International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 9, September 2014

Highly secured data hiding in Encrypted images by RRBE using RDH

[1]H.D.Praveena
Asst Professor, Dept. of ECE
Sree Vidyanikethan Engg College
Tirupati – 517 102 India

[2]B.Deepthi
M.Tech Student, CMS
Sree Vidyanikethan Engg College
Tirupati – 517 102 India

Abstract— In this paper Reversible Data Hiding (RDH) is applied to encrypted images. This technique maintains excellent property that the original image can be recovered without any loss after embedded data is extracted while protecting the hiding image content's confidentiality. All previous methods RDH in encrypted images by vacating room after encryption which may be subjected to some errors in data extraction and image restoration .In the proposed method RDH in encrypted images by reserving room before encryption can achieve real reversibility that is image extraction and original image recovery are free of any error . It is easy for data hider to reversibly embed data in encrypted image. The Algorithm is developed and tested using Mat lab.

Index Terms—*Histogram shift, image encryption, privacy protection. Reversible Data Hiding (RDH),*

I. Introduction

Reversible Data Hiding (RDH) in images is a technique by which the original cover can be recovered without any loss after embedded data is extracted. RDH is also called the loss less data hiding. It means invisibly hides data (which is called a payload) into host data (i.e. pixels in image) in reversible fashion. Being reversible both the original data and the embedded data can be completely restored. Two important measurement of RDH is embedding capacity and quality degradation. It achieves high capacity and low distortion. All existing and previous methods embed data into encrypted images by reversibly vacating room after encryption which may be subjected to some errors on data extraction and /or image restoration. In the proposed method more attention is paid to reversible data hiding in encrypted images by reserving room before encryption. It is easy for the data hider to reversibly embed data in the encrypted image. This method can embed data more than 10 times as large payloads for the same image quality as the previous methods. It is more secure than previous method. This technique is usually used in medical images, military images and law forensics.

II. Preliminaries

The methods used in [1]-[3] can be summarized as framework, Vacating room after encryption(VRAE) is as shown in Figure 1.In this frame work the original image can encrypted by using a standard code with an encryption key. After encrypted image generated the content owner hands over it to a data hider and the data hider can embed some auxiliary data into encrypted image by vacating room in encrypted image. Data hiding key is used to hide data in that image. Then in the receiver side content owner extract the embedded data and recover the original image from encrypted version by using hiding key and encrypted key respectively.

