International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.245-253
DOI: http://dx.doi.org/10.21172/1.81.033
e-ISSN:2278-621X

REVERSIBLE STEGANOGRAPHY IN IMAGE: AN OVERVIEW AND REVIEW

Krati Pandey[1], Dr. Manish Shrivastava[2] and Shraddha Pandit[3]

Abstract- Modern day researchers are focusing mainly on Reversible data hiding (RDH) techniques for the encrypted images. The number of researchers putting in their efforts on Reversible data hiding techniques is burgeoning day by day. Reversible data hiding techniques are deployed in order to achieve the lossless and high quality embedding of very large images. It also ensures that the extraction of embedded information is done the received images matches the original one. There are two sides to Reversible data hiding method; Separable Reversible data hiding and Non-Separable Reversible data hiding. This paper deals with the concept of Reversible data hiding ,classification of Reversible data hiding, performance parameters to check the quality of Reversible data hiding methods and survey on various techniques developed by many researchers.

Keywords – Reversible data hiding, Encryption, Decryption.

I. INTRODUCTION

Data hiding is the techniques which is used for embedding the important information/data into cover media. The covers may be audio, video, image or any other file. Data hiding is used for copyright protection, authentication, covert communication etc. Most of the data hiding processes 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, make secure perceptual transparency [1]. The method of embedding will usually introduce everlasting alteration to the cover and it is very difficult to rebuild 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 assemble 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 (genuine) 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].

[1] *Department of Information Technology & M-tech Scholar LNCT RGPV University, Bhopal, India*
[2] *Department of Information Technology & Professor LNCT RGPV University, Bhopal, India*
[3] *Department of Information Technology & Assistant Professor LNCT RGPV University, Bhopal, India*

II. REVERSIBLE DATA HIDING

Reversible data hiding is the technique of hiding the vital 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 assemble the image same as the genuine (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 genuine (original) message can be recovered [3].

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

- Payload capacity limit
- Visual quality
- Complexity

A. Separable Reversible Data Hiding

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

One and other i.e. both the parts are separated from each other. It means if we have the data hiding key then we can extract the unseen i.e. hidden data but cannot reassemble the original image and if we have the encryption key then we can construct the image same as the genuine image but cannot read the hidden data. We need both of the keys to read the whole received data[4].

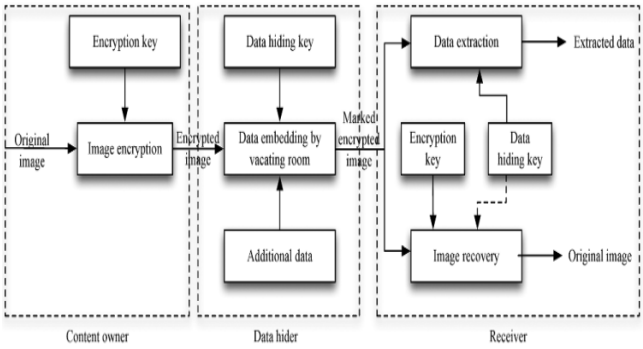

Fig.1. separable Reversible Data hiding

B. Non-Separable Reversible Data Hiding

Another approach of reversible data hiding is non-separable Reversible Data hiding. In this method first the content legatee encrypts the image using encryption key then passes it to the data hider. The data hider then embedded some supplementary i.e. additional data in the image using the data hiding key. Here, the main characteristic of Non-Separable Reversible Data hiding is different from Separable Reversible data hiding. At the receiver point we need both the keys i.e. encryption key and the data hiding key to extract the genuine data and the genuine image [5].

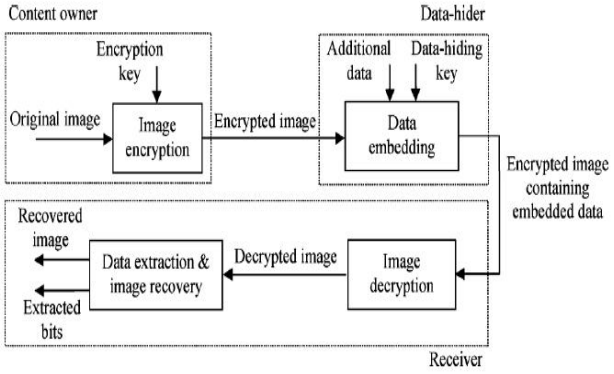

Fig.2. Non-separable reversible data hiding in encrypted Image

III. PROPERTIES OF RDH

A. Image Encryption

The sender selects the file and applies his encryption algorithm to encrypt the image. Encryption is the method of applying or altering some of the attributes of the genuine (original) image to form a very different image. Nobody can read the accurate (exact) image if he is unknown of the changed done by the content owner [6].

