Designing Secured Data Using a Combination of Compression and Encryption Technique

Sayli S. Relekar[1], Prof. V. B. Raskar[2]

[1]ME Candidate, Electronic and Telecomunication, JSPM's Imperial College of Engineering and Research Pune, India

[2]Professor, Electronic and Telecomunication, JSPM's Imperial College of Engineering and Research Pune, India

Email – sayli.relekar@gmail.com, raskar_vishal@yahoo.com

Abstract: *In the 21st century, with more use of internet there has been significant increase in various attacks on the network. Here we describe the technique of how can a secrete communication take place between two or more parties secretly. In this paper the technique of cryptography and Steganography are used all together for to achieve message confidentiality. In cryptography, message gets encrypted and in Steganography, it gets embedded within the selected image. For that, we first substitute the original message by using the fourteen square substitution algorithms. After the substitution of text, we then encrypt this text message using RSA algorithm. The encrypted message compressed by JPEG 2000 (Huffman coding) 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 DWT (Discrete Wavelet Transform) techniques. With the incorporation of encryption techniques, steganography, and compression, the acquired information is more secure and its capacity is larger. At the receivers end, same operations are performed to decrypt the original message in reverse order. It is found that here we are using the double ciphering techniques which makes the system very robust and secures it from known hacking attacks. It makes very difficult for the intruders to hack the image and then decrypt the message in a feasible amount of time thus securing it from many known network attacks.*

Key Words: *Input image, Pre-processing, DWT, 2 stage Encryption, JPRG2000 Compression, LSB substitution, Parameter analysis (PSNR,MSE).*

1. INTRODUCTION:

Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it's projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next 20 years was focused on the attack. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient.

Why then pursue the field of information hiding? Several good reasons exist, the first being that "security through 3rd party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in the pictures is still encrypted, but attracts far less attention being distributed in the picture then it would otherwise.

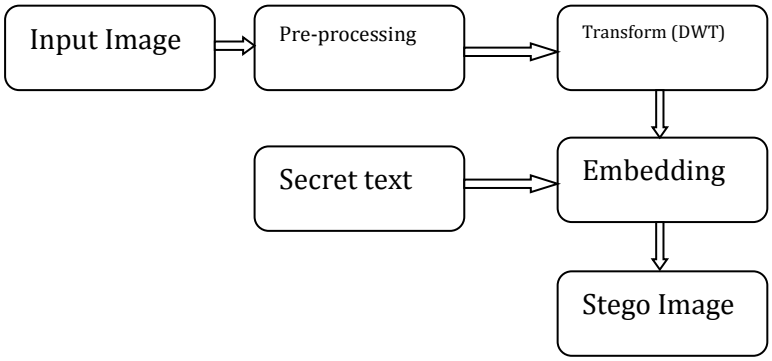


Fig1.1: Tentative Model

The technique is compared with previous techniques as applied to simulated and unwanted parameters ie, mean square error and peak signal to noise ratio will be calculated for performance evaluation. Cryptography and steganography plays an important role in the network security. Cryptography is use to encrypt data. Steganography is use to hide the data into image, video or in any multimedia file. Using such techniques the data is secured and transfer over internet without getting misplace or hack.

Cryptography is a science and study of secret writing. It is synonymous to the encryption technique. In cryptography data is been encrypted. And this encrypted data is known as the secret key. So the cryptography is called as the secret encryption or secret writing. The process of converting the plaintext into ciphertext is called as the encryption. And same in the reverse order converting ciphertext into plaintext is called as decryption.

2. LITERATURE OVERVIEW:

2.1.1 LSB: LSB [5], [6] is one of the earliest and simplest methods for hiding information in audio signals. It is the commonly used technique for audio steganography. In LSB encoding, the least significant bits of the cover media/original audio is altered to include the secret message. Even though this is a simple method, an attacker can easily extract the secret message from the stegano object.

