ISSN 2319 - 5975

Volume 4, No.3, April - May 2015

International Journal of Networks and Systems

Available Online at http://www.warse.org/ijns/static/pdf/file/ijns02432015.pdf

Improved Reversible Data Hiding in Encrypted Images by Histogram Shifting Algorithm

Dr. L. M. Varalakshmi[1], M.A. Lovna Maria[2], S. Sivaranjini[3]

[1]Associate Professor, Dept. of ECE, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry, India.
varalakshmi_1@yahoo.co.in

[2]B.Tech Student, Dept. of ECE, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry, India.
lovnamaria@gmail.com

[3]B.Tech Student, Dept. of ECE, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry, India.
smvec.imageprocessing@gmail.com

Abstract: In this work an improved reversible data hiding scheme based on histogram shifting algorithm is proposed. Initially, the original image is encrypted by the sender by using a suitable encryption key. Then the data hider hides the data into the encrypted image without the knowledge of the sender by using a data hiding key to generate the marked image. Finally, the receiver by using both the keys can retrieve the data, as well as recover the original image without any distortion from the marked image. This algorithm divides the encrypted image into two blocks and the histogram shifting is performed for each block. The proposed method proves to be efficient compared to the other methods. Both the Peak Signal to Noise Ratio (PSNR) as well as the embedding rate has been highly improved.

Keywords: Reversible data hiding, DCT, histogram shifting, marked image.

1 INTRODUCTION

Reversible Data Hiding (RDH) is a method that hides the data into the original image without accessing the content of the image. This RDH algorithm provides a feature to transmit two different types of data namely, image and text at the same instant. Finally, the hidden data can be recovered error free from the original image without affecting its parameters. There are various data hiding techniques evolved in recent years for lossless extraction of data as well as image. Wu et al [15] proposed a data hiding scheme based on prediction error by making use of two methods namely joint method and separable method. Ni et al [7] introduced the data hiding based on histogram modification of the original image. But this algorithm does not support for data hiding in the encrypted images. Qian et al [14] performed the RDH by the n-nary histogram modification algorithm. Ma et al [4] proposed a reversible data hiding by reserving room before the encryption of the image. Zang et al [17] introduced a data hiding scheme in which some of pixels are estimated before the encryption so that the additional data can be embedded in the estimated errors. Zun [6] introduced a difference expansion scheme where the difference values of the neighboring pixels are calculated and the data bits are embedded into those difference values. Chang et al [1] proposed a RDH scheme based on Side Match Vector Quantization where the secret data bits are hidden in the compressed cover images and retrieved back. Zhang et al [18] introduced an RDH scheme in which the data hiding is performed in the compressed encrypted image and finally decompressed to bring back to its original form. Fei et al [9] introduced a method where the data hiding is based on adaptive level embedding, based on the block size. Li et al[5] performed data hiding by dividing the images into blocks of equal sizes and the data is embedded based on the maximum and minimum values determined by the pixel value ordering algorithm.

In all the above methods the image parameters are greatly affected for high payload images. Hence the proposed work aims to improve the above drawbacks. In this proposed work reversible data hiding scheme based on histogram shifting of the encrypted image is adopted. Here, first the original image is encrypted using a suitable transform like DCT (Discrete Cosine Transform). Then the secret data is hidden into the encrypted image by dviding the encrypted image into blocks and by shifting the histogram of each blocks to obtain the marked image. Then at the receiver side by using the decryption key and the data hiding key, the original image and the secret bits are retrieved.

The rest of this paper is organized as follows: The proposed scheme is explained in Section 2. The Simulation results and the parameters involved are given in Section 3. Some of the future works and conclusion are given in Section 4.

2 PROPOSED SCHEME

The proposed scheme consists of three phases. In the first phase, the owner of the image encrypts the image by using a suitable encryption key. In the second phase, the data hider hides the data by data by using another data hiding key. Finally in the third phase the receiver can access the data as well as reconstruct the original image by using the respective decryption key and data extraction keys. The block diagram of the proposed work is shown in Figure 1.

