Secure Reversible Image Data Hiding

[1] Pooja Chourasia,[2] Dr. Anubhuti Khare
[1]P.G. Student, [2] Professor,
Electronic & Communication Department
[1]U.I.T. RGPV College, Bhopal, India

***Abstract*— Today, the demand of internets has made the transmission of digital media much easier and faster. Open nature of internet, risks of illegitimate accessing and unauthorized tempering with transmitted data is increased day by day. Protection of secret information from unauthorized users in a public network has become an important issue. Data hiding is one of the most demanding techniques to protect the security of digital media. We have proposed reversible data hiding techniques for digital images. In this technique, cover image is divided into block equal size. Extracted secret text is similar to original secret text. Maximum capacity is more than bits and peak signal noise ratio (PSNR) is also higher than previous work. Embedding capacity and PSNR are higher than existing data hiding techniques.*)**

***Index Terms*— Reversible image data hiding (RIDH), DWT, steganogrphy, LSB,**

I. INTRODUCTION

A The Reversible image data hiding (RIDH) starts with the term steganogrphy first which suggests hiding any style of information within the multimedia file like audio, video, image, etc. the most flaw of steganogrphy is that the cover media is get damaged once recovering the embedded information with success. the main motive of proposing the RIDH scheme is to develop a method by that we are able to recover the embedded information while not causing any damage to the cover media [1]-[3].

Data hiding is that the method to hide information (representing some information) into cover media. That is, the information hiding method links 2 sets a collection of the embedded information and another set of the cover media image. The link between these 2 sets characterizes completely different applications. Variety of reversible information hiding techniques is projected, and that they will be roughly classified into 3 types: lossless compression primarily based strategies, difference expansion (DE) strategies, and histogram modification (HM) strategies. In sensible aspect, several RDH techniques have emerged in recent years [3]-[7]. Previously, the information RIDH primarily add the non encrypted domain that is, it embeds the plain text within a picture with the lossless compression technique. Since the lossless compression is useful so, embedding the plain text within the image is that the lack of security.

Fig.1 shows easy model of Reversible data hiding (RDH) Message this will be done by choosing an encoding key that is use to encode the first data once encrypting the information data hiding key is used and this information hiding key is embedded on the encrypted data with the assistance of information hider block and this encrypted information containing embedded data is send on the channel.

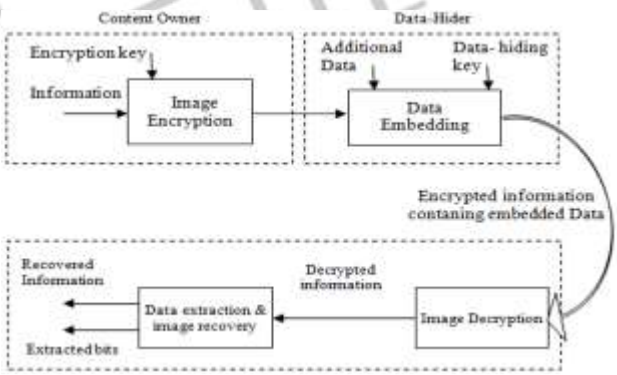

Fig. 1 Simple model of Reversible data hiding (RDH) Message

This will received by image Decryption that will decrypt the received data and by this decrypt information the original information is extracted by performing the reverse operation by using the same Encrypt key. Recently, reversible data embedding techniques have drawn more and more interest.

II. DATA HIDING

Wherever the so far, several algorithms for information hiding are projected however most of them fail to recover the cover image when information extraction. However, in some medical and military applications, it's desired that the initial cover media

to be recovered losslessly when information extraction. The marking techniques satisfying this demand are stated as reversible information hiding techniques.

