ISSN:0975-9646

Non-Saperable Reversible Data Hiding in Encrypted Image Using Chaoutic Map

Nilesh Solanki[1], Mahesh Parmar[2], Dr. Vineet Richhariya[3]
[1]M. Tech. Scholar, [2]Assistant Professor, [3]Professor
LNCT College Bhopal

Abstract-Nowadays, more and more attention is given to reversible data hiding (RDH) techniques in encrypted images by researcher. There are too many researchers who are regularly doing their efforts on the RDH. Reversible Data hiding techniques are intended to solve the major problem of lossless embedding of very large image and after the embedded information is extracted the received image is to be same as the original one.RDH method is divided into two parts i.e. Separable Reversible Data Hiding and Non- Separable Reversible Data Hiding. This paper deals with the concept of RDH, classification of RDH , performance parameters to check the quality of RDH methods , and survey on various techniques developed by many researchers.

Index Terms: - Reversible data hiding, Image encryption, Image decryption.

1. INTRODUCTION

Data hiding is the technique which is used for embedding the important information into covers. The covers may be audio, video, image or any other file. Data hiding is used for copyright protection, authentication, covert communication and others. Most of the data hiding methods embed the given messages into the cover media to generate the Output media by only modifying the least significant part of the cover media and, thus, ensure perceptual transparency. The method of embedding will usually introduce everlasting alteration to the cover and it is very difficult to reconstruct the original cover. In some applications, however, such as medical, military, and law forensics degradation of the original cover is not allowed. In this type of cases we want to construct a method which may provide efficient results. Reversible data hiding (RDH) is one of the types of method which provide good result in the data hiding methodology. By using reversible data hiding method the original cover can be lossless recovered. After the received message is extracted because there are many people who can temper the image so the authentication is must. There are many techniques used in image authentication.

2. REVERSIBLE DATA HIDING

Reversible data hiding is the technique of hiding the important information behind the images for secret data communication. It is the technique to hide the extra message into the cover media by using a reversible manner, i.e. after extraction of received image we can construct the image same as the original image and can read the message hide behind it. First we encrypt the message from the sender side and after that at the receiver side the original message can be recovered.

In this method first the content owner encrypts the original content before passing it to the data hider for further transmission. The data hider then add some extra information in the image by applying some data hiding methods and [ass it to the receiver side. The receiver side then extract the encoded message and can recover the image same as the original image. The performance of a reversible data hiding algorithm can be calculated on the basis of following tolls:-

- Payload capacity limit
- Visual quality
- Complexity

3. SEPARABLE REVERSIBLE DATA HIDING

The form of reversible data hiding is the separable reversible data hiding. Here the separable means to separate in other words we can separate something. The main concept of separable reversible data hiding is that we can extract the original image by using the encryption key and the extraction of the payload by using the data hiding key.

Both the parts are separated from each other. It means if we have the data hiding key then we can extract the hidden data but cannot reconstruct the original image and if we have the encryption key then we can construct the image same as the original but cannot read the hidden data. We need both of the keys to read the whole received data.

4. NON-SEPARABLE REVERSIBLE DATA HIDING

Another technique of reversible data hiding is non-separable Reversible Data hiding. In this method first the content owner encrypts the image using encryption key then passes it to the data hider. The data hider then embedded some additional data in the image using the data hiding key. The main feature of Non-Separable Reversible Data hiding differs from Separable Reversible Data hiding from here. At the receiver point we need both of the keys i.e. encryption key and the data hiding key to extract the original data and the original image.

5. PROPERTIES OF RDH

- **Image Encryption**- The sender selects the file and applies his encryption algorithm to encrypt the image. Encryption is the method of applying or changing some of the attributes of the original image to form a very different image. Nobody can read the exact image if he is unknown of the changed done by the content owner.
- **Data Embedding**- After encrypting the image the sender embed some additional data behind the selected part of the image before transmission. Any type of image can be selected for the encryption like JPEG, PNG or BMP.

