Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Reversible Data Hiding

Yojna Chandel
M.Tech. Student, C-DAC
Mohali, Punjab, India

Sunil Chhillar
Senior Engineer, STD, C-DAC,
Mohali, Punjab, India

Abstract: ***Reversible data hiding (RDH) is mainly concern with in encrypted images, as it maintains the brilliant property that the losslessly recovery of original image cover after data embedded is mined while shielding the image content's as confidential. In this survey paper different reversible data hiding methods are studied. The method by reserving room before encryption with a old-fashioned RDH algorithm, it is easy for the data hider to reversibly embed data in the encrypted image. This paper also concerns with a method that embeds image/ text data invisibly into a video based on IWT and to minimize the mean square distortion between the original and watermarked image and also to increase Peak signal to noise ratio. The broadcast and exchange of image also desires a high security. Cryptography is used to maintain security.***

Keywords: IWT, DE, HM

I. OVERVIEW

Encryption is an effective and popular means of secrecy protection. In order to securely share a secret image with others, a content owner may encrypt the image before transmission. In some situations, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content.

II. REVERSIBLE DATA HIDING TECHNIQUE

The term "reversible data hiding" means getting the exact retrieval of the data after performing the process like encryption-decryption and data hiding. A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. The detailed procedure of reversible data hiding techniques is as follows
It mainly consists of three basic steps

a) Image Encryption

Encryption is a process which changes image into a stream of coded data which makes it difficult to understand by unauthorized user. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

b) Data Embedding

After Image encryption data embedding step will be executed. In this step, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data

c) Data extraction & image recovery

At receiver site when encrypted image with embded data is received, we have to decrypt original data and image. With calculation of encrypted key and data hiding key, a user can extract an image and then added data from that image.
A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types:

a) lossless compression based methods,
b) difference expansion (DE) methods,
c) Histogram modification (HM) methods.

In reversible data hiding scheme, the data extraction is not separable from the content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any information from the encrypted image containing additional data.

2.1 Separable Reversible Data hiding Technique

The concept of separable reversible data hiding technique is based on steganography and related with internet security. The owner of the image first encrypts the image using the encryption key. Then, the data hider, without any knowledge about the original image content, hides data using the data hiding key. At the receiver side the receiver extracts the data and decrypts the image in a separable manner, making use of data hiding and encryption keys.

At receiver side it occurs three cases.

1. if a receiver has the data-hiding key only, he can take out the secure data even he does not know the cover media i.e. cover image content.
2. if the receiver has the encryption key only, he can decrypt the received data to obtain an image similar to the original one, but he cannot extract the additional data.
3. If the receiver has both the keys i.e. data-hiding key and the encryption key he can extract the additional data and recover the original image.

2.1.1 Advantages

1) User can extract the additional data with the help of data-hiding key only.
2) With encryption key, he can decrypt the received data to obtain an image similar to the original one.

III. LITERATURE REVIEW

A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. In practical aspect, many RDH techniques have emerged in recent years. Fridrich et al [1] created a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for inserting auxiliary data. One reversible marking technique is watermarking. The watermarking is a form of digital rights management that uses data embedded into a recording to secure the music(image) by identifying the computer or device attempting to play it and determining whether a license to play the music(image) exists on that device. These watermark programs can also spread info about the consumer- for example, credit card numbers-back to the content owner, such as a record company or website. Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video or image signals and documents. Such hidden message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place etc) Another method is histogram. In an image processing context, the histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph display the number of pixels in an image at each different intensity value found in that image.

The image is scanned in a single pass and a running count of the number of pixels found at each intensity value is kept. Then it is used to construct a proper histogram.

Weiming Zhang, Biao Chen, and Nenghai Yu proposed a decompression algorithm [2] as the coding scheme for embedding data. Three RDH schemes that use binary feature arrangement as covers, i.e., one scheme for spatial images, one scheme for JPEG images, and pattern exchange scheme for binary images.

Nosrati and some other people [3] present the paper Reversible Data Hiding: Principles, Techniques, and Recent Studies. In this main technique as the principles of RHD are talked. Pairwise logical computation data hiding technique (PWLC) and Data hiding by template ranking with symmetrical Central pixels(DHTC) technique.

Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong suggested a method, [4] which can embed a large amount of covert data into images. It utilize the interpolation-error, the difference between interpolation value and matching pixel value, to embed bit "1" or "0" by expanding it additively or leaving it unchanged.

Vasiliy Sachnev, Hyoung Joong Kim, Jeho Nam Sundaram Suresh, and Yun Qing Shi introduced a [5] Reversible Watermarking Algorithm Using Sorting and Prediction. Here sorted prediction errors and, a reduced size location map allow embedding more data into the image with less distortion. Also sorting technique is used to record the prediction errors based on magnitude of its local variance.

K.Shankar, Dr.C.Yaashuwanth develop the system [6] that routines the method RRBE (Reserving Room Before encryption). This survey paper helps us to explain the technique.

In [7] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti , Mr. T. Sri Harish Reddy , Dr. S. Kiran suggested an Actual Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding .

Xinpeng Zhang did the [8] Reversible data hiding with optimal value transfer. In this the secret data, as well as the secondary information used for content recovery, are accepted by the differences between the original pixel-values and the corresponding values estimated from the neighbors. Here, the estimation errors are modified according to the optimal value transfer rule.

Another method [9] embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortion between the original and watermarked image and also to increase Peak signal to noise ratio. In Separable Reversible Data Hiding in Encrypted Image [10], a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.

In [7] Bhaskara Reddy et.al suggested an Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding .In this paper, they implemented security for image. They

considered an image, read its pixels and convert it into pixels matrix of order as height and width of the image. Replace that pixels into some fixed numbers, generate the key using random generation technique .Encrypting the image using this key ,performing random transposition on encrypted image, converting it into one dimensional encrypted array and finally applied Huffman coding on that array , due this size of the encrypted image is reduced and image is encrypted again. The decryption is reverse process of encryption. Hence the proposed method provides a high security for an image with minimum memory usage. The main steps in the encryption algorithm is

Step 1. Replace each pixel by fixed number values.

Step 2 .Generate the secrete key by using random generation technique

Step 3. Huffman Coding.

The steps in image decryption is reverse of encryption algorithm

In [9] Subhanya R.J , Anjani Dayanandh N presented the paper " Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". In this project, they present a new scheme of image watermarking to guard intellectual properties and to secure the content of digital images. It is an effective way to protect the copyright by image watermarking. The work concerns 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 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.

Zhang [10] suggests a completely unique methodology for divisible reversible knowledge activity .Here content owner initial encrypts the initial uncompressed image mistreatment associate secret writing key to provide associate encrypted image. Then, the knowledge-hider compresses the smallest amount important bits (LSB) of the encrypted image employing a data-hiding key to form a thin house to accommodate the extra data. At the receiver facet, {the knowledge|the info|the information} embedded within the created house will be simply retrieved from the encrypted image containing extra data in line with the data-hiding key. Since the info embedding solely affects the LSB,a decipherment with the secret writing key may result in a picture similar tothe original version. once mistreatment each of the secret writing and data-hiding keys, the embedded extra knowledge will be with success extracted and also the original image will be dead recovered by exploiting the abstraction correlation in natural image

In [11] C. Anuradha and S. Lavanya proposed a secure and authenticated discrete reversible Data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate 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, can decrypt the received data to obtain an image 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 additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. It is also a drawback because if the receiver has any one key as known, and then he can take any one information from the encrypted data. In order to achieve authentication SHA-1 algorithm is being used.

Che-Wei Lee and Wen-Hsiang Tsai1[12] 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 method 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 the one which provides the largest data hiding capacity is selected adaptively.

In [13] a novel reversible data hiding scheme for encrypted image was proposed. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

[14] proposes 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, making 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. Peak Signal to Noise Ratio (PSNR) of this decrypted image is much higher than the existing methods. 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. The method also has a higher data hiding capacity than the existing reversible data hiding techniques in encrypted image.

Table 3.1gives a summary of Literature Review.

