IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**

***(Volume2, Issue5)***

Available online at: www.Ijariit.com

# Image Encryption Using Huffman Coding for Steganography, Elliptic Curve Cryptography and DWT for Compression

**Lavisha Sharma**[1]
*Computer Science Department, Sri Sai University*
sharma.lavisha88@gmail.com

**Anuj Gupta**[2]
*Computer Science Department, Sri Sai University*
anujgupta3588@yahoo.com

***Abstract- An abstract is a brief summary of a research article or in-depth analysis of a particular subject or discipline, and is often used to help the reader quickly ascertain the paper's purpose. Images can be encrypted in several ways, by using different techniques and different encryption methods. In this paper, I am using Huffman Coding method for image steganography, Elliptic Curve Cryptography for image encryption and Discrete Wavelet Transform for image compression. In my work I am using steganography, encryption and compression all together on the image data. After applying all these techniques on image data it results in an encryption method which is highly secure. For the implementation of the proposed work we are using Matlab software.***

***Index Terms- Cryptography, Huffman Coding, Elliptic Curve Cryptography, Discrete Wavelet Transform.***

## I. INTRODUCTION

Today the whole world is almost entirely dependent on inter-networks and information systems. Each user wants his/her private message to be sent to the intended receiver securely over the internet. The system that is accepted to send data over the internet must guarantee that no intruder is able to see the original message by breaking the original code through which the message is enciphered. For this, different cryptosystems have been used.

This is a general technique for coding symbols based on their statistical occurrence frequencies (probabilities). The pixels within 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. Huffman code is a prefix code. This means that the (binary) code of any symbol is not the prefix of the code of any other symbol. Most image coding standards use lossy techniques in the earlier stages of compression and use Huffman coding as the final step. Huffman coding is an entropy encoding algorithm.

Out of all the cryptosystems, the Elliptic Curve Cryptosystem is by far the most secured. The main attraction of Elliptic Curve Cryptography is that it provides the same level of security as Diffie-Hellman or RSA but with much shorter keys. For shorter key length, ECC has more advantages: higher speeds, lower power consumption, bandwidth savings and storage efficiencies. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability or storage are needed. Such applications include Chip card, Electronic commerce, Web servers, Cellular telephones, Pagers etc. ECC is mainly used in Key exchange mechanism, Digital signature and certificate.

Also wavelets are best suited to time-limited data and wavelet based compression technique maintains better image quality by reducing errors. DWT is by far the best compression standard. Wavelets have the great advantage of being able to separate the fine details in a signal. Very small wavelets can be used to differentiate very fine details in a signal, while very large wavelets can identify coarse details.

## II. LITERATURE SURVEY

**In[1]:** S **V V Sateesh, R Sakthivel, K Nirosha, Harish M Kittur**: In this manuscript, auhors implemented a new architecture simultaneous for image compression and encryption technique suitable for real-time applications. Here, contrary to traditional compression algorithms, only special points of DCT outputs are calculated. For the encryption process, LFSR is used to generate random number and added to some DCT outputs. Both DCT algorithm and arithmetic operators used in algorithm are optimized in order to realize a compression with reduced operator requirements and to have a faster throughput.

**In[2]: S. Ashwin, S. Aravind Kumar, J. Ramesh, K. Gunavathi:** The author's here gives a short survey on diverse types of steganography techniques for image in spatial and transform domains Although only some of the main image steganographic techniques were discussed in this paper. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one system lacks in payload capacity, the other lacks in robustness.

**In[3]: M. Mozammel Hoque Chowdhury and Amina Khatun:** In this research the author suggests a new image compression scheme with pruning proposal based on discrete wavelet transformation (DWT). The effectiveness of the algorithm has been justified over some real images, and the performance of the algorithm has been compared with other common compression standards.

**In[4]: V.V.Divya, S.K.Sudha and V.R.Resmy**: In the proposed work, the image to be encrypted is decomposed into 8X8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT ,Then, only selected DCT coefficients i.e. the DCT coefficients correlated to the higher frequencies of the image block are encrypted. For encryption the DCT coefficients are xored with pseudorandom bit, Pseudorandom bit is generated by Non-Linear Shift back Register. To enhance the security further the unencrypted DCT coefficients are shuffled, since some information may also be stored in DCT coefficient correlating to lower frequency.

