www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 11104-11108

Reversible Data Hiding Technique with Improved Reversibility in Encrypted Images

Himangi Mohan Mujumdar[1], Prof. Sachin B. Takale[2]

[1]Savitribai Phule Pune University, Sinhgad College of Engineering,
Sy.No. 44/1, Off Sinhgad Road, Vadgaon, Budruk, Pune, Maharashtra 411041, India
Mujumdar.h@gmail.com

[2] Savitribai Phule Pune University, Sinhgad College of Engineering,
Sy.No. 44/1, Off Sinhgad Road, Vadgaon, Budruk, Pune, Maharashtra 411041, India
sbtakale.scoe@sinhgad.edu

Abstract: ***Reversible Data Hiding is a form of Steganography, in which embedded information is recovered at the destination without any distortion with respect to information as well as cover media. This paper proposes a novel technique which deals with embedding data into encrypted images and recovering back the data as well as image without any distortion. Proposed technique also separates data embedding and image encryption steps. Person having only data hiding key can embed and extract the embedded data without the knowledge of encryption key. Room required to hide data is created before image encryption by estimating values of some randomly selected pixel positions. Improved histogram sifting method is used to hide data into the estimating errors of randomly selected pixel locations. Data is embedded with data hiding key. These estimating errors and remaining image pixel points are encrypted with standard encryption algorithm like AES (Advanced Encryption Standard). To encrypt estimating errors special encryption technique may be used. Proposed technique yields in complete reversibility.***

Keywords: reversible data hiding, image encryption, image recovery, RDH.

1. Introduction

Increasing threats to data getting transferred onto internetworks has led issues related to vulnerability of digital data to attacks. Security and confidentiality of online data is of prime concern. Data hiding is a form of steganography which is used to provide security to the sensitive data by hiding sensitive data into some media. While hiding data into cover media, distortion gets introduced in the cover media during embedding step. Data hiding techniques derived so far can be broadly classified as reversible and irreversible techniques. Reversible data hiding techniques can not erase distortion introduced during data embedding step and return cover media at the receiver side or at the destination side with inevitable distortion. On the other hand irreversible data hiding techniques show property of reversibility at the destination side. Embedded data as well as cover media can be completely recovered at the destination in reversible techniques. In application areas like medical, military imagery and law forensics, cover image with very small distortion is also not acceptable. These areas prove importance of complete reversibility and hence reversible data hiding techniques.

This paper proposes a novel Reversible data hiding (RDH) technique in encrypted images. Up till now the techniques proposed are based on histogram shift [1], lossless compression and difference expansion. All these techniques try to create space for additional data into the encrypted image. Creating space into encrypted image is computationally inefficient, difficult and returns distortion in the cover media.

In [2], extension of histogram modification technique is proposed. An image shows property of correlation. Neighboring pixels in image are highly correlated, hence their pixel value difference is close to zero and theses pixel differences are used to embed data. In [3], author proposed higher dimensional histogram for data hiding. It uses each pixel pair and its surrounding to compute sequence of pairs of pixel difference. Using these values two dimensional histogram is generated and data is embedded in it. In this technique only one pixel in the selected pixel pair is changed by 1, its embedding capacity is low. [4] Author proposes novel concept of reserving room before encryption (RRBE). In this technique room require to hide data is emptied out before image encryption. By this technique data hiding becomes effortless as space require to hide data is already emptied out. Author suggested any traditional RDH techniques to hide data. RDH techniques proposed in [5], [6] and [7] create room for additional data after image encryption. Hence these techniques provide low embedding capacity and at the destination are prone to errors while data extraction or image decryption. In [8] the idea of RRBE is extended and the proposed technique makes data hiding and image encryption tasks separate. This is now a days requirement in cloud computing scenario. To extract data at the destination there is no need to decrypt the cover image first. Person having data hiding key can extract the embedded without knowing the contents of image. In this way image privacy is maintained. To hide data author proposed bin shifting technique which has distortion which is directly proportional to number of bins shifted. The aim of reversible data hiding technique is complete reversibility of cover image. As distortion is directly proportional to number of bins shifted,

this technique may fail in erasing the distortion introduced during data embedding step.

This paper proposes a novel reversible data hiding technique which

- creates space for additional data prior to image encryption,
- makes image encryption and data hiding tasks separate to maintain image and data privacy,
- uses improved histogram bin shifting technique for data hiding,
- results in complete reversibility.

