ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 4, Special Issue 1, March 2015*

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

Room Reserved Reversible Data Hiding in Encrypted Images

Ann Mary Thomas [1], Binson V A[2]

PG Student, Dept. of ECE, College of Engineering, Kalloopparaa, Kerala, India[1]

Assistant Professor, Dept. of AEI, Saintgits College of Engineering, Pathamuttom, Kerala, India [2]

ABSTRACT:Reversible data hiding (RDH), a technique for hiding data in encrypted images, is gaining its publicity day by day.The reason is that it maintains the excellent property of losslessly recovering the cover imageand embedded data meanwhile it protects the image content's confidentiality. In all previous methods data is embedded by reversibly vacating room from the encrypted images, which may create some errorsat the time of data extraction and image restoration. Here themethod describes reserving room before encryption so that it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method is capable of achieving real reversibility, that is, ultimately data extraction and image recovery will be free of any error.

KEYWORDS: Reversible data hiding, image encryption, privacy protection, histogram shift.

I.INTRODUCTION

Data hiding is a process to hide data into cover media, which may be image or any other digital media.Data hiding process combines two different sets of data, first set of the embedded data and set of the cover media data. In most cases, the cover media becomes distorted due to data hiding and cannot be recovered as the original media. That is, cover media gets permanent distorted even after the hidden data is extracted. In applications, such as medical diagnosis, military imagery and law forensic, it is expected that, the original cover media can be recovered efficiently with no loss. The techniques satisfying this requirement are referred to as reversible, lossless or invertible data hiding techniques .

The motivation of reversible data embedding is distortion-free data embedding.Thoughimperceptible,embedding some data will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required.

From the application point of view, reversible data embedding can be used as an information carrier. Since the difference between the embedded image and original image is almost imperceptible from human eyes, reversible data embedding could be thought as a covert communication channel. By embedding its message authentication code, reversible data embedding provides a true self authentication scheme, without the use of metadata.

From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state. The performance of a reversible data-embedding algorithm can be measured by the following.

1) Payload capacity limit*:* the maximal amount of information can be embedded
2) Visual quality*:*the visual quality on the embedded image
3) Complexity:complexity of the algorithm

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This major applications of this technique is that it is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest. In practical aspect, many RDH techniques have emerged in recent years. In RDH, by first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 4, Special Issue 1, March 2015

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift, in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods usually combined difference expansion or histogram shift to residuals of the image, e.g., the predicted errors, to achieve better performance

II.EXISTING TECHNIQUES

Techniques available for reversible data hiding are as follows:

a) RDH techniques for plain spatial domain

A method of reversible data embedding based on difference expansion is proposed in [1]. Due to redundancy between the values of neighboring pixel in natural images, differences between pixels are used to embed data. In method of difference expansion method, the differences between two adjacent neighboring pixels are calculated and expanded or doubled i. e. multiplied by 2 and new least significant bits are generated. New least significant bits are used to hide additional data.

The advantages are – (i) no loss of data due to compression and decompression, (ii) it can be applicable to audio and video data. The disadvantages include – (i) there may be some round off errors , though very little, (ii) mainly depends on the smoothness of natural image; so cannot be applied to textured image where the capacity will be zero or very low, and (iii) there is significant degradation of visual quality due to bit-replacements of gray scale pixels.

A histogram-based reversible data hiding technique is discussed in [2], where the data is embedded into the bins of histogram. This method utilizes pairs of peak points and zero points to achieve low embedding distortion. The advantages of this method are – (i) it is simple to use, (ii) it always gives a constant PSNR 48.0dB, (iii) distortions are quite invisible, and (iv) capacity is high. The disadvantages are – (i) capacity is limited by the frequency of peak-pixel value in the histogram, and (ii) it searches the image more times, so the algorithm is more time consuming.

b) RDH techniques for encrypted domain

There are two different types of reversible data hiding for an encrypted image; non separable and separable reversible data hiding. A method of non separable reversible data hiding in encrypted image is as shown in Fig.1 Non separable data hiding technique is consisting of image encryption, data embedding, image decryption and image recovery/data extraction phases.

First content owner encrypt the original uncompressed image by using encryption key to produce encrypted image and then data hider embeds additional data into encrypted image using data hiding key though he does not know the content of original image. With encrypted image containing additional data, the receiver may first decrypt it using encryption key and then extract the embedded data and recover the original image using data hiding. That is in this technique, the data extraction is not separate from image recovery.