**In[5]: Bhonde Nilesh, Shinde Sachin, Nagmode Pradip, D.B. Rane:** This Project presents an approach towards MATLAB implementation of the Discrete Wavelet Transform (DWT) for image compression. The design follows the JPEG2000 standard and can be used for both lossy and lossless compression. In order to reduce complexities of the design linear algebra view of DWT has been used in this concept.

**In[6]: Ashutosh Shukla, Jay Shah, Nikhil Prabhu:** The author here deals with encryption of image using Elliptic curve cryptography (ECC).Elliptic curve cryptography (ECC) is an approach to public key cryptography based on algebraic structure of elliptic curves over finite fields. Basic ElGamal elliptic curve encryption is used for encryption of the image. It brings about confidential, authentication and integrity in the exchange of data. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements.

**In[7]: Sourabh Singh, Anurag Jain:** In this paper a method is proposed which at first transforms the text into an image using an RGB substitution, and then encrypts the resulting image using AES Algorithm, under this approach, the secret key is smartly Sent along with the cipher text in a single transmission, thus it also Solves the key exchange problem that generally arises in most of The encryption models. The encryption and decryption process Make the use of a combination database for text to image Transformation.

**In[8]: Dr. ParmaNand Astya, Ms. Bhairvee Singh, Mr. Divyanshu Chauhan:** In this paper the image is considered to be in the form of a grid, is first transformed on an elliptic curve. These points or coordinates are then encrypted and send to the recipient. At the receiver end decryption algorithm is used to convert the encrypted image into the original image. Brute force attack is infeasible for ECC because of the discrete logarithmic nature of elliptic curves. This paper presents the technique to encrypt and decrypt the digital image (BMP) from Elliptic Curve Cryptography.

**In[9]: Rupali Srivastava, O. P. Singh:** In this paper, authors introduced block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm cipher block chaining (CBC) using key generation. In this algorithm the original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Block Based algorithm.

**In [10]: Satwinder Singh and Varinder Kaur Attri:** In this paper authors present the dual layer of security to the data, in which first layer is to encode data using Least Significant Bit image steganography method and in the second layer encrypt the data using Advance Encryption Standard Algorithm. Steganography does not replace the encryption of data, instead it provides extra security feature to it. In our work secret text message is hiding behind the digital image file and this image file is then encrypted using AES encryption algorithm.

**In[11]: Pooja Rani , Apoorva Arora:** In this research, a hybrid image security framework has been proposed, which will be implemented by combining various techniques together to achieve the image security goal. The techniques included in the combination would be image compression, cryptography and steganography. DWT compression has been used, because it is a stronger compression algorithm. The steganography image would be compressed to reduce its size. Blowfish encryption algorithm would be used for the encryption purposes. It offers maximum throughput (faster) and also energy efficient.

**In[12] Hayder Raheem Hashim, Irtifaa Abdalkadum Neamaa:** In this paper, a particular public key cryptosystem called the ElGamal Cryptosystem is presented considered with the help MATLAB Program to be used over Images. Since the ElGamal cryptosystem over a primitive root of a large prime is used in messages encryption in the free GNU Privacy Guard software, recent versions of Pretty Good Privacy (PGP), and other cryptosystems.

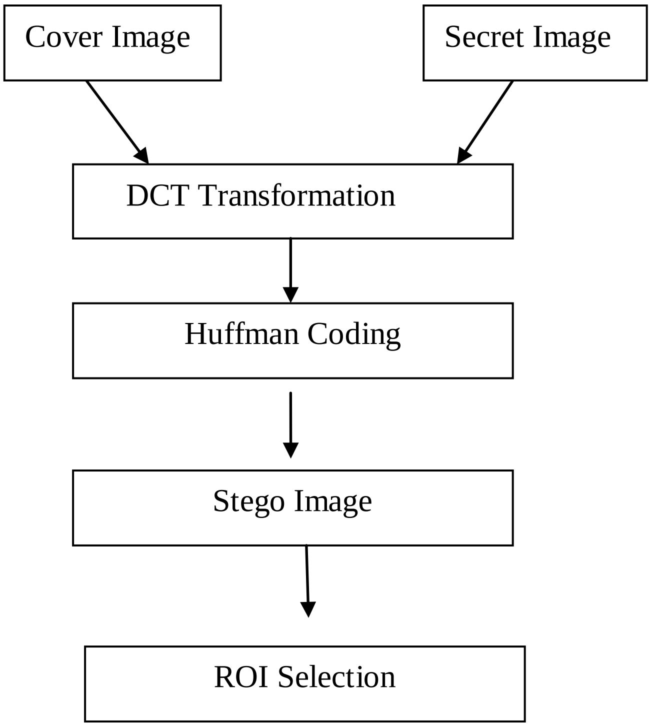
## III. PROPOSED METHODOLOGY

Various steps are:

1) To implement steganography Huffman coding technique is used.

