ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.7

Secured Data Transmission using Advanced Image Watermarking

Umaira[1], Divya .K..K[2]
M.Tech Student[1, 2]
Department of Computer Science and Engineering
P.A College of Engineering, Mangalore, Karnataka, India

Abstract:
Protection of information that is transmitted over the network is the major issue in today's world. Hacking, copyrighting or modification of data makes the information unusable. Securing of confidential data can be achieved by using cryptography and steganography. In this paper we are proposing a new methodology for the protection of data by using both steganography and cryptography. Cryptography makes the data meaningless preventing the hacker from reading the original data. By using steganography we can hide the encrypted data within the host data (image, audio or video). Here, in the proposed system the secret message is encrypted to make the data unreadable and then using image watermarking technique, the encrypted data is embedded into the host image; this makes the data undetectable to the intruder. By using the proposed technique we can ensure that the data is safe even if the embedded image is in wrong hands.

Keywords: Cryptography, Image stenograph, Least Significant Bit (LSB), Steganography.

I. INTRODUCTION

Nowadays security of data has become a major concern. The growth of modern communication technologies imposes a special means of security mechanisms especially in case of data networks [1]. Sensitive information if exposed to some intruder may pose a threat to nation's security or company's critical decisions. Thus, such information must be secured at any cost and to serve the purpose there has been a trend to encrypt or hide the secret information. The two important techniques for providing security are cryptography and steganography [4]. Both are well known and widely used methods in information security. Encryption makes the data unstructured and meaningless and unintelligible. At the source, confidential data is encrypted using encryption techniques; at the receiver end encrypted data called cipher data is decoded to the original form using the same technique that is used at the sender side. This encryption can be done in many ways. Cryptography may draw the suspicion of the intruder towards the data that is in encoded format. Steganography (composed of Greek word 'steganos', meaning covered and 'graphein' meaning to write) on the other hand, is used to hide the data behind some other media. Steganography do not lure the eavesdropper as it hides the message. Steganography can be classified based on the type of media it uses to hide the data [2]. This paper proposes a new system to embed a secret message in a cover image using LSB insertion method with Additive type cipher algorithm. Our system is designed to encrypt data and hide all the data in image to keep the privacy of the data. Then, the rest of the paper is organized as follows: Description of proposed system architecture, Experimental results and discussion and conclusion of the research.

II. LITERATURE REVIEW

In paper "Image encryption and decryption with symmetric key cryptography", [5] published by Jai singh, kanaklata describes about Encryption method to work on Image Encryption & Decryption with Symmetric Key Cryptography. Author defines the encryption and decryption techniques using symmetric key. Symmetric key algorithms are the quickest and the most commonly used type of encryption. Here, a single key is used for both encryption and decryption. "Encrypted Steganography: A Combined Approach for Enhancing Image Security", [6] by Ripal Rathod, Darshan Mistry, Khushbu Patel, describes about digital watermarking. Which uses both cryptography and steganography, pixels of original image are displaced using Matrix Reordering method and then encrypted using Blowfish encrypting algorithm finally watermarked using LSB embedding method . This provides the double security to the data. "Robust watermarking of AES encrypted images for DRM systems", [7] by V.Chandra Prasad And S.Maheswari proposed a system in which the input image to be transmitted is separated into wavelet sub-bands using 1-level haar transform. AES encryption algorithm is proposed to encrypt the LL sub-band and Block DCT based watermarking algorithm is used to embed binary watermark in LH sub-band.
"Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption",[8] by Ms. Roshan Jahan presents a system is the combination of our different modules, they are as follows: Encryption of watermark image using chaotic encryption with GA , Embedding the encrypted watermark image into original image using DWT-SVD watermarking technique. , Extraction of the encrypted watermark image from the original image and Decryption of watermark image. Discrete Wavelet Transform (DWT) is a multi-resolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains. The basic is to decompose the image to sub images with different space and frequency, after that coefficient is processed. The watermark image is embedded directly on the elements of singular values of the original image's DWT sub bands.

III. PROPOSED METHOD

This paper is devised by developing a new security system with additional features in securing data where the data to be transferred are hidden by combining steganographic security technique with cryptography to ensure a confidential structure

in transferring options. A modified approach on symmetric encryption algorithm is encouraged in this paper for encryption of secret data and encrypted data file is made to be hidden in an image. In the proposed system, original data file from user is encrypted using a private key, the encrypted data is embedded into the image, and the watermarked image is transmitted over the public channel or the network. At the destination, ciphered information is extracted from the received image and decrypted using private key to get the original secret data back.