2. Previous State of Art

Figure 1 (a) shows framework of techniques summarized in [1], [2], [3], [5], [6] and [7]. The idea is called as Reserving Room After image Encryption (RRAE). As shown in figure 1 (a), original image is encrypted using encryption key. Any one of the standard algorithm can be used to encrypt the image. Encryption is done by content owner. This encrypted image is given to data hider to hide additional data. Here, data hider first creates room to accommodate additional data to be embedded then it embeds the data in the vacated room using any traditional RDH techniques.

This technique is reversible separable data hiding technique. Data hiding and image encryption tasks are made separate. At the receiver side person having data hiding key can extract the data first without the need of image decryption first. Hence data extraction is possible without knowing the image contents. Image privacy is maintained. Similarly person having encryption key can decrypt the image without knowing the hidden data in it.

The rest of this paper is organized as follows. Section 2 explains previous state of art work. The scheme of the proposed method is explained in Section 3. Evaluation parameters are discussed in section 4. We conclude our paper with a discussion in Section 5.

3. Proposed Method

As we discussed before all previous techniques try to vacate room for additional data to hide in the encrypted image which is difficult and prone to error during recovery of embedded data and cover image at the destination. Also, these techniques result in less embedding capacity.

The paper discusses technique to hide data in encrypted images by reserving room before encryption and using improved RDH algorithm to hide data.

