Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Reversible Data Hiding Techniques: A Survey

Kritika Jaidka
Department of CSE
PTU, Punjab, India

Neha Mahajan
Department of CSE
PTU, Punjab, India

Sheetal Khokhar
Assistant Professor
PTU, Punjab, India

Abstract— Reversible data hiding is a technique to hide the secret data into the image and secret data is hidden in such a way that after extracting the data at receiver end, image is recovered as same as original one. There are two challenging areas of research for integrity and security of data and this technique is best suitable for military and medical applications. This review paper is exploring various algorithms of reversible data hiding

Keywords— Reversible data Hiding (RDH), Image Encryption, Optimal value transfer, Hough Transfer.

I. INTRODUCTION

Now a days, internet is the fast growing communication way and vital part of infrastructure. Now a day exchange of images between different places has become a popular practice [1]. There are number of reasons for exchanging the information like teleconference, distance learning of personnel interdisciplinary. It is therefore essential to efficiently embed large amount of data in the images while achieving high imperceptibility in order to meet the demand of these application

Data hiding is a term used to embedding secret message in media context. Whenever, we are hiding the information in to the image, it destroys the host image after extracting the secret message. In many application area like military, medical, artwork preservation and law enforcement etc. distortion of an image is unbearable. For example, Medical Application area, small change on an image can cause the risk of physician misinterpreting the image [2]. Thus, RDH Technique is intended to solve the problem of lossless embedding of large message in digital images so that after the embedding message is extracted, the image can be completely restored to its original state.

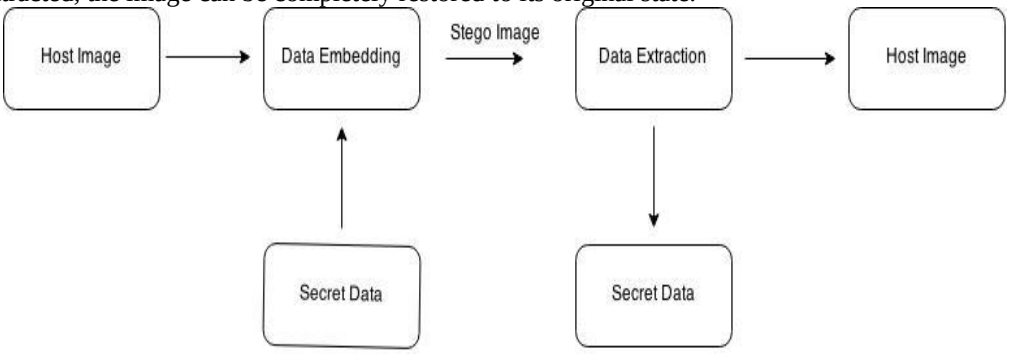

Fig.1: Reversible data hiding

Data hiding can be applied to [3]

- Images
- Audio/video
- Text
- Software

Reversible data hiding in Encrypted images- In this, sender encrypts the original image using an encryption key. Then data hider create a sparse space with the help of data hiding key for accommodating the secret data with the compression of LSB of encrypted image. If recipient has the data hiding key, he can extract the secret data but he does not extract the original image. If recipient has encryption key, then recipient recover the image similar to original one but cannot take out the secret data. If recipient has both keys (data hiding and encryption) he can take out the secret data and also recover the original image.

Hough transform**: -** It is a feature extraction technique used in digital image processing and computer network. Basic Hough transform technique used for line identification in image, But Modified Hough transform concerned with identification of arbitrary shapes (Circle, Ellipse, Curves) to hide data in these positions.

Spatial and Frequency Domain:- Embedding data in time domain can be studious by using difference expansion, histogram etc. Embedded data in frequency domain can studious by Discrete cosine Transform (DCT) or Discrete wavelet transform (DWT) in which message bits are embedded into corresponding coefficients.

Optimal value transform:-In RDH with optimal value rule, value of original data are altered by using iterative procedure. For content recovery, the secret data as well as auxiliary information are used. The original image and secret data are divided into number of subsets and the auxiliary information is always embedded into estimation error.

