Reversible Data Hiding By Reserving Room before Encryption

Vijaya Patil [1], Prof. B.P. Chaudhari [2]
[1]Mtech –Student, [2]Assistant Professor, Department Of Computer Science & Technology,
Maharashtra Institute of Technology, Aurangabad, India
Email - patilvijaya1256@gmail.com

Abstract: *Now A Days ,attention is paid to Reversible Data Hiding(RDH) in encrypted images to maintain some properties ,after that data is extracted, recover the original cover losslessly while protecting contents of images confidentially. By using all previous methods, data extraction and restoration of images maybe subject to some errors on which embed data by reversibly vacating room from encrypted images. But in this paper I proposed Rhombus Method which reversing room before encryption by traditional RDH algorithm and so to embed data in the encrypted images to data hider its easy. By this method ,data extraction and images recovery are free of any error i.e. Real Reversibility. Experimentally this method shows that it can embed larger than the 10 times as more payload for as alike image quality as the previous methods.*

Keywords: *Image encryption, LSB, privacy protection, RDH.*

1. INTRODUCTION:

The important technique, Reversible Data Hiding (RDH) in images recovered the original cover lossessly after message is extracted. It is used in many applications where distortion is not allowed of original images such as law forensics, military images, and medical imagery. In theory, rate restoration model established by Kelkars and willems[1], proposed code construction recursively and proved RDH for rate restoration bounds for memory less covers.

By theoretical views, Jun Tian [2] states that the each and every pixel group differences are expanded which is used to embed messages example multiplied it by two and so LSBs (Least Significant Bits) of differences all are zero. Another popular theoretical aspect [3], for RDH is HS (Histogram Shift) to embed the data space is saved by shifting bins of gray values of histogram. In practical aspects [4], to embed data, empty space is saved by compressing original cover lossesly before the first compressible features are extracted and RDH framework is constructed.

In another aspects [5] ,to keep the images confidential, encryption is the secure and efficient as it convert the original content of images to incompressible contents. By constructing trust management scheme [6], Hwang et al. showed the practical with the watermarked software and data coloring, which provides the ability by data encryption and data coloring that the guarantees of content's owners privacy and integrity.

In theoretical aspect, [7] proved resolution compression problem, which shown to have better coding efficiency and have lower complexity than previous arts. Another aspects, Wien Hing[8], proposed improved version of data extraction and image recovery based on existing strategies and used some algorithms to construct better smoothness of image block. RDH after encryption is proposed in [9] by Zhangs aspect that including of image encryption, data embedding and data extraction or image recovery steps.

2. SYSTEM ANALYSIS:

Existing System:-

The previous method, i.e "Vacating Room After encryption (VARE)" as shown in figure fig. (1). in this method, at content owner side the original image is encrypted by us.

In fig. 1(a) framework of VARE i.e. vacating room after encryption [7]-[9 shown below], at the content owner side first image is encrypted with encryption key using standard cipher method. The image passed to data hider after the image encrypted in which data hider embed data by lossesly vacating room by data hiding key .Then at the receivers side ,embed data extracted maybe by the content owner side with data hiding key to recover the original cover of image using data hiding key.

Proposed System:-

As shown in fig 1(b) RRBE i.e. reserving room before encryption. If we Reverse this method of encryption and vacate room i. e. reserving room before encryption at side of content owner made the encrypted images of RDH task more naturally as well as easier which result in framework "Reserving Room before Encryption (RRBE)".

