International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP274-280

Reversible Data Hiding system for Encrypted Image by Reserving Room

Chaitrali Chormale[1], Prof. R. B Singh[2]
[1, 2. (]*Department of Computer Science, Pune University, India.)*

Abstract-Communication over the internet is facing moreproblems such as copyright control, data security, authentication, datasize capacity, etc. Here we introduce a novel scheme for reversible data hiding inencrypted image domain in which we use image as a cover medium. Reversible Data Hiding (RDH) gives clear image after data extraction and image encryption without any loss. This paper illustrates how to vacate the room after encryption. The room is reserved for data embedding before image encryption. All previous methods embedding data into image by reversibly vacating room in the encrypted images, which may be result as some errors on data extraction and/or image restoration. RDH task in encrypted images would be more natural and much easier. This important technique is used in medical science, military imagery etc. Benefit of this method is that data hider gets extra space to embedding additional data. Our proposed method can achieve reversibility i.e. data extraction and image recovery are free of error. Our proposed method show this method can embed more than 8 times as large payload for the same image quality as the previous existing methods, such as for PSNR=30 dB.
Keyword: Reversible data hiding, image encryption, image decryption, security, protection.

I. INTRODUCTION

Data Hiding is a technique to hide data into cover media. The data may be any text related to the image such as authentication data or author information.Reversible data hiding (RDH) is a technique in image processing area for encryption, by which the original covercan be losslessly recovered after data extraction and image encryption.Reversible data hiding is used to embed additional data into some cover media and original image could be perfectly restored after extraction of the hidden data. Reversible data hiding is very important technique. This technique is used in medical science, military imagery, where no variation of the original message or cover is allowed. This type of technique is also known as reversible data hiding or it is also named as
lossless, distortion free, or invertible data hiding technique [1].
The Xinpeng Zhang explained an special reversible (lossless) data hiding technique which helps the recovery of the original cover medium with the extraction of the embedded hidden information. And the technique of this recovery with lossless data is nothing but the reversible data hiding. Generally the LSB (least significant bit) method is used as the additional data embedding method. Reversible data hiding is a technique that is mainly used for the authentication of data like videos, images, electronic documents etc. Mainly the reversible data hiding is relevant for conditional access, authentication, and protection. In some application it is important to provide authentication, security, and privacy while communication or transferring data. To provide the data security or to hide the data we need some new approach in communication.
Most of the existing techniques are not reversible. Most of the works on data hiding concentrations on data hiding and the extraction on plain image [2]-[4].Reversible data hiding by histogram shifting is described in [2]. In [3] data is hidden into the histogram of pixel differences. Data hiding in [4] all data are stored by making changes to LSB bits.

In recent years many new RDH techniques are developed. Fridrich*et al.* [5] established a general structure for RDH. By first extracting the features of the original cover and then compressing them losslessly, extra space can be emptied out by embedding auxiliary data. The data embedding/extracting on the original image is more important work in the reversible data hiding. But, in some uses, administrator want to add some additional data, i.e. the original hidden data, image notation or authentication data or protected, within that encrypted image though the administration does not know the original content of image. The original content should be recovered without any error after image encryption and the image should be encrypted by the encrypted key and data extraction at receiver side. Reference [6] presents applied scheme satisfying the above-mentioned requirements.

II. LITERATURESURVEY

Reversible data hiding technique contains following actions like compression, decompression, decryption, encryption,data embedding-data extracting, creating space at LSB in images and providing authentication, security, using automatic key

generation and etc. The way of sending data is to first compress the data into image to reduce the redundancy and then to encrypt the compressed data. At the receiver side the decompression operations and decryption are performed to recover the original cover image. However in some applications a sender wants to send some information to the receiver and want to keep the information private, means the sender should encrypt the original data i.e. image. At receiver side to extract the original data and the image.

For hiding the information into the encrypted image Zhang [6] separated the encrypted image into several blocks. By reversing 3 LSBs bit of the half of pixels in each block, room can be reserved for the embedded bit. Therecovery of image and data extraction proceeds by finding which part has been reserved in one block.