At present, fragile reversible data-hiding techniques is conducted in 3 domains, that is, the special domain, the transformed domain, and therefore the compressed domain. Semi-fragile data-hiding techniques are conducted only within the special and transformed domains, as a result of high-level data regarding the structure of information stream sometimes isn't out there in compressed streams with embedded secret data. Within the special domain, the values of the pixels of the cover image are altered directly to embed the info. Within the transformed domain, the cover image ought to be preprocessed by a transform, like the integer wave transform (IWT), the discrete cos transform (DCT), the discrete wavelets transform, or the discrete Fourier transform, to induce the frequency coefficients. Then, the frequency coefficients are changed slightly to embed information, and therefore the stego image is obtained by exploitation the changed frequency coefficients. Within the compression domain, the compression code is altered to embed the data.

2.1. Principle of Data hiding

Embedding process and extracting process are the two main processes of data hiding. In embedding process, secret data is embedded into cover media. Cover media is modified after embedding the secret data. This modified cover media which contain secret data is known as marked data. Secret data is extracted from the marked data and recovers the original cover media.

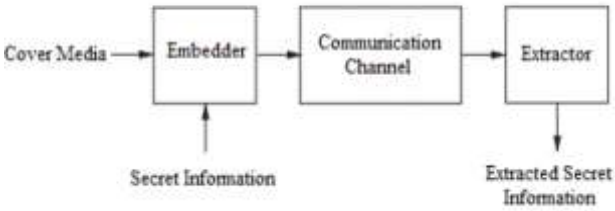

Fig.2 Traditional Data Hiding System

A traditional data hiding system, shown in fig.2, includes embedder and extractor. The input to the embedder is multimedia data and secret data, which is to be embedded into original multimedia data. The output of embedder is marked data. There are different types of file/data formats which are used for data hiding, as shown in fig.3.

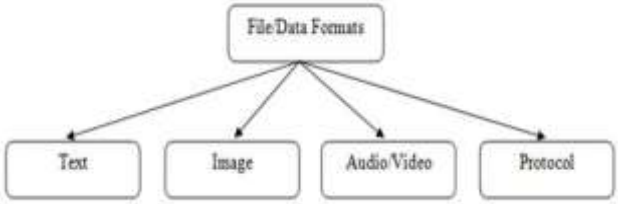

Fig.3 Different types of files used for data hiding

III. PROPOSED METHODOLOGY

The propose approach that uses numerous techniques like thresholding, DWT, Steganography it works with efficiency and supply maximum space at a similar time will increase security level, wherever because the quality of Steganographic image is additionally improved.

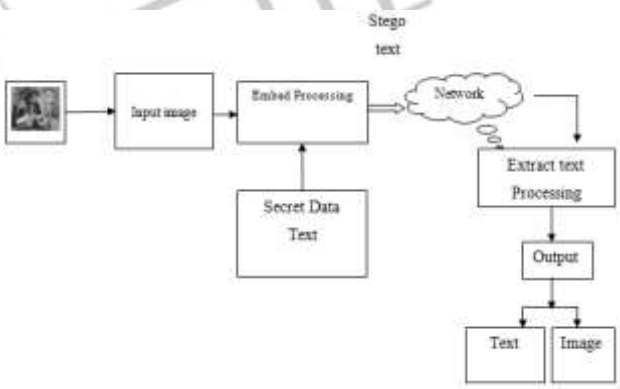

Fig.4 Block diagram of proposed methodology

3.1. Steganography

Steganography is defined as a way to hide information into pictures in such a way that is undetectable. Steganography and Cryptography, each are used for security functions however with completely different implementation and approaches. In cryptography, the text file get regenerate to alternative kind which offer confidentiality to sensitive information however in steganography we tend to hide the particular file in image kind so if leakage get occurred the third party fails to recognize the particular information. This provides confidentiality similarly as security to the sensitive information. The concept is to cover text in image with the conditions that the image quality is preserved alongside the size of the image instead we are able to

encode the information. That the want is, in cryptography output of unreadable information files are being send over an online is definitely detectable that some vital data is being sent. Whereas in steganography hiding message in a picture, alongside the conditions, it build appear of simply an exchange of image between 2 user ends. The steps being followed in steganography are as under:-

1. Firstly the text message is being written, then encryption of the message is done.
2. Later, text is hidden in the selected media like image file and transmitted at the receiver side.
3. at receiver end, reverse method is done to implement and recover the original text message.