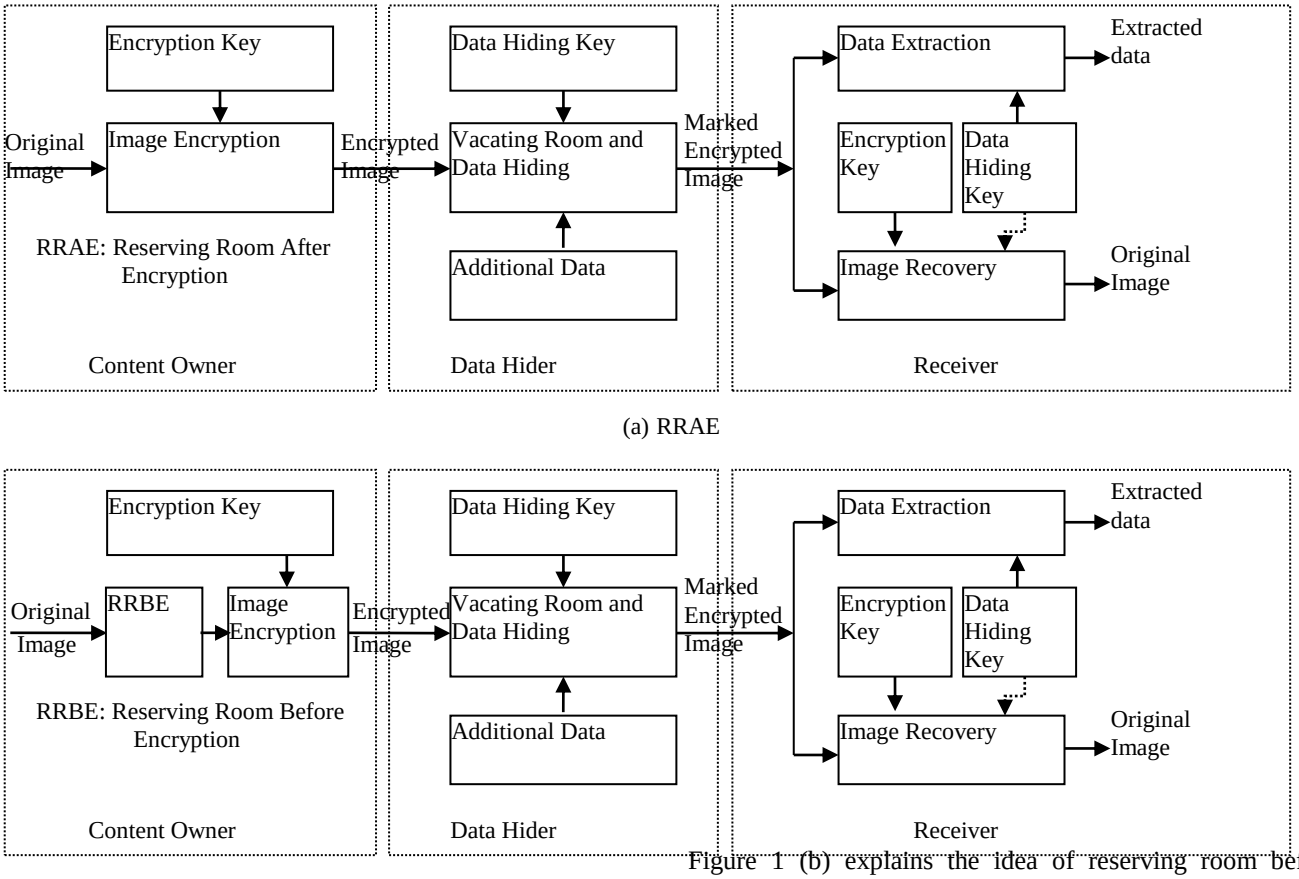

Figure 1: Framework of the proposed idea, (a) RRAE (b) RRBE [4]

Figure 1 (b) explains the idea of reserving room before image encryption (RRBE). As shown in figure 1 (b), original image is first fed to RRBE block. Here room required for additional data to hide is created. Then this image is fed to encryption block. Any one of the standard encryption techniques can be used. This encrypted image is passed to data hider. Data hider embeds the data in already vacated room by any one of standard RDH technique. As this is reversible separable data hiding technique, any one of the data extraction or image decryption tasks can be done prior to other depending on the key a person is having. In this way data as well as image contents are protected from unauthorized access.

Figure 2 shows the framework of the proposed technique. Proposed technique has four primary steps as,

Step 1: Vacating room prior to encryption

Step 2: Embedding data

Step 3: Data extraction

Step 4: Image recovery

Either of the Steps 3 and 4 can be performed first depending upon the right of the person accessing it.

3.1 Vacating room prior to encryption

3.1.1 Estimation

Consider the original Image X of size M×N 8-bit gray scale image. Hence pixel values X (i,j) Є [0,255], 1≤i≤M, 1≤j≤N. Space for data to be embedded is created at this step as follows. Using encryption key content owner randomly selects some pixels. These randomly selected pixels are estimated which means their pixel values are estimated. For estimation mask of 3*3 size is used. This mask is used over the selected pixel position by keeping center of the mask at the selected pixel position. Then using pixel values of the surrounding pixels of the center pixel, the center pixel value is estimated. Any mathematical formula like Average or mean, root mean square (rms) can be used to estimate the selected pixel position value. This process is repeated for all selected pixel positions and selected pixels are estimated. Then error is calculated as difference of original pixel value and estimated pixel value of selected pixels.

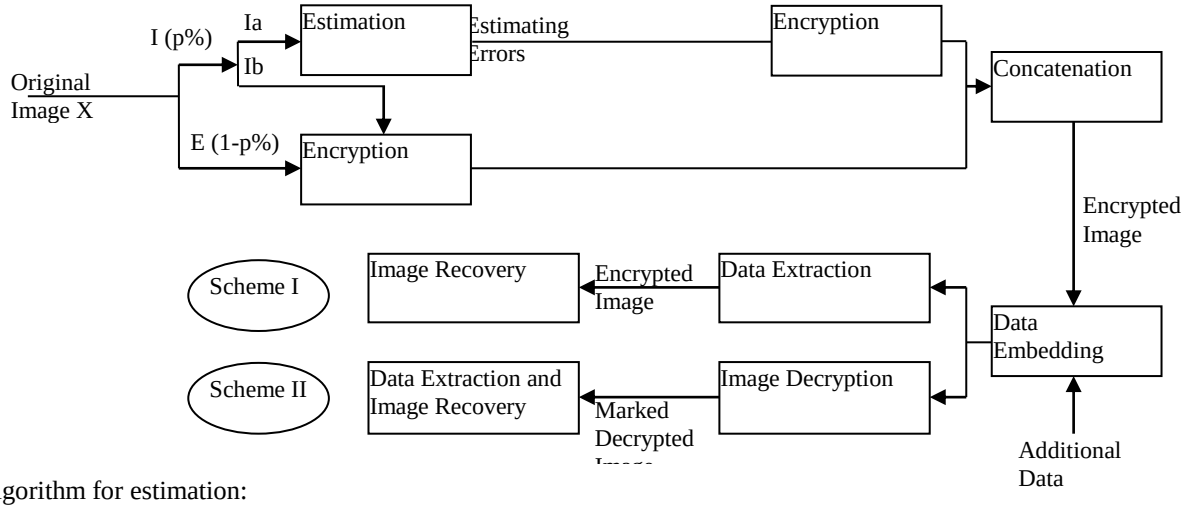

Figure 2: Overview of the proposed technique

Algorithm for estimation:

1. Using encryption key select p% of pixel positions.
2. Consider selected pixel positions as belonging to I matrix and remaining pixel positions belonging to E matrix.
3. Estimate pixel values of pixel positions belonging to I matrix using surrounding pixel values of pixel positions belonging to E matrix.
4. Find error as difference of original pixel values and selected pixel values.
5. Replace error values in the pixel positions belonging to I matrix.

3.1.2 Vacating Room

After getting error values of pixels positions belonging to matrix I, these positions are used to hide additional data. Room required for additional data is created by shifting histogram of these estimated errors.

The basic idea behind histogram shifting method is use the pixel value having zero number of corresponding pixels in the image. For exact recovery of original image location map of pixels whose value is changed during embedding step is required. Advantage of this method is such location map is not required if image has perfect zero point. Also computational overhead of this method is much less compared to other most data hiding reversible techniques. This method is very effective and simple to implement. In [8], for data embedding author has proposed standard histogram bin shifting method.

Here we explain Standard Histogram Bin shifting and Improved Histogram Bin shifting methods.

Standard Histogram Bin shifting:

Let 'P' be the grayscale pixel value corresponding to peak of the histogram and 'Z' be the grayscale pixel value corresponding to zero point. The bins or span of histogram between 'P+1' and 'Z-1' is shifted to right by 1 position and a zero point is created at 'P+1' grayscale pixel value to accommodate additional data. Data embedding is done in a way that when grayscale pixel value 'P' is occurred, if the bit to be embedded is '1', increase the pixel value by '1, otherwise leave pixel value as is (for bit to be embedded is '0').

Here grayscale pixel value 'P' is considered as embedding point and embedding capacity is equal to the frequency of occurrence of this grayscale pixel value 'P'. Data extraction is exactly opposite process. When a grayscale pixel value 'P+1' is occurred extracted bit is '1' and the pixel value is reduced to 'P'. When a grayscale pixel value 'P' is occurred extracted bit is '0'. After all message bits have been extracted shift span of histogram between 'P+2' and 'Z-1' to left by '1'. If in this process exact zero point is absent in the histogram then a minimum point is selected and histogram between peak and minimum point is shifted to accommodate additional data. However pixels corresponding to minimum point needed to be recorded in the sense that their position and pixel values for exact recovery of cover image.

Improved Histogram Bin shifting:

Data embedding point is the peak point of the histogram in standard histogram method. Bins between peak and zero or

minimum are shifted to create space for additional data. The quality of the recovered image depends upon the number of shifted bins. More the number of shifted bins more the distortion gets introduced. Also, not always peak point as data embedding point is required. Embedding point should depend upon the amount of data to be embedded. So embedding point should be variable depending upon the length of data to be embedded. All these drawbacks of standard histogram bin shifting method are eliminated in Improved histogram bin shifting method.

The distortion can be reduced if number of bins between embedded point and zero point are less.

Algorithm to vacate room for data:

1. Plot the histogram of estimating errors.
2. From the histogram find the zero point, ie, the pixel value having zero number of corresponding pixels.
3. If zero point is absent in the histogram find the minimum point, ie, pixel value having minimum number of corresponding pixels.
4. Choose the pixel value whose frequency of occurrence is greater than or equal to the size of the data to be embedded.
5. Shift the bins between this embedding point and zero/minimum point to accommodate additional data.

After creating room for data the rest of the pixels, ie pixels belonging to matrix E are encrypted using standard or advanced encryption standard. Content owner gives these shifted errors to data hider to embed the data in. This process may reveal the distribution of the estimating errors. Hence estimating errors are also encrypted as shown in figure 2. After encryption estimating errors and rest of the pixels are rearranged as estimating errors to the top followed by rest of the pixels to protect estimating errors from being revealed out.