Hong et al [7] alter the Zhang's method at the decoder side by illuminate the correlation using the dissimilar estimation equation and by using new technique he can achieve much lower rates before data extraction the encrypted image should be decrypted.

To separate out the data extraction from decrypted image [8] Zhang compressed the encrypted LSBs to empty room for additional data by finding patterns of a parity-check matrix, and the information used at the receiver side is also the spatial correlation of decrypted images.

The methods [9]–[13] usually combined DE or HS to residuals of the image, e.g., the predictable errors, to complete better performance. However, since the entropy of encrypted images has been maximized, these can only succeed small payloads [6], [7] or generate marked image with poor quality for large payload [14] and all of them are subject to some error rates on data extraction and/or image restoration. Although the methods in [6], [7] can eliminate errors by error-correcting codes, the pure payloads will be further consumed.

III. IMPLEMENTATION DETAILS

In the first part, we give the input as the original image, a content owner encrypts the original uncompressed image using an encryption key. After that, a data-hider may compress the LSB of the encrypted image using a data-hiding key to create a extra space to hide some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he/she can extract the additional data though he does not know the image content means hidden data. To get an image similar to the original image the receiver must have the encryption key, and then only he/she can encrypt the received image but cannot extract the additional data without data hiding key. Receiver can extract the additional hidden data and recover the original image without any error if the receiver has both the data-hiding key and the encryption key.

Our main aim is to partition an encrypted image into blocks to hide the data, and each block transmits one bit by flipping five LSBs of a set of pre-defined pixels. Thedata extraction and image recovery can be achieved by identifying the block softness.

A) Proposed work

We do not “vacate room after encryption” but we want “reserve room before encryption”. In our proposed method, first we reserve the room from original image for the purpose of the embedding additional data. If we reverse the vacating room, i.e., reserving room to image encryption at content owner side, the RDH responsibilities in encrypted images would be more natural and much easier which leads us to the framework, “reserving room before encryption (RRBE)”.

From fig 1, there are three phase in our proposed method content owner, data-hider, and receiver. At the first phase, we give the input as original image. Content owner reserve the room from the original image to embed the additional data then that original image will be encrypted by the image encryption key. Then that encrypted image will hand over to the data-hider, the data-hider takes that encrypted image and hide the additional data into the encrypted image with the help of data hiding key and finally we get the marked encrypted image. And at last the marked encrypted image is given to the receiver. The receiver have both the image encryption key and the data hiding key then and then only the receiver can extract the data and recover the image.

Note that the reserving room operation we accept in the proposed method is a traditional RDH approach.

Our proposed method consists of four stages:

- generation of encrypted image
- data hiding in encrypted image
- data extraction and Image recovery