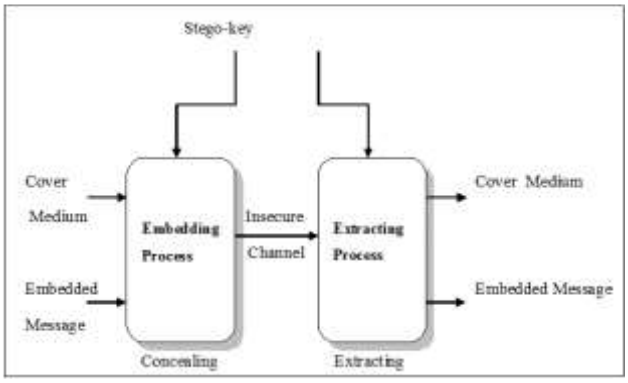

Fig.5 Steganographic Process

3.2. Least Significant Bit Modification

A digital image is represented employing a 2-D matrix of the colour intestines at every grid point (i.e. pixel). Generally gray pictures use 8 bits, whereas colored utilizes 24 bits to explain the colour model, like RGB model. The Steganography system that uses a picture because the cover, there are many techniques to hide data within cover-image. The spacial domain techniques manipulate the cover-image component bit values to embed the key data. The key bits are written on to the cover image pixel bytes. Consequently, the special domain techniques are easy and simple to implement. The least significant Bit (LSB) is one among the most techniques in special domain image Steganography.

The LSB is that the lowest important bit within the byte value of the image component. The LSB based image steganography embeds the key within the least important bits of component values of the cover image.

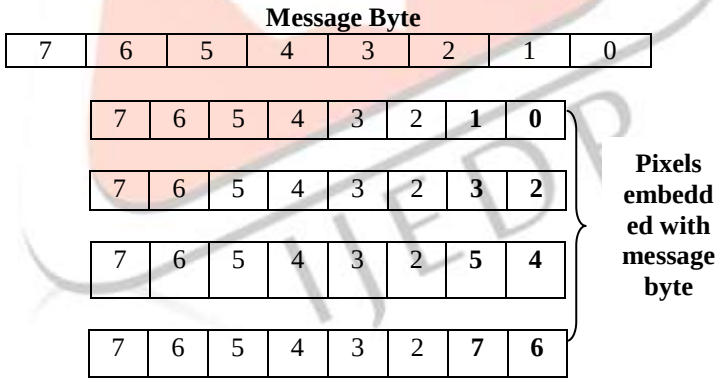

Fig.6: Proposed LSB Algorithm

The conception of LSB Embedding is easy. It exploits the actual fact that the extent of precision in several image formats is much larger than that perceivable by average human vision. Therefore, an altered image with slight variations in its colours is indistinguishable from the initial by a human being, simply by staring at it. In typical LSB technique, which needs eight bytes of pixels to store 1byte of secret information however in planned LSB technique, simply four bytes of pixels are sufficient to carry one message byte. Remainder of the bits within the pixels remains an equivalent.

3.3. Discrete Wavelet Transform (DWT)

The discrete wavelet transform (DWT), supported time-scale illustration, provides economical multi-resolution sub-band decomposition of signals. it's become a robust tool for signal process and finds varied applications in numerous fields similar to audio compression, pattern recognition, texture discrimination, computer graphics etc. Specifically the 2-D DWT and its counterpart 2- D Inverse DWT (IDWT) play a major role in several image/video coding applications. The DWT design, the input image is decomposed into high pass and low pass elements exploitation HPF and LPF filters giving rise to the primary level of hierarchy. the method is sustained till multiple hierarchies are obtained.