As shown in below fig. proposed framework first of all at the contents owner side some space is reserved to embed data, and then image encrypted with encryption key. Then the image is passed to data hider to hide the some data in spare space reserved previously with data hiding key. After that, at the receiver side data extraction and image recovery identical to that of existing method i. e. VARE. This proposed method can achieve some excellent two important features:

1) Data extraction and image recovery are free of all errors i.e. Real Reversibility.
2) And the PSNR of decrypted image which contains embedded data get improved

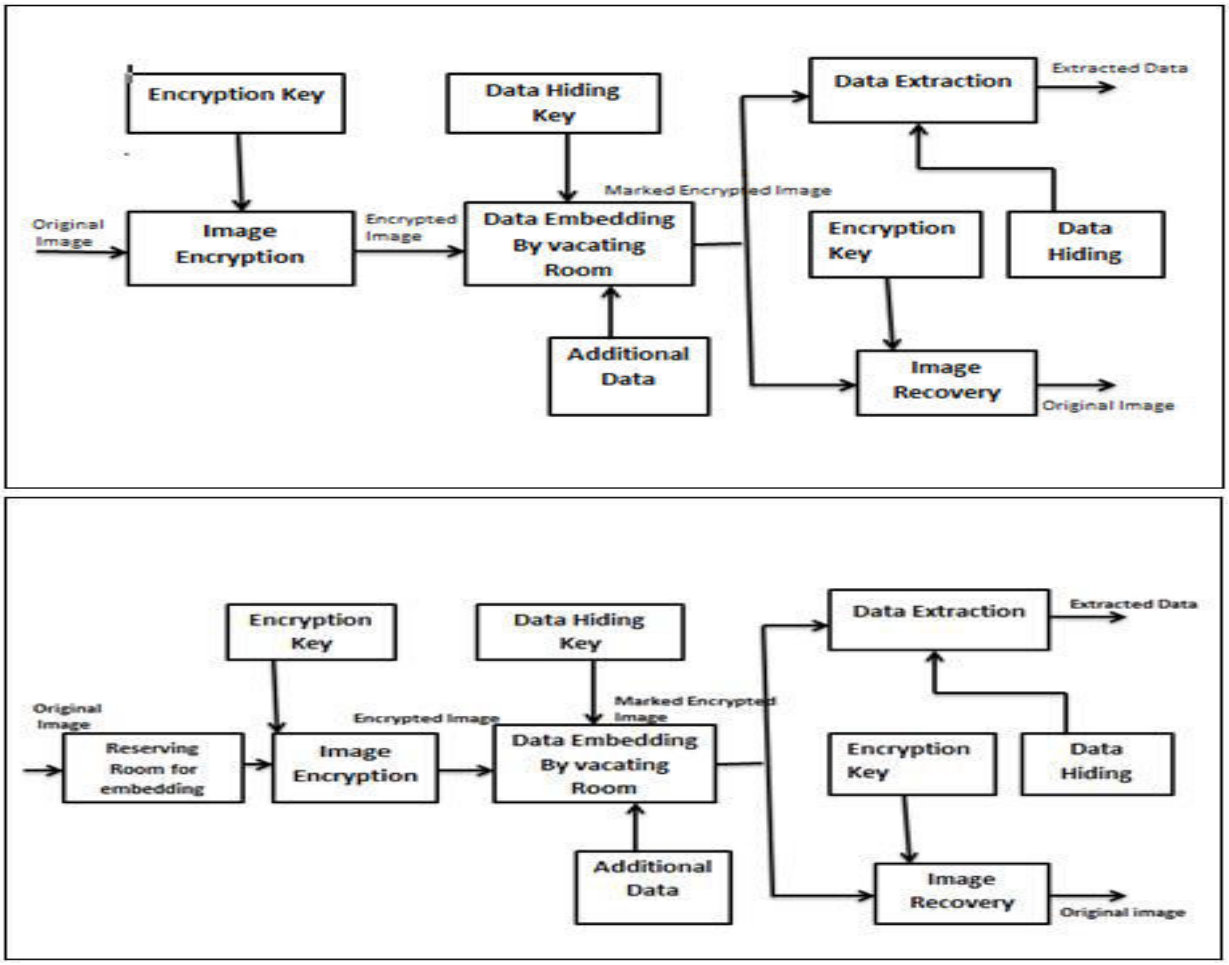

Fig.1 (a) Framework "VRAE" Vacating Room Before Encryption (b) Framework "RRBE" Reserving Room Before Encryption

Next, we state the practical approach of "RRBE", which includes of four steps: generate encrypted image, extraction of data and then image recovery.