- **Data Extraction**- This is the action performed at the receiver side. After receiving the data the main task of the receiver is to extract the original data hide behind the image. This technique is known as data extraction.
- **Image Recovery**- Image recovery is the technique of decrypting the received image. The main task is to generate the image same as the original image. And this is done by the reversibly perform the encryption action i.e. by using the decryption key.

6. PREVIOUS WORKS

In RDH method, the original cover image can be restored without any loss after the information is extracted. This method is also known as lossless method. Weiming Zhang, et al [1] used a decompression method for recursive code construction. In the first phase of their scheme the content owner encrypts an uncompressed cover image by using an encryption key. Then, a data hider compresses LSB's of the received encrypted image using a special data hiding key to accommodate a sparse space to put up some additional data. In this scheme if anyone has the data hiding key, the additional data can be extracted. But it cannot get the image content and if he has the encryption key then he can reconstruct the image same as the original one but cannot get the additional data.he need both the keys to get the whole information. Xinpeng Zhang [2] shows the embedding rate is 0.017 bit per pixel (bpp) in The encrypted image containing the embedded data. C.Anuradha and S.Lavanya,[3] in "Secure and Authenticated Reversible Data Hiding in Encrypted Image shows a completely different method for authentication of the image. The uses SHA-1 algorithm for authenticating the image. Rintu Jose and Gincy Abraham [4] in the very different method. And as per the result the Peak Signal to Noise Ratio of the decrypted image was much higher. The data hiding capacity was also much higher. V. Suresh and C. Saraswathy [5] they discussed about the bandwidth constrained over the communication channel. They uses the RC-4 algorithm to create the pseudo-random sequence using the 128-bit encryption key. They achieves the accuracy in recovering the original image as compared to others. Hun-Chi Lo et al [6] proposed a scheme of reversible data hiding the compressed images for block truncation coding (BTC). to embed the secret data The histogram shifting technique is used. The results showed good image quality after receiving. From the experimental results Average hiding capacity of 2686.125 and 4540.5 bits are obtained. Divyani UdayKumar Singh et al [7] also shows a very different method by using fake data. The concept of steganography is used in the paper. They uses the AES algorithm to encrypt data using AES algorithm and hides the encrypted data in Image by LSB technique. If the user is unauthenticated then the system will generate the fake information for the intruder. Ambika Oad et al [8] surveys on the different techniques of data hiding and find various of them very use full and security prone. Wagh Mahesh et al [9] proposed a navel method by reserving room before encryption. Improved image efficiency of the image is achieved By using the new RHD method the new method using RDH algorithm results in the reduced noise effect. Lalit Dhande et al [10] proposed another scheme of data hiding. They uses the traditionally RDH method for encryption for reserving room before encryption. There scheme produce real reversibility and image recovery and extraction of data are free of error. Zhaoxia Yin et al [11] proposed a separable RDH method in encrypted image and as a result it shows higher payload capacity & error-free data extraction. To obtain the encrypted image, the envelop image is partitioned into non-overlapping blocks & multi-granularity encryption is applied. The method achieves the high PSNR and effective payload without any complicated calculation and that's why produces high efficiency.

7. PROPOSED METHODOLOGY

A content owner take the inverse s-order of the histogram.After that data hider hides the additional data into the image using data hiding key and then encrypts the image with the help of encryption key though the receiver does not know about the original content. With an encrypted image containing additional data, a receiver can only get the contents of the image after decryption it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.

In the scheme, the data extraction is Non-separable from the content decryption. Fig .1 shows Non-separable reversible data hiding in encrypted image.