II. RELATED WORK

A. Classification of Reversible Data Hiding

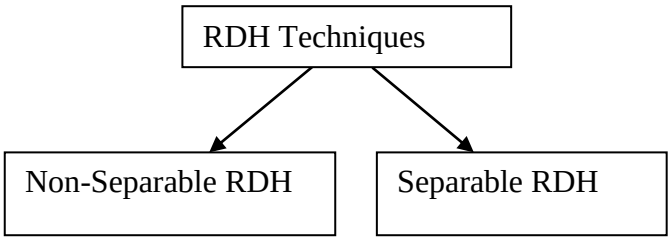

Fig.1: Classification of RDH Techniques

1) Non-Separable Reversible Data Hiding

The way of non- separable method is consists of image encryption, data embedding and data extraction/ image recovery. At sender side, a sender encrypts the uncompressed image with the help of encryption key to produce a encrypted image and then a data hider embed secret data into a encrypted image with the help of data hiding key, as he does not know the original content. At receiver side, a receiver may decrypt the encrypted image containing secret data with the help of encryption key and decrypted image is similar to original image. With the help of data hiding key, he can extract the embedded data and recover image from the decrypted image [4].

2) Separable Reversible Data Hiding

At sender side, Original content is encrypted with the help of encryption key and secret data are embedded into the encrypted image with the help of data hiding key.

At receiver side, there are three cases :

Case 1: If receiver has only data hiding key, then he can extract the secret data but he does not know the image content.

Case 2: If receiver has only data hiding key, then he can decrypt the image similar to original image.

Case 3: If receiver has both keys (data hiding key and decryption key) receiver can extract the secret data and recover the original image [4].

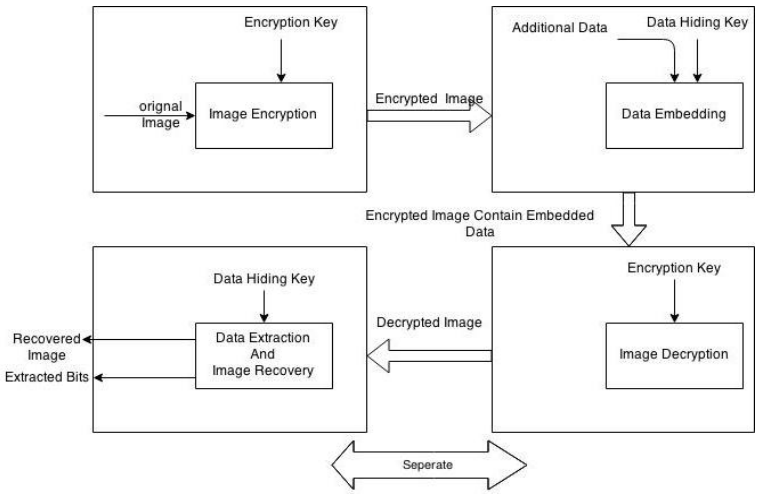

Fig .2: Separable reversible data hiding

B. RDH Technique

1) Separable Reversible Data Hiding in Encrypted Image

In [5] D. U. K. Singh, el. al. proposed Separable Reversible Data technique in which sender encrypt the data with the help of AES algorithm and embed encrypted data into a cover image by using LSB technique. Both keys (hide and decryption) automatically generated by a system and these keys are mailed to the receiver. For authentication purpose receiver is logging into system using his id and password. If he is authorized then receiver gets both keys and by using these keys he can get the image as well as original data. Otherwise receiver will get fake data. This method provides data integrity, authentication, security, and confidentiality. In [6] lalit dhande el.al proposed a novel approach for reversible data hiding in which firstly reserve ideal memory space and then encrypt the image after that embed secret data in reserved memory space by using LSB modification technique. In [7] C. Anuradha and S. Lavanaya present a paper "Secure and Authenticated Reversible data hiding in Encrypted Image". In the first Phase sender encrypts the uncompressed image using encryption key then data hider select a pseudo random location of encrypted image and compressed the LSB of the encrypted image to add the secret data. At receiver side, if receiver has encrypted key, he can

decrypt the image but cannot extract the secret data. If receiver has data hiding key, he can extract the additional data. If receiver has both keys, then extract data as well as recover the original image. In this paper SHA-1 algorithm is used for authentication.