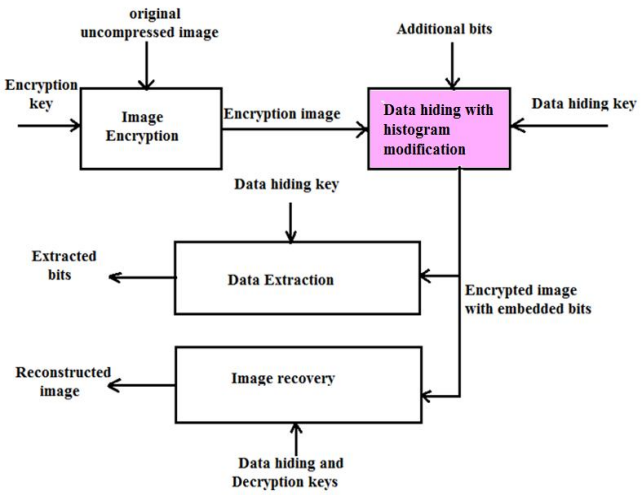


Figure 1. Block diagram of proposed scheme

2.1 Image Encryption

In the first phase, image encryption based on Discrete Cosine Transform (DCT) is performed. The various steps involved in this process are as follows, i) Take an original uncompressed image of pixel size m x n (0,255), ii) The image is broken into 8 x 8 blocks of pixels, iii) DCT is applied to each of these blocks, iv) Each block is compressed through quantization, v) The array of compressed blocks is stored in a drastically reduced amount of space.

The i,j^{th} entry of the DCT of an image is computed by the Eq. (1).

$$D(i,j) = \frac{1}{\sqrt{2}}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} p(x,y)cos\left[\frac{(2x+1)i\pi}{2N}\right]cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (1)$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, & if\ u = 0 \\ 1, & if\ u > 0 \end{cases} \quad (2)$$

To get the DCT matrix of Eq. (1), the Eq. (3) is used.

$$T_{i,j} = \begin{cases} \frac{1}{\sqrt{N}}, & if\ i = 0 \\ \sqrt{\frac{2}{N}}\cos\left[\frac{(2j+1)i\pi}{2N}\right], & if\ i > 0 \end{cases} \quad (3)$$

The DCT is performed by the Eq. (4).

$$D = TMT' \quad (4)$$

Where, M is the resultant matrix after subtracting 128.

To get the DCT matrix of Eq. (1), the Eq. (3) is used.

$$C(i,j) = round\left(\frac{D_{i,j}}{Q_{i,j}}\right) \quad (5)$$

The histogram of this encrypted image E is generated which retains the same information as that of the original image. And a key k_e is used for authentication access of this histogram.

2.2 Data Hiding

In the data hiding phase, the data hider hides the secret bits into the received encrypted image E without the knowledge about the original image.

The Embedding of the secret bit is performed by first dividing the encrypted image into two blocks. And for these blocks the histogram is generated separately. A binary tree is considered as shown in Figure 2. The no. of peak point are considered to be 2^K. The tree level K of the binary tree is found.. If the pixel difference is less than 2^K, the child node to the left is visited if the secret bit to be embedded is 0. Similarly the child node to the right is visited if the secret bit to be embedded is 1. Image distortion increases with increase in K value.

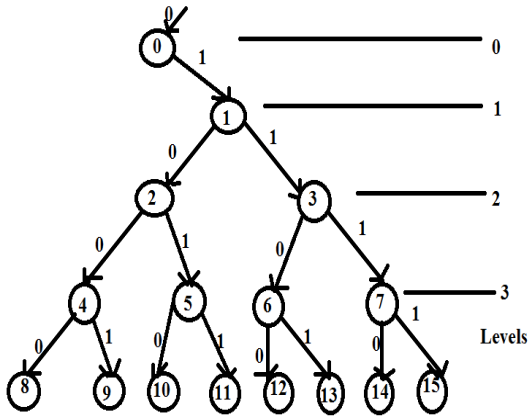


Figure 2. Binary Tree

Consider the first block's histogram. Now narrow the histogram range to 2^K, 255-2^K by shifting the histogram from both sides. Then scan the first block in the inverse S order .Now find the adjacent pixel's value differences. And once again scan the image in the same order. If the difference value d_i is greater than 2^K, the shifting is done by 2^K units as given in Eq. (6).