ISSN: 2278 – 909X

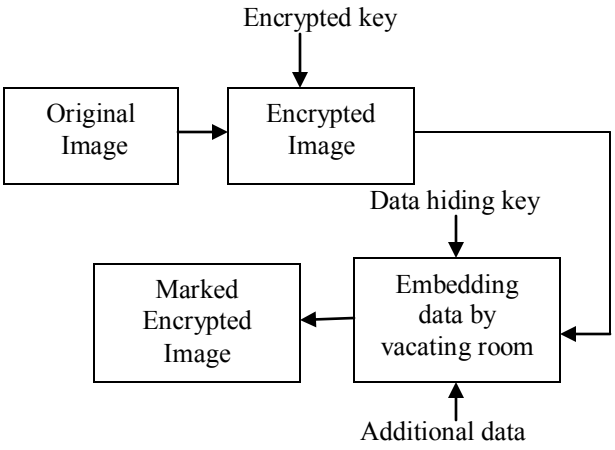

Figure 1(a) Transmission

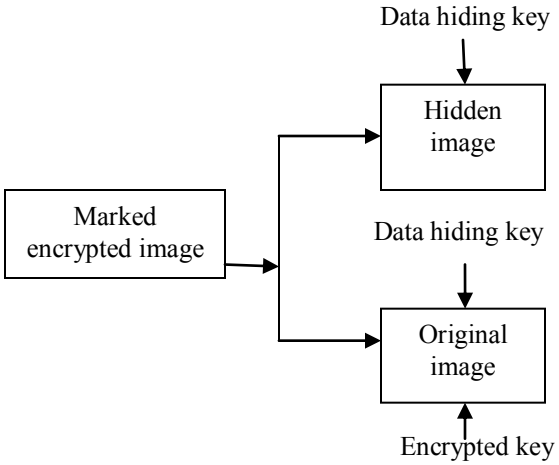

Figure 1(b) Reception

Figure 1 Framework: VRAE

All previous methods [1]-[3], the encrypted image is generated by encrypting every bit planes with a stream code. Zhang's method in [1] pseudo-randomly permuted and divided encrypted image into a number of groups. The LSB-planes of each group are compressed with a parity-check matrix and the vacated room is used for to add additional data. For example, denote the pixels of one group by $x_{1,\ldots,}x_L$, and its encrypted LSB-planes by c that consists of P.L bits .where as p is no of LSB bits and L is the no of groups. The data hider generates a parity-check matrix G and compresses c as its syndrome s such that s=G.c. Because the length of s is (P.L-S), S bits are available for data place. At the receiver side, the most significant bits (MSB) of pixels are obtained by decryption directly. The receiver generates an estimated version c and selects the one most similar to the estimated version as the restored LSBs. All these previous method try to vacate room from the encrypted images directly. These techniques can achieve small payloads [2] or generate image with poor quality for large payloads [1].

III. Proposed Method

In the present paper, we propose a novel method for RDH in encrypted images, for which we do not vacate the room after encryption, but we reverse the order of encryption and vacating room before image encryption at transmission side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel frame work reserving room before encryption " It means we first empty out room by embedding LSBs of some pixels into other pixels by using traditional RDH method and then encrypt the image. This encrypted image can be used to embed data. It achieves excellent performance in two different prospects:

- Real reversibly is realized.
- PSNR also improved.

Real reversibility is recognized, that is image recovery and data extraction are free of any error, the PSNRs of decrypted image containing the embedded data for given embedding rates are significantly improved.

ISSN: 2278 – 909X

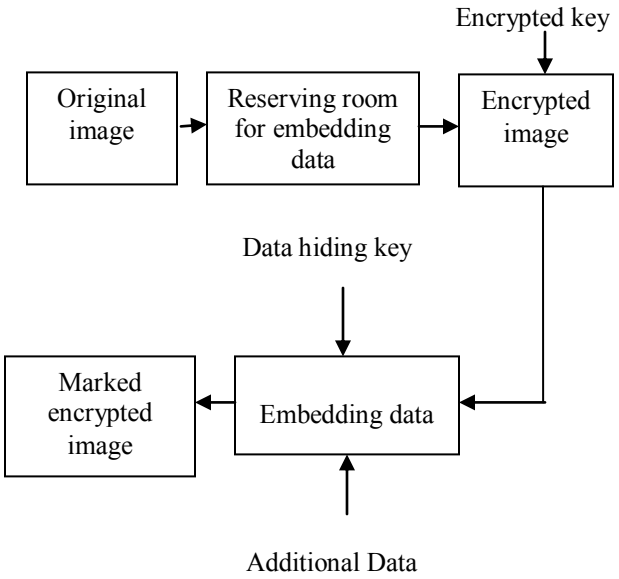

Figure 2(a) Transmission

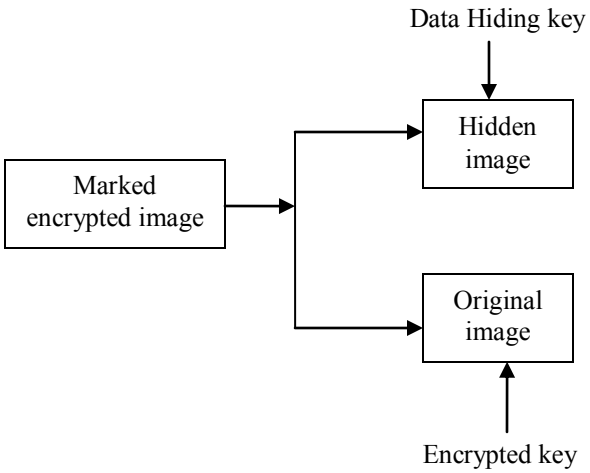

Figure 2(b) Reception

Figure 2 Frame work of RDH in encrypted images by Reserving room before encryption

The frame work of Reserving room before encryption (RRBE) is as shown in Figure 2, the content owner first reserves enough space on original image and then converts the image into its encrypted version by using encrypted key. After encryption process completed the data hider hides data in the previous emptied out spare space. The data embedding process in encrypted image is inherently reversible for the data hider. The data extraction and image recovery are identical to that of frame work VRAE. Apparently, standard RDH algorithm are the ideal operator for reserving room before encryption and can easily applied to framework RRBE to achieve better performance compared with techniques from frame work VRAE. This is because in this new frame work, we follow the idea that first compress the redundant image content using RDH techniques without any loss and then encrypts it with respect to protecting privacy.