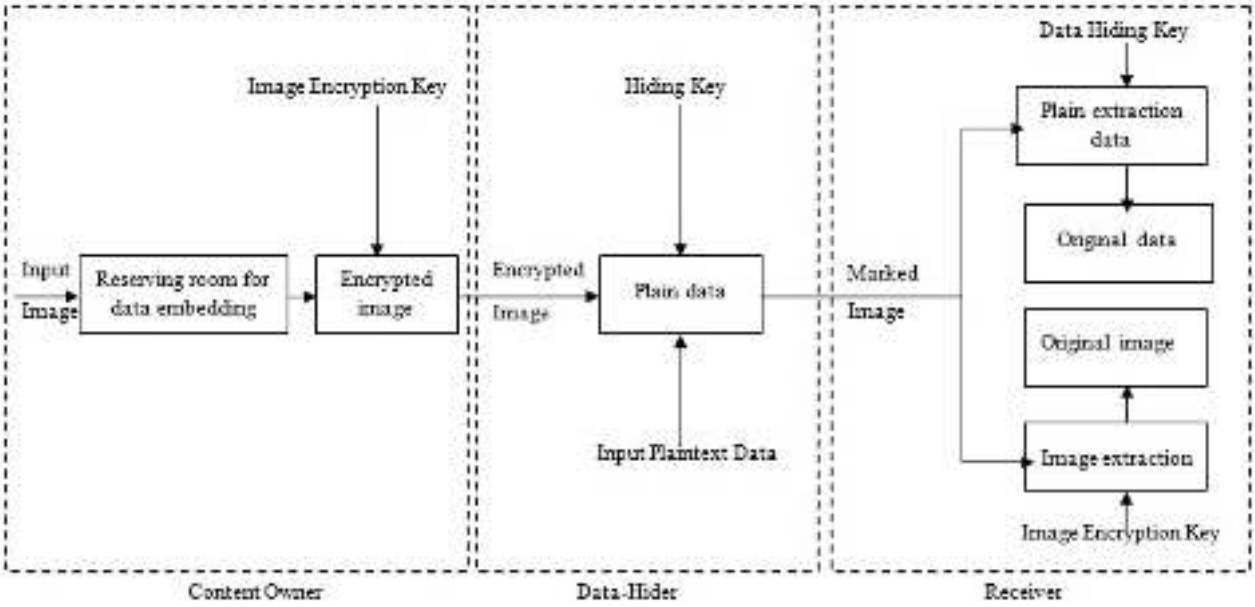

Fig1: Framework Reserving Room before Encryption

B) Algorithm-Reversible data Hiding

1)Generation of Encrypted Image-

Give the input as the original image divide the original image into two part A and B , first the original image can be divided into three steps: image partition, and the self-reversible embedding followed by image encryption.

i) Image Partition*:* we can partition the image on the basis of height(h) and width (w) and image as (I).

$$f = \sum_{u=2}^{h} \sum_{v=2}^{w} |Iu, v - \frac{Iu-1,v+Iu+1,v+Iu,v-1+Iu,v+1}{4}| \quad (1)$$

ii) Self-Reversible Embedding*:* There are two sets: white pixels with its indices i and j satisfying (i+j) mod2=0 and black pixels whose indices meet (i+j) mod2=1. Then, each white pixel Wi,j, is estimated by the interpolation value obtained with the four black pixels surrounding it as follows

$$W'i,j = w_1 W_{i-1,j} + w_2 W_{i+1,j} + w_3 W_{i,j-1} + w_4 W_{i,j+1} (2)$$

iii) **Image Encryption***:* After rearranged self-embedded image, denoted by I , is generated, we can encrypts I to constructthe encrypted image , denoted by E. For example, a gray value $I_{i,j}$ ranging from 0 to 255 can be represented by 8 bits,$I_{i,j}(1), I_{i,j}(2), I_{i,j}(3) \dots \dots \dots I_{i,j}7$,such that

$$I_{i,j}(k) = \left|\frac{Ii,j}{2^k}\right| \bmod 2, \qquad k = 0,1 \dots \dots \dots 7 \ (3)$$

The encrypted bits can be calculated by

$I_{i,j}(k) = I_{i,j}(k) \oplus r_{i,j}(k) (4)$

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

2)Data Hiding in Encrypted Image-

Input: encrypted image

Output: encrypted image with hidden data (marked encrypted image)

Step 1: Read the input encrypted image

Step 2: Perform image partition(i)

Step 3:Give additional data

Step 4: apply data hiding key to hide the data.

Step 5: Apply LSB Algorithm to embed data

Step 8: Generate encrypted image with hidden data (marked encrypted image)

