ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 6, June 2015

RDH: Reversible Data Hiding with Encrypted Images

Ms. Sunita V. Pawar , Prof. N. G. Pardeshi

***Abstract*— Reversible Data Hiding techniques are used to recover image losslessly after recovery of the secrete message. There are many data hiding technique used to hide the Information or secrete message. But they cause distortion in the original image permanently; such distortion is not acceptable in some application like medical, military, forensic. Therefore for such application RDH techniques are used. In this paper RDH method is applied on the original image then this image is encrypted , which create the room for data as well as preserve privacy of the original image. This recover the original image without any error, also improves the quality of the image.**

***Index Terms*—Reversible data hiding, Image encryption, privacy preservation.**

I. Introduction

As the popularization of Internet, people share digital information , therefore information is easily available to Internet users. But while sharing digital information privacy preservation becomes important. Also there are some annotations that are transmitted with this information, these annotation should be transmitted securely. Data hiding techniques are used to hide some secrete information into cover media. In case of irreversible data hiding technique cover media is distorted permanently, this is not applicable in applications such as military, medical ,forensic, etc. For such application reversible data hiding techniques are applied, which recover the cover after extraction of secrete message/information. These methods are also used for cloud services for privacy preservation, where large amount of user data is stored. In this paper RDH methods are applied on the original image then image encryption is performed to provide security while transmission. Instead of inverse scan method new scan method is used to achieve the better quality. To embed data histogram shift method is used.

Motivation behind RDH techniques is to achieve the reversibility for the cover or original image as well as provide the security for data or secrete message as well as cover image. This improves the data embedding rate (bpp) as well as quality of image

II. Literature Survey

Many data hiding technique permanently distort the cover image and cannot recover correctly after secrete data have been extracted from the stego image. Zhang [6] divided encrypted image by flipping 3 LSB of half of each pixel in each block, to create the room for secrete data. Zhang's method rely on spatial correlation of original image to extract data. So that to recover data encrypted image should be decrypted first before data extraction. Consider the example if Bob have only data hiding key to extract only data, he is not concern with cover image. In this case without image decryption he could not extract secrete message with the help of only data hiding key. This has small payload cause error on data extraction. To separate out both image recovery and data extraction. Zhang [7] emptied out space for embedding, which is called separable reversible data hiding. This method vacates room from encrypted images. In separable reversible data hiding data extraction and cover image recovery is independent of each other , receiver can either extract data or recover image or both by providing data hiding key and image encryption key.

In Zhao's [1] method room is created for secrete message before image encryption which Reserve Room before Encryption, so that separable reversible data hiding is achieved in encrypted images. Advantage of RRBE is image can be recovered without any error .Data hiding is achieved based on histogram shifting and local complexity to improve the embedding capacity and quality of stego image. Local complexity is calculated based on reference pixel of adjacent block to divide image into two parts. Complex blocks are not used for embedding for high visual quality image. Offer better embedding capacity as well as quality of image.

Most spatial domain reversible data hiding are developed based on difference expansion (DE) and histogram modification. In general, the both kind of methods can provide a higher capacity while the latter can produce a better quality marked image.

This paper proposes a reversible data hiding scheme based on histogram modification. Its principle is to modify the Histogram constructed based on neighbour pixel differences instead of the host image's histogram. The basic idea of their scheme is to shift each pixel only one grayscale value after data embedding so that the visual quality of the stego-image can be retained .Also instead of inverse S scan path new scan path is used. Based on this pixel difference pixels are divided into smooth and complex block.

Manuscript received June 12, 2015.

*Ms. **Sunita V. Pawar**, PG Computer Science Student , Savitribai phule Pune University,*

***Prof. N. G. Pardeshi,**, Project Guide, Computer Engineering Department, SRES COE Kopargaon, Savitribai Phule Pune University.*

III. Proposed Method

This paper is based on Reserve Room Before Encryption , which reserve room for the secrete message at content owner side then encrypt image. As RDH technique is applied on original image to create room for secrete message , Image recovery process becomes easier . So that after quality of image is preserved. After encryption data hider hide secrete message inside the encrypted image. Then data hider generates the marked encrypted image. At the receiver's side receiver can extract secrete data and recover original image. As content owner as well as data hider generates the encrypted image privacy is preserved.

Reserve Room Before Encryption consist of three User:

- Content owner.
- Data Hider.
- Receiver.

1.Content Owner:
Role of content owner is to create room for secrete message and image encryption.