The frame work RRBE, which primarily consists of four stages: Generation of encrypted image, data hiding in encrypted image, data extraction and image recovery.

A. Encrypted image

To generate encrypted image, the first stage can be divided into three steps: image partition, self reversible embedding and image encryption.

1. Image Partition: First step of image partition is dividing the original image into two parts A and B then LSBs of A is reversibly embedded into B with a standard RDH algorithm[4],[5]. So that LSBs of A can be used for accommodating messages. The operator here for reserving room before encryption is standard RDH technique. Assume the original image C is an 8 bits gray scale image. Size of original image is M x N. There are several overlapping blocks in the image, that each block is overlapped by previous and/or sub sequential block along the rows .For each block, describe a function to measure its first order smoothness. Denoted by *f*. highest *f* denoted as A and rest part as B.A contains higher textured areas, B contains lower textured areas.

ISSN: 2278 – 909X

2. Self reversible embedding: The objective of self reversible embedding is to embed the LSB planes of A into B by using traditional RDH algorithm.

Pixels in the part B are divided into two sets white pixels and black pixels. White pixels with indices *i* and j satisfying $(i + j)$ mod 2=0 and black pixels with indices *i* and j satisfying $(i + j)$ mod 2=1.Then each white pixel $B_{i,j,}$,is estimated by the interpolation value obtained with the four black pixels surrounding it.

$$B'_{i,y} = w_1 B_{i-1,j} + w_2 B_{i+1,j+} w_3 B_{i,j-1} + w_4 B_{i,j+1}$$

Where *w* is the weight and it is determined by same method as defined in [10].After that we find out the estimation error. It is difference between the $B_{i,j}$ and $B'_{i,j}$. Then some data can be embedded into the estimation error sequence with histogram shift. After that we further calculate the estimation errors of black pixels with the help of surrounding white pixels .Then another estimating error sequence is generated in that also we can accommodate messages.

Histogram shift is used to embed data into original image, by using histogram shift find out the estimating errors, in that estimating error some messages are inserted. That is, first divide the histogram of estimating errors into two parts, i.e., left and right ,find out the highest point in each part, denoted by LM and RM , respectively. For classic images, LM=-1and RM=0. Besides, search for the zero point in each part, denoted by LN and RN . To embed messages into positions with an estimating error that is equal to RM, shift all error values between RM+1 and RN-1with one step towards right, and then, we can represent the bit 0 with RM and the bit 1 with RM+1.The embedding process in the left part is alike except that the shifting direction. the shift direction is left, it is realized by subtracting 1 from the equivalent pixel values.

Suppose to implement the embedding system *n* times to accommodate additional data. In the earlier *n-1* single-layer embedding rounds, two error sequences peak points are selected and employed to embed messages as mentioned in above paragraph. Coming to the *n*th single-layer embedding process, only a small portion of messages is missing to be embedded, so to accommodate small data into that layer by shifting of all error values between peak points and their corresponding zero points is unadvisable. To deal with this problem use only part of error sequences which has enough peak points to embed the remaining messages while leaving the rest error sequences unchanged, or find two proper points, denoted by LP and RP, whose sum is large, on the other hand adjoining the size of remaining messages. By shifting error values between LP.RP and their corresponding zero points, messages can be embedded into LP and RP instead of peak points. Generally speaking, two solutions can gain significantly improvement in terms of PSNR when the length of data is relatively short that is when *n=1.*

3) Image Encryption: After self reversible embedding one image is formed, it is denoted by X. To generate encrypted image we can encrypt the image by using encrypted algorithm, it is denoted by E .With a stream code the encryption version of image X is easily obtained. The below given formula is used to obtain image encryption.

$$Ei, j(K) = Xi, j \oplus ri, j$$

Here $X_{i,j}$ is a gray value ranging from 0 to 255 .It is represented by 8 bits and r_{ij} is generated via a standard stream cipher determined by the encryption key. encrypted bits $E_{i,j}(k)$ can be calculated through exclusive-or operation as shown in the above equation. Finally, the encrypted image is generated and it is denoted by A. In that encrypted image A data hider can embed information. Without encryption key the data hider or a third party cannot access the content of original image, thus privacy of the content owner being protected.