A] Generate encrypted image:

To generate encrypted image, this step divides into basically three stages: image partition, self-reversible embedding and image encryption. At first step, partition the original image into A and B two parts and by using standard RDH algorithm A's LSB's are reversibly embedded into part B. These LSB's of A used to accommodate data or messages and at the end generated the encrypted image

1) Image Partition: The purpose of image partitioning is to smoother area for B because Reserving Room before Encryption is standard RDH technique, which can obtain best performance.

For doing this, consider, for lossless of generality, original image C which 8-Bit Gray scale image with size M x N & pixels $C_{i,j} \epsilon[0,255]$, where $1 \leq i \leq M$, $1 \leq j \leq N$. The content owner first extracts data from original image of several overlapping blocks denotes with l, whose number is represented based on size of message to embedded. Each block included of m rows, where m = [l/N]. Computation of no. of blocks through n=M-m+1 is done.

Here is function for measurement of first-order smoothness, for each and every block

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \right| \quad (1)$$

Where (i+j) mod 2=0 , which is white pixels. And where (i+j) mod 2= 1, which is black pixels. Then evaluate white pixels $B_{i,j}$,with the four black pixels surrounding of white pixels, by interpolation value method as follows,

Where more complex structure represented and denoted by higher f. So that content owner has selected the specific block and takes it in front of B as shown in fig. (2).

To reduce the size of A by content owner side embed the LSB planes of A into B, which result in half or more than that. This is the result of above gossips that recorded only single LSB plans of A.

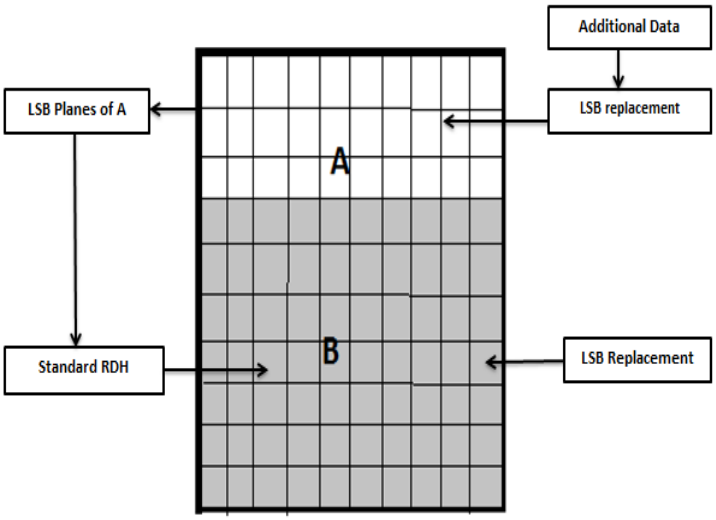

Fig. (2) Partitioning of Image and embedding process

2) Self -Reversible Embedding: By standard RDH Algorithm, the LSB's of A is embedding into plane B, this is the aim of this step. The image B of pixels is divided into two parts white and black pixels with i and j indices

$$B'_{i,j} = w_1 B_{i-1,j} + w_2 B_{i+1,j} + w_3 B_{i,j-1} + w_4 B_{i,j+1} \quad (2)$$

Where w_i is defined as weight , $1 \leq i \leq 4$, same method defined as in proposed method. By $e_{i,j} = B_{i,j} - B'_{i,j}$ the estimating error is computed and then this estimating error is used to embed some data with HS(Histogram Shift).With the four white surrounding to black pixels ,estimating error is calculated as same methods using of white estimating error , which also used to embed message.