$$\begin{aligned} m_i = \{&x_i, \text{if } i = 0 \text{ or } d_i < 2^K, \\ &x_i + 2^K, \text{if } d_i > 2^K \text{and } x_i \geq x_{i-1}, \\ &x_i - 2^K, \text{if } d_i > 2^K \text{ and } x_i < x_{i-1}\} \end{aligned} \quad (6)$$

Where, m_i represents the watermarked image pixels.

If $d_i<2^K$, then message bits are embedded by Eq. (7).

$$m_i = \begin{matrix} \{x_i+(d_i+b)\ if x_i \geq x_{i-1} \\ x_i-(d_i+b)\ if\ x_i < x_{i-1}\} \end{matrix} \quad (7)$$

Similarly the same process is performed for the second blocks. And finally the encrypted image with secret bits in it leads to the formation of the marked image.

2.3 Data extraction and image reconstruction

After receiving the marked image at the receiver side, the receiver by using the data extraction key k_d and image decryption key k_e which are symmetric, the receiver can extract the original image along with the secret bits.

Now for this marked image of pixel value m_i,the secrets bits are extracted as follows. Consider the first block's histogram and scan it in inverse S order.

If $|m_i\ x_{i-1}| < 2^{(K+1)}$, extract secret bits by Eq. (8).

$$b=\{0,\text{if}|m_i-x_{i-1}|\ \text{is even} \quad 1,\text{if}|m_i-x_{i-1}|\ \text{is odd} \tag{8}$$

Where, x_{i-1} denotes the recovered value of m_{i-1}.

And the original pixel value of the encrypted image is recovered by Eq. (9).

$$\begin{cases} x_i = m_i + \text{floor}(|m_i - x_{i-1}|/2) & \text{if} |m_i - x_{i-1}| < 2^{(K-1)} \text{and } m_i < x_{i-1} \\ m_i - \text{floor}(|m_i - x_{i-1}|/2) & \text{if} |m_i - x_{i-1}| < 2^{(K-1)} \text{and } m_i > x_{i-1} \\ m_i + 2^K & \text{if} |m_i - x_{i-1}| \geq 2^{(K-1)} \text{and } m_i < x_{i-1} \\ m_i - 2^K & \text{if} |m_i - x_{i-1}| \geq 2^{(K-1)} \text{and } m_i > x_{i-1} \\ m_i & \text{otherwise} \end{cases} \tag{9}$$

This process is repeated until all the secret bits are extracted from the two image blocks.

Secondly after extracting the secret bits the receiver by using the key k_e can recover the image. The receiver can regenerate the original image from the encrypted image by Eq. (11). Here inverse DCT is used for recover the image. Reconstruction of the image begins by decoding the bit stream representing the quantized matrix. Each element of quantized matrix is then multiplied by the corresponding element of the quantization matrix originally used.

$$R_{i,j} = Q_{i,j} \times C_{i,j} \tag{10}$$

The IDCT is next applied to matrix R and finally 128 are added to each element of that result of matrix then the original image is retrieved by using Eq. (11).

$$N = round(T' R\, T) + 128 \tag{11}$$

3 SIMULATION RESULTS AND ANALYSIS

Experiments were conducted using Matlab R2012a to verify the proposed method. The test images are standard gray scale images of sizes 256x256 shown in Figure 3.