B. Data Embedding

After encrypting the image the sender embed some supplementary i.e. additional data behind the selected part of the image before transmission. Any kind of image can be selected for the encryption like JPEG, PNG or BMP.

C. Data Extraction

This is the action implemented at the receiver side. After receiving the data, the main work of the receiver is to extract the original data hide behind the image. This approach is known as data extraction.

D. Image Recovery

Image recovery is the technique of decrypting the received image. The main action 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.

IV. PERFORMANCE PARAMETERS

The quality of the encrypted image is measured by calculation of certain evaluation measurement metrics. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed on the basis of these values. The metrics used in this paper are as follows: Mean Square error (MSE), peak signal- to-noise ratio (PSNR), Number Of Pixel Change Rate (NPCR) and Embedding ratio in BPP.[7] [8]

A. Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE can be defined as the measurement of average of the squares of the difference between the

intensities of the Encrypted image and the original image. It is popularly used because of the mathematical tractability it offers. It is represented as:

Where C(i, j) is the original image and C' (i, j) is the encrypted image. A large value for MSE means that the image is of poor quality.

B. Peak signal to noise ratio (PSNR)

The PSNR [5] depicts the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover and encrypted image. The advantage of this measure is easy computation. It is formulated as:

$$PSNR = 20 \log 255^2 / MSE$$

A low value of PSNR shows that the constructed image is of poor quality.

C. Number of Pixel Change Rate(NPCR)

Attacker tries to find out a correlation between the plain image and the cipher-image, by studying how differences in an input can affect the resultant difference at the output in an attempt to determine the key. Trying to make a slight change such as modifying one pixel of the encrypted image, aggressor (attacker) observes the change of the plain-image. To test the influence of one pixel change on the entire encrypted image by the proposed algorithm, two common measures are used [5]:

Number of Pixel Change Rate (NPCR)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

C1 and C2: two ciphered images, whose corresponding genuine images have only one-pixel difference. C1 and C2 have the exactly same size.

C1(i, j) and C2(i, j): grey-scale values of the pixels at grid (i,j).

D(i, j): determined by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0.W and H: columns and rows of the image.

D. Payload

We use the different techniques to hide the data behind the image. The data which we want to hide behind the image is known as the payload. If we want to hide more data behind the image we need more space for. There are many methods which provides the high payload capacity. We will discuss them later

V. LITERATURE SURVEY

Lots of research has been done in the field of reversible data hiding. In last few years various efficient methods have been proposed for reversible data hiding. Some noticeable work in area of reversible data hiding is as follows:

Jun Tian [9] developed a simple and efficient reversible data embedding method for digital images in which he explored the redundancy in the digital content to accomplish reversibility. Both the payload capacity limit and the visual quality of embedded images are among the best in

the literature. As a basic requirement, He achieved the policy that quality degradation on the image after data embedding should be low.

Shiguo Lian and et.al [10] suggested a different scheme composed of joint data-hiding and encryption schemes. In this system a part of cover data is used to carry the supplementary (additional) message and the rest of the data are encrypted, so that both the copyright and the privacy can be secured. Here motion vector difference and signs of DCT coefficients are encrypted, although a watermark is embedded into the amplitudes of DCT coefficients. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be rewatermarked.

Wei-Liang Tai et.al.[11] present a reversible data hiding scheme based on histogram modification. Authors exploit a binary tree structure to resolve the problem of communicating pairs of peak points. Distribution of pixel differences is used to achieve large hiding capacity while keeping the distortion low. Authors also adopt a histogram shifting technique to inhibit overflow and underflow. Performance comparisons with other existing schemes are provided to demonstrate the superiority of the proposed scheme.

Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong suggested a method , [12] which can embed a large amount of covert data into images. It make use of the interpolation-error, the difference between interpolation value and corresponding pixel value, to embed bit “1” or “0” by expanding it additively or leaving it unchanged.

Che-Wei Lee and Wen-Hsiang Tsai[13] proposed a lossless data hiding method based on histogram shifting, which employs a scheme of adaptive division of cover images into blocks to yield large data hiding capacities as well as high stego-image qualities. The technique is shown to break a bottleneck of data-hiding-rate increasing at the image block size of 8×8, which is found in existing histogram-shifting methods. Four ways of block divisions are designed, and ones which provides the largest data hiding capacity is selected adaptively.