2.1.2 Parity coding: Parity coding technique [3], [4] operates on a group of samples instead of individual samples. Here individual samples are grouped and parity of

each group is calculated. For inserting message bit one by one, check the parity bit of a group of samples. If the parity bit and message bit matches do nothing. Otherwise change the LSB's of any one of the individual samples in that group to make the parity bit equal to the message bit.

2.1.3 Echo hiding: In echo hiding [7] method data is embedded in the echo part of the host audio signal. The echo is a resonance added to the host signal and hence the problem with the additive noise is avoided here. While using echo hiding three parameters are to be considered: they are initial amplitude, offset (delay), and decay rate, so that echo is not audible. The main disadvantage of this method is lenient detection and low detection ratio. Due to its low embedding rate and low security no researches are going on echo hiding technique.

3. PROPOSED METHOD THEORY:

Below block diagram explains as follows. The input secret data is given as input, and then apply 1st stage encryption using 14 square algorithm. Again apply 2nd stage RSA algorithm to encrypt data. Use JPEG2000 compression to compress the encrypted data. The input image is converted to RGB to Gray scale image and apply DWT transform and apply LSB algorithm to hide the data, same reverse process to extract the data.

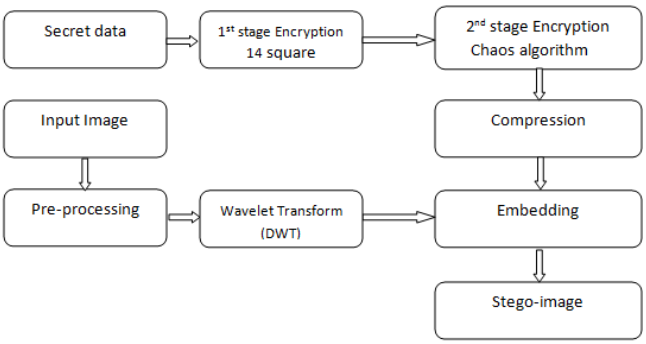


Fig 3.1: Proposed Model

3.1 Fourteen Square Substitution Cipher

In the earlier paper the twelve square cipher substitution is represented which includes only lower case alphabets, numbers and some special characters. This is extended in to fourteen square substitution ciphers to include numerals, upper and lower alphabets and all special characters including space bar which are present on keyboard. At first, the fourteen-square substitutes the alphabets, digits and special characters so it is less susceptible to frequency analysis attacks. It uses eight 9 by 6 matrices each arranged in a square, as shown in figure-1. Each of the 9 by 6 matrices contains the letters of the alphabets (upper case and lower case) and another six 6 by 7 matrices arranged in a squares

for digits and special characters, as shown in figure-2. All the special characters from your desktop/laptop keyboard are included in this figure.

So the following describes how the figure-1 is prepared: in square-1, we have taken fifty two alphabets and two special characters, out of which twenty six are capital letters and twenty six, are small letters. In each row we have arranged nine alphabets and each column contains six alphabets. Square- 2 is made from square- 1 by taking the first row of the square-1 to sixth row place and other rows one position up. Similarly square-3 is created from square 2 by taking the first row of square 2 to sixth row place and other rows are position up. The same procedure is for square- 4 which created from square-3 by taking first row of square-3 to sixth row of square-4 and other rows are position up. In square-5, we have converted rows into column and interchanged first and last alphabets. The same step follows in square-6 to square-8 by taking first row of previous square to sixth row and other rows one position up. The same method we have followed in figure- 2. It is shown in figure-1 and figure-2

Square 1	Square 2	Square 3	Square 4
s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z @? a b c d e f g h i j k l m n o p q r	B C D E F G H I J K L M N O P Q R S T U V W X Y Z @? a b c d e f g h i j k l m n o p q r s t u v w x y z A	K L M N O P Q R S T U V W X Y Z @? a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J	T U V W X Y Z @? a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S
Square 5	**Square 6**	**Square 7**	**Square 8**
r y E K Q W a g m t z F L R X b h n u A G M S Y c i o v B H N T Z d j p w C I O U @ e k q x D J P V ? f l s	t z F L R X b h n u A G M S Y c i o v B H N T Z d j p w C I O U @ e k q x D J P V ? f l s r y E K Q W a g m	u A G M S Y c i o v B H N T Z d j p w C I O U @ e k q x D J P V ? f l s r y E K Q W a g m t z F L R X b h n	v B H N T Z d j p w C I O U @ e k q x D J P V ? f l s r y E K Q W a g m t z F L R X b h n u A G M S Y c i o

