International Journal of Research in Science and Technology http://www.ijrst.com

(IJRST) 2016, Vol. No. 6, Issue No. III, Jul-Sep **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

IMAGE ENCRYPTION USING STEGNOGRAPHY, ELLIPTIC CURVE CRYPTOGRAPHY AND COMPRESSION

Lavisha Sharma[1], Anuj Gupta[2]

Computer Science Department, Sri Sai University Palampur (H.P)

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, a general introduction about cryptography is given. The concept of image encryption/decryption, stegnography and data compression is also explained. 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 this proposed work we are using Matlab software.

Index Terms- *Cryptography, Steganography, Image Encryption, Image Compression.*

INTRODUCTION

Image encryption decryption has become an important research area and it has broad application prospects. The field of encryption is becoming very important in the present era. Image security is of utmost concern as web attacks have become more and more serious. Image encryption decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication.

To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

The word "Steganography" is a Greek word which means "covered or hidden writing". In other words Steganography is technique of hiding information behind the cover medium. Steganography can be done with Text, images, video, audio media. Images have a large amount of redundant data and for this reason it is possible to hide message inside image file. Image Steganography requires following elements to carry out the work:

- **Cover medium:** It is an image that holds secret message.
- **The Secret message:** it is message to be transmitted. It can be plain or encrypted text, images or any other data.
- **The Stego-key:** it is key used to hide the message.

In Data Encryption, data is converted from its original to other form so that information cannot be accessed from the data without decrypting the data i.e the reverse process of encryption. The original data is usually referred as plain data and the converted form is called cipher data. Encryption can be defined as the art of converting data into coded form which can be decode by intended receiver only who poses knowledge about the decryption of the ciphered data. Encryption can be applied to text, image, video for data protection.

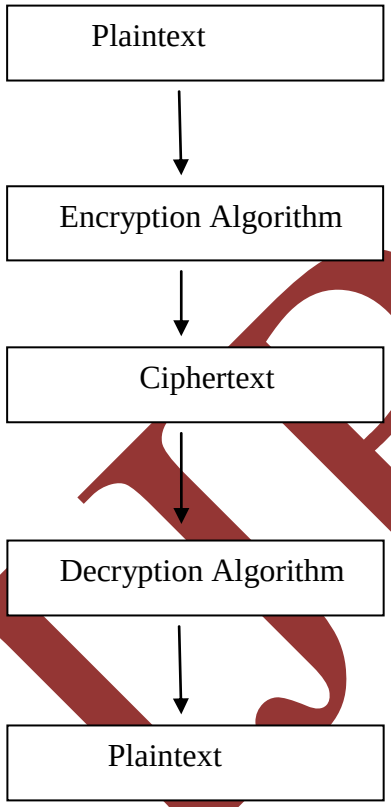

Figure 1.1 Encryption/Decryption Process

Although RSA and ElGamal are secure asymmetric-key cryptosystems, they use either integer or polynomial arithmetic with very large numbers/polynomials imposes a significant load in storing and processing keys and messages. An alternative is to use elliptic curves offers same security with smaller bit sizes, newer, but not as well analyzed. ECC is an approach to public key cryptography based on the

algebraic structure of elliptic curves over finite fields. Its security is based on the possibility of efficient additive exponentiation and absence of efficient (classical) algorithms for additive logarithm.

Compression is a process by which the depiction of computerized information is modified so that the competence necessary for storing or the bit-rate required for transmitting it is reduced. Since image files not only occupy storage but also take up a large portion of bandwidth during transmission, the process of compressing images has become a necessity. Compression reduces the utilization of exclusive resources such as hard disk space or communication bandwidth. There are two types of compression techniques namely Lossy and Lossless compression.

By image compression we mean to reduce the storage space required to store the digital images. The objective of compression is to reduce the number of bits as much as possible, while keeping the visual quality of the reconstructed image as close to the original image as possible. Image compression systems are composed of two distinct structural blocks: an encoder and a decoder.