2) Reversible Data Hiding using Hough Transfer

In [8] Sukhpreet Kaur presents a reversible data hiding in the images using circular Hough transfer. The main purpose of reversible data hiding is designed for embedded message into the digital image after extracting the data we can also restore the host image. In this paper, circular Hough transfer is used for extract the circular object from a image .With the help of circular Hough transfer, find the energy density of pixels and also apply a nearest neighbour search to find the value of pixels and embedded a data on the pixel which is near about the value of data so that distortion in a image is less. The circular Hough transfer is practice to reduce the error rate.

3) Spatial and Frequency based Reversible Data Hiding

In[9] Sowmyashre et. al. present a modified pixel frequency based reversible data hiding for secure data communication in which image is divided into 4×4 size block to form prediction difference image. Count the number of frequency of each block. The pixel which have maximum frequency consider as a mode value. In this method if two or more pixel has same frequency then calculate the average of pixel of same frequency and consider as a mode value. Mode value is used to built up the prediction difference and then generate a histogram of prediction difference. In the prediction difference image peak point and zero point used for hiding the secret data. In this method 1000 bytes of text data embedded in to 512×512 gray scale images. In [10] Zhicheng Ni et.al proposed "Reversible Data hiding" this algorithm use the zero point and peak point of histogram of an image which is used to embed the secret data by modify grey scale pixel of image. This algorithm applies to various images like medical, aerial, textual image and also 1096 images of CorelDraw database. To embedding and extracting data following algorithm are used:

- Pseudo-code Embedding algorithm
- Pseudo-code Extraction algorithm

This algorithm successfully embed data up to 5-80 kb into image (512×512×8) whose PSNR is more than 48db. In [11] Ching–Yu Yang proposed a "Reversible Data Hiding by a coefficient bias algorithm" In this, Primary and secondary message are embedded into spatial and frequency domain with the help of coefficient bias algorithm. To hide primary message in spatial domain in mean removed block with the help of coefficient bias algorithm and produce a stego image as an output and stego image is convert into a frequency domain with IWT to increase robustness and security. By this algorithm secondary message is embedded into sub-band (low-high and high-low) of IWT domain. This algorithm unbiased the attack likes JPEG 2000, JPEG, brightness and inverting.

4) Optimal value Transfer based Reversible Data Hiding

Xinpeng Zhang [12] proposed a " Reversible data hiding with optimal value transfer rule" In this paper, by using some specific rules, the value of original data are altered and at receiver side, after extraction of hidden data original content can be perfectly restored. By using iterative procedure, the optimal value rule of value modification under payload-distortion criteria is found. For content recovery, the hidden data as well as auxiliary information are used. Auxiliary information, which is carried by difference between original pixel values and corresponding values calculated from neighbours with the help of optimal value transfer rule estimated error are altered. Moreover, the original image and secret data are divided into number of pixel subsets and in the next subset, auxiliary information is always embedded into estimation error. At receiver side, both secret data and original content are extracted and recovered respectively in inverse order. In this way, performance of reversible data hiding is improved

Table 1-Comparative Study of Reversible Data Hiding

Paper	Author, Year	Technique Used	Advantage	Disadvantage
1.	D. U. K. Singh et. al., 2014	AES Algorithm	1.If user is not authenticated in Login process, then system generates fake data 2.Plain text size and cipher text are same	1. This algorithm does not work on multimedia files transmission.
2.	C. Anuradha, et. al., 2013	SHA-1 algorithm used for authentication	1.Low computation complexity 2.Simple algorithm 3.Better Performance	1.Amount of additional data is not too large
3.	S. Kaur et. al.,2014	Circular Hough Transform	1.Better Performance 2. Error rate is low.	1. It requires larger computation time. 2.larger memory storage 3. Increasing complexity of extracted information.

4.	Xinpeng Zhang, 2013	Optimal Value Transfer	1.Achieve good payload distortion	1. Compute complexity is low
5.	Soumyashree et. al.,2014	Frequency based RDH	1.Better quality of image 2.High Security	1. Capacity of hidden data is limited (1000 bytes).
6.	Z. Ni. et. al.,	Histogram Modification	1. Computation Complexity is low. 2.Execution time is short	1. It embedded data up to 5-80kb.
7.	C.-Y. Yang, et. al.,2010	Co-efficient Bias algorithm	High security and robustness	1. Need to improve payload size reduction of overhead bits.

