ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Reversible Data Hiding in Encrypted Image: Algorithm, Result and Analysis

Chetan G. Tappe[1], Prof. A.V. Deorankar[2]

P.G. Student, Department of Computer Engineering, Govt. College of Engineering, Amravati, India[1]

Associate Professor, Department of Information Technology, Govt. College of Engineering, Amravati, India[2]

ABSTRACT: The proposed scheme is made up of image encryption, data embedding and data extraction, image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the information hide compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a scrubby space to accommodate the embedded data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

KEYWORDS:RDH, Image encryption, Secure communication, LSB, Reversible image transformation (RIT).

I. INTRODUCTION

Now, images from various bases are recurrently used and conveyed through the internet for various applications, such as online personal photograph albums, private enterprise archives, document storage systems, medicinal imaging systems, and army image databases. These images usually contain private or confidential information so that they should be protected from leakages during communications. Recently, many methods have been planned for securing image transmission, for which two collectivemethods are image encryption and data hiding. Another normally used method for secure image transmission is data hiding, in data hiding secret image is hidden behind a carrier; carrier can be anything an image, document, audio file and a video file. Now a day for secure image transmission a new concept is being in used that is of mosaic image in the field of data hiding.

Application scenarios, an inferior assistant or a channel administrator hopes to append some added message, such as the origin data, image symbolization or secret data, within the encrypted image though he does not know the original image data. For example, when medical images have been encrypted for protecting the patient secrecy, a database manager may aim to embed the private information into the consistent encrypted images. It may be also confident that the original content can be retrieve without any error after decryption and recover of extra message at receiver side. That means a reversible data hiding scheme for encrypted image is necessary.

II. RELATED WORK

Newly weimingzhang, huiwang, dongdonghou, and nenghaiyu proposition a novel context [1], for RDH-EI based on reversible image transformation (RIT). different from all previous encryption-based contexts, in which the cipher texts may invite the representation of the snooping cloud, RIT based context permits the user to transform the contented of real image into the content of another entity image with the same size. the converted image that looks like the target image is used as the scrambled image. reversible data hiding in images is a technique that hides data in digital images for secret communication. it is a technique to hide other message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

DOI: 10.15680/IJIRCCE.2017. 0504317

zhang separated the encrypted image into some blocks. by flipping 3 LSBs (least significant bits) of the half of pixels in each block, room can be vacated for the embedded bit. the data insertion and image retrieval proceed by finding which part has been flipped in one block. this process can be recognized with the help of spatial association in the decrypted image. the decoder side by further exploiting the spatial correlation using a dissimilar estimation equation and side match technique. for both methods in [2] and [3], decrypting image and extracting data must be jointly executed.

Recently, zhou et al. [4] proposed a novel RDH-EI method for joint decryption and extraction, in which the correlation of plaintexts is further exploited by unique the scrambled and non-scrambled pixel blocks with a two-class classifier. to separate the data extraction from image decryption, zhang emptied out space for data embedding by directly using the typical manner of cipher text compression that is, compressing the encrypted pixels in a lossless manner by using the syndromes of parity-check matrix of channel codes.

III. PROPOSED ALGORITHM

A. Least Significant Bit Algorithm

1. Read image and convert pixel value in binary format.
2. Convert data byte into binary format.
3. Perform binary addition.
4. Convert resultant binary values into pixels RGB values.
5. Initialize new bitmap image with changed pixels.
6. Continue steps 2,3,4,5 until all the data bytes get processed.
7. Save the resultant image.

- **Example of LSB**

Let's assume that we want to embed the letter 'A' into a 24-bit cover image. The binary value of 'A' is 10000011.
Assume the three adjacent pixels of the image are the following:

(10110100 11010111 10001110)
(00011100 11110110 11010111)
(10001110 00011100 11100101)

After applying LSB steganography algorithm the following pixels of stego-image is acquired. Bits that have been changed because the cover image pixels did not match the message bits are represented in red.

(10110101 11010110 10001110)
(00011100 11110110 11010110)
(10001111 00011101 11100101)

The algorithm first selects a pixel (xi) sequentially. Then it checks whether the least significant bit of (xi) matches with the message bit (mi). Least significant bit of a pixel is the redundant bit which is the most right bit of a byte. If LSB (xi) = mi, then no change otherwise LSB of xi is substituted with mi. Then it selects the next pixel and message bit and checks whether they match or not. This process continues until reaching the end of secret message bits where all secret bits are embedded in the image.