Zhenfei Zhao and et.al [14] showed a reversible data hiding method for natural images. Due to the similarity of neighbor i.e. acquaintance pixels values most differences between pairs of adjacent pixels are equal or close to zero. In this work, a histogram is assembled i.e. constructed based on these difference statistics. In the data embedding stage, a multilevel histogram modification mechanism is employed. As more peak points are used for secret bits modulation, the hiding capacity is improved compared with those conventional methods based on one or two level histogram modification. Moreover, as in the data extraction and image recovery stage, the embedding level instead of the peak points and zero points is used.

X Zhang [15] suggests a novel method for separable reversible data hiding .Here content owner firstly encrypts the original uncompressed image using an encryption key to formed an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to contain the additional data. At the receiver side, the data embedded in the created space can be easily get back from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only influences the LSB, a decryption with the encryption key can result in an image which is similar to the original version. When using both of the encryption and data-hiding keys, the embedded supplementary i.e. additional data can be successfully extracted and the genuine i.e. original image can be perfectly recovered by exploiting the spatial correlation in natural image.

Xinpeng Zhang [16] presented a practical scheme where a content owner encrypts the original image using an encryption key, and a data-hider embeds supplementary i.e. additional data into the encrypted image using a data-hiding key yet receives does not know the original content. With

an encrypted image containing supplementary data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and find again recover the original image according to the data-hiding key. In the scheme, the state of data extraction is not separable from the activity of content decryption. This means that the additional data must be extracted from the decrypted image, so that the principal content of genuine image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot to extract any information from the encrypted image containing additional data.

Weiming Zhang, Biao Chen, and Benghazi Yu proposed a decompression algorithm [17] as the coding scheme for embedding data. Three Reversible data hiding techniques that use binary feature sequence as covers, i.e., one scheme for spatial images, one scheme for JPEG images, and pattern substitution scheme for binary images.

Xian-ting Zeng et al. [18] presented a method for lossless data hiding with large payload based on histogram shifting and multi layer embedding. In this technique the genuine i.e. original image and secret information is extracted from the stego image by using only the length of the hidden data and no other extra information is needed. In the proposed scheme 13 layer embedding could be applied and achieved greater bits per pixels compared to existing method.

V. Suresh et.al [4], the problem of transmitting redundant data over an insecure, bandwidth-constrained communications channel is discussed. A content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the smallest i.e. least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. Using data hiding key the receiver can extract supplementary (additional) data even the receiver has no information about the original image content. Using the decryption key the receiver can extract data to acquire an image which is similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, the receiver can extract the additional data and the genuine i.e. original image without any loss.

Rintu Jose and C. Saraswathy [19] propose a novel scheme to reversibly hide data into encrypted grayscale image in a separable manner. During the first phase, the content owner encrypts the image by permuting the pixels using the encryption key. The data hider then hides some data into the encrypted image by histogram modification based data hiding, makes use of data hiding key. At the receiver side, if the receiver has only encryption key, he can generate an image similar to the original one, but cannot read the hidden data. If the receiver has only data hiding key, he can extract the data, but cannot read the content of the image. If the receiver has both keys, he may first extract the data using data hiding key and then decrypt the image using encryption key.

Yong Zhang [20] proposed a RHD technique that is An Improvement over An Image Encryption Method Based on Total Shuffling, proposed by X Zhang [13]. In [13] a plaintext related image encryption method based on chaos and permutation-diffusion is defined. Author presented another improvement over Eslami's scheme using a lookup table to improve the speed of encryption algorithm without loss of security, which makes it more feasible in practical communication.

G. Coatrieux, et.al. [21] Propose a new reversible watermarking scheme. One first contribution is a histogram shifting modulation which adaptively takes care of the local specificities of the image content. By applying it to the image prediction-errors and by taking everything in mind of their immediate neighborhood, the scheme they propose inserts data in textured areas where other methods fail to do so. Furthermore, their scheme makes use of a classification process for identifying parts of the image that can be watermarked with the most suited reversible modulation. This classification is based on a reference image determined from the image itself, a

prediction of it, which has the property of being invariant to the watermark insertion. In this way, the watermark embedded and extractor remain synchronized for message extraction and image reconstruction.

C. Anuradha and S. Lavanya [22] proposed a secure, protected and authenticated discrete reversible Data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the genuine i.e. original uncompressed image using an encryption key. Then, a data hider may compress the smallest i.e. least significant bits of the encrypted image using a data hiding key to create a sparse space to neighborhood i.e. accomodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, then the receiver can decrypt the received data to obtain an image which is similar to the original one, but cannot extract the additional data. If the receiver has both the data hiding key and the encryption key, can extract the supplementary (additional) data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of supplementary i.e. additional data is not too large. It is also a drawback because if the receiver has only any one key as known, and then he can take any one information from the encrypted data. In order to obtain authentication SHA-1 algorithm is being used.