3)Data Extraction and Image Recovery-

Input: marked encrypted image

Output: hidden data and original image

Step 1: Read marked encrypted image

Step 2: Apply data encryption key

Step 3: Apply data hiding key

Step 4: Separate hidden data

Step 5: Get Original image

IV. EXPERMENTAL RESULT

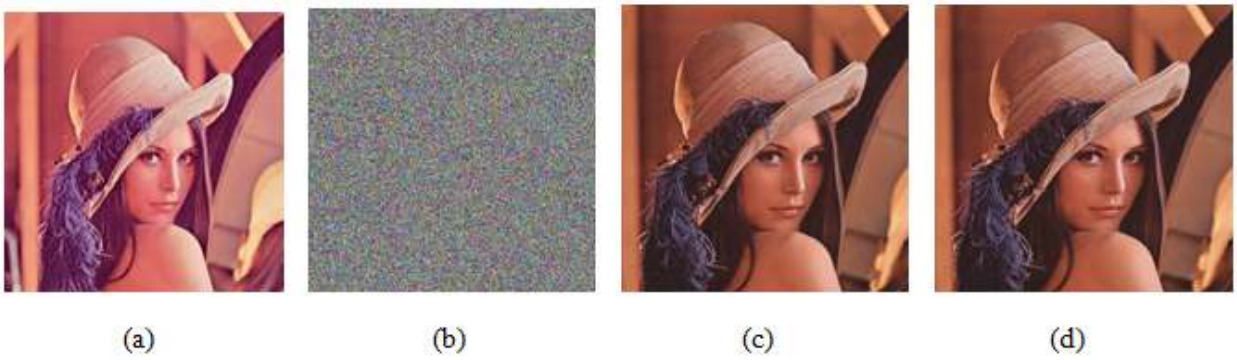

Fig 2: (a) Lena Input Image, (b) encrypted image,(c)Encrypted image with hidden data,(d)Lena Output Image

The proposed approach will be tested on public available standard images, which include "Lena", "Baboon" and "Boat" [18]. The size of all images is 512 ×512×8.

The excellence of marked decrypted images is compare in the idiom of PSNR. The PSNR consequences of diverse marked decrypted images under given embedding rates. Out of justice, we adjust the methods in [16], [17] with error-correcting codes to eradicate errors.

TABLE 1:
PSNR COMPARISON FOR THREE DIFFERENT LSB-PLANE CHOICES UNDER VARIOUS EMBEDDING RATES

	PSNR results (dB)								
	Embedding Rate	0.005	0.01	0.05	0.1	0.2	0.3	0.4	0.5
Lena	1 LSB-PLANE	65.15	60.40	53.42	50.31	47.05	43.00	39.62	34.84
	2 LSB-PLANE	63.44	59.63	51.65	49.51	46.30	42.69	38.55	32.40
	5 LSB-PLANE	61.40	57.00	48.66	47.90	44.46	41.78	36.21	31.00
Baboon	1 LSB-PLANE	57.49	55.71	50.19	46.17	40.68	35.87	31.16	25.92
	2 LSB-PLANE	57.43	55.47	49.87	45.92	40.41	36.47	33.08	29.85
	5 LSB-PLANE	57.10	55.13	49.23	45.40	40.09	36.33	32.96	------
Boat	1 LSB-PLANE	67.22	64.13	56.75	52.62	49.10	45.21	41.2	35.99
	2 LSB-PLANE	66.72	63.26	55.75	51.71	48.40	44.98	42.46	39.98
	5 LSB-PLANE	64.57	61.34	53.73	50.02	46.71	43.81	41.70	39.46

By introducing error-correcting codes, the pure payload of [15], [16] is strong from *Cap* to, where is the double entropy function among error rate. Take test image Baboon. If each
embedding block is sized of 8 with error rate 15.55% [15], then the pure payload is 1543 bits rather than 4096 bits. As

for the method, we only choose those results with a significantly high chance of flourishing data withdrawal and ideal image revival to draw the curve.

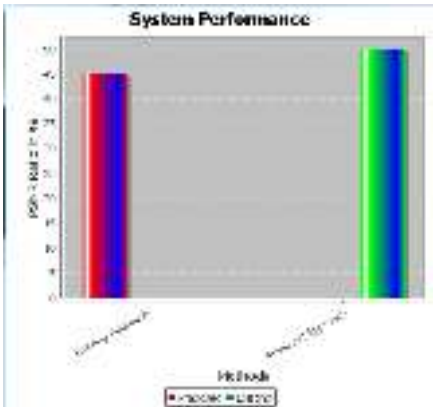

Fig 3: Graph for System performance

The Fig 3 shows the system performance in between the existing system and the proposed system. The performance of the proposed system is faster than the existing system. As the embedding is more than the system performance is high.The green graph shows the proposed approach and the red graph shows the existing approach.