2) Encryption is implemented by using ECC (Elliptic Curve Cryptography) algorithm.

3) To reduce the storage space used to store digital images, DWT (Discrete Wavelet Transform) technique is used along with EZW compression method.



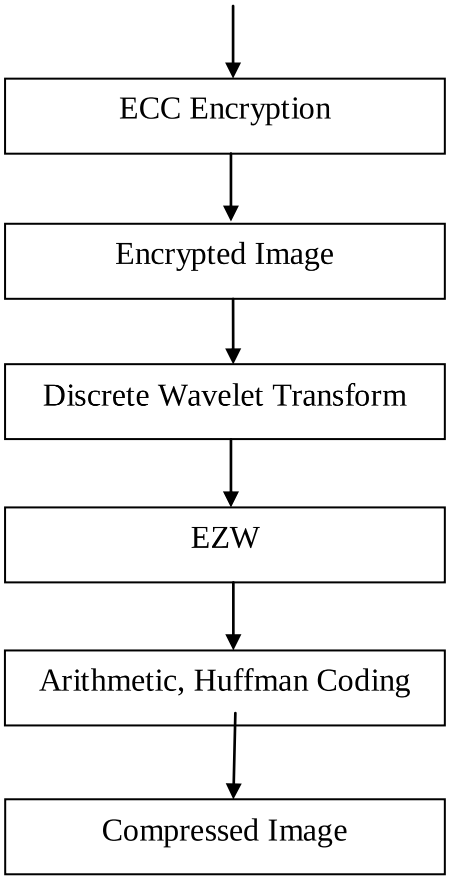


Fig. 1 Flow Chart of image encryption process

*A. Step 1: Steganography*

Huffman encoding is used for hiding a large amount of data with high security, good invisibility and no loss of secret message.
The main objective is to develop a procedure which will provide a better security to the secret image without compromising on the quality of the stego image.

Various Steps in Message Embedding:

**1)** Apply DCT on cover image on block wise by dividing it into block of size 8*8 to get DCT blocks.
**2)** Encode the message image using Huffman Coding.
**3)** Each DCT block is quantized by using standard Quantization matrix of scale factor 0.001.
**4)** Encoded message bits, Huffman table bits and message image dimensions information bits are embedded into LSB of quantized DCT coefficients in binary form.
**5)** Apply de-quantization and inverse DCT to get the stego image.

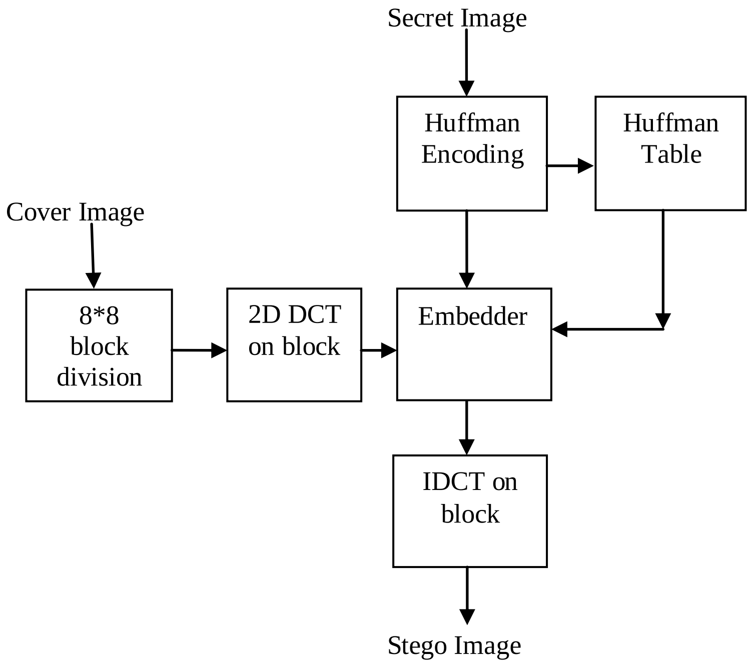


Fig. 2 Insertion of the Secret Image into a Cover Image (Message Embedding)

*B. Step 2: Encryption*

An elliptic curve is not an ellipse! The reason for the name is a little more indirect. It has to do with "elliptic integrals", which occurs in computing the arc length of an ellipse. An elliptic curve has different and much more appealing properties as compared to an ellipse.

