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

[1]Krina Patel,[2]Ms. HinalSomani

[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 an art of hiding the existence of secret message to 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 paper, proposed an algorithm using chaos on EZW compression technique to provide security along with image compression and chaos encryption used to reduce the negative compression.And also discuss two-level DWT using steganography to used hide information and securely transfer image to receiver side. This technique used to a secure data to narrow bandwidth and unsecure channel to transmit a successfully to receiver side.

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 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 usedminimizing 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.

II. 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.

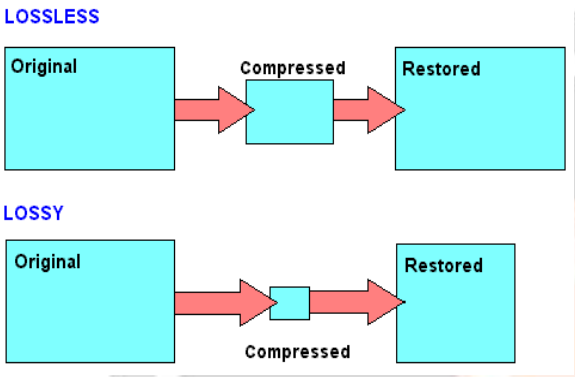

Figure 1 Lossless and Lossy Image Compression[6]

2.1Lossy 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. Lossy compression is most commonly used to compress multimedia data like audio, video, and images, especially in applications such as streaming media and internet telephony. Lossy compression reduces a file by permanently eliminating certain information.

1. **Block Truncation Coding** technique is used for digitized gray scale images which divides the image into non overlapping blocks of pixels and for each block, threshold and reconstruction values are determined. The threshold is usually the mean of the pixel values in the block. Then a bitmap of the block is derived by replacing all pixels whose values are greater than or equal (less than) to the threshold by a 1 (0).Block Truncation encoding is very fast encoding of lossy image compression technique, requires little memory space, easy to implement, Standard BTC involves less computational complexity, very less prone to transmission errors.
2. **Transformation coding** technique data is divided in to square blocks and transforms the raw data to a domain that more accurately reflects the information content ex. Audio file. Discrete Cosine Transform (DCT) is the known transform in the image compression field because of its excellent properties of energy compaction. DWT is the most recent transform used to high frequency images.
3. **Vector quantization** technique is to develop a dictionary of fixed-size vectors, called code vectors. A vector is usually a block of pixel values. A given image is then partitioned into non-overlapping blocks (vectors) called image vectors. VQ (vector quantization) replaces each block of input pixels with the index of a vector in the dictionary, which is close to the input vector by using some closeness measurements.
4. **Fractal coding** method decomposes the image into segments by using standard image processing techniques such as color separation, edge detection, and spectrum and texture analysis. Then each segment is looked up in a library of fractals which contains codes called iterated function system (IFS)

codes, are compact sets of numbers. This scheme is highly effective for compressing images because they have good regularity and self-similarity but it is so costly.

5. **Subband coding** decompose the input signal into different frequency bands. After the input is decomposed to its constituents than the best coding technique can be used to each constituent to improvethe compression performance. The advantage of this scheme is that the quantization and coding well suited for each of the sub bands can be designed separately.

2.2 Lossless Image Compression

Lossless image compression is used when transmission time of data is not important but quality, information, data are important. Lossless compression allows the original data to be perfectly reconstructed from the compressed data. Most satellite images uses lossless image compression techniques because in satellite image compression each and every small data affect the performance of image processing.

1. **Run Length Encoding** is a very simple compression method used for sequential data and very useful in case of repetitive data. This technique Replaces sequences of identical symbols (pixels), called runs by shorter symbols.
2. **Huffman Encoding** is a matter of course technique for coding symbols based on their statistical occurrence frequencies. The pixels in the image are treated as symbols. The symbols that occur more frequently are assigned a smaller number of bits, while the symbols that occur less frequently are assigned a relatively larger number of bits.
3. **LZW Coding** is a dictionary based coding whose full set of strings is determined before coding begins and does not change during the coding process. LZW is widely used in computer industry and is implemented as compress command on UNIX.
4. **Area Coding** is an intensified form of run length coding, reflecting the two dimensional character of images. These algorithm used rectangular regions are coded in a descriptive form as an element with two points and a certain structure. This type of coding can be highly effective but it bears the problem of a nonlinear method, which cannot be implemented in hardware.

III. RELATED WORK

3.1 IWT Steganography on Medical images

In this method [2] IWT (Integer Wavelet Transform) is an image compression technique where in the output is in the form of integers thus consuming less memory space. This technique allows high quality data hiding and image compression. To transmit many such images over a network, sometimes over low-capacity phone lines to remote sites, or to store large numbers of images over a long period of time as part of the medical records for patients to compress that real time images.

