A Hybrid Approach for Image Steganography with Compression to Enhance Security and Accuracy

[1]Krina Patel,[2]Mr. Swarndeep Saket J.

[1]Student, Computer Department, LJIET (GTU), Gujarat, India.

[2]Asst. Prof., Computer Department, LJIET (GTU), Gujarat, India.

ABSTRACT

Security of secret data has been a major issue of concern from ancient time. Steganography and cryptography are the two techniques which are used to reduce the security threat. Cryptography is an art of converting secret message in other than human readable form. Steganography is a technique of hiding the secret message and transmission of confidential data through public channel like Internet. These techniques are required to protect the data over the network. An Advance approach the image security along with compression and encryption used to a high quality of secret message and data. Image compression is used to minimize the amount of memory and fast transmission over internet to represent an image or data. And encryption is used to protect the data over the noise and different attacks. In this thesis, proposed an algorithm steganography and EZW compression technique to provide hiding the large amount of secret data with Chaos encryption used to securely transfer image to receiver side. And also discuss 2-level DWT using steganography to reduce the variation of recovered image. This technique used to a securely data transfer from narrow band and unsecure channel.

Keywords: EZW compression, chaos based encryption, 2 –level DWT, Information Hiding, Security.

I. INTRODUCTION

In today's world, transmission of the information over the channel is not secure for example patient records, military information, banking data and other sensitive information. In order to protect this sensitive information it is coded within the image, audio or text files which is decodable only with the help of a particular key. Steganography is used to hide a secret message within a cover image, thereby yielding a stego image such that even the trace of the presence of secret message cannot be detected. In the modern steganography, steganography meaning evolved into withholding information on a digital media file, the media can include images, sound or video. In steganography main component is image compression. Image compression used minimizing the size, reduce transmission time. But this technique some challenge with image communication is to maintain the image quality during the communication. Sometimes, because of low speed transmission or signal distortion, the quality of image can be affected. But some applications are sensitive to image quality; because of this there is requirement to maintain the quality of image.

The main goals of algorithms is to provide a robust security against any type of intrusion and also the algorithm need to be as simple as possible in terms of ease of implementation, cost of implementation, complexity and its durability or sustainability against the different kinds of intrusions. And also used to a high quality of reconstruct image to used some techniques.

An Advance approach the image security along with compression and encryption used to a high quality of secret message and data. Image compression is used to minimize the amount of memory needed to represent an image. Transmitting or storing an image is major problem in current scenario.

II. STEGANOGRAPHY

Steganography is a technique of hiding a message in a host image without any perceptual distortion of the host image. The main terminologies used in the steganography systems are: the cover message, secret message, secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.

In image steganography approaches are broadly classified into Spatial Domain and Transform Domain.

A. 2-Level DWT

Wavelet transform provides both frequency and spatial description of an image. DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges. The 1-level Discrete wavelet transform decomposes an image into lower resolution approximation image (LL1) as well as horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. To compute 2 level of 2D-DWT the DWT algorithm is again applied on the LL1 which further decompose the LL1 part in four subbands LL2, HL2, LH2 and HH2.

III. IMAGE COMPRESSION

Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in file size allows more images to be stored in a given amount of disk or memory space. Image compression also reduces the time required for images to be sent over the internet or downloaded from web pages.

In image compression approaches are broadly classified into lossy image compression and lossless image compression. In Lossy image Compression after reconstruction of image data loss is more so it is used when transmission time is important and quality of image can be negligible. Lossless image compression is used when transmission time of data is not important but quality, information, data are important.

