RESEARCH ARTICLE OPEN ACCESS

A Survey on Reversible Image Data Hiding

Asha S Raj [1], Mrs.Gayathri Nair P [2]
M.Tech student [1], Department of Computer Science and Engineering
Asst.Professor [2], Department of Information Technology
Mohandas College of Engineering, Anad, Trivandrum
Kerala - India

ABSTRACT
Reversible data hiding is a widely used technique on the basis of watermarking. The host image can be recovered exactly. Reversible Data Hiding technique is applied at medical and military applications. The data embedding process will usually introduce permanent loss to the cover medium. In several fields such as medical, military, and law forensics degradation of cover is not allowed. Reversible data hiding is used in medical and military applications, digital images that embeds data in it and alters the pixel values for secret communication thus the cover image can be recovered to its original state after the extraction. Reversible Data Hiding which enables images to data in hidden form and restored to their origin by removing digital hidden data.
Keywords:- Reversible Data Hiding, PSNR, RDH

I. INTRODUCTION

A reversible data hiding can recover the original image without any distortion from the marked image after the hidden data have been extracted. The techniques utilizes the zero or the minimum points of the histogram of an image. It modifies the pixel values to embed data into the image. It can embed more data than many of the existing reversible data hiding techniques. It is proved that the peak signal-to-noise ratio (PSNR) of the marked image generated by the method. The PSNR is higher for all reversible data hiding techniques.

Reversible Data Hiding is used to embed a piece of information into the host images to generate the marked one. Original image can be exactly recovered after extracting the embedded data. The original cover can be reversibly restored after the embedded information is extracted. The Reversible Data Hiding process eliminates the disadvantages of reversible watermarking. The process to reverse the marked images back to the original cover images after the hidden data are extracted. The process which can be used the Peak Signal Noise Ratio (PSNR) to check the quality of reversed image.

The PSNR value is the maximum possible power of a signal and the power of corrupting noise. It is the most commonly used measure of quality of reconstruction. PSNR represent the distortion level between marked image and cover image. Reversible Data Hiding mostly used Difference expansion (DE).It is one of the most important techniques which are used for reversible data hiding. With the help of PSNR value the recovered images can be checked.

Reversible data hiding is used for embedding information into covers such as image, audio, and video files. It can be used for media notation, copyright protection etc. Most data hiding methods embed messages into the cover media to generate the marked media. The only modifying the least significant part of the cover image. The embedding process will usually introduce permanent distortion in original image. That is, the original cover can never be reconstructed image from the marked cover. In the medical imagery, military imagery, and law forensics, no degradation of the original cover is allowed. It need a special kind of data hiding method, which is reversible data hiding (RDH) or lossless data hiding. The original cover can be reversibly restored after the embedded message is extracted.

Reversible data hiding that embeds essential data into images, audio, video, and so on. Sender side, the data is embedded by the reversible transform .The receiver side, the data is extracted by the converse transform. Once the secret data are embedded in the compression domain. The receiver store the cover image in a compression mode to save storage space. The output must extract the secret data to reconstruct the cover image. Then press the cover image again to generate compression codes.

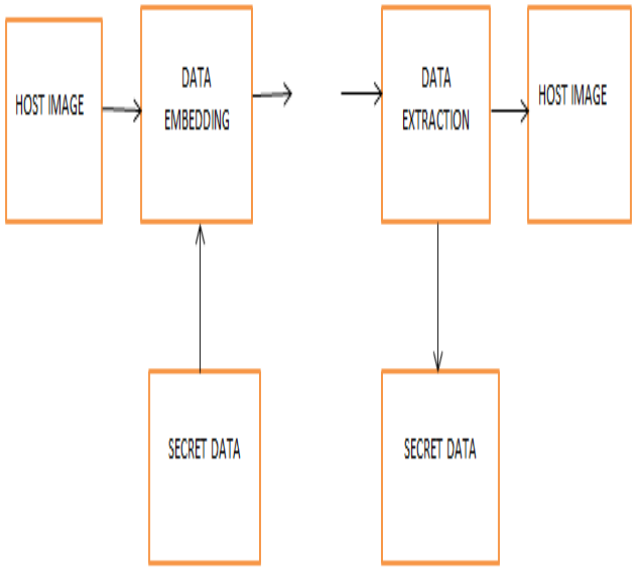

Fig I.1 Reversible data hiding

II. LITERATURE SURVEY

In [2] Subhanya R.J , Anjani Dayanandh N presented the paper " Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". It present a new scheme of image watermarking.The properties and to secure the content of digital images.The wavelet function are easy to calculate. It is an effective method to protect the copyright by image watermarking. It included with the watermarking algorithm that embeds image or text data. Invisible data into a video based on Integer Wavelet Transform. To minimize the mean square distortion between the original and watermarked image. Also to increase Peak signal to noise ratio.The message bits or image are hidden into gray and color images. The size of secret data and image is smaller than cover image. To transfer the secret image or text confidentiality. The secret image or text itself is not hidden. Keys are generated for each gray or color component. The IWT is used to hide the keys in the corresponding gray or color component of the cover image. The watermarks are invisible and robust against noise. The commonly image processing methods used in the wavelet transform.