3) Image Encryption:-

We can encrypt X, where X is generated self-embedding image, for constructing the encrypted image Encryption version of X obtained by stream cipher. For eg. Take three channels as three gray scale images, a gray value $X_{i,j}$ranging from 0 to 255,denoted by 8 bits , $X_{i,j}(0), X_{i,j}(1), \ldots X_{i,j}(7)$,

$$X_{i,j}(k) = \lfloor X_{i,j} / 2^k \rfloor \bmod 2, \quad k=0,1,2\ldots.7 \quad (3)$$

By using XOR operation encrypted bits $E_{i,j}(k)$ can be calculated,

$$E_{i,j}(k) = X_{i,j}(k) \text{ XoR } r_{i,}(k) \quad (4)$$

Where, ri,j(k) is generated by standard stream cipher decided by encryption key. At last, embed 10 bits information of first 10 pixels into LSBs in encrypted version of A.

B] Data Hiding In Encrypted Images:

The data hider embeds some data into it, as soon as data hider obtains the encrypted image E, even if not getting access to original image. The embedding process starts with A_E which is encrypted version of A. It is easy for data hider for reading 10 bits of information in LSBs of first 10 encrypted pixels, as A_E has to be arranged at the top of E. Data hider after knows about to modify how many bit-planes and pixels of row , he adopts LSB replacement for substituting the available bit planes with data m. At last, he gives label to denote end position of embedding process, as m. Then by using data hiding key encrypt the m to produce encrypted image denoted by E'.

C] Data Extraction and Image Recovery:-

Data extraction is totally different from image decryption.

1)Case 1 : Extracting Data From Encrypted Images: For managing and updating some personal information of encrypted images to keep secure clients privacy, only data hiding key can access data base manager and should manipulate data of encrypted domain .Our work in this case guarantees the feasibility for process of data extraction

before image encryption. Then Data base manager decrypt the LSB planes of A_E by using data hiding key and extract additional data m.

2) Case 2: Extracting Data From Decrypted Images:- We can go with following steps.

a) Generating Marked Decrypted Image:-Content owner should do following steps To create marked decrypted image X" which made up of A" and B":

STEP 1: The content owner decrypt image, by using encryption key, except LSB-plane of A_E. Then calculate the decrypted version of E' containing embedded data,

$$X"_{i,j}(k) = E'_{i,j}(k) \text{ XoR } r_{i,j}(k) \quad (5)$$

and

$$X"_{i,j} = \sum^{7}_{k=0} X"_{i,j}(k) \times 2^k \quad (6)$$

Where, $E'_{I,j}(k)$ and $X"_{I,j}(k)$ are binary bits of $E'_{I,j}$ and $X"_{I,j.}$ resp.

STEP 2: In marginal area of B'', extract SR and ER. The plain image contains the embedded data is obtained, by rearranging A'' [1] and B'' to its original state.

b) Data Extraction and Image Restoration [1]:The content owner can extract the data and recover original image [1], when generating the marked decrypted image.

Fig.3 Encrypted Image Lina

fig 4. Decrypted Image Lina

Table I. PSNR Comparison for three Different LSB-Planes Choices under VariousEmbedding Rates

Embedding rates	0.1	0.2	0.3	0.4	0.5
Lena	71.1	70.5	65.4	59.1	57.6
Barbon	82.9	81.6	77.5	71.2	70.3
Barbara	81.1	80.7	79.1	75.9	71.4

3. CONCLUSION:

RDH for encrypted images is the new topic which is important to pay attention because of demand of privacy preventing from cloud management. Existing system can't unable to do this. The proposed method can achieve excellent property that the data extraction and image recovery are free of any error and take benefits of all traditional RDH techniques.

REFERENCES:

1. Kede Ma, Weiming Zhang, Xianfeng Zhao,"Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL:8 NO:3 YEAR March 2013 .
2. T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.
3. J. Tian, "Reversible data embedding using a difference expansion,"IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.
4. 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.
5. J. Fridrich and M. Goljan, "Lossless data embedding for all image formats,"in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
6. K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.
7. 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.
8. 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.
9. Xinpeng Zhang, "Separable reversible data hiding in Encrypted images" IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012. IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
10. Xinpeng Zhang, "Separable reversible data hiding in Encrypted images" IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
11. Vijaya B. patil,prof. B.P.Chaudhari "RDH by using Reserving room Before Encryption in Encrypted Images" IJETAE-Volume 6, Issue 2, February 2016