The image is 1st decomposed into four sub bands of LL, LH, HL and HH. More the LL sub band is decomposed into four a lot of sub bands as shown within the figure. The LL element has the maximum data content as shown. The opposite higher order sub bands contain the sides within the vertical, horizontal and diagonal directions. a picture of size N X N is decomposed to N/2 X N/2 of 4 sub bands. Selecting the LL sub band and rejecting the opposite sub bands at the primary level of hiding the text data in image by 75th. So DWT assists in stegnography

IV. RESULT ANALYSIS

The cover image is taken for embedding and extraction process. In this proposed work text are hiding through MATLAB. After embedding and extraction process the performance analysis is done with the help of PSNR and MSE and Embedded Capacity. In this project applied discrete wavelet transform and steganography, for Reversible Image Data Hiding with Contrast Enhancement.

Fig.6 Program Run Then Open Window

This figure shows the data hiding window. When we run the program file then open this window.

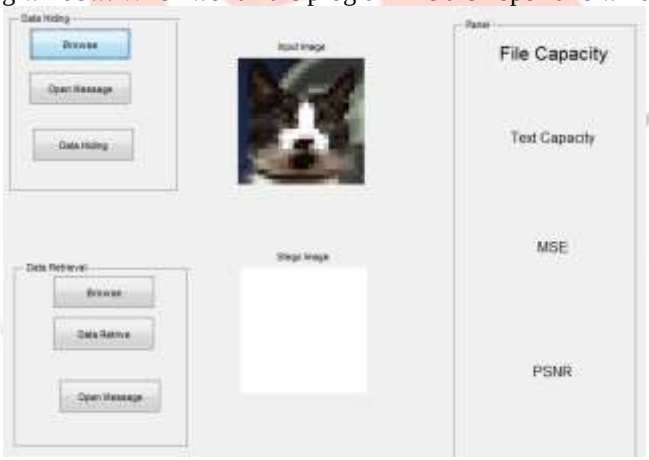

Fig.7 Input Image Window

This figure shows when we browse the main input image then this window is open.

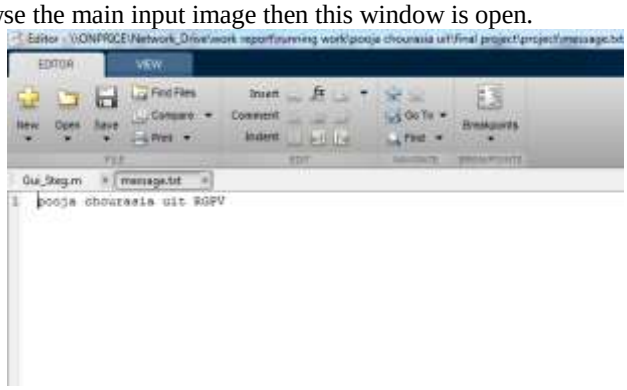

Fig.8 Message Text Editor Window

In this figure we write the text message which text message is hide.

Fig9 Data Hiding

In this figure we are hide the text message then press the data hide button then open the dialog box that is our data is hided successfully in secret.bmp.

Fig.10Data Retrieval process

In this figure we are press the data retrieve button are press then open the dialog box in our window that is we know that our data is successfully retrieved.

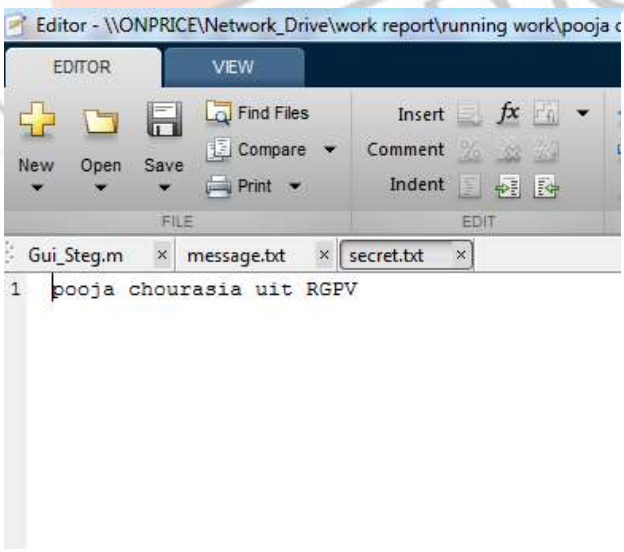

Fig.11 Message retrieved

This figure shows the messages are successfully retrieved.