B. Pixel Shuffling Algorithms

i. X Reverse

ii. Y Reverse

i. X Reverse

```
1. Initialise string str with with x pixel  values
2. initialize rev[] character array
3. initialize i=str.length-1
Initialize counter cnt=0
4. for i= str.length-1 to 0
5. rev[cnt]=str[i]
6. decrement value of i by 1
7. if i<0 then repeat steps 5 & 6
8.else stop
```

ii. Y Reverse

```
1. Initialise string str with y pixel  values
2. initialize rev[] character array
3. initialize i=str.length-1
   Initialize counter cnt=0
4. for i= str.length-1 to 0
5. rev[cnt]=str[i]
6. decrement value of i by 1
7. if i<0 then repeat steps 5 & 6
8.else stop
```

IV. SIMULATION RESULTS

This section gives brief idea about comparison of computational analysis and experimental analysis. Here we are compare both model on the basis of some analysis parameter. Here we choose two parameter for Peak Signal Noise Ratio and Mean Square Error. Which is expressed in terms of bits per pixel (bpp)? The objective of any reversible image transformation algorithm is to reduce the mean square error. And increase peak signal noise ratio improves for image quality.

Then the statistical measurement like peak signal to noise ratio (PSNR) and mean square error (MSE) are obtained using .net platform and shown in Table 4.4.1.

The peak signal to noise ratio is the most important terms with respect to measure the quality of a cover image and its corresponding stego-image. The PSNR is measured using the following equation-

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

Where M is peak signal level for a color image and MSE is computed by the equation:

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{M} (C(i,j) - S(i,j))^2$$

H and W are the height and width of the frame and C(i, j) and S(i, j) represents the cover image and corresponding stego-image respectively. A high value of PSNR indicates the less distortion in stego-image, hence the discrepancy between cover image and stego-image is more invisible to human eyes.

Table:4.4.1 Statistical Measurement Propose System

Encoded Image size (MB) 8 bit Image	PSNR dB	MSE	SD	Mean
8	62.62	0.032	38.018	142.99
14	80.55	0.005	48.74	118.60
7	53.08	0.319	30.85	87.74
14	54.032	0.256	36.35	160.66
3	54.12	0.319	36.69	159.20
2	44.02	0.619	48.41	118.171
2	40.07	0.719	43.29	141.21
2	34.02	25.74	48.41	118.17
3	34.19	24.50	29.92	87.43
4	35.96	16.29	30.32	87.37

Table 4.4.1. gives the Peak Signal Noise Ratio, Mean Square Error, Standard Deviation of the image file. While Comparing the result on the basis of Analytic and experimental result outlines can be depicts. A graphical figure 4.4.1 showing a result for different images on the basis of the PSNR and MSE of the provided images.

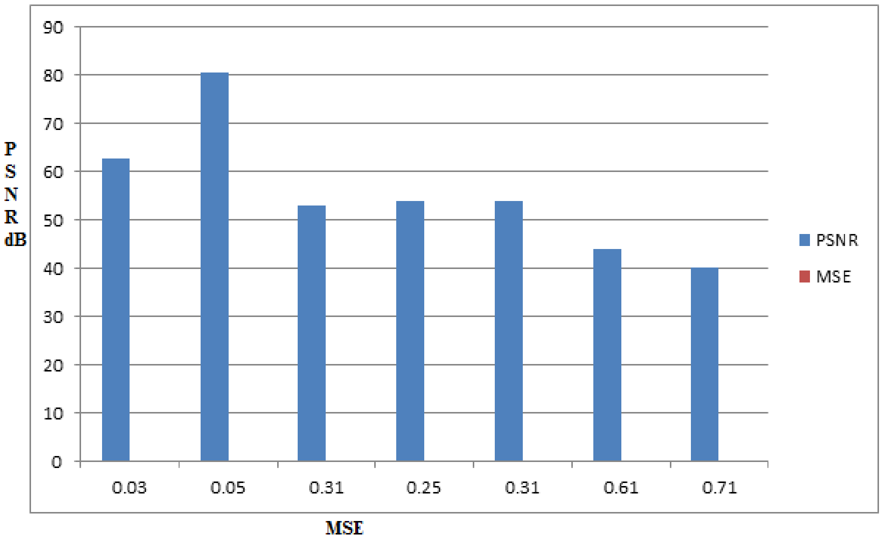

Figure 4.4.1: Graphical Representation of PSNR and MSE

The statistical measurements of the proposed method ensure the better PSNR and MSE value compared to existing system vs propose system as following Table 4.4.2:

DOI: 10.15680/IJIRCCE.2017. 0504317

Table 4.4.2: Comparison Between Existing System vs Propose System

Experiment Images	Existing System	Propose System
	PSNR dB	PSNR dB
A	30.68	54.032
B	30.72	54.12
C	30.95	44.02
D	30.09	40.07
E	30.83	34.02

Table 4.4.2 gives the statistical measurements of the proposed method ensure the better PSNR value compared to existing system. A graphical figure 4.4.2 showing a result for different images on the basis of the PSNR for comparing existing system vs propose system.