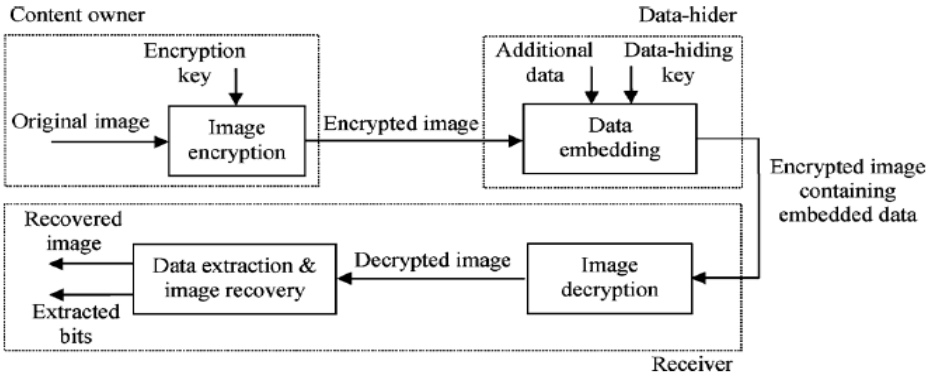

Fig- Non-Separable Reversible Data Hiding

1. Data Embedding

This is the first prosess of embedding.First Input a gray scale image with L bits per pixel. Shift the histogram from both sides by 1 unit. Note that the histogram shifting information is recorded as overhead bookkeeping information that will be embedded into the image itself with payload.

Scan the whole image in an inverse s-order. Calculate the pixel difference between the neighbouring pixles by the formula,

$$d_t = \begin{cases} x_t, & if\ t = 0 \\ |x_{t-1} - x_t|, & otherwise \end{cases}$$

Determine the peak point P from the pixel differences. Scan the whole image in the same inverse s-order as in Step 1.

$$y_t = \begin{cases} x_t, & if\ t = 0\ or\ d_t < P, \\ x_t + 1, & if\ d_t > P\ and\ x_t \geq x_{t-1}, \\ x_t - 1, & if\ d_t > P\ and\ x_t < x_{t-1}, \end{cases}$$

Use this this fourmula where yi is the stego value of pixel i. If di = P, modify xi according to the message bit

$$d_t = \begin{cases} x_t + b, if\ d_t = p\ and\ x_t \geq x_{t-1} \\ x_t - b, if\ d_t = P\ and\ x_t < x_{t-1} \end{cases}$$

Where b is a message bit to be embedded.

After modifying the pixel value of original image X we get the stego image Y and it is ready of encryption.

2. Image Encryption

To encrypt the image generate a pseudo random sequence of size same as size of Y Based on Chaotic sequence with the help of equation (listed below)

$$a_{p+1} = \mu * a_p * (1 - a_p)$$

Where $0 < \mu < 4\ and\ a_p \in [0,1]$ (1)

a0 is an initial seed and combination of a0 and μ serves as the encryption key. Generate N = mn pseudorandom numbers using (1) and store them in a vector P. Sort the vector P in ascending order to generate a location map L.

Arrange pixels of the stego image Y into a vector V. Rearrange V according to the location map L. reshape vector V into matrix sized m × n to get the encrypted stego image E.

3. Data Extraction

To extract data from encrypted stego image E it must be decrypt first. To do this the receiver decrypt the encrypted image. So, he generates the same chaotic sequence as in encryption phase using and the initial conditions. The logistic map is generated by sorting the sequence in ascending order. Using the logistic map, pixels of the encrypted image are rearranged to their original position to get the decrypted image Y.

Now receiver can extract the data from decrypted image Y. the recipient extracts message bits from the decrypted stego image by scanning the image in the same order as during the embedding. The message bit b can be extracted by

$$b = \begin{cases} 0, & if\ |y_t - x_{t-1}| = P \\ 1, & if\ |y_t - x_{t-1}| = P + 1 \end{cases}$$

Where xi-1 denotes the restored value of yi-1. The original pixel value of xi can be restored by

$$x_t = \begin{cases} y_t + 1, & if\ |y_t - x_{t-1}| > P\ and\ y_t < x_{t-1} \\ y_t - 1, & if\ |y_t - x_{t-1}| > P\ and\ y_t > x_{t-1} \\ y_t, & otherwise \end{cases}$$

Extract the overhead information from the extracted message. If a value 1 is assigned in the location i , restore xi to its original state by shifting it by 1 unit; otherwise, no shifting is required.