Step1: Generation of Grayscale Image
First original image is converted into grayscale image.

Step2: Image Partition
With the Local Complexity function image is divided into local and complex region as shown in fig.1[1]. Block A is Complex region and block B is smooth region. Boundary map is use to hide extra information.

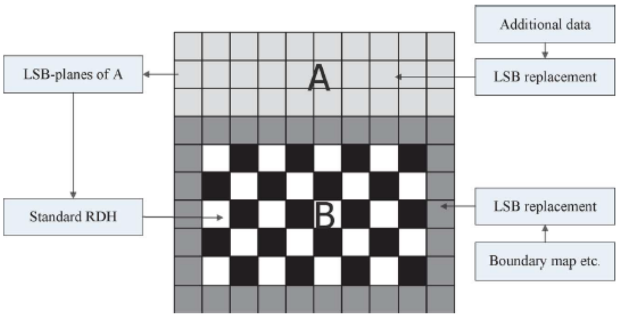

Fig. 1 Image Partition into smooth and complex region.

In fig.1 block A is Complex region and block B is smooth region. Boundary map is use to hide extra information.

Step 3: Self Reversible Embedding:
Once we have complex and smooth region, LSB pixel of complex region is embedded into smooth region to create room for secrete message.
Here for the self reversible embedding any traditional RDH method is used.

Step 4: Image Encryption:
To provide security to this cover image ,Image encryption is done. After image encryption generates **A_E**, the data hider or a third party cannot access the content of original image without the encryption key.

2.Data Hider:

Role of data hider is to hide message inside $\mathbf{A_E}$. First data hider accept data hiding key and secrete message from user, then these bits are stored at the position where room is created for this message. This generates the marked encrypted image. As message hiding key is used any unauthorised user can not able to read secrete message.

3. Receiver:
Receiver can extract the secrete message by providing data hiding key as well as recover the original image by image encryption key.

Algorithm for Self Reversible Embedding:

Step 1: The embeddable area of the modified cover image *I'* is divided into blocks with sizes of 3×3 pixels. Then, the blocks are classified as smooth blocks (S-blocks) and complex blocks (C-blocks).

Step 2: For each block *B*i Ɛ S-block, compute the difference values *d*i of the non-reference pixels with Equation (1)

$d_2=P_2\text{-}C_i$
$d_1=P_1\text{-}P_2$
$d_4=P_4\text{-}C_i$
$d_3=P_3\text{-}P_4$
$d_6=P_6\text{-}C_i$
$d_5=P_5\text{-}P_6$
$d_8=P_8\text{-}C_i$
$d_7=P_7\text{-}P_8$ (1)

Step 3: The difference histogram of the non-reference pixels is constructed. Then, two pairs, i.e., (*PP*1, *ZP*1) and (*PP*2, *ZP*2), of the peak and zero points of the histogram are obtained. Without loss of generality we assume that *ZP*1 <*PP*1 <*PP*2 <*ZP*2. Note that (*PP*1, *ZP*1) ∩ (*PP*2, *ZP*2) = Ø.

Step 4: Scan the difference values *d*i sequentially. If *d*i =*PP*1 or *d*i = *PP*2, a secret bit s, scan difference value *d*i has to be modified to *d*i' using Equation (2)

$$d'_i = \begin{cases} d_i & \text{if } s=0 \\ d_i\text{-}1 & \text{if } s=1 \text{ and } d_i=PP1 \\ d_i+1 & \text{if } s=1 \text{ and } d_i=PP2 \end{cases} \qquad (2)$$

Step 5: Repeat Step 6 until the embedded data S are embedded completely.

Step 8: Construct the stego-image block *B'* i using Equation (3).

$P'_1=d'_1+P_2$
$P'_3=d'_3+P_4$
$P'_5=d'_5+P_6$
$P'_7=d'_7+P_8$
$P'_2=d'_2+C_i$
$P'_4=d'_4+C_i$
$P'_6=d'_6+C_i$
$P'_8=d'_8+C_i$ (3)

Finally, the stego-image *I''* is generated [2] .

Data Embedding Process
Fig.2 [2]shows the data embedding phase, in this two lowest rows and the two right-most columns of the cover image. The LSBs of the pixels in the non-embeddable area are used to

record the information of the location map and the side information.