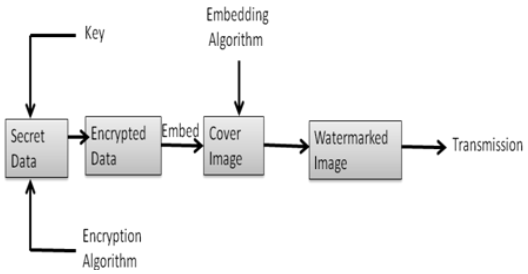

Figure.1. Block diagram for secret data encryption and watermarking.

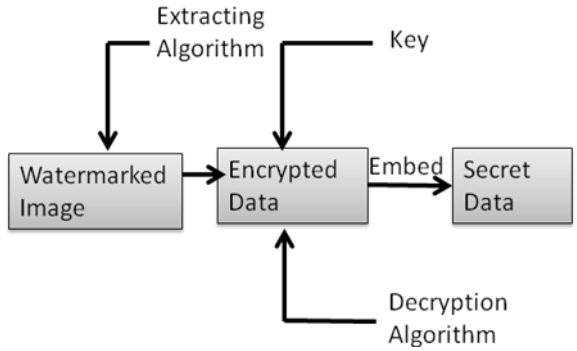

Figure.2. Block diagram for decryption and extraction of secret data.

At Source: Data Encryption and Image Watermarking**;** At the source, original data (text or image) from the user is encrypted using additive type encryption technique. Here we are using symmetric key encryption method. That is, same key for the encryption and decryption, to enhance the security we use feedback shift register key generation technique. In the proposed method, in case of text data, each character from file is added with key and in case of image, each image pixel RGB components with key. General form is,

Encrypted Data = Original Data + Key.

Feedback shift register is used to create key stream. Linear feedback shift register input is linear function of previous state. Linear function is XOR of third and sixth bits of shift register value.

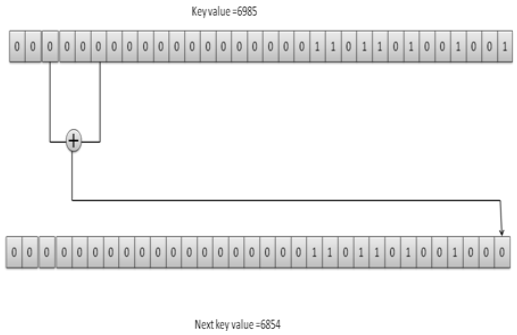

Figure.3. Feedback shift register.

After encryption, the cipher data is embedded to an image using LSB image watermarking technique. Embedding each bits from the encrypted data to the blue and green component of each pixel of an image. Host image for embedding the encrypted text data should be two times larger than the encrypted text file size, because each character of ciphered text requires two pixels from cover image. And in case of image, host image for embedding encrypted image should be six times larger than the encrypted image file size, because each pixels of ciphered image requires six pixels from cover image. Below show the algorithm for encryption and watermarking of image at source.

Algorithm at source:

Step 1: Enter secret data (text/image) file.

Step 2: Enter integer value as key.

Step 3: Enter cover image for embedding.

Step 4: For each character/pixels, using forward shift register, 3rd and 6th bits from key is XORed to generate unique key.

Step 5: For each bits from character/pixels add unique key to generate encrypted data.

Encrypted data = secret data + key

Step 6: Store the encrypted data to a file.

Step 7: Embed two-two bits from encrypted data to the last two LSB bits of green and blue components of each cover image pixels.

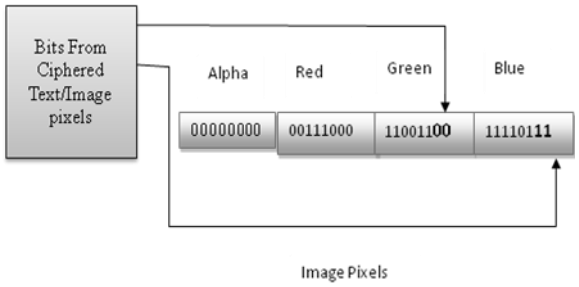

Figure.4. LSB Based Image watermarking.

At destination: Extraction of Encrypted Data and Decryption: Extracting two bits from each blue and green pixels of watermarked image. First, we extract the size of the encrypted data file, and then, extracting contents of encrypted data till the corresponding size that we extracted. Finally, the encrypted data that we extracted from the image is decrypted using the private key. The decryption process is reverse of the encryption process. Key values generated using shift function which is similar to the encryption key generation process. Below algorithm represents the proposed system at receiving side.

Algorithm at destination:

Step 1: Extract two-two bits from each green and blue components of watermarked image.

Step 2: Form the encrypted image/text file from the extracted data.

Step 3: For each encrypted data bits, subtract the unique key value from it. (unique key generation is using feedback shift register).