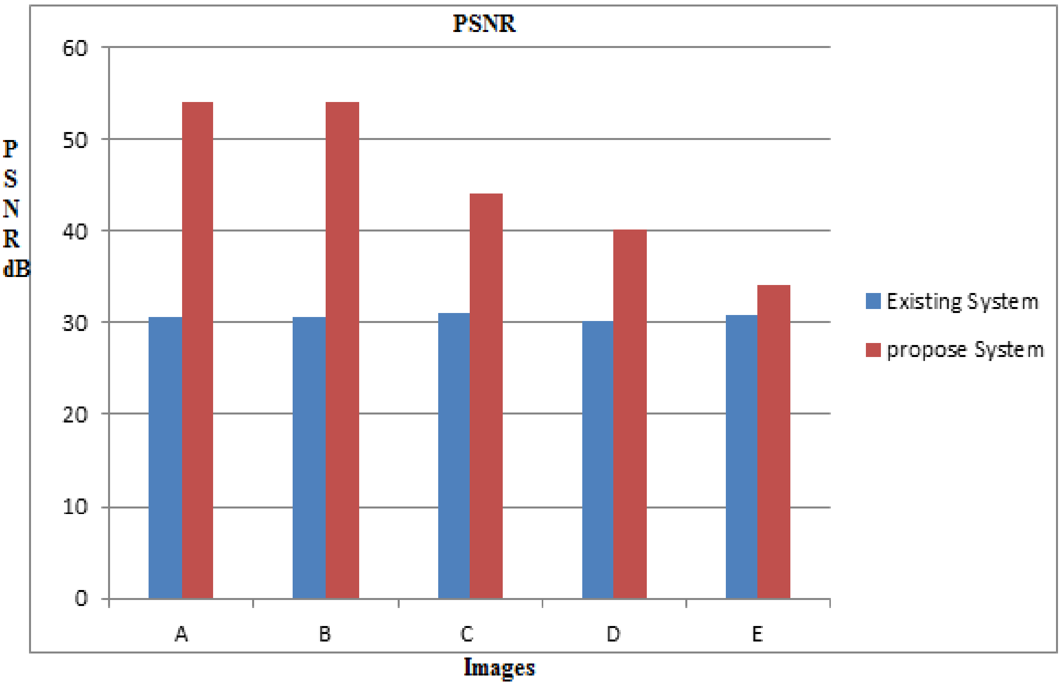

Figure 4.4.2: Graphical Representation of Comparison of Existing Vs Propose System

V. Conclusion and Future Work

An algorithm for Enhanced Image Security with Reversible Data Hiding. The method consists of image encryption, data hiding, and data extraction and image recovery phases. In the first phase, owner of the image encrypts the image by chaotic permutation using encryption key. The data hider without knowing the original content can hide data into the encrypted image using data hiding key. For this histogram modification based method is used. Data hiding capacity of this method is much higher than that of the data hiding methods used in existing reversible data hiding in encrypted image techniques. At the receiver side, data extraction and image recovery are performed in a separable manner. The receiver with data hiding key only can extract the hidden data, but cannot decrypt the image. The receiver with encryption key only can generate an image similar to the original image by decryption, but cannot read the hidden data.

PSNR value obtained is much higher than that of existing reversible data hiding techniques in encrypted image. If the receiver has both keys, he can extract the data and recover the original image completely.

REFERENCES

1. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process, vol. 18, No. 4, pp. 255–258, Apr. 2011.
2. W. Liu,W. Zeng, L. Dong, andQ.Yao, "Efficient compression of encrypted gray scale images," IEEE Trans. Image Process., vol. 19, No. 4, pp. 1097–1102, Apr. 2010.
3. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. vol. 18, No. 4, pp. 255–258, Apr. 2011.
4. X. Zhang, " data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, No. 2, pp. 826–832, Apr. 2012.
5. 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. Cybern., vol. 46, No. 5, pp. 1132–1143, May 2016.