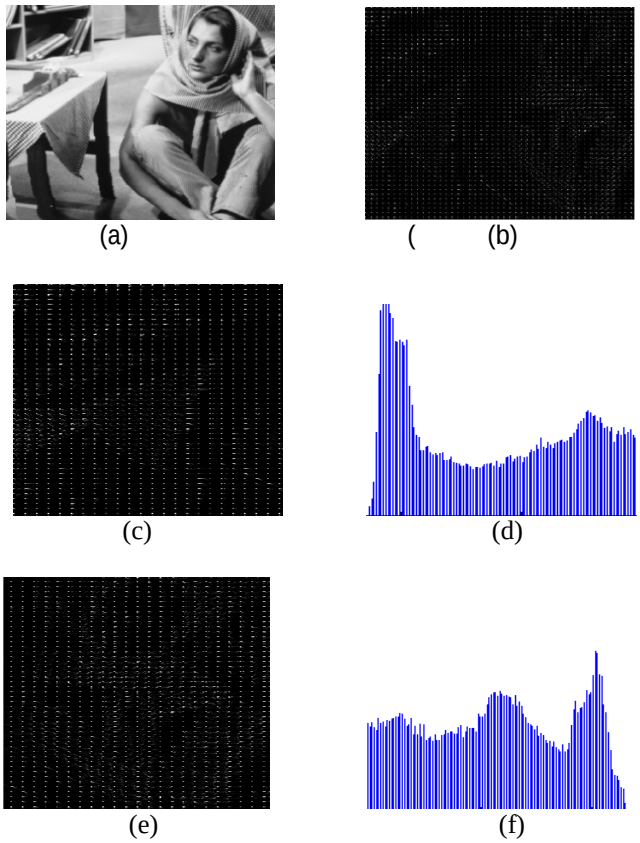
(a) (b)

(c)

Figure 3. Test images (a) Barbara (b) Lena (c) Camera man

The experimental results on the test image Barbara is shown below in Figure 4.

(a)The original image,
(b)Encrypted Image,
(c) Block 1 Encrypted image, (d) Histogram of (c),
(e) Block 2 Encrypted image, (f) Histogram of (e),
(g) Approximately recovered image (image with secret data),
(h) Recovered original image.



(a) ((b)

(c) (d)

(e) (f)


(g)


(h)

Figure 4. Experimental results for test image barbara

3.1 Performance Results

The following performance parameters are discussed: Peak Signal To Noise Ratio(PSNR), Embedding rate, Mean Square Error, Maximum difference. These parameters are used to analyse the performance of experiment conducted.

Embedding rate is defined as the amount of secret bits hidden in the given image.This is one of the important parameter to measure the data hiding capacity. It is is given by Eq. (12).

$$Embedding\ Rate = \frac{Total\ embedded\ bits}{Total\ image\ pixels} \quad (12)$$

The Mean Square Error is used to measure the Peak signal to Noise Ratio and it is given by Eq. (13).

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(O_{i,j} - D_{i,j}\right) \quad (13)$$

Peak Signal to Noise Ratio is used to measure the quality of the reconstructed image and it is calculated from the MSE by Eq. (14).

$$PSNR = 10log_{10}\frac{255^2}{\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(O_{i,j}-D_{i,j}\right)^2} \quad (14)$$

The average difference estimates the amount by which the experimental results changes the outcome of the average compared with the control. It is given by Eq. (15).

$$AD = \sum_{i=1}^{m}\sum_{j=1}^{n} f(y_i)f(y_j)|y_i - y_i| \quad (15)$$

The Structural Content is the measure of similarity between the original image and the decrypted image and it is given by Eq. (16).

PARAMETERS	Histogram Shifting Algorithm	Existing Work[15]
PSNR(db)	40.214	33.14
MeanSquare Error	6.189	7.17
Average Difference	0.0789	0.081
Structural Content	1.0010	0.998
Embedding Rate(bpp)	0.45	0.122

Table 1 – Performance Analysis

$$SC = \frac{\sum_{i=1}^{m}\sum_{j=}^{n}\left(o_{i,j}^2\right)}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(D_{i,j}^2\right)} \quad (16)$$

Where, m and n are the no of pixels present in the rows and columns (256 x 256) with the limits $1 \le i \le m$ and $1 \le j \le n$ and f(y) is a function.