An Elliptic Curve is a curve given by an equation of the form:

$$y^2 = x^3 + ax + b$$

Where *x,y,a,b* belong to R(real numbers), Q(rational numbers), C(complex numbers) or Fp(finite field).

Various Steps in Encryption

1) At first step an ROI (Region of Interest) is selected.
2) Then ECC algorithm is applied on the selected ROI.

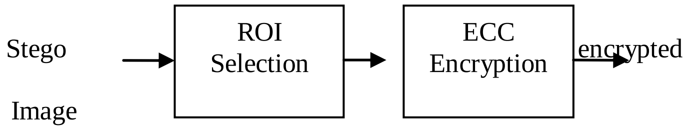


Fig. 3 Process of Encryption

*C. Step 3: Compression*

Steps in Image Compression
1) Discrete Wavelet Transform.
2) Embedded Zerotree Wavelet Compression.
3) Huffman and Arithmetic Coding.

Wavelets are signals which are local in time and scale and generally have an asymmetrical shape. A wavelet is a waveform of effectively limited duration that has an average value of zero. A wavelet transform can be used to decompose a signal into component wavelets. Once this is done the coefficients of the wavelets can be decimated to eliminate some of the details. Wavelets have the great benefit of being able to separate the fine details in a signal. Various types of wavelets are: Haar, Morlet, Daubechies, etc.

It decomposes images into wavelet coefficients and scaling function. In Discrete Wavelet Transform, signal energy concentrates to specific wavelet coefficients. This characteristic is useful for compressing images. Image consists of pixels that are arranged in two dimensional matrixes, each pixel represents the digital equivalent of image intensity. In spatial domain neighboring pixel values are highly correlated and hence redundant. In order to compress images, these redundancies existing among pixels needs to be eliminated. DWT processor transforms the spatial domain pixels into frequency domain information that are represented in multiple sub-bands, representing different time scale and frequency points.

*1) Embedded Zerotree Wavelet Compression:* The concept of EZW compression is given by Shapiro's. The embedded zerotree wavelet algorithm (EZW) is a simple, yet remarkably effective, image compression algorithm, having the property that the bits in the bit stream are generated in order of importance, yielding a fully embedded code. EZW is a lossy image compression algorithm.

EZW Algorithm:

1) Determine the initial threshold.

$T_0 = 2[\log_2(MAX|\gamma(x,y)|)]$

Where, (*x*,*y*) denotes the coefficient.

MAX(.) means the maximum coefficient value in the image.

2) After that two passes are used to code the image.

a) Dominant Pass

b) Subordinate Pass

Dominant Pass: At this step image is scanned and symbol is output for every coefficient. Dominant List consists of coordinates of coefficients not yet found significant.

Subordinate Pass: It is the refinement pass. Subordinate List consists of magnitudes of coefficients already found to be significant.

*2) Arithmetic Coding:* Arithmetic coding is a data compression technique that encodes data (the data string) by creating a code string which represents a fractional value on the number line between 0 and 1. . Each symbol of input data narrows this interval. As interval becomes shorter, bits needed to specify it increases.

The coding algorithm is symbol wise recursive; i.e., it operates upon and encodes (decodes) one data symbol per iteration or recursion. On each recursion, the algorithm successively partitions an interval of the number line between 0 and 1, and retains one of the partitions as the new interval. Thus, the algorithm successively deals with smaller intervals, and the code string, viewed as a magnitude, lies in each of the nested intervals.

Arithmetic Coding Algorithm

1) We began with correct interval initialized to [0, 1].

2) For each symbol of file, we perform two steps:

a) We subdivide the correct interval into sub-intervals, one for each alphabet symbol. The size of symbol's sub-interval is proportional to the estimated probability that a symbol will be next symbol in the file according to model of input.

b) We select the sub-interval corresponding to the symbol that occurs next in the file and make it the new current interval.