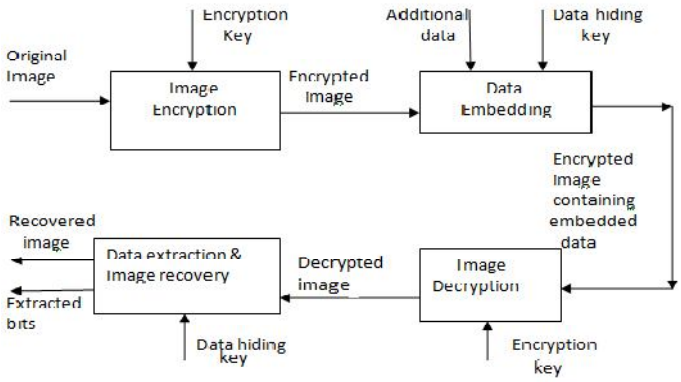

Figure 1 : Non separable RDH

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 4, Special Issue 1, March 2015*

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

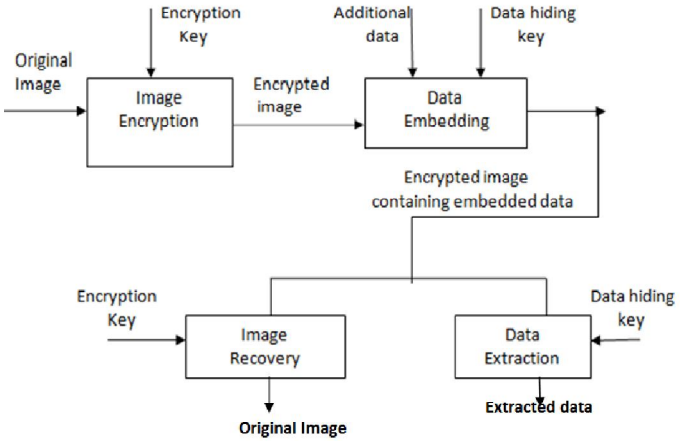

Figure 2 : Separable RDH

In [3], a reversible data hiding scheme for encrypted image consisting of image encryption, data embedding and data extraction and image recovery phases are proposed. First content owner encrypts the original image by a stream cipher.

Then segments the encrypted image into number of non overlapping blocks of size a× a; each block is used to carry one additional bit. For this, pixels in each block are pseudo-randomly divided into two different sets S1 and S2 according to a data hiding key. If the bit to be embedded is 0, flip the 3 LSBs of every encrypted pixel in S1 otherwise flip the 3 encrypted LSBs of pixels in S2. For extraction of data and image recovery, the receiver flips all three LSBs of pixels in S1 to form a new decrypted block, and flips all three LSBs of pixels in S2 to form another new block; one of them will be decrypted to the original block. Because of spatial correlation in natural images, original block is presumed to be smoother than interfered block and embedded bit can be extracted correspondingly.

But the work mentioned above did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel corrections in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. In [4],atechnique for separable reversible data hiding in encrypted images is suggested. Separable reversible data hiding technique is as shown in Fig.2

Space for data embedding by following the idea of compressing encrypted images is discussed in [6] and [7]. First the content owner encrypts the original image using an encryption key. Once image is encrypted, data hider compresses the least significant bits of the encrypted image using a data-hiding key and creates a sparse space to accommodate the additional data. On other end, from an encrypted image containing additional data, using only the data-hiding key, the receiver may extract the additional data, or obtain an image as the original one using only the encryption key. When the receiver has both data hiding and encryption keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

The method in [4], based on framework reserving room after encryption. Losslessly vacating room from encrypted images is relatively difficult and sometimes inefficient and generate marked image with poor quality for large payloads.

III.PROPOSED METHOD

The proposed method primarily follows 4 steps:

- Reserving room for hiding data

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 4, Special Issue 1, March 2015

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

- Image encryption
- Hiding data in encrypted image
- Data extraction and image recovery