B. EZW Compression

The Embedded Zero Wavelet (EZW) is simple and effective algorithm for image compression which has a property of coding the bits in the order of their importance. Basic concept behind EZW is the concept of zero tree structure which occurs in the Discrete Wavelet Transform (DWT) applied image due to the spatial correlation of DWT. To apply EZW on an image we need to follow 3 steps. In first step is to apply multi-level DWT on image. Second step consists of 2 passes namely Dominant pass and Sub-ordinate pass. Dominant pass start with finding a threshold and modifying the image pixel values depending on threshold. Now the image is scanned and assigned with codes positive, negative, isolated zero and zero tree respectively. In next pass, elements in subordinate list are processed in the entry order. The elements which are coded with POS and NEG are replaced by zeros in the image and the same process is repeated by making the threshold half of the previous, this process can be done up to the user defined threshold value or up to the threshold limit 1.

Finally, the generated string is coded using entropy coding algorithms such as Huffman coding, Arithmetic coding etc. Using the coded string the image can be decoded in the same manner of encoding. One of the advantage of EZW is that we can stop decoding at any point of time to view the decoded image.

III. CHAOS ENCRYPTION

The chaos-based image cryptosystem mainly consists of two stages are confusion stage and diffusion stage. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. The pixel permutation is carried out by a chaotic system. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the

encryption process aims at changing the value of each pixel in the whole image an important tool to protect image from attackers.

In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

IV. COMPARISION OF IMPLEMENTED TECHNIQUES

Table 1 Comparison of Implemented Techniques

Sr. No	Title	Method Used	Advantages	Disadvantages
1	Real-Time Implementation of Steganography in Medical Images using Integer Wavelet Transform.	IWT.	Less memory space. High quality data hiding and compression. Highly secure. Use different images.	Output from integer so that is not maintain accuracy.
2	An Edge Based Image Steganography with Compression and Encryption.	LZW, RSA.	Huge hiding capacity. Used for unsecure channel. High compression.	Data lost.
3	Designing Secured Data Using a Combination of LZW Compression, RSA Encryption, and DCT Steganography.	DCT, LZW, RSA	More secure. Capacity is larger. Reduce processing time.	Asynchronization.
4	Image Security using Chaos and EZW Compression.	EZW, Chaos	Best suitable because high security and high compression.	Required prior knowledge.
5	Analysis of Facebook Steganographic Capabilities.	DCT.	20% or more compression capacity. Random location on cover image to perform hiding.	Data lost.
6	Securing the Architecture of the JPEG Compression by an Dynamic Encryption.	JPEG, Hill Cipher.	Robust crypto system. Good for security	Less Accurate. It is not used for Real time images.

V. PROPOSED WORK

In proposed technique, First pre-processing is applied on cover image. In pre-processing we applied resize of image. Then applied 2-level DWT transforms. Then added secret message using LSB embedding techniques. Then converted stego image and applied EZW compression and Chaos based encryption and converted advance stego image. Then extracting process take advance stego image applied decryption using secret key and decompress and decryption techniques. Last applied inverse transform and receive secret message and image.

Flow chart for embedding process:

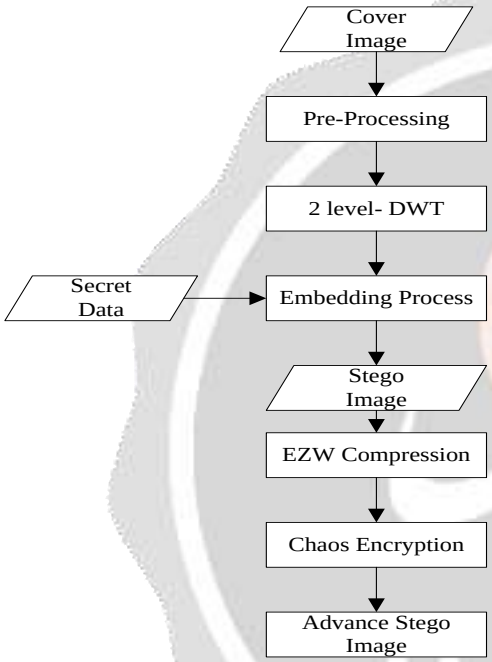


Fig 1 Embedded Proposed System

Flow chart for extraction process:

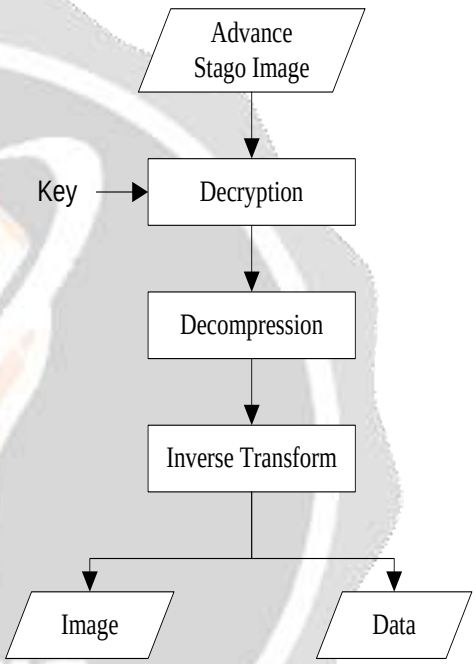
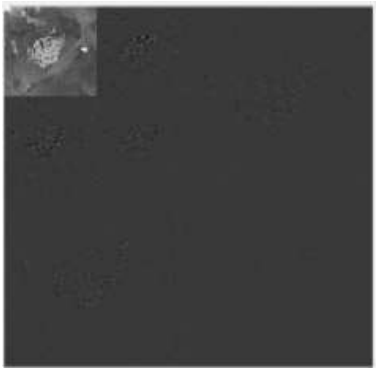


Fig 2 Extracted Proposed System

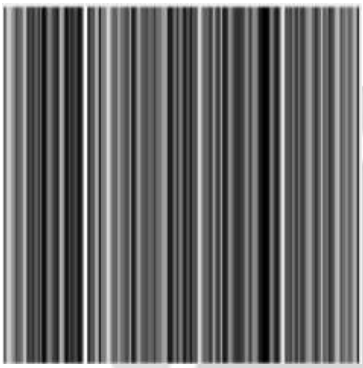
VI. RESULT ANALYSIS

Implementation results of the proposed system tested on MATLAB R2014b was used and operation carried out on desktop computer having Intel i5 processor with 8GB of RAM. In results the screenshots of the intermediate results are kept which are used for generating the final result of the system. The parameter selected for result analysis of proposed system is PSNR, MSE, Compression Ratio, Embedded capacity and Execution time. Based on the parameter decided the Accuracy and robustness of this system. For result analysis we takes image is calculated to different parameters and comparison of result analysis of two classification without attack and with attack is done that different attack accuracy is near by the original accuracy from given table. Thus the as well as same to a PSNR and MSR as original image.

