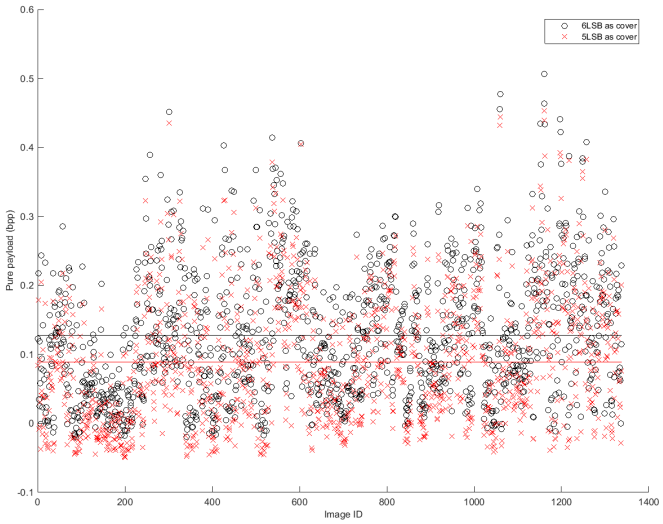

Fig. 3 The pure embedding payload performed on UCID database

The quality of the directly decrypted image, i.e. decrypted-marked-image quality, is another evaluation criterion. In order to further prove our proposed method, we compare the PSNR of the decrypted-marked-image generated by Wu [15] and the proposed method, with the results shown in Table 1.

Table 1. Examples of reversibility and image quality experimental results comparison

Image	Method	Payload	PSNR	Reversibility
Sailboat	Our	0.01	58.6	1
	Wu		30.63	0.9
	Our	0.03	53.89	1
	Wu		30.46	0.7
	Our	0.04	51.29	1
	Wu		30.38	0.64
Man	Our	0.01	59.28	1
	Wu		31.29	0.79
	Our	0.03	53.87	1
	Wu		31.07	0.6
	Our	0.04	52.41	1
	Wu		30.95	0.26
Tiffany	Our	0.01	58.29	1
	Wu		34.42	0.41
	Our	0.03	53.3	1
	Wu		34.25	0.21
	Our	0.04	52.09	1
	Wu		34.16	0.13
Jet	Our	0.04	52.46	1
	Wu		33.95	0.94
	Our	0.08	52.07	1
	Wu		33.15	0.9
	Our	0.12	51.33	1
	Wu		32.27	0.82

From the 4-th column of Table 1, we can see that the PSNR of the decrypted-marked-image generated by the proposed method is considerably better than the separable RDHEI proposed in [15].

The final criterion, the reversibility of the original image, is the possibility of lossless recovery, and its maximum value is 1 (i.e. fully recovered). If both keys are available, the original image ought to be recovered error-free. However, not all images can be fully recovered in [12-15]. To compare with state-of-the-art research, the last column of Table 1 shows the reversibility of Wu's method [15] and our proposed method. To get the strongest results, the eighth bit of the host pixel is used to embed data in Wu's method, and we perform the experiment in each image 100 times with the key ranging from 1 to 100 to calculate the mean possibility of lossless recovery. All experimental results show that the possibility of lossless recovery of our proposed method is 1, better than Wu's method [15] with the same payload.

4. CONCLUSION

This paper proposed and evaluated a new separable RDHEI framework. The results demonstrate that higher data embedding capacity, better decrypted-marked-image quality, error-free data extraction and accurate image reconstruction are achieved compared with other state-of-the-art research.

5. ACKNOWLEDGEMENTS

This research work is supported by National Science Fund for Distinguished Young Scholars under Grant No. 61525203, National Natural Science Foundation of China (61502009, 61472235, 61572308), "Shu Guang" project supported by Shanghai Municipal Education Commission and Shanghai Education Development Foundation, Anhui Provincial Natural Science Foundation (1508085SQF216), Project gxyqZD2016011 supported by the Key Program for Excellent Young Talents in Colleges and Universities of Anhui Province and the "Sino-UK" Higher Education Research Partnership for PhD studies" joint-project (2013-2015) funded by the British Council China and the China Scholarship Council (CSC).

REFERENCES

[1] W. Hong and T.S. Chen, "A Novel Data Embedding Method using Adaptive Pixel Pair Matching," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 1, pp. 176-184, Feb. 2012.

[2] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783, Nov. 2006.

[3] Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1500–1511, Dec. 2008.

[4] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[5] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 456–465, Sep. 2008.

[6] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, Mar. 2006.

[7] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906–910, Jun. 2009.

[8] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, no. 6, pp. 1129–1143, Jun. 2009.

[9] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 21, no. 8, pp. 1061-1070, Aug. 2011.

[10] X. Li, B. Ying, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[11] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.Q. Shi, "Pairwise prediction error expansion for efficient reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

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

[13] W. Hong, T. S. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[14] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[15] X. Wu and W. Sun, "High-capacity Reversible Data Hiding in Encrypted Images by Prediction Error," *Signal Processing*, vol. 104, pp. 387-400, Nov. 2014.

[16] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Process.*, vol. 94, pp. 118–127, Jan. 2014.

[17] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans.Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[18] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation," *IEEE Trans. On Cybernetics*, Doi: 10.1109/TCYB.2015.2423678, Apr. 2015.

[19] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *Journal of Visual Communication and Image Representation*, vol. 28, pp. 21-27, Apr. 2015.

[20] D. Xiang and Y. Xiong, "Digital image scrambling based on Josephus traversing," *Computer Engineering and Applications*, vol. 41, no. 10, pp. 44-46, May 2005.

[21] G. Schaefer and M. Stich, "UCID-an uncompressed color image database, *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, pp. 472–480, Dec. 2003.