The comparison table for various parameters are shown in Table1.

4 CONCLUSION

This work proposes an improved reversible data hiding in encrypted images by histogram shifting technique. This work provides full security for the image as well as the data by using two distinct symmetric keys. Hence the receiver can easily extract the image and the secret data error free according to his needs by using both the keys or any one of them, as this method is highly separable. Compared to the other existing RDH methods, the proposed scheme highly improves the embedding rate as well as the PSNR of the image. The above work is simulated using MATLAB simulation tool.

The future work of this proposed RDH algorithm is to implement this to video sequences by dividing the sequences into frames and performing the similar process to each of these frames and to obtain better results.

REFERENCES

[1] Chang et al," **A Reversible data hiding scheme based on side match vector quantization**", IEEE Trans Circuits System Video Technology, Vol.16, No.10, October 2006, pp. 1301-1308.

[2] Celik et al, "**Lossless generalized – LSB data embedding**", IEEE Trans. Image Process, Vol.14, No.2, 2005, pp. 253-266.

[3] Hu et al, "**DE-Based Reversible data hiding with improved overflow location map**", IEEE Trans Circuits System Video Technology, Vol.19, No.2, February 2009, pp. 250-260.

[4] Hong et al,"**An improved reversible data hiding in encrypted images using side match**", IEEE Signal Process, Vol. 19, No.4, 2012, pp. 199-202.

[5] Li et a;, "**High-fidelity reversible data hiding scheme based on pixel value ordering and prediction error expansion**", Signal Process. Vol. 93, No. 1, 2013, pp. 198-205.

[6] Liu et al,"**Efficient compression of encrypted grayscale images**", IEEE Trans. Image Process. Vol. 19, No. 4, 2010, pp. 1097-1102.

[7] Ni et al, "**Reversible data hiding**", IEEE Transaction Circuits Systems Video Technology, Vol.16, No.3, 2006, pp. 354-362.

[8] Tai et al, "**Reversible data hiding based on histogram modification of pixel differences**", IEEE Trans. Circuits System Video Technology, Vol.19, No. 6, June 2009. pp. 906-910.

[9] Thodi et al, "**Expansion embedding techniques for reversible watermarking**", IEEE Trans. Image Process. Vol. 16, No. 3, 2007, pp. 721-730.

[10] J.Tian, "**Reversible data embedding using a difference expansion**", IEEE Trans Circuits System Video Technology, Vol. 13, No.8, August 2003, pp. 890-896.

[11] X.Zhang, "**Separable reversible data hiding in encrypted image**", Trans. Inf. Forensics Secure, Vol. 7, No.2, March 2012, pp. 826-832.

[12] Peng et al, "**Adaptive reversible data hiding scheme based on integer transform**", Signal Process, Vol.92, No. 1, 2012, pp. 54-62.

[13] Puech et al, "**A reversible data hiding method for encrypted images**", in: Electronic Imaging, International Society for Optics and Photonics, 2008, pp. 68191E-1-68191E-9.

[14] Qian et al,"**Separable reversible data hiding in encrypted images by histogram modification**", in: The Third International Conference on Multimedia Technology, Atlantis Press, Paris, 2013, pp. 869-876.

[15] Wu et al, "**High-capacity reversible data hiding in encrypted images**", Elsevier B.V., Signal Processing, Vol. 104, 2014, pp. 387-400.

[16] Zhang, "**Separable reversible data hiding in encrypted image**", IEEE Trans.Inf.Forensics Secur, Vol.7, No.2, 2012, Pg. No. 826-832.

[17] Zhang et al, "**Reversible data hiding in encrypted images using pseudorandom sequence modulation**", in: Digital Forensics and Watermarking, Springer, Berlin, 2013, Pg. No. 358-367.

[18] Zhang et al, "**Reversibility improved data hiding in encrypted images**", Signal Process, Vol. 94, 2014, Pg. No. 118-127.