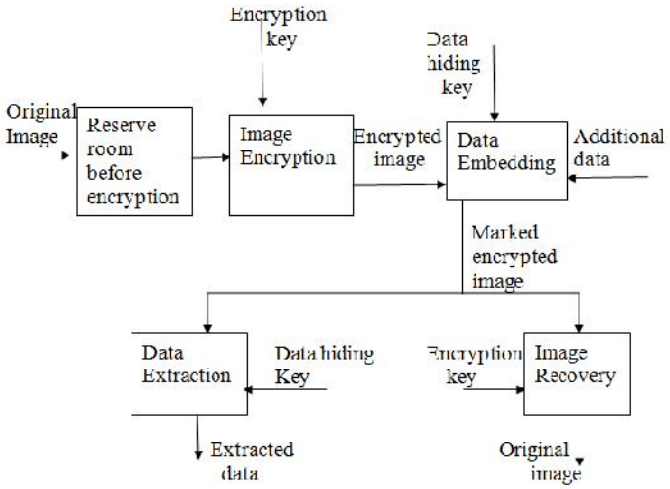

Fig 3: Architecture of the proposed system

Room reserving:

Reserving room for data hiding stage includes the partition of image and self reversible embedding steps. At the beginning, in an original image with variable size, space is reserved for hiding data in encrypted image by using the method of partitioning the original image into two parts: A and B. The image is symmetrically divided and this division is done which would be helpful in the next stage of process.

Once image is partitioned into two parts, self reversible technique is applied. The LSBs of A are reversibly embedded into B. Now concatenating A and B, we will get the room reserved image.

Image encryption:

Once room is reserved for data hiding, image is encrypted using RC4 algorithm. RC4 is a stream cipher and symmetric key algorithm, i.e., both encryption and decryption of image uses the same keys. In RC4, Data stream is XORed with the generated key sequence. The key stream is not dependent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext. Image encryption using RC4 is consists of generation of encryption key and generation of pseudo-random sequence.

Generation of Encryption Key

Encryption key is 128 bit value. It is generated randomly by using the random function. The random function generates the random key in an uniformly distributed function

.

Generation of Pseudo-Random Sequence

Pseudo random sequence consists of random bits generated using the encryption key. In our system, RC-4 algorithm is used to create the pseudo-random sequence using the 128-bit encryption key. It is represented as sequence of bytes (An array of bytes). The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in pseudorandom sequence should be double the number of pixels.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 4, Special Issue 1, March 2015*

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

For example, a grayvalue$X_{i,j}$ ranging from 0 to 255 can be represented by 8 bits, $X_{i,j}$ (0), $X_{i,j}$ (1), $X_{i,j}$ (2)..... $X_{i,j}$ (7), such that

$X_{i,j}(k)=\lfloor Xi,j/2^{k} \rfloor \bmod 2, \quad k=0,1,2.....7$

The encrypted bits $E_{i,j}(k)$ be calculated through exclusive- OR operation.

$E_{i,j}(k) = X_{i,j}(k) \oplus r_{i,j}(k)$

where $r_{i,j}(k)$ is generated via a standard stream cipher determined by the encryption key.

Note that after image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

Data hiding in encrypted image:

Once the encrypted version of image is generated, the content owner sends it to a data hider. Once the data hider receives the encrypted version of original image, data hider embeds additional data into space which is already emptied out by using data hiding key , although the data hider doesnot get access to the original image.Here data is embedded simply using LSB replacement.Anyone who doesnot possess the data hiding key could not extract the additional data embedded.

Data extraction and image recovery:

At the receiver side, if receiver has encryption key only, then he can obtain image as the original one and may extract the additional data using only data hiding key. When receiver has both encryption key data hiding key, he can recover the original image as well as extract the additional data. This method separates the data extraction from image decryption as well as reversible in nature, i.e., data extraction and image recovery will be free of any error. As data extraction is not dependent on image decryption, this implies two different practical applications. Also the proposed method improves the data embedding capacity as compared to the existing method for data hiding in encrypted images. Also the proposed method based on the concept of reserving room achieves real reversibility, that is , data extraction and recovery of original image will be free of any error.

.IV. WORK IMPLEMENTION

The following screenshots represents the implemented work of the system.Here standard image Lena is taken to demonstrate the feasibility of proposed method.

a b

Fig 4: a) input image b) room reserved image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 4, Special Issue 1, March 2015*

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

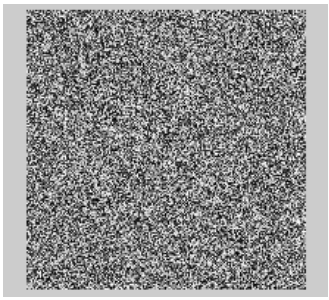

Fig 5: encrypted image

a b

fig 6: a) input message b) encrypted message

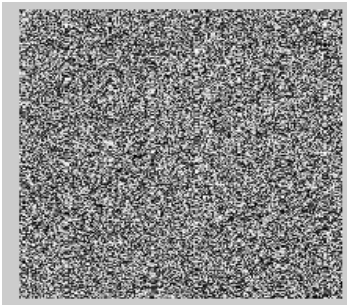

Fig 7: image after data hiding

a b

fig 8: a) extracted message b) decrypted messag

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 4, Special Issue 1, March 2015*