(a) Original Image

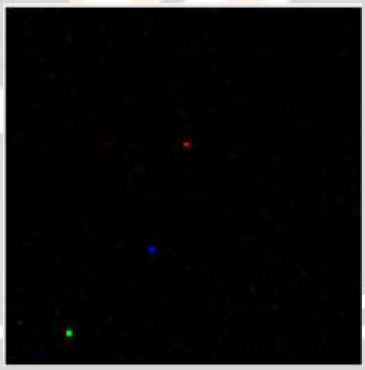


(b) 2-level DWT Image



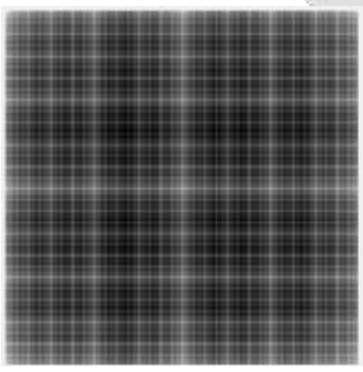
(c) Embedded Image

(d) Compressed Image

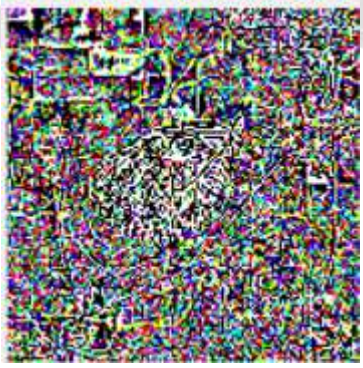


(e) Encrypted Image

(f) Decrypted Image



(g) Decompressed Image



(h) Inverse DWT Image

(i) Final Recovered Image

Images	PSNR (dB)	MSE (dB)	Compression Ratio	Embedded Capacity	Execution Time (sec.)
Original Image	54.1177	0.6656	0.0194	16384	5.735431
Salt & Pepper	54.1227	0.6649	0.0194	16384	5.735431
Gaussian	54.1186	0.6655	0.0194	16384	5.735431
Noise	51.1176	0.6657	0.0194	16384	5.735431
Rotate	51.1160	0.6659	0.0194	16384	5.735431
Unsharp	51.1190	0.6655	0.0194	16384	5.735431
Blur	51.1167	0.6658	0.0194	16384	5.735431

VII. CONCLUSION

Information security and transmission is a key factor in image processing. According to literature review and paper analysis to balance security with steganography and compression of data is primary limitation of existing system. Using proposed flow improve to security and compression for data and image. For security use hybrid model and for compression use EZW compression. Also work on different type of attacks like that Noise, Gaussian, Rotate, Salt & Pepper, Speckle, Unsharp and Blur to prove that our system is robust. Also work on different type of parameters like that PSNR, MSE, Compression Ratio, Capacity and Execution time. In future try to add some often compression for better transmission.

REFERENCES

[1] Faiq Gmira, Said Hraoui, Abderrahim Saaidi, Abderrahmane Jarrar Oulidi, Khali Satori. "Securing the Architecture of the JPEG Compression by an Dynamic Encryption." *IEEE Intelligent Systems and Computer Vision (ISCV)*, Morocco, 25-26 March 2015, DOI 10.1109/ISACV.2015.7106192 Print ISBN: 978-1-4799-7511-2.

[2] Shubham Lavania, Palash Sushil Matey, Thanikaiselvan V. "Real-Time Implementation of Steganography in Medical Images using Integer Wavelet Transform." *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, TamilNadu, 18-20 Dec. 2014, DOI 10.1109/ICCIC.2014.7238344 Print ISBN: 978-1-4799-3975-6.

[3] Rina Mishra, Atish Mishra, Praveen Bhanodiya. "An Edge Based Image Steganography with Compression and Encryption." *IEEE International conference on Computer, Communication and Control (IC4-2015)*, Indore, 10-12 Sept. 2015, DOI 10.1109/IC4.2015.7375510 Print ISBN: 978-1-4799-8165-6.

[4] Nathaniel D. Amsden, Lei Chen. "Analysis of Facebook Steganographic Capabilities." *2015 International Conference on Computing, Networking and Communications, Communications and Information Security Symposium*, Huntsville, 16-19 Feb. 2015, DOI 10.1109/ICCNC.2015.7069317 Print ISBN: 978-1-4799-6959-3, pp. 67-71.

[5] T. Venkata Sainath Gupta, Ch. Naveen, V. R. Satpute, A. S. Gandhi. "Image Security using Chaos and EZW Compression." *2014 Students Conference on Engineering and Systems (SCES)*, 28-30 May 2014, DOI 10.1109/SCES.2014.6880108 Print ISBN: 978-1-4799-4939-7.

[6] Ledya Novamizanti, Gelar Budiman, Iwan Iwut Tritoasmoro. "Designing Secured Data Using a Combination of LZW Compression, RSA Encryption, and DCT Steganography." *2015 1st International Conference on Wireless and Telematics (ICWT)*, Indonesia, 17-18 Nov. 2015, DOI 10.1109/ICWT.2015.7449245 Print ISBN: 978-1-4673-8434-6.