Zhang [3] used a novel method for separable reversible data hiding .The content owner first encrypts the original uncompressed image using an encryption key. Then produce an encrypted image. The data hider compresses the LSB bits of the image using a data hiding key. To create a sparse space to accommodate the additional data. At the receiver side the data embedded in the created space. It can be easily retrieved from the encrypted image. The data according to the data hiding key for encryption. The data embedding only affects the LSB. A decryption with the encryption key can result in an image. To the original version. Using both of the encryption and data hiding keys. The embedded additional data can be successfully extracted. The original image can be perfectly recovered by exploiting the spatial correlation in natural image. The data and the image that can be recovered easily. The calculations are very easy.

Xinpeng Zhang used the [4] Reversible data hiding with optimal value transfer. In the secret data as well as the valuable information used for content recovery. It carried by the differences between the original pixel values. The nearest pixel values estimated from the neighbors. The estimation errors are modified according to the optimal value transfer rule. Another method embeds image or text data invisibly into a video based on Integer Wavelet Transform. The mean square value difference between the original and watermarked image. It is also to increase Peak signal to noise ratio. Separable Reversible Data Hiding in Encrypted Image can be used. A content owner encrypts the original uncompressed image using an encryption key. A data hider may compress the least significant bits of the encrypted image. It using a data hiding key to create a pixel difference to accommodate some additional data.

Che-Wei Lee and Wen-Hsiang Tsai1[5] proposed a lossless data hiding method based on histogram shifting. It employs a method of adaptive division of cover images into blocks. To use large data hiding capacities as well as high stego image qualities. The method is to break a bottleneck of data hiding rate increasing at the image block size of 8×8. It is found in existing histogram shifting methods. Four ways of block divisions are designed. The method provides the largest data hiding capacity is selected area. To use the histogram shifting method. Histogram shifting used in a easy way to find out the encrypted images.

In [6] C. Anuradha and S. Lavanya proposed a secure and authenticated descrete reversible Data hiding in cipher images. It deals with security and authentication. In the first phase a content owner encrypts the original uncompressed image. It using an encryption key. Then a data hider may compress the least significant bits of the encrypted image. It used a data

hiding key to create a sparse space. It can be used some exceptional data. It can encrypted image containing extra data. If a receiver has the data hiding key receiver can extract the exceptional data. The receiver used the image content for encryption and decryption. If the receiver has the encryption key. It can decrypt the received data to obtain an image similar to the original one. It cannot extract the additional data. If the receiver has both the data hiding key and the encryption key. Then it can extract the additional data. It recover the original content without any error. It exploiting the exceptional data in natural image. when the amount of additional data is not too large.

Che-Wei Lee and Wen-Hsiang Tsai1[7] proposed a lossless data hiding method based on histogram shifting. It employs a scheme of adaptive division of cover images. The cover images into blocks. To yield large data hiding capacities. High stego image qualities improved a lot. The method is to break a bottleneck of data hiding rate increasing at the image. The image block size of 8 × 8 size. It is found in existing histogram shifting methods. Four ways of block divisions are designed. The one which provides the largest data hiding capacity is selected adaptively.

In [8] Bhaskara Reddy,et.al suggested an Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding .The implemented security for image used the random number generator. It uses an image read its pixels and convert it into pixels matrix. The matrix of order as height and width of the image. It change that pixels into some fixed numbers. It generate the key using random generation technique. Encrypting the image using this key. It performing random transposition on encrypted image. Converting it into one dimensional encrypted array. Finally applied Huffman coding on that array. Due to this size of the encrypted image is reduced. The image is encrypted with the data used.The decryption is reverse process of encryption. Hence the proposed method provides a high security for an image with minimum memory usage.

Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong suggested a method , [9] which can embed a value and corresponding pixel value. To embed bit “1” or “0” by expanding it additively or leaving it unchanged. Vasiliy

Table.1.Comparison of different Reversible Data Hiding Techniques

Title	Method	Advantages	Disadvantages
Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach [2]	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	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
"Separable reversible data hiding in encrypted image"[3]	a novel scheme for separable reversible data hiding, which consists of image encryption data	Simple Less Computation	Data compression is not efficient
"Reversible Data Hiding With Optimal Value Transfer"[4]	the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a scheme is proposed uses the watermarking algorithm that embeds image/ text data	the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values	computation complexity be higher
"lossless data hiding method based on histogram shifting"[5]	Histogram used for data embedding process	Simple to calculate and easy to implement	Time complexity higher
"A secure and authenticated reversible Data hiding in encrypted images"	The encryption and decryption techniques used	More data encryption using less distortion	There will be no idea for suitable domain
"A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme"	Histogram shifting based on adaptive block	Can improve the quality of the image	Low hiding capacity
" An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding"	Algorithm based on Ceaser cypher techniques	Provide high security to an image	Some problem in the decoding section
"Reversible image watermarking using interpolation technique,"	It utilizes interpolation difference between interpolation value and curresponding pixel value	Which can embed into large amound of cover media	Any mistake in the calculation made the interpolation error
"Reversible watermarking algorithm using sorting and prediction"	Sorting and prediction of pixel value can be used	Calculations are very simple	Clarity of the image will be poor
"Reversible Image Data Hiding with contrast Enhancement"[11]	An algorithm is provided to compressed and decompressed the data into images	Histogram and Location map gives the easy calculations	Algorithm Robustness

Sachnev, Hyoung Joong Kim, Jeho Nam Sundaram Suresh, and Yun Qing Shi introduced a [10] Reversible Watermarking Algorithm Using Sorting and Prediction. The sorted prediction errors and, a reduced size location map allows to embed more data. The data into the image with less distortion. Also sorting technique is used to record the prediction errors based on magnitude of its local variance.

Hao-Tian Wu, Jean-Luc Dugelay, and Yun-Qing Shi[11] proposed Reversible Image data Hiding with Contrast Enhancement. A novel reversible data hiding (RDH) algorithm is proposed for digital images. Instead of trying to keep the PSNR value high, the proposed algorithm enhances the con-trast of a host image to improve its visual quality. The highest two bins in the histogram are selected for data embedding so that histogram equalization can be performed by repeating the process. The side information is embedded along with the message bits into the host image so that the original image is completely recoverable. The proposed algorithm was implemented on two sets of images to demonstrate its efficiency. To the best knowledge, it is the first algorithm that achieves image contrast enhancement by RDH. Further-more, the evaluation results show that the visual quality can be pre-served after a considerable amount of message bits have been embedded into the contrast-enhanced images.

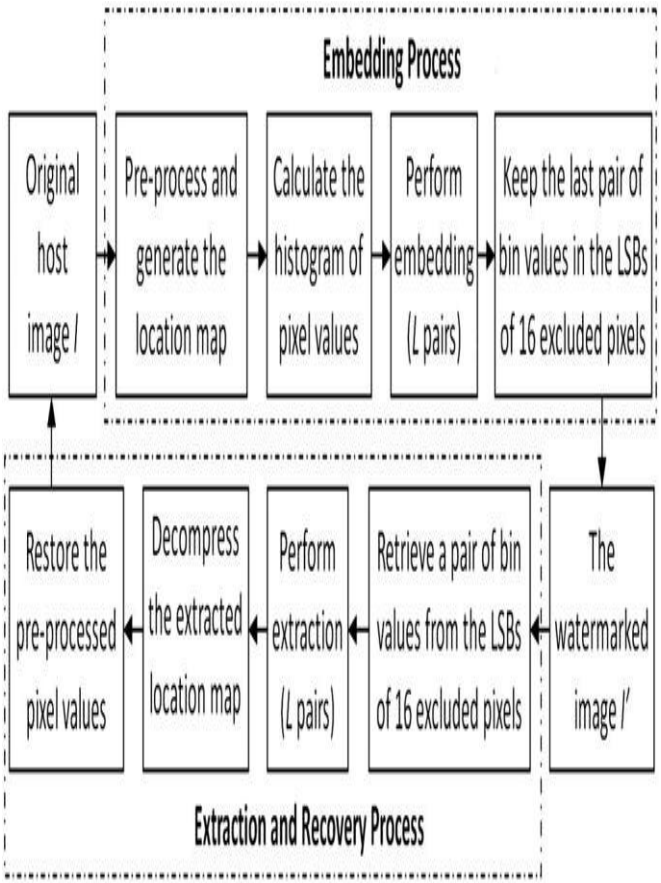

Fig II.1 The proposed RDH algorithm

The PSNR of a marked image generated with a pre-diction error based algorithm is kept high, the visual quality can hardly be improved because more or less distortion has been introduced by the embedding operations. For the images acquired with poor illumination, improving the visual quality is more important than keeping the PSNR value high. Moreover, contrast enhancement of medical or satellite images is desired to show the details for visual inspection. Although the PSNR value of the enhanced image is often low, the visibility of image details has been improved. To the best knowledge, there is no existing RDH algorithm that performs the task of contrast enhancement.