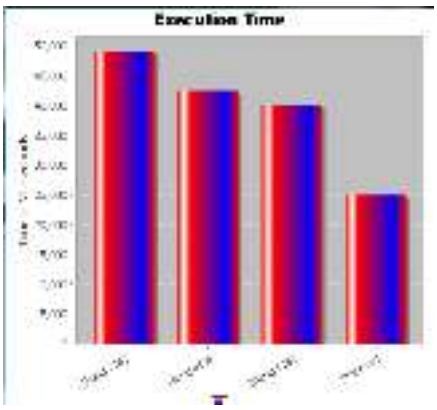

Fig 4: Graph for Execution time

The Fig 4 shows the Execution time in between the existing system and the proposed system. To hide the data into the image required more execution time but in our proposed system required less execution time as compared to existing system.

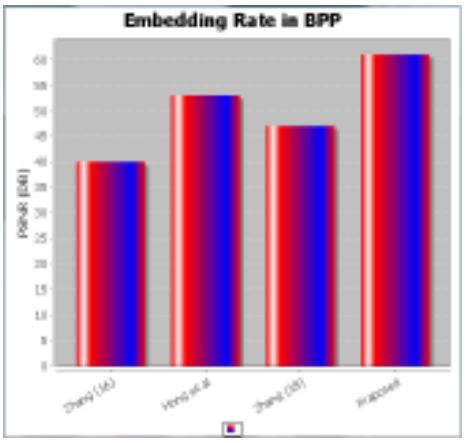

Fig 5: Graph for embedding rate

From the Fig. 5, it can be observed that over all range of embedding rate, for all cases, our style performs state-of-the-art RDH algorithms in encrypted images .The advance in terms of PSNR is significantly high at embedding rate range that the methods in [16]–[18] can achieve. In addition, one more benefit of our approach is the much wider range of embedding rate for satisfactory PSNRs. In fact, the future method can embed more than 10 times as huge payloads for the same acceptable PSNR (e.g.PSNR=30 dB) as the method in [16]–[17], which implies a very good potential for practical applications.

V. CONCLUSION

After completion the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects: Real reversibility is understood, that is, image recovery and data extraction are free error. For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the good enough PSNR, the range of embedding rates is really enlarged.

Basically the reversible data hiding in encrypted images is an innovative topic drawing attention because of the privacy-preserving necessities from cloud data supervision. Previous methods implement RDH in encrypted imagesby vacating room behind encryption, as opposite to which we proposed by reserving room proceeding to encryption. Thus the data hider can

advantage from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve brilliant performance without loss of perfect privacy. Furthermore, this method can achieve real reversibility, separate data extraction and greatly improvement on the superiority of marked decrypted images.

VI.ACKNOWLEDGEMENT

We authors would like to thanks to Yun Q. Shi, Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su for sharing their valuable knowledge.

REFERENCES

[1] Yun Q. Shi, "Reversible Data Hiding," New Jersey Institute of Technology, Newark, NJ 07102, USA.
[2] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, "Reversible data hiding", IEEE *Trans. on Circuits and Systems for Video Technology*, vol. 16, No. 3, Mar. 2006.
[3] Jun Tian, "Reversible data embedding using a difference expansion", IEEE *Trans. on Circuits and Systems for Video Technology*, vol. 13, No. 8, Aug. 2003.
[4] Mehmet UtkuCelik, Gaurav Sharma, Ahmet Murat Tekalp, Eli Saber, "Lossless generalized-LSB data embedding", IEEE *Trans. on Image Processing*, vol. 14, No. 2, Feb. 2005.
[5] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[6] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.
[7]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.
[8]X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[9] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.
[10] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec.2011.
[11] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, 2009.
[12] L. Luo*et al.*, "Reversible image watermarking using interpolation technique,"*IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193,Mar. 2010.
[13] 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.
[14] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012
[15] 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.
[16] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.