3.2 Embedding data

Data hider hides the data in the encrypted image received from the content owner with data hiding key. Purpose of embedding data may be for authentication, to check for data integrity or for management of encrypted images.

Let's consider pixel value of the embedding point as x. This value changes for every image as it depends upon the histogram of a particular image. First few generally 16 pixel positions having value 'x' are used to save length of the total 'x' valued pixel positions. Data hider reads this length by extracting first 16 'x' valued pixels. He encrypts the data to be embedded before embed to give additional security to data. For encryption of the data to be embedded he uses the data hiding key. Then he embeds the encrypted data into rest of the 'x' valued pixels. Finally he rearranges the image with data hiding key

3.3 Data extraction and image recovery

As shown in figure 2, steps 3 and 4 can change their order. Depending on their order two schemes are possible as shown in figure 2.

3.3.1Scheme 1: Data extraction prior to image decryption.

(a) Data Extraction:

At the receiver side, the person authorized to view the embedded data acquires the data hiding key. With the help of data hiding key he rearranges back the encrypted image. At this stage he gets image with estimating errors at the top and rest followed by the rest of the pixels. From the estimated errors he extracts the encrypted data. He then decrypts the encrypted data with data hiding key and retrieves the original embedded data.

(b) Image Restoration:

1. From the rearranged image read the length of the embedded data from first 16 'x' valued pixels.
2. Decrypt all the estimating errors using encryption key.
3. Decrypt all the rest pixels belonging to matrix E using encryption key.
4. Pixel positions selected with encryption key are encryption key specific. Using encryption key select pixel positions from marked image.
5. Remaining pixels are put sequentially as E matrix.
6. Estimate the values of selected pixel locations.
7. Obtain the original value by adding error to the step 6.
8. Replace values in step 7 in the image.

3.3.2Scheme 2: Image decryption prior to data extraction.

Process of image restoration is same in schemes 1 and 2.

(a) Data Extraction:

After image restoration, the image is decrypted but still contains data and called marked decrypted image. To get data from marked image,

1. Using encryption key find locations of pixels in matrix E and matrix I .
2. Find the errors of pixel belonging to matrix I.
3. Extract data from these pixel locations

4. Evaluation Parameters

Performance of the proposed method can be studied by following performance parameters.

1. Peak Signal to Noise Ration (PSNR): The quality of the retrieved image in both the schemes can be determined by PSNR. Formula is:

$$\text{PSNR: } 10 \times \log_{10}\left(\frac{255 \times 255}{p\% \times (1-q)\%}\right) \qquad (1)$$

Where,
p%: percentage of pixels selected for data hiding.
q%: percentage of encrypted estimated errors.

2. Embedding Rate (ER): The Average number of bits embedded per pixels. Unit is bpp (bits per pixel).

3. Complete Reversibility: can be evaluated by average error pixels Aep. Formula is

$$Aep = \frac{U}{Y} \qquad (2)$$

Where,

U = Total number of pixels those are not recovered.
Y = Total number of images tested.

5. Conclusion

This paper proposes a novel RDH technique for encrypted image by reserving room before encryption and using improved histogram bin shifting technique for data embedding. As creating room in already encrypted image is difficult this technique exploits estimation formula and creates space for additional data prior to Image encryption. Lossless recovery of data as well as image is possible with this technique. This method separates image decryption and data extraction tasks and hence useful for variety of applications. With this technique privacy of embedded data as well as encrypted image is maintained. The person having only data hiding key can embed the data in and extract the data out without knowing the image contents and hence image contents are protected. Similarly with the encryption key only the image can be decrypted without knowing the embedded data.

References

[1] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006.

[2] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, Fellow, IEEE "Reversible Data Hiding Based on Histogram Modification of Pixel Differences", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 6, JUNE 2009.

[3] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang, "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013.

[4] 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.

[5] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image", IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011.

[6] Wien Hong, Tung-Shou Chen, Han-Yan Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match", IEEE SIGNAL PROCESSING LETTERS, VOL. 19, NO. 4, APRIL 2012.

[7] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[8] Weiming Zhang, Kede Ma, Nenghai Yu, "Reversibility improved data hiding in encrypted images", School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China.

[9] Pasunuri Nagarju, Ruchira Naskar and Rajat Subhra Chakraborty, "Improved Histogram Bin Shifting based Reversible Watermarking", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).