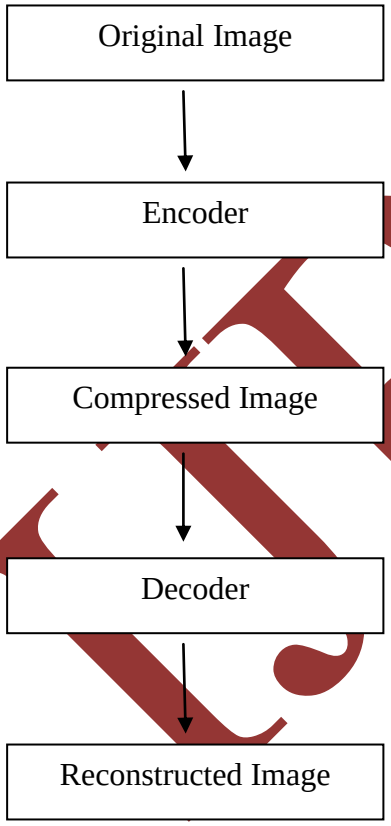

Figure 1.2 Block Diagram of Image Compression System

CHARACTERISTICS OF IMAGE ENCRYPTION SYSTEM

For studying image encryption, we must first analyze the implementing differences between image and text data:

1) At the receiver end, the decrypted text must be equal to the original text in a full lossless manner. This requirement is not necessary for image; the cipher image can be decrypted to a original image in some lossy manner.

2) Text data is a sequence of words, it which can be encrypted directly by using block or stream ciphers. However, digital image data are represented as 2D array.

3)Since the storage space of a picture is very large, it is inefficient to encrypt or decrypt image directly. One of the best methods is to only encrypt/decrypt information that is used by image compression for reducing both its storage space and transmission.

LITERATURE REVIEW

[1] Pooja Rani , Apoorva Arora: In this research, a hybrid image security framework has been proposed to overcome the problem stated earlier, 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 steganographed 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. Compressed image would be encrypted to enhance the image security. Real image will be hidden into another image. A cluster based steganographic technique will be used.

[2] Satwinder Singh and Varinder Kaur Attri: In this paper the author present 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.

[3] Sourabh Singh, Anurag Jain: In this paper a method is proposed which 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. This paper is divided into four sections; Section- I, presents basic introduction of Network Security, In section-II, a survey on related algorithms has been presented, Section-III discusses the proposed model and section IV concludes the paper.

[4] Rupali Srivastava, O. P. Singh: This paper introduce 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. There are many measures for examining image quality, such as the Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). It is computed by averaging the squared intensity differences of distorted and original image pixels, along with the related quantity of the PSNR.

[5] 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. This paper shows a modification of the cryptosystem by applying it over gray and color images. That would be by transforming an image into its corresponding matrix using MATLAB Program, then applying the encryption and decryption algorithms over it.

[6] 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. The bits generated by Non-Linear Shift back Register cannot be predicted so cryptanalysis becomes difficult. 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, While encrypting selected DCT coefficients alone will provide complete perceptual encryption, it would be possible for an attacker to gain information about the image from the other coefficients, especially in images that have a lot of edges.

[7]: S V V Sateesh, R Sakthivel, K Nirosha, Harish M Kittur: In this manuscript, authors 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. High Performance Multiplier (HPM) is being used for integer

multiplications. Simulation results show the compression ratio around 66% and a PSNR about 24dB. The throughput of this architecture is 624 M samples/s with a clock frequency of78 MHz.

[8] S. Ashwin, S. Aravind Kumar, J. Ramesh, K. Gunavathi: The paper describes 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, one can see that there exists a large assortment of approaches to hiding information in images. 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.

[9]: Ms. Pallavi M. Sune, Prof. Vijaya K. Shandilya: This paper discusses about the image classification, wavelet compression, and converted an image into an array using Delphi image control tool. Image control can be used to display a graphical image Icon, Bitmap, metafile, GIF, JPEG, etc then an algorithm is created in Delphi to implement Huffman coding. Hence image compression has proved to be a valuable technique as one solution. The Wavelet Compression Engine was used in this study. In this paper we have to present classification of image, and Normalized Information Distance (NID) is measure, and wavelet of image compression. The best technique Huffman coding in lossless compression, in that the image uncompressed need have some specific knowledge of the symbol of probabilities in the compressed files and this can need more bit to encode the file also Huffman coding required two passes if the information is unavailable compressing the file: find frequency of each symbol and construct tree Huffman to compress the file.

[10] Dr. ParmaNand Astya, Ms. Bhairvee Singh, Mr. Divyanshu Chauhan : In this paper the image which 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.

[11] Ashutosh Shukla1, Jay Shah2, Nikhil Prabhu: This paper 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.

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] 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 ISSN-2319-8354(E).

[11] 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.

[12] Willian Stalliangs, 'Cyptography and Network Security', Fifth Edition.