8. Experimental Results

We tested the proposed Non-separable method with 5 commonly used test images namely Airplane, Parrot, Cameraman, Pepper, Ship each of size 256×256. In our implementation we used the s-order difference to hide data. We have used those pixels whose difference with their preceding pixel is equal to the peak point of the difference matrices.

Below table shows the data hiding rate in bits per pixel (bpp) here PSNR of decrypted images and PSNR of recovered images. The "+α" value shows that the original image is completely recovered without any error.

Image	Data hiding rate (bpp)	PSNR of directly decrypted image (dB)	PSNR of recovered image (dB)
Airplane	0.0372	52.5838	+α
Cameraman	0.0372	53.7551	+α
Ship	0.0372	53.5436	+α
Pepper	0.0372	52.6566	+α
Parrot	0.0372	57.2154	+α

Receiver can only get the content of the image after decrypting the image.The PSNR of all directly decrypted images were above 48.13dB and verifies the theoretical result. When the receiver has the data hiding key he can extract the can extract the hidden data without any error. He can extract the hidden data exactly and recover the image. The recovered image is exactly same as the original image.

9. Conclusion

A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though the receiver does not know the original content. With an encrypted image containing additional data, a receiver first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.

In the scheme, the data extraction is Non-separable from the content decryption.

REFERENCES

[1] Weiming Zhang, Biao Chen, and Nenghai Yu," Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 6, JUNE 2012.

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

[3] C.Anuradha, S.Lavanya, "Secure and Authenticated Reversible Data Hiding in Encrypted Image Volume 3, Issue 4, April 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering".

[4] Rintu Jose, Gincy Abraham " A Separable Reversible Data Hiding in Encrypted Image with Improved Performance" ICMiCR-2013.

[5] V. Suresh C. Saraswathy "Separable Reversible Data Hiding Using Rc4 Algorithm "Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22

[6] Chun-Chi Lo1,Yu-Chen Hu2,Wu-Lin Chen2and Chang-Ming Wu3 " Reversible Data Hiding Scheme for BTC-compressed Images Based on Histogram Shifting" International Journal of Security and Its Applications Vol.8, No.2 (2014), pp.301-314 http://dx.doi.org/10.14257/ijsia.2014.8.2.31

[7] Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav "Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation" International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3469-3473.

[8] Ambika Oad, Himanshu Yadav, Anurag Jain "A Review: Image Encryption Techniques and its Terminologies" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[9] Wagh Mahesh J.1, Manish Koul2, Murtadak Sona U.3, Shinde Kavita S.4, Prof. Bhandare M.G.5 ""RDH(Reversible Data Hiding) in Encrypted Images by Reserving Room Before Encryption" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014).

[10] Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade Hide Inside-Separable Reversible Data Hiding in Encrypted Image International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-9, February 2014.

[11] Zhaoxia Yin,1 Bin Luo,1 andWien Hong2 "Separable and Error-Free Reversible Data Hiding in Encrypted Image with High Payload " Hindawi Publishing Corporation e Scientific World Journal Volume 2014, Article ID 604876, 8 pages http://dx.doi.org/10.1155/2014/604876.

AUTHOR' BIOGRAPHY

NILESH SOLANKI has received the B.E. degree in INFORMATION TECHNOLOGY from RKDF college, Rajiv Gandhi Technical University Bhopal. He is currently working toward the Master degree in Software Engineering at LNCT college, Rajiv Gandhi Technical University. His research interests include data hiding and image recovery.