Original secret data= Encrypted data - key

Step 4: Store the decrypted data back to the file.

IV. RESULT AND ANALYSIS

The proposed system is executed using Net Beans 8.0.2 IDE and Java language to develop our system. Based on the findings in the existing papers studied, a new algorithm is

being proposed here can ensure all of the security principles i.e. robustness, confidentiality, authentication.

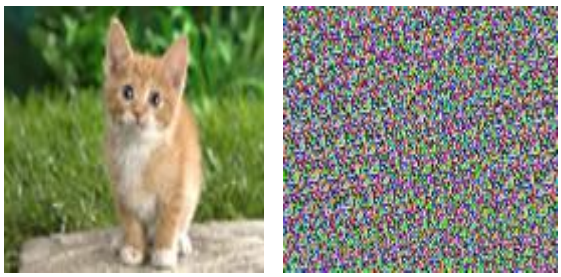

Figure. 5. (a): Original image and encrypted image.

Figure.6. (b) : Host image.

```
public class encdec {

   public void doencryption(int key, string inputfilename) throws ioex
        int limit = inputfilename.indexOf(".");
        string filename = inputfilename.substring(0, limit);

        File f = new File(inputfilename);
        int flen = (int) f.length();

        // char[]fchar=new char[flen];
        char[] echar = new char[flen];
        BufferedReader bis = null;

        BufferedWriter bfw = null;

        bfw = new BufferedWriter(new FileWriter(filename + "_enc"));

        bis = new BufferedReader(new FileReader(inputfilename));
        int key1 = key;
        for (int i = 0; i < flen; ++i) {
            int content = bis.read();
            if (content == -1) {
```

Figure .7. (c) : Original text data.

Figure. 8. (d): Encrypted text data.

Figure .9. (e): Watermarked image. `

Results of proposed system are shown above. Figure 5(a) represents the original image and encrypted image and 5(b) represents the original text from user that needs to be transmitted. Encrypted cipher text is represented in 5(c) , And in figure 5(d) shows host image and 5(e) shows the watermarked image that has cipher data inside it.

V. HISTOGRAM ANALYSIS

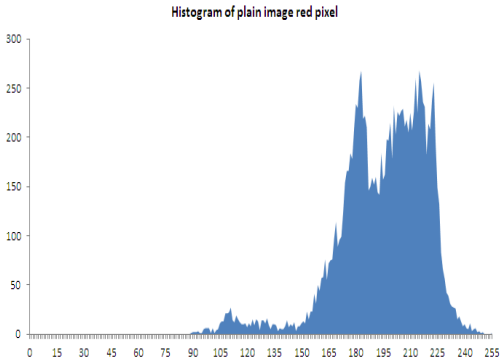

Figure.10.(a): Histogram of secret image Red pixel component values.

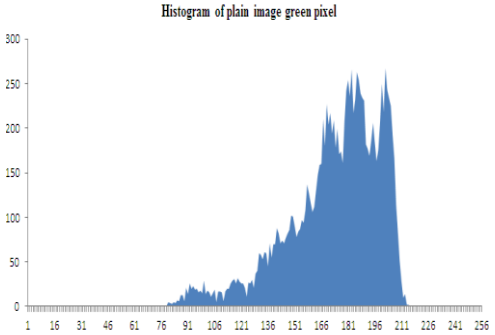

Figure.11.(b): Histogram of secret image Green pixel component values.

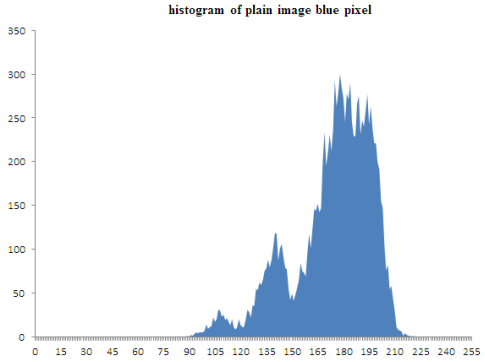

Figure.12.(c): Histogram of secret image Blue pixel component values.

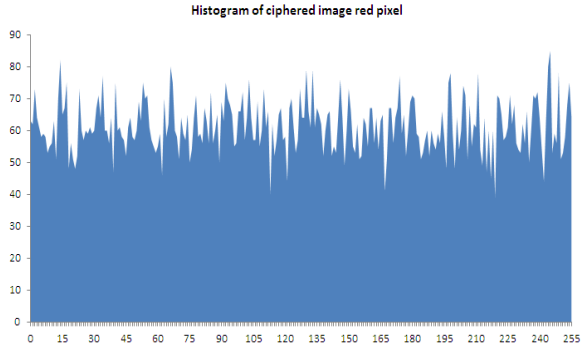

Figure.13. (d): Histogram of encrypted secret image Red pixel component values.