## IV. RESULTS

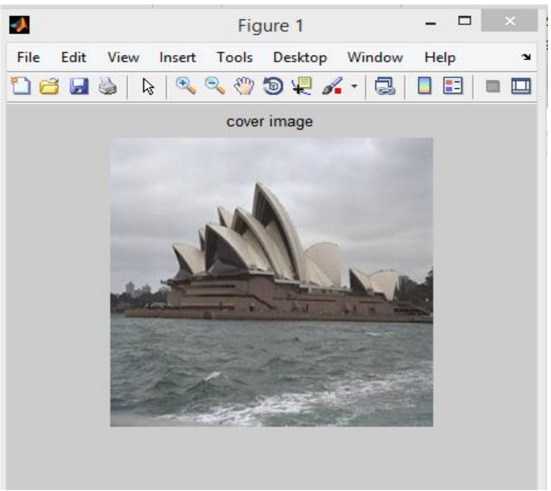


Fig. 4 Cover Image

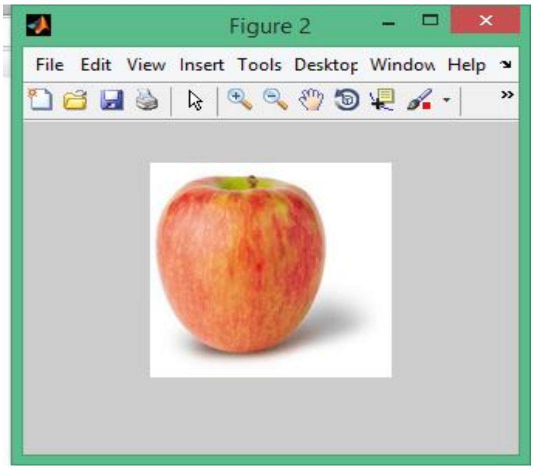


Fig. 5 Secret Image

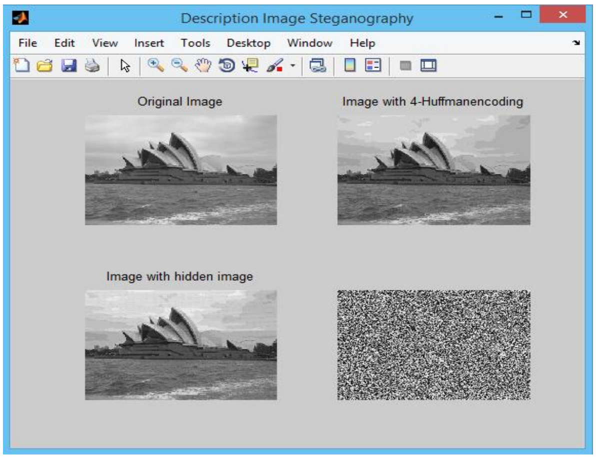

Description Image Steganography
File Edit View Insert Tools Desktop Window Help
Original Image
Image with 4-Huffmanencoding
Image with hidden image

Fig. 6 Output of Steganography and Encryption

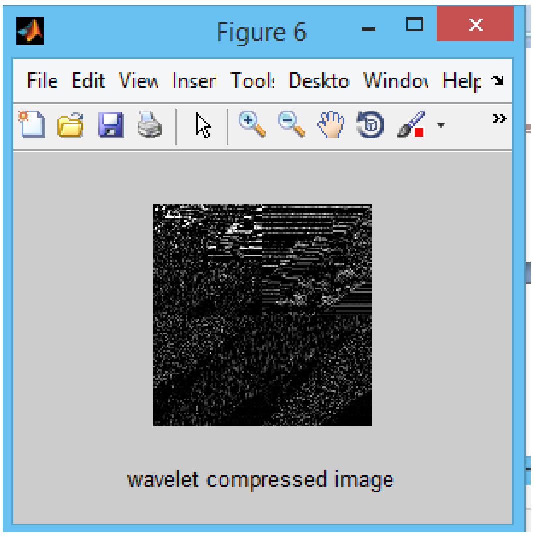


Fig. 7 Compressed Image

| IMAGES TAKEN | PSNR | MSE | Compression ratio |
|---|---|---|---|
| | 45.035 | 2.0556 | 12.5 |
| | 64.004 | 0.0261 | 12.5 |
| | 50.646 | 0.5647 | 6.4 |

| | | | |
|---|---|---|---|
| | 47.860 | 1.0726 | 42.3 |
| Riverside Yorba Linda Placentia Corona Anaheim Orange Santa Ana Irvine Lake Forest Mission Viejo Laguna | 50.699 | 0.5579 | 42.3 |

Table 1 Results of proposed work

## V. CONCLUSION

In my work I am using steganography, encryption and compression all together on the image data. For steganography I am using Huffman Coding, for encryption purpose I am using Elliptic Curve Cryptography and for compression I am using Discrete Wavelet Transform. After applying all these techniques on image data it results in an encryption method which is highly secure. The values of PSNR, MSE and Compression Ratio for encryption of images are highly acceptable in my work. For the implementation of this proposed work we are using Matlab software.