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

Fig 9: recovered image

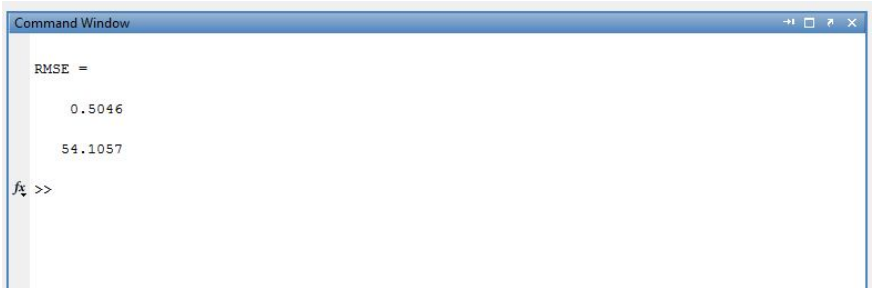

Fig 10: MSE and PSNR

Fig 11: recovered image

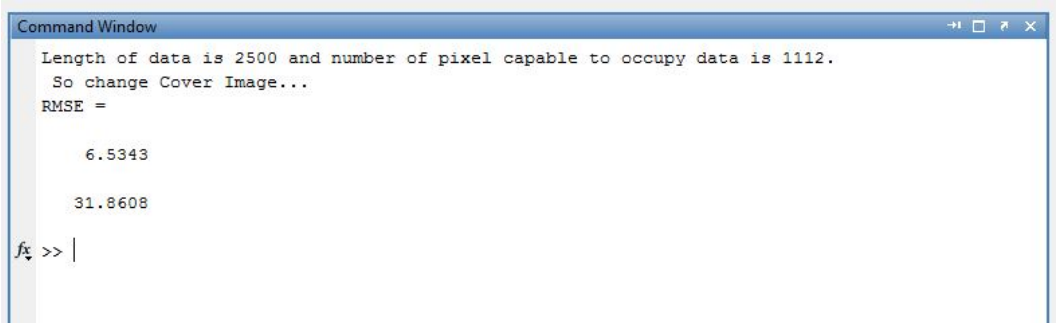

Fig 12: MSE and PSNR

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 4, Special Issue 1, March 2015*

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

On 26th & 27th March 2015

Figures 4 through 9 represents the input and output screenshots of the implemented system. Fig 10 shows the value of MSE and PSNR from command window.

V. COMPARISONS

The proposed method is compared with the work mentioned in [2]. As mentioned in the section of previous works, all methodsmay introduce some errors on data extraction and image restoration, while the proposed method assures error free results for all kinds of images.Fig11 shows the recovered image of the existing system and there we can see the distortion clearly. Fig 12 shows the value of PSNR which is low when compared with the proposed method.The quality of marked decrypted images is compared in terms of PSNR.

The following table gives comparison of the proposed system with the work mentioned in [2].

TEST IMAGES	EXISTING METHOD PSNR(dB)	PROPOSED METHOD PSNR(dB)
cameraman	31.9914	53.8730
lena	27.3799	54.1031

Table 1: comparison based on PSNR value

VI.CONCLUSION

This room reserved reversible data hiding scheme in encrypted images, draws more attention as requirements for preserving data and original image contents from eavesdroppers is becoming a necessity now a days. Here, surveys onbasic data hiding techniques which is reversible were made, both non separable and separable reversible data hiding techniques for encrypted images were analysed. The methods that already exists for hiding data in encrypted images based on method of vacating room after encryption (VRAE) may subject to errors during data extraction and image recovery. Competing with the existing method, proposed system is based on theconcept of reserving room before encryption. Hereafter the data hider will get extra space which was already emptied out during room reserving stage so that the data hiding process could be done with grater ease.

REFERENCES

[1] J.Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006

[3] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

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

[5] 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, Apr. 2010.

[6] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption‖, IEEE Trans.Information forensics and security, vol. 8, no. 3,pp. 553-562 march 2013.