Fig. 1. Plain Text and Cipher Text Table(Alphabets)

Square 9	Square 10	Square 11
0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & * ( ) _ - + = { [}] ; : “ ‘ \ | <, >. € /	7 8 9 ` ~ ! # $ % ^ & * ( ) _ - + = { [}] ; : “ ‘ \ | <, >. € / 0 1 2 3 4 5 6	# $ % ^ & * ( ) _ - + = { [}] ; : “ ‘ \ | <, >. € / 0 1 2 3 4 5 6 7 8 9 ` ~ !
Square 12	**Square 13**	**Square 14**
0 6 ! & + ; < 1 7 * = : , 2 8 # ({ “ > 3 9 $) [‘ . 4 ` % _ } \ € 5 ~ ^ -] | /	1 7 * = : , 2 8 # ({ “ > 0 6 ! & + ; < 3 9 $) [‘ . 4 ` % _ } \ € 5 ~ ^ -] | /	1 7 * = : , 2 8 # ({ “ > 3 9 $) [‘ . 4 ` % _ } \ € 5 ~ ^ -] | / 0 6 ! & + ; <

Fig. 2. Plain Text and Cipher Text Table(Digits and Special Characters)

3.2 Chaotic Encryption Scheme:

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. The advantage of chaotic encryption is High level security. The encryption is achieved by iteration. Simplest. No short cuts are available Whereas the requirement of large cipher storage and slow in speed are considered the major disadvantages.

The properties of chaos are slightly producing some changes in the entire cryptography. Sensitive on initial stage and topology transitivity are the properties in it. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectory sectional value. Identical trajectory only can produce the same values. The topology transitivity defines that the state points reside in a bounded space state and approaches.

Process Flow:

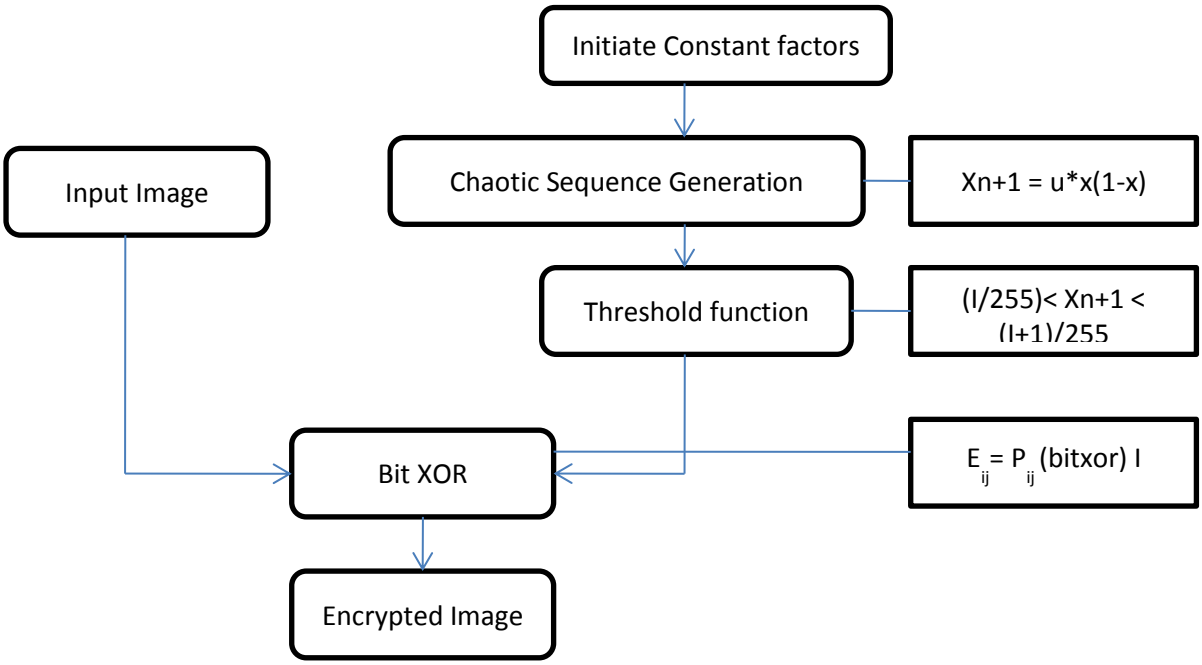


Fig 3.2: Chaos Model

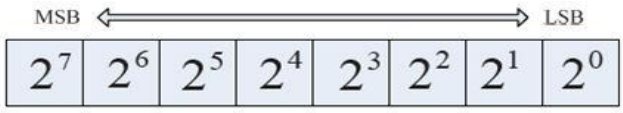
3.3 JPEG2000 Compression technique:

Huffman coding is a lossless data compression technique. JPEG2000 compression technique mainly works on Huffman coding. As the Huffman coding and JPEG2000 work on the same lossless compression technique. Huffman coding is based on the frequency in image pixel that is the data item. JPEG2000 compression technique is use to code the data at the lower bit in the image pixel. The lower number bits is use to encode into the binary codes data, this is done frequently. It is used in JPEG files also. JPEG 2000 is based on the discrete wavelet transform for data compression or image compression standard. Discrete Wavelets transform satisfies the mathematical requirement and they are used to represent in the data or other functions.

Huffman coding is use to encode the data at the lower frequency in the image. The principle of the Huffman coding is to encode the data at the lower bit. The encoded data is stored in the code book. Code book plus encoded data is use to transmute and to enable for decoding.

3.4 LSB substitution:

The most frequently used steganography method is the technique of LSB substitution. In a gray-level image, every pixel consists of 8 bits. One pixel can hence display 28=256 variations. The weighting configuration of an 8-bit number is illustrated in Figure 4.



The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB method is: x represents the i th pixel value of the stego-image, i x represents that of the original cover-image, and i m represents the decimal value of the i th block in confidential data. The number of LSBs to be substituted is denoted as k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:
Hence, a simple permutation of the extracted i m gives us the original confidential data. This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly.

3.5 QUALITY MEASURES FOR IMAGE

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σq2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

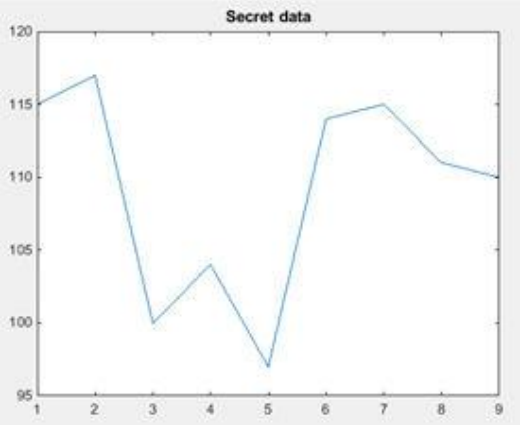
$$\text{MSE} = \sigma_q^2 = \frac{1}{N} \sum_{j,k} (f[j,k] - g[j,k])^2$$

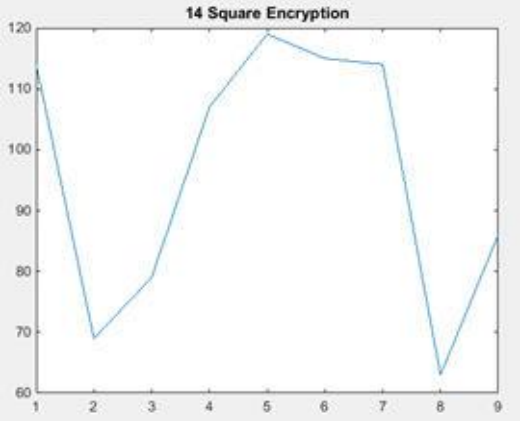
Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