Table 3.1: Summary of Literature Review

Paper	Authors, Year	Technique used	Advantages	Drawback
Improving various reversible data hiding schemes via optimal codes for binary covers	W. Zhang, B. Chen, and N. Yu2012	Decompression algorithm as the coding scheme for embedding the data is used	When the compression algorithm reaches entropy, the proposed code is found optimal.	It only uses two simple methods to modify HS, so the problem is whether there exists other more effective modifying methods or not. Other problem is how the recursive codes can be designed for gray scale covers.
Reversible Data Hiding:Principles, Techniques, and Recent Studies".	Nosrati , Ronak Karimi Mehdi Hariri 2011	primary techniques as the principles of RHD are talked. Pairwise logical computation data hiding technique (PWLC) and Data hiding by template ranking with symmetrical Central pixels (DHTC) technique.	Some RDH techniques were discussed with their advantages and disadvantages	The idea about suitable domain was not in the paper.
Reversible image watermarking using interpolation technique	Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong .2010	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	a large amount of covert data into images can be embedded, and achieves better image quality The computational cost of the scheme is small.	Any mistake in the calculation of interpolation will affect the secret information
"Reversible watermarking algorithm using sorting and prediction,"	V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi,2009	Sorting technique is used to record the prediction errors based on magnitude of its local variance.	The proposed scheme can embed more data with less distortion**.**	More calculations are needed Size of location map affects the efficiency of the system
An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding"	. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti , Mr.T. Sri Harish Reddy, S. Kiran 2013	This algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding.	provides high security to an image and occupies minimum memory space.	Some problems in the decoding section such that , here Huffman coding is used
Reversible Data Hiding With Optimal Value Transfer	Xinpeng Zhang, 2013	the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed	the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values	computation complexity due to the prediction will be higher
Difference Expansion Reversible Image Watermarking Schemes	Subhanya R.J (1), Anjani Dayanandh N (2)" 2014	uses the watermarking algorithm that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square	can improve the quality of the watermarked image and give more robustness of the watermark and also increasing PSNR	Low hiding capacity and complex computations

Using Integer Wavelet Transform Based Approach		distortion between the original and watermarked image and also to increase Peak signal to noise ratio.		
"Separable reversible data hiding in encrypted image,"	X. Zhang, 2012	a novel scheme for separable reversible data hiding, which consists of image encryption, data embedding and data-extraction/image-recovery phases.	Simple Less computation	Data compression is not efficient
Reversible Data Hiding in Encrypted Image"	Xinpeng Zhang, 2011	With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version.	he does not know the data-hiding key, it is still impossible to extract the additional data and recover the original image.	Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB-steganalytic methods
A Separable Reversible Data Hiding in Encrypted Image with Improved Performance	Rintu Jose, Gincy Abraham, 2013	The method consists of image encryption, data hiding, and data extraction and image recovery phases.	Data hiding capacity of this method is much higher than that of the data hiding methods used in existing reversible data hiding in encrypted image techniques.	

IV. CONCLUSION

A survey on various reversible data hiding techniques is executed. Reversible data hiding systems for encrypted image with a low computation complexity is analysed, which consists of image encryption, data hiding and data extraction. The original images are encrypted by an encryption strategy. So a revision about an encryption strategy is done. Although a data hider does not know the novel content, he can embed the top-secret data into the encrypted image by altering a part of encrypted data. So methods for data embedding are also noticed.

REFERENCES

[1] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA, USA,Jan. 2002, vol. 4675, pp. 572–583

[2] 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.

[3] 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

[4] L. Luo et al., "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[5] [5]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans.Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989– 999, Jul. 2009.

[6] K.Shankar, 2Dr.C.Yaashuwanth" Data Hiding and Retrieval in Encrypted Images". © 2014 IJEDR | Volume 2, Issue 1 | ISSN: 2321-9939

[7] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti , Mr.T. Sri Harish Reddy, Dr. S. Kiran " An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" Hema Suresh Yaragunti et al, Int.J.Computer Technology & Applications,Vol 4 (6),883-891

[8] Xinpeng Zhang, Member, IEEE "Reversible Data Hiding With Optimal Value Transfer" IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 2, FEBRUARY 2013.

[9] Subhanya R.J (1), 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).

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

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

[12] Che-Wei Lee1 and Wen-Hsiang Tsai1 "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme" c 2010 River Publishers.

[13] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image", in IEEE signal processing letters, VOL. 18, NO. 4, pp 255-258, april 2011

[14] Rintu Jose, Gincy Abraham, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance", in International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