V. PERFORMANCE EVALUATIONS

After we are comparing PSNR with the PANR of [15]. PSNR and MSE value comparison shows in below:

Algorithm	Image Size	PSNR(dB)			MSE			File Capacity	Text Capacity
		R	G	B	R	G	B		
Proposed	2KB	49.91	49.28	60.21	0.668	0.772	0.062	625	24
Existing	2KB	36.988			-			-	-

VI. CONCLUSION

Ensure digital information security, numerous techniques are conferred in recent researchers work. In the work a data hiding techniques using steganography is proposed. The marked image obtained using this approach produces better hiding capacity. The concept is used to hide the secret information in digital images to enhance the embedding capacity. This technique produces high embedding capacity and better hiding capacity as compared to various existing techniques. This research presents reversible data hiding techniques and approaches. In this proposed work PSNR value is higher than the previous work. So, image quality obtained by proposed work is better than the previous work result. Here also Comparison results shows that large embedding capacity is defined as payload while keeping distortion low.

REFERENCES

[1] Z. Jiantao, W. Sun, Li Dong, X. Liu, O.C. Au, and Yuan Yan Tang. "Secure reversible image data hiding over encrypted domain via key modulation" IEEE Transactions on Circuits and Systems for Video Technology 26, no. 3 (2016): 441-452.

[2] Tian, Jun. "Reversible data embedding using a difference expansion." IEEE transactions on circuits and systems for video technology 13, no. 8 (2003): 890-896.

[3] Wu, Hao-Tian, Jean-Luc Dugelay, and Yun-Qing Shi. "Reversible image data hiding with contrast enhancement." IEEE signal processing letters 22, no. 1 (2015): 81-85.

[4] Luo, Hao, Fa-Xin Yu, Hua Chen, Zheng-Liang Huang, Hui Li, and Ping-Hui Wang. "Reversible data hiding based on block median preservation." Information sciences 181, no. 2 (2011): 308-328.

[5] Gao, Guangyong, and Yun-Qing Shi. "Reversible data hiding using controlled contrast enhancement and integer wavelet transform." IEEE Signal Processing Letters 22, no. 11 (2015): 2078-2082.

[6] Jung, Seung-Won, and Sung-Jea Ko. "A new histogram modification based reversible data hiding algorithm considering the human visual system." IEEE Signal Processing Letters 18, no. 2 (2011): 95-98.

[7] Z. Zhao,H.Luo,Z.-M. Lu, and J.-S. Pan, "Reversible data hiding basedon multilevel histogram modification and sequential recovery," Int. J. Electron. Commun. (AEÜ), vol. 65, pp. 814–826, 2011.

[8] H. T.Wu and J. Huang, "Reversible image watermarking on prediction error by efficient histogram modification," Signal Process., vol. 92, no. 12, pp. 3000–3009, Dec. 2012.

[9] Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast-sensitive reversible visible image watermarking technique," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 5, pp. 656–667, May 2009.

[10] J. A. Stark, "Adaptive image contrast enhancement using generalizations of histogram equalization," IEEE Trans. Image Process., vol. 9, no. 5, pp. 889–896, May 2000.

[11] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer, and W. J. Rucklidge, "The emerging JBIG2 standard," IEEE Trans. Circuits Syst. Video Technol., vol. 8, no. 7, pp. 838–848, Jul. 1998.

[12] The USC-SIPI Image Database [Online]. Available: http://sipi.usc.edu/ database/

[13] [Kodak Lossless True Color Image Suite [Online]. Available: http:// www.r0k.us/graphics/kodak/

[14] M.-Z.Gao, Z.-G.Wu, and L.Wang, "Comprehensive evaluation for HE based contrast enhancement techniques," Adv. Intell. Syst. Applicat., vol. 2, pp. 331–338, 2013.

[15] Gupta, Neha, and Nidhi Sharma. "DWT and LSB based Audio Steganography." Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on. IEEE, 2014.