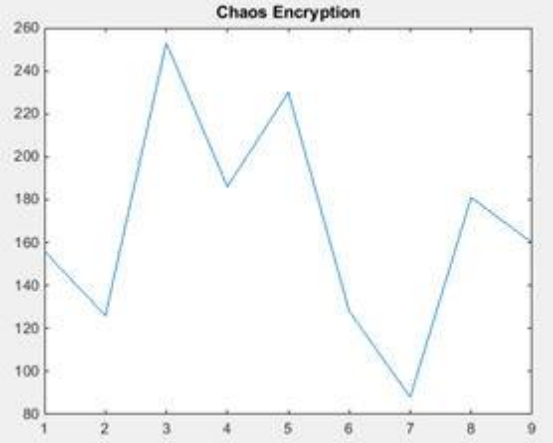
$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{MSE}\right)$$

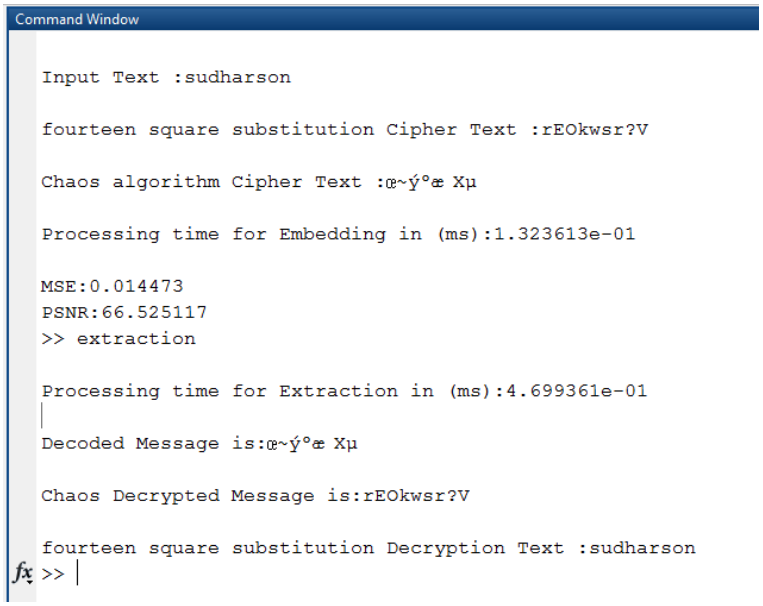
Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