To create a sparse space to accommodate the additional data. At the receiver side the data embedded in the created space. It can be easily retrieved from the encrypted image. The data according to the data hiding key for encryption. The data embedding only affects the LSB. A decryption with the encryption key can result in an image. The secret image or text itself is not hidden. Keys are generated for each gray or color component. The IWT is used to hide the keys in the corresponding gray or color component of the cover image. The watermarks are invisible and robust against noise. The commonly image processing methods used in the wavelet transform.

To the original version. Using both of the encryption and data hiding keys. The embedded additional data can be successfully extracted. The original image can be perfectly recovered by exploiting the spatial correlation in natural image. To the best knowledge, there is no existing RDH algorithm that performs the task of contrast enhancement. The method is to break a bottleneck of data hiding rate increasing at the image block size of 8 × 8. It is found in existing histogram shifting methods. Four ways of block divisions are designed.

The method provides the largest data hiding capacity is selected area. To use the histogram shifting method. Histogram shifting used in a easy way to find out the encrypted images. To the original version. Using both of the encryption and data hiding keys. The embedded additional data can be successfully extracted. A decryption with the encryption key can result in an image. The secret image or text itself is not hidden.

The PSNR of a marked image generated with a pre-diction error based algorithm is kept high, the visual quality can hardly be improved because more or less distortion has been introduced by the embedding operations. For the images acquired with poor illumination, improving the visual quality is more important than keeping the PSNR value high. Moreover, contrast enhancement of medical or satellite images is desired to show the details for visual inspection. Although the PSNR value of the enhanced image is often low, the visibility of image details has been improved. To the best knowledge, there is no existing RDH algorithm that performs the task of contrast enhancement.

III. SUMMARY

Reversible data hiding in all the images is a new techniques because of the privacy-preserving requirements from cloud data. Previous methods implement RDH in encrypted images by encryption and decryption. The proposed by reserving room before encryption. The data hider can benefit from the extra space. The previous stage to make data hiding process very easy. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. The novel method can achieve real reversibility. Separate data extraction and greatly improved on the quality of marked decrypted images. The previous RDH techniques used for encrypted and decrypted the image.

Also considers a new algorithm of encryption and decryption of images. This algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding. Encryption and Decryption of an image by this algorithm protect the image from an unauthorized access. This Algorithm provides high security to an image and occupies minimum memory space. And for data embedding process , by using the Integer Wavelet Transform we can minimize the mean square distortion between the original and watermarked image and also to increase Peak signal to noise ratio. Also all these experiments are done in the gray scale images.

The proposed method also used in color images. A new reversible data hiding algorithm has been proposed with the property of contrast enhancement. The two peaks in the histogram are selected for data embedding so that histogram equalization can be performed by repeating the process. The results that the image contrasts can be enhanced by splitting a number of histogram peaks pair by pair. The enhanced contrast enhancement can be used in the proposed techniques. The 2 peaks in the histogram can be calculated from the pixel values of the given images.

IV. CONCLUSION

The Reversible Data Hiding techniques used in the proposed method with contrast enhancement. The 2 peaks values can be used for hiding the data into the image. The histogram can be used to easily find out the 2 highest peak values. In the proposed method can also used for the military and medical field also. The image can be used to histogram specification. The histogram values compare to that image pixel value. The proposed method used in the color images and that can be enhanced the contrast techniques.

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] 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)

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

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

[5] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging,

Security and Watermarking of Multimedia Contents, San Jose, CA, USA,Jan. 2002, vol. 4675, pp. 572–583

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

[7] 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.

[8] 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

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

[10] 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.

[11] HaoTian Wu, Member, IEEE, JeanLuc Dugelay, Fellow, IEEE, And YunQing Shi, Fellow, IEEE,"Reversible Image Data Hiding With Contrast Enhancement",IEEE SIGNAL PROCESSING LETTERS, VOL. 22, NO. 1, JANUARY 2015

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