In Subhanya R.J , Anjani Dayanandh N presented [23] the paper " Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". In this paper, Authors present a new scheme of image watermarking to guard intellectual properties and to secure and protect the content of digital images. It is an effective way to protect the copyright by image watermarking. The work interests with the watermarking algorithm that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortion between the genuine i.e. original and watermarked image and also to increase Peak signal to noise ratio. Here the message bits (image) are (is) hidden into gray/color images. The size of secret data/image is smaller than cover image. To transfer the secret image/text confidentiality, the secret image/text itself is not hidden, keys are generated for each gray/color component and the IWT is used to hide the keys in the corresponding gray/color component of the cover image. The watermarks are invisible and robust against noise and commonly image processing methods.

VI. CONCLUSION

In this paper, we presented the efforts of various researchers in the field of reversible data hiding. RDH is one of the major techniques of data hiding in image processing. Reversible data hiding schemes consists of image encryption, data hiding and data extraction/ image recovery phases.

Since the strength of the RDH technique depends mainly on three factors - robustness, imperceptibility level in the stego image, and embedding capacity. The RDH system leaves unique patterns on the cover images and these patterns feats the steganalyst. When the size of the secret message is small, the transform domain based techniques such as DCT, DWT and adaptive RDH are not less prone to steganalysis. In this technique the distortion will be also less because embedding is performed in transform domain. All the above problems must be addressed while designing a RDH technique which should be robust to attacks. We need to develop RDH techniques where we can embed data equal or more than existing techniques and without any distortion in stego image so that the security of the message can be enhanced.

REFERENCES

[1] Nosrati,Ronak Karimi Mehdi Hariri," Reversible Data Hiding:Principles, Techniques, and Recent Studies". World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222-2510©2011 WAP journal. www.waprogramming.com.

[2] Mr P. S. Nalwade , Ms Pooja Prabhakar Petkar ," A Survey on Reversible Data Hiding Techniques ", IJCTA | May-June 2014.

[3] 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, march 2013.

[4] V. Suresh, C. Saraswathy," Separable Reversible Data Hiding Using Rc4 Algorithm" IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 2013.

[5] San Diego, California, USA "Applications of Digital Image Processing", Part of the SPIE International Symposium on Optical Engineering and Applications, 10-14 August 2008.

[6] Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi," Overview: Main Fundamentals for Steganography ", journal of computing, volume 2, issue 3, March 2010.

[7] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans.Circuits Syst. Video Technol,vol. 16, no. 3, pp. 354–362, Mar.2006.

[8] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," Eur. Assoc. Signal Process. J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 2002.

[9] J. Tian, Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol, vol. 13, no. 8, Aug 2003, pp. 890-896.

[10] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol, vol. 17, no. 6, Jun 2007, pp.774-778.

[11] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang," 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.

[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] Che-Wei Lee and Wen-Hsiang Tsai "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme" c 2010 River Publishers.

[14] Zhenfei Zhao, Ka-Yin Chau and Zhe-Ming Lu," High Capacity Data Hiding In Reversible Secret Sharing", International Journal of Innovative Computing, Information and Control Volume 7, Number 11, November 2011.

[15] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process, vol. 18, no. 4, Apr 2011,pp. 255-778.

[16] X. Zhang, "Separable reversible data hiding in encrypted image,"IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr.2012.

[17] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans.Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012

[18] Xian-ting Zeng , Zhuo Li , Ling-di Ping , Reversible data hiding scheme using reference pixel and multi-layer embedding , International Journal of Electronics and Communications (AEÜ) 66 (2012) 532– 539.

[19] Rintu Jose, Gincy Abraham," Separable Reversible Data Hiding in Encrypted Image with Improved Performance", IEEE International Conference on Microelectronics, Communication and Renewable Energy,2013.

[20] Yong Zhang," Encryption Speed Improvement on "An Improvement over An Image Encryption Method Based on Total Shuffling, IEEE International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013.

[21] Gouenou Coatrieux, Wei Pan, Nora Cuppens-Boulahia," Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting", IEEE Transactions On Information Forensics And Security, Vol. 8, no. 1, January 2013.

[22] C. Anuradha and S. Lavanya "A secure and authenticated reversible Data hiding in encrpted images" © 2013, IJARCSSE

[23] Subhanya R.J , Anjani Dayanandh N (2)" Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014).