4. RESULTS & DISCUSSION:

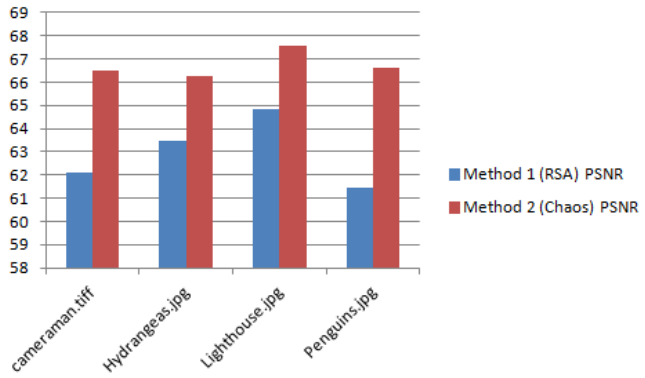


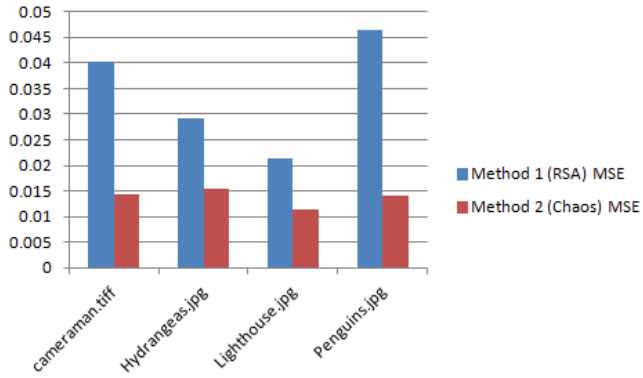






S.no	Input image	Method 1 (RSA)		Method 2 (Chaos)	
		MSE	PSNR	MSE	PSNR
1	cameraman.tiff	0.040317	62.075928	0.014473	66.52511
2	Hydrangeas.jpg	0.029235	63.471702	0.015316	66.27930
3	Lighthouse.jpg	0.021282	64.850657	0.011375	67.57112
4	Penguins.jpg	0.046535	61.453013	0.014122	66.63198





6. CONCLUSION:

In this paper dual encryption and dual decryption is done. In this project we can take any jpeg image to hide the secrete data. In this project we have implemented the fourteen square algorithm and chaos algorithm. In this base paper the LZW compression technique with RSA encryption and it is use to transmit the data using the discrete cosine transform. But there are some drawback, so to overcome these drawback we have implemented the chaos algorithm, JPEG2000 compression with the discrete wavelet transform and in additional to increase the security level, one encryption level has been increased that is the fourteen square algorithm.

Various parameters are used for testing the image Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE) has been proposed. The extracted stego image is perceptually similar to the original secret image. Mainly this paper is compatible for video and image processing using same algorithm.

REFERENCES:

1. Gandharba Swain, Saroj Kumar Lenka, ”Steganography using the Twelve Square Substitution Cipher and Index Variable”,IEEE transactions on Image Processing, 2011.

2. Saleh Saraireh. "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.
3. Geeta Kasana , Kulbir Singh "Steganography Technique for JPEG2000 Compressed Images Using Histogram in Wavelet Domain" Vol.8, No.6 (2014).
4. Manoj, I. V. S., "Cryptography and Steganography". International Journal of Computer Applications (0975–8887), Vol.1, No.12, 2010.
5. Saleh Saraireh. "A Secure Data Communication System UsingCryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.
6. Rajyaguru, M. H., "Combination of Cryptography and Steganography With Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, Vol.2, No.10, 2012, pp 329-332.
7. Kekre, H. B., Sudeep D. Thepade dan Ratnesh N. Chaturvedi. 2013. Novel Transformed Block Based Information Hiding Using Cosine, Sine, Hartley, Walsh and Haar Transforms. International Journal of Advances in Engineering &Technology, Vol. 6, No. 1, Hal. 274-281.
8. Singh, Dr. Ajit dan Meenakshi Gahlawat. 2013. Secure Data Transmission using Watermarking and Image Compression. International Journal of Advanced Research in Computer Engineering & Technology, Vol. 2, No.5, Hal. 1709-1715.
9. Katzenbeisser, S. and Petitcolas, F.A.P. 2000, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.
10. T. Morkel, J. Eloff, and M. Olivier, ―An overview of image steganography, In Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), (Sandton, South Africa, Jun/Jul. 2005).
11. M. Kharrazi06, H. Sencar, and N. Memon, ―Performance study of common image steganography and steganalysis techniques,Communications of the SPIE and IS&T, 15, No.4, pp. 1017-9909, Oct-Dec., 2006.
12. Varsha and Dr. Rajender singh Chhillar-Data Hiding using steganography and cryptography (IJCSMC) vol 4, Issue 4, April 2015.
13. Saleh Saraireh-A secure data communication system using cryptography and steganography (IJCNC) Vol 5, no.3, may 2013.
14. Geeta Kasana, Kalbir singh and Satvinder Singh Bhatia- Steganography technique for JEPG2000 compression image using histogram in wavelet domain, International journal of security and its application vol 8, no. 6 2014.
15. Hemlata H. Patil, S. P. Hingway- Improved way of image steganography for JPEG2000 compression standard by using EBCOT (SIPIJ) vol 4, no. 1,feb 2013.