III. PARAMETER EVALUATION

Reversible data embedding algorithm performance can be determine by following methods [13]

- Payload capacity limit**:** - It means how much information can be embedded.
- Visual quality**:** - It means what is the visual quality of embedded image.
- Complexity**:** - It is used to measure the complexity of algorithm.

These above terms can be measured by number of parameters i.e. PSNR, quality factor, Watson metric etc. PSNR (peak signal to noise ratio) simply defined as the energy of distortion effected by data hiding. PSNR is defined by the mean squared error (*MSE*).Given a noise free image I and its noisy approximation *K*, *MSE* is defined as [14]:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10}\left({MAX_1}^2/_{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(MAX_1/_{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_1) - 10 \cdot \log_{10}(MSE)$$

Watson Metric is used to measure total perceptual error and quality factor is also known as Q-factor. Image quality can be measure by Quality Ratio. To define better quality of images PSNR and Quality Factor should be high and Watson metric should be low in reversible data hiding [7].

IV. CONCLUSIONS

Reversible data hiding is a new technique which is getting noticeable because of security, integrity and authenticated in images. In this review paper, different type of reversible data hiding algorithms in images are studied and analysed i.e. reversible data hiding in encrypted images, spatial and frequency domain, optimal value transfer and Hough transform. These different algorithms provide different results when tested on images. For reversibility, these above methods provide better result in reversible data hiding..

REFERENCES

[1] S. –S. Wang, Sz-J. Fan, C.-S. Li, "A New Reversible Data Hiding Based on Fuzzy Predictor," International Conference on Fuzzy Theory and its application, pp. 258-261, Nov. 2012.

[2] H. M. Kelash,A. F. Alenezi,O. S. Faragallah, "Improved histogram-based reversible data hiding for Digital images," IEEE(NRSC), pp. 237-244, Feb. 2013.

[3] C. Bansal, P. Gupta, "A Survey on Histogram Shifting Techniques in Reversible Data Hiding," IEEE(IACC), pp. 1008-1012, Feb. 2014.

[4] V. Agham, T. Pattewar, "A Survey on Reversible data hiding Technique,"IMACST, vol 4, no. 1, pp. 9-13, May. 2013.

[5] D. U. K. Singh, K. M. Padwal and M. P. Jadhav, "Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation," IJCSIT, vol. 5, no. 3, pp. 3469-3473, 2014.

[6] L. Dhande, P. Khune, V. Deore, D. Gawade, "Hide Inside-Separable Reversible Data Hiding in Encrypted Image," IJITEE ISSN: 2278-3075, Volume-3, Issue-9, vol. 3, pp. 88-91, February 2014.

[7] C. Anuradha, S. Lavanaya, " Secure and Authenticated Reversible data hiding in Encrypted Image" IJARCSSE, vol. 3, Issue 4, pp. 1010-1014, April 2013.

[8] S. Kaur, M. Shukla," Reversible Data Hiding in Images using Circular Hough Transform," IJCSIT, vol. 5, no. 5, pp. 6659-6663, 2014.

[9] Sowmyashree, R. R. Sedamkar, S. Sharma, "A Modified Pixel Frequency Based Reversible Data Hiding for Secure Data Communication" IJCSIT, vol. 5, no. 6, pp. 7035-7040, 2014.

[10] Z Ni, Y. -Q Shi, N. Ansari and W. Su "Reversible data hiding ," IEEE Trans. Circits Syst. Video Technol, vol. 13, no. 3, pp. 354-362, Mar. 2006.

[11] C.-Yu Yang, Wu-Chih Hu, Chih-Hung Lin," Reversible Data Hiding by a coefficient bias algorithm," JIH-MSP., vol. , no. 2, pp. 91-100, April 2010.

[12] X. zhang, "Reversible data hiding With Optimal Value Transfer," IEEE Trans. On Multimedia, vol. 15, no. 2, pp. 316-325, Feb. 2013.

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

[14] Online Available: http://en.wikipedia.org wiki/ Peak signal-to-noise ratio.