ISSN: 2278 – 909X

B. Data Hiding in Encrypted Image

Once the data hider gets the encrypted image, he can embed some data into it, even though he does not get access to the original image. The embedding process begins with placing the encrypted version of A, denoted by A_E. While A_E is set in the top of the E .It is easy for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider point out the end position of embedding process .hide and encrypts the image according to the data hiding key and encrypted key. Prepared image is marked encrypted image denoted by E'. Who does not know the data hiding key they could not extract the additional data.

C. Data Extraction and Image Recovery

Since data extraction is completely independent from image Decryption. The procedure used to extracting data from encrypted images is similar to RDH in[4],[5]. The sort of data extraction before image decryption assurances the possibility of our work in this case.

When the database manager gets the data hiding key, he can decrypt the LSB-planes of A_E and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

IV. Results & Implementation Issues

The proposed method will be tested on standard images, Lena, Baboon, and Boat [6]. The size of all images is 512 × 512× 8.The PSNR, NC, BER values are employed. To estimate the quality of decrypted image.

Table 1 metric values of boat

Embedded rate	0.1	0.2	0.3	0.4	0.5
PSNR	46.49	46.09	45.41	45.16	44.45
BER	0.25	0.27	0.25	0.26	0.25
NC	0.0147	0.0147	0.0147	0.0147	0.0147

Table 2 metric values of Baboon

Embedded rate	0.1	0.2	0.3	0.4	0.5
PSNR	45.72	45.26	44.57	43.32	42.25
BER	0.24	0.25	0.26	0.26	0.24
NC	0.120	0.120	0.120	0.120	0.120

Table 2 metric values of Lena

Embedded rate	0.1	0.2	0.3	0.4	0.5
PSNR	49.19	45.90	45.54	45.03	44.89
BER	0.28	0.24	0.25	0.28	0.25
NC	0.179	0.179	0.179	0.179	0.179

ISSN: 2278 – 909X

The Figure 3 shown below is the input image.

Figure 3 original image

Encrypted image of the original image containing room To hide data is shown in below Figure 4.

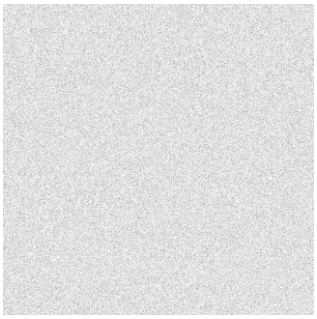

Figure 4 encrypted image

Decrypted image containing hiding image is shown below Figure 5

Figure 5 Decrypted image

The hiding image which is recovered from original image is shown below Figure 6

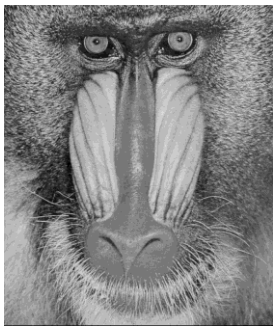

Figure 6 Recovered hidden image

The original image after recovery is shown below figure 7.It is the recovery version of original image without any loss.

Figure 7 Recovered original image

V. Conclusion

Reversible data hiding in encrypted images by reserving room before encryption is highly secured compare to previous methods it achieve real reversibility. By using proposed method Large amount of data can hide in the original image and transmit. In the receiver side we can extract the hidden data and original image without any loss. PSNR value is

ISSN: 2278 – 909X

improved. Further it can be used in videos also. This method is used for security purpose.

References

[1] W. Hong, T. 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.

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

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

[4] L. Luo *et al.*, "Reversible image watermarking using interpolation technique,"*IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[6] Miscelaneous Gray Level Images [Online]. Available:http://decsai.ugr.es/cvg/dbimagenes/g512.php.

AUTHOR'S BIOGRAPHY

[1]Mrs.H.D. Praveena is Currently working as Assistant Professor, received B.Tech (ECE) from Nagarjuna University, Guntur in 1995 and M.Tech (Digital Electronics and Communication Systems) from Sree Vidyanikethan Engineering College, Tirupati affiliated to JNTUA, Anantapur in 2010. She published and presented 11 technical papers in various International Journals & conferences. She has 10 years of teaching experience. Her areas of interest include Communication Systems and Signal Processing. She is Llife Member of ISTE and a member of The Indian Science Congress Association and Institute of Doctors Engineers and Scientists

[2]B.Deepthi is Currently M.Tech Student(Communication Systems) from Sree Vidyanikethan Engineering College, Tirupati,India, , received B.Tech (ECE) from MITS,Madanapalli, affiliated to JNTUA, Anantapur in 2011.

ISSN: 2278 – 909X