## REFERENCES

[1] Pooja Rani ,Apoorva Arora , *'Image Security System using Encryption and Steganography'*, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June 2015.

[2] Satwinder Singh and Varinder Kaur Attri , *'Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm'*, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 8, No. 5 (2015), pp. 259-266 .

[3] Sourabh Singh, Anurag Jain, *'An Enhanced Text to Image Encryption Technique using RGB Substitution and AES'*, International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5- May 2013.

[4] Rupali Srivastava,O.P. Singh, *'Performance Analysis of Image Encryption Using Block Based Technique'*, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , Vol. 4, Issue 5, May 2015.

[5] Hayder Raheem Hashim, Irtifaa Abdalkadum Neamaa, *'Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB'*, International Journal of Sciences: Basic and Applied Research (IJSBAR) ISSN 2307-4531.

[6] V.V.Divya, S.K.Sudha and V.R.Resmy, *'Simple and Secure Image Encryption'*, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012 ISSN (Online): 1694-0814.

[7] SVV Sateesh,R Sakthivel,K Nirosha,Harish M Kittur, *' An optimized architecture to perform image Compression and encryption simultaneously using Modified dct algorithm'*, IEEE 2011.

[8] S. Ashwin, S. Aravind Kumar, J. Ramesh, K. Gunavathi, *' Novel and Secure Encoding and Hiding Techniques using Image Steganography: A Survey'*, IEEE 2012.

[9] Ms. Pallavi M. Sune, Prof. Vijaya K.Shandilya, *' Image Compression Techniques based On Wavelet and Huffman Coding',* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN: 2277 128X.

[10] Rajinder Kaur, Er.Kanwalprit Singh, *'Image Encryption Techniques:A Selected Review'*, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013).

[11] Ronak Doshi, Pratik Jain, Lalit Gupta, *'Steganography and Its Applications in Security',* International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012.

[12] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal, *'A Review on Different Image Steganography Techniques',* International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014.

[13] Ashutosh Shukla, Jay Shah, Nikhil Prabhu, *'Image encryption using elliptic curve cryptography'*, International Journal of Students Research in Technology & Management Vol 1(2), April 2013.

[14] Dr. ParmaNand Astya, Ms. Bhairvee Singh, Mr. Divyanshu Chauhan, *'Image encryption and decryption using elliptic curve cryptography'*, International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.3, Issue No.10, October 2014.

[15] Mrs. Megha Kolhekar, Mrs. Anita Jadhav, '*Implementation of elliptic curve cryptography on text and image'*, International Journal of EnterpriseComputing and Business Systems Vol. 1 Issue 2 July 2011.

[16] Bhonde Nilesh, Shinde Sachin, Nagmode Pradip, D.B. Rane, *'Image Compression Using Discrete Wavelet Transform',* International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 3, Special Issue, March-April 2013.

[17] M. Mozammel Hoque Chowdhury and Amina Khatun, *'Image Compression Using Discrete Wavelet Transform'*, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012.

[18] Dipalee Gupta, Siddhartha Choubey, *'Discrete Wavelet Transform for Image Processing',* International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 3, March 2015.

[19] Rajinder Kaur, Er. Kanwalpreet Singh, *'Comparative Analysis and Implementation of Image Encryption Algorithms'*, International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 4, April 2013.

[20] Shivangi Goyal, *' A Survey on the Applications of Cryptography'*, International Journal of Science and Technology Volume 1 No. 3, March, 2012.

[21] Richa Goyal, Jasmeen Jaura, *'A Review of Various Image Compression Techniques'*, International Journal of Advanced Research in Computer Science and Software Engineering
Volume 4, Issue 7, July 2014.

[22] Cryptography and Network Security (Principles and Practices)-Fifth Edition by William Stallings.