In DWT, wavelet filters that have floating point coefficients are used so that when data is hidden inside their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information. This would result in the data hiding system to fail. In case where the input data is integer as in digital images, the output data will cease to be integer which in turn doesn't allow perfect reconstruction of the input image. IWT ensures no loss of information through forward and inverse transforms.

3.2 Edge based LZW Compressionwith RSA encryption

Authors [3] have proposed method to secret data is compressed first using LZW algorithm before embedding it behind any cover media. Data is compressed to reduce its size. After compression data encryption is performed to increase the security. Encryption is performed with the help of a key which make it difficult to get the secret message even if the existence of the secret message is revelled. RSA encryption algorithm, it is performed by using receiver's public key, a random no. n and last ciphertext is generated.

In Last decryption of the secret message is performed with ciphertext, private key of the receiver and a random number.

3.3 Combination of DCT Steganography, LZW Compression, RSA encryption

In this paper [7] author discussed methods to start RSA encryption method and using the key which will be used in the decryption process. Messages are encrypted after compressed by losslessLZW method, so it will reduce the size of the message that will be inserted and increase the capacity of messages that can be inserted. Messages that have been compressed and encrypted, is then hidden by DCT techniques. With the incorporation of encryption techniques, steganography, and compression, the acquired information is more secure and its capacity is larger.

The image will be processed to get a text message hidden in the image. A text message has been obtained from the image is decompressed back to using LZW decompression technique. Text messages result from decompression was still not final results for the previous message encrypted with RSA method so that the necessary processes by using the decryption key that already exists. After the decryption process is complete we will get the actual text message.

3.4Lossy EZW Compression with Chaos based encryption

In this paper [5] authors using chaos on EZW compression technique to provide security along with image compression. Chaos for image security due to its robustness to initial condition and mixing property. This technique providing image security starts with compressing the image using EZW. In EZW providing additional security to image along with main function of compression.

In EZW, we don't know the DWT level applied to image and number of EZW passes we cannot bring back the original image. If keys are known without the prior knowledge of level applied, number of passes and storage pattern we cannot reconstruct the image back. Also this way by having an unknown level of DWT it will be very difficult for an hacker to get back the original contents.

If scramble the data it may lead to increase details in the image, which is not suitable for compression. If apply EZW on such type of scrambled image it leads to negative compression, instead of compressing the image it increase the space occupied by the image. So, to overcome this problem we are going to apply EZW first and then chaos based scrambling on the resultant data. This will save memory space and also transmission bandwidth.

3.5 Analysis of facebook steganography for different methods

In this paper [4] author discussed methods Steganography can be employed to send covert information via Facebook photos and potentially videos as well. Facebook Cover Photos can effectively utilize steganography, of at least 15.75% capacity using DCT coefficient embedding algorithms. Network traffic analysis determined no distinguishable differences between network traffic patterns of normal images and cover photos as they were uploaded to the Facebook servers.

3.6 JPEG Compression by dynamic Hill-Cipher encryption

Authors [1] have proposed new approach that integrates dynamic Hill-Cipher encryption added to the step of quantizing of JPEG compression. The effectiveness and robustness of this scheme is validated by measuring its security strength and quality is high of reconstructed images.

An robust cryptosystem is presented and implemented by combining the JPEG compression and an encryption using a modified Hill cipher method in mode by block what gives us the possibility of deciphering in a individual way blocks 8x8 pixels the compression rate is modifiable and therefore the proposed method provides an optimal use of bandwidth with a very good level of security.

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 is not completely but lost is acceptable.
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	Quality is good but not excellent. Is not used for Real time images.

V. PROPOSED WORK

In order to enhance the security and accuracy for different technique has been proposed and following are the steps.

Step 1: Take cover image.

Step 2: Differentiate image in R, G, B component.

Step 3: Apply 2-level DWT.

Step 4: LSB embedded process and add to a secure message and receive stego image.

Step 5: Apply EZW compression.
Step 6: Apply chaos based encryption and receive advance stego image and transfer to a receiver side.
Step 7: Apply decryption technique and decompress technique.
Step 8: Apply inverse transform and receive data and image.

VI. CONCLUSION

Information security and transmission is a key factor in image processing. According to literature review and paper analysis to balance security with steganographyand compression of data is primary limitation of existing system. Using proposed flow try to improve security and compression for data and image. For security use hybrid model and for compression use EZW compression. In future try to add some often compression for better transmission.

REFERENCES

[1] FaiqGmira, Said Hraoui, AbderrahimSaaidi, AbderrahmaneJarrarOulidi, 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] ShubhamLavania, 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. VenkataSainath 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] Pcmag.com. (2016). *lossy compression Definition from PC Magazine Encyclopedia*. [online] Available at: http://www.pcmag.com/encyclopedia/term/46335/lossy-compression [Accessed 25 Aug. 2016].

[7] LedyaNovamizanti, GelarBudiman, IwanIwutTritoasmoro. "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.