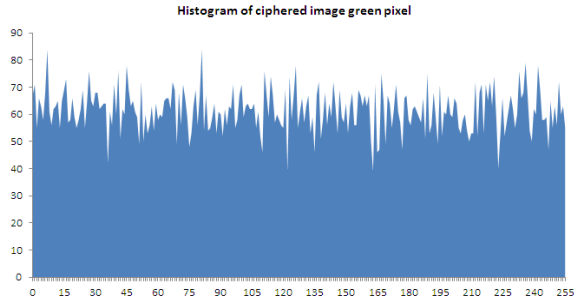

Figure.14. (e): Histogram of encrypted secret image Green pixel component values.

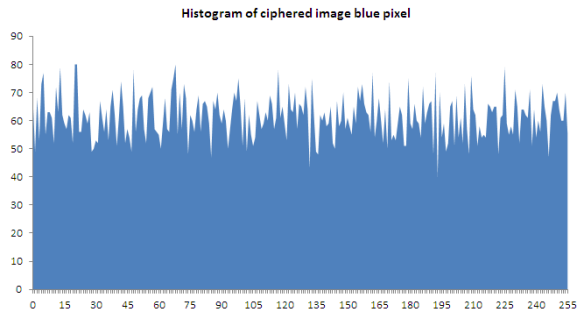

Figure.15. (f): Histogram of encrypted secret image Blue pixel component values.

The above figures show histogram of secret image and encrypted secret image. As results of this, we see in figure 6 the pixels distributions of the original image and the pixel distributions of the encrypted image. Encryption process returns noisy images. Histograms of encrypted images in figure 6(d), 6(e), 6(f) are very close to uniform distributions which are different from that of the corresponding original images in figure 6(a), 6(b), 6(c). These indicate high level of security against the attack.

Table. 1. Time required for encryption and decryption.

Size		Encryption Time(ms)		Decryption Time(ms)	
Text(kb)	Image(kb)	Text (ms)	Image (ms)	Text (ms)	Image (ms)
3	18	negligible	31	negligible	16
18	463	78	187	40	171

Table. 2. PSNR and MSE values.

Original Image	PSNR	MSE
Lena.png(463kb)	78.24	0.0010
VTU logo(44kb)	62.64	0.0015

Information Entropy Analysis:

Entropy is a measure of uncertainty. Entropy of a source gives idea about self information i.e., information provided by a random process about itself. Higher the value of entropy of cipher, better the security. Entropy near to 8, indicating that in the cipher text all the character occurs with almost equal probability. The entropy, H (m) of any message can be calculated as

$$\text{Entropy} = -\sum_{i} P_i \text{Log}_2 P_i$$

In our tests the average entropy of the Cat cipher image is 7.8771 and for the Lena cipher image is equal to 7.8671, which are very close to the optimal value, and here, we can justify that entropy is 7.87.

VI. CONCLUSION

Using proposed method we can secure the text data from the attackers. Using cryptography along with steganograpghy gives more security and confidentiality for the data. LSB based watermarking technique gives the robustness to the embedded text data and people can't detect that the image contains the secret data inside it. The technique of "Digital Watermarking" is the recent research in the field of multimedia and internet copyright protection. Further research is needed to make it work if the embedding/extraction is to be performed in real time. The security of information can further be improved by other techniques like exploring parallel algorithms, more complex key based encryption algorithms and embedding techniques.

VII. REFERENCES

[1]. Aprajita, Ajay Rana, "Steganography-The Art of Hiding Information-Comparison from Cryptography", International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753, Vol. 1(5), May 2013, pp. 1308-1312.

[2]. H.Kabetta, B.Y. Dwiandiyanta, Suyoto, "Information hiding in CSS: A secure scheme text-stegangraphy using public key Cryptosystem",IJCIS,pp. 13-22 ,Vol.1, No.1,December 2011.

[3]. S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, Dec 2012, pp. 171-177.

[4]. Mihir H Rajyaguru, "Crystography -Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012, pp. 329-332.

[5]. Jai singh, kanaklata and Javed Ashraf on "image encryption and decryption with symmetric key cryptography", International Journal of Current Engineering and Technology)(2015).

[6]. Ripal Rathod, Darshan Mistry Khushbu Patel, "Encrypted Steganograpghy: A Combined Approach for Enhancing Image Security", International Journal of Innovative Research in

Computer and Communication Engineering, ISSN: 2320-9801, Vol.4, May 2016.

.

[7]. "Robust watermarking of AES encrypted images for DRM systems v.chandra prasad and s.maheswari 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013).

[8]. International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 10, October 2013 Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption Ms. Roshan Jahan.