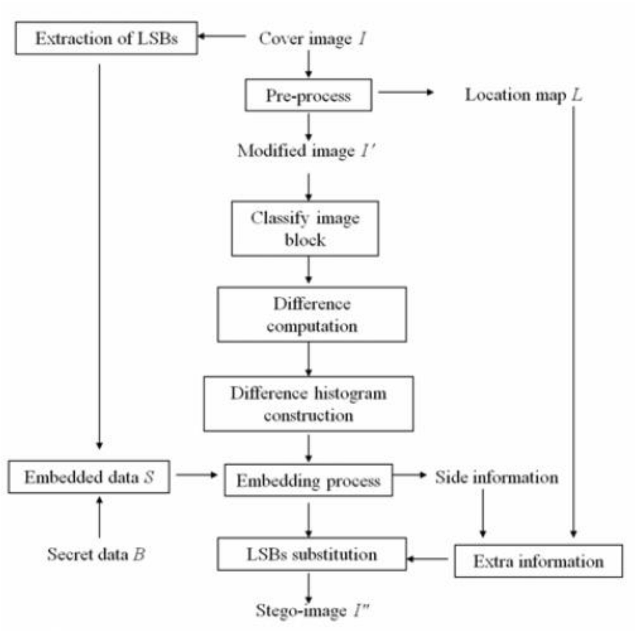

Fig2: Data Embedding process

In this algorithm space is created for new data in complex block and this LSB bits of complex block are embedded into complex block. At the receiver side to recover image again these LSB bits are self reversibly embedded into complex block. In this way original image is recovered losslessly. This method also gives better message embedding rate in bpp.

The peak signal-to-noise ratio (PSNR) is used to estimate the difference between the quality of the original cover image and its stego-image. A large PSNR value indicates that the visual quality of the stego-image is good because it means that a small amount of distortion has occurred. In contrast, a small PSNR value denotes that the stego-image has poor visual quality due to its large distortion. The equation for calculating PSNR is:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

[2]

Where MSE for grayscale image of M X N for grayscale image is :

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_{ij} - I'_{ij}\right)^2 \quad .$$

where *I*ij and *I'*ij are pixel values of the original cover image and the stego-image, respectively.

Embedding capacity (*EC*) indicates the number of secret bits that can be embedded into the cover image. We used bits per pixel (bpp) as the unit of embedding capacity, which is calculated by:

$$EC = \frac{\|B\|}{M \times N}(bpp) \quad .$$

where ||*B*|| is the length of the secret data *B* that can be embedded into a cover image that has a size of *M* × *N*

pixels.

IV. Experiments and Results

Results shows that as reversible data hiding is applied on encrypted image gives better quality of image and histogram shift gives better embedding capacity in bpp.

Input:

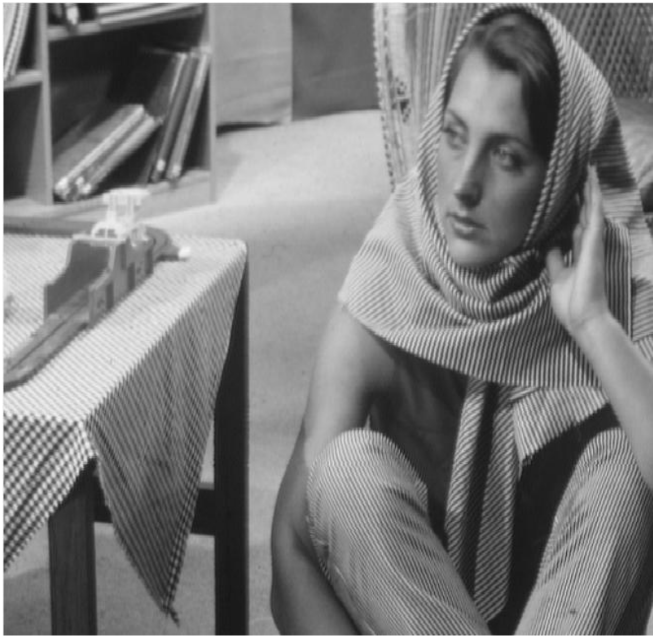

Fig. 3: Original Test Image

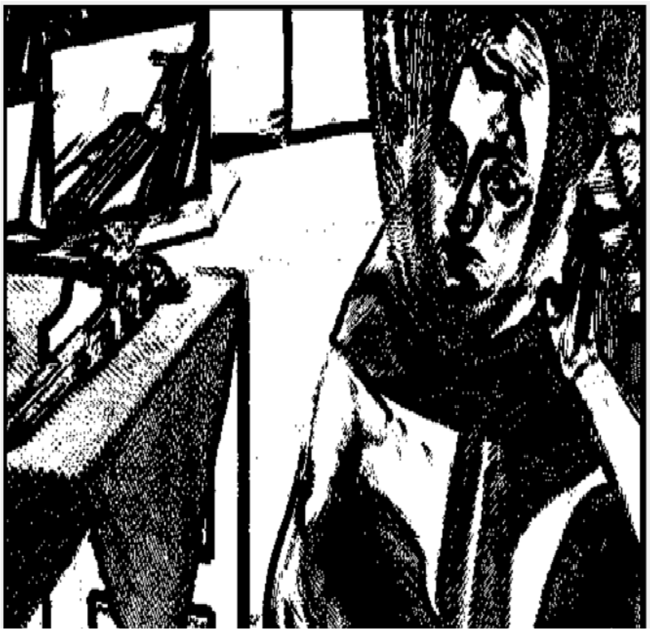

Fig. 4: Image after partitioned into smooth and complex region.

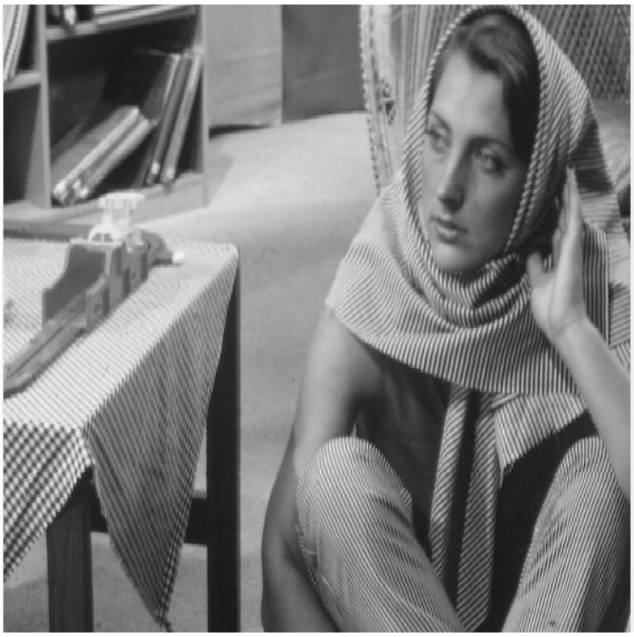

Fig. 5: Image After self -reversible embedding

As shown in fig.4 Input image is divided into two block smooth and complex region. After self-reversible embedding LSB bit of complex region is embedded into smooth block as shown in fig.5. This gives PSNR 51.42 dB

Table 1 gives PSNR and embedding capacity of the stago image generated after self-reversible embedding for six 8 bit gray scale test images of size 512 X 512 .

Image Name	**EC (bpp)**	**Chang et al.'s scheme**	**Proposed Scheme**
		PSNR (dB)	**PSNR (dB)**
Lena	0.26	49.31	52.80
Airplane	0.33	49.37	50.07
Baboon	0.10	51.05	49.21
Peppers	0.26	49.18	50.71
Zelda	0.23	49.04	52.35
Barbara	0.18	51.04	52.21
Average	**0.23**	**49.83**	**51.22**

Table1:Embedding capacity and PSNR for six test images

V. Conclusion

Reversible data hiding recovers the original image with better image quality. As RDH is applied on original image, recovery becomes easier. In comparison with previous method after self - reversible embedding gives better quality of image. Also security is provided for the cover image as well as secrete data during transmission.

Acknowledgment

I am glad to express my sentiments of gratitude to all who rendered their valuable help for the successful completion of the paper. I am thankful to my guide Prof. N. G. Pardeshi, for his guidance and encouragement in this work. I am also thankful to Prof. D. B. Kshirsagar , Head of Department, Computer Engineering,S. R. E. S COE, Kopargaon.

I would also like to express my appreciation and thanks to all my colleagues and family members who knowingly or unknowingly have assisted and encouraged me for the completion of the paper.

REFERENCES

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li.,‖ Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption‖ IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013.

[2] Chin-Chen Chang, Thai-Son Nguyen, and Chia-Chen Lin, Reversible Image Hiding for High Image Quality based on Histogram Shifting and Local Complexity‖ International Journal of Network Security, Vol.16, No.3, PP.201-213, May 2014.

[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] 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.

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

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