Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017)
7 - 9 March 2017

An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms

Assist.Lec. May H.Abood
Computer Engineering dept.
College of Engineering, Al-iraqia University
Baghdad, Iraq
may_it2004@yahoo.com

***Abstract*—for secure data transmission over internet, it is important to transfer data in high security and high confidentiality, information security is the most important issue of data communication in networks and internet. To secure transferred information from intruders, it is important to convert the information into cryptic format .Different methods used to ensure data security and confidentiality during transmission like steganography and cryptography.**

This paper improve information security through developing efficient image cryptography algorithm by using encryption with steganography. The proposed algorithm ensure the encryption and decryption using RC4 stream cipher and RGB pixel shuffling with steganography by using hash-least significant Bit (HLSB) that make use of hash function to developed significant way to insert data bits in LSB bits of RGB pixels of cover image . The security evaluations are presented by calculating a peak signal to noise ratio and mean square error. For secret image, PSNR is infinity and MSE is 0. For cover image, PSNR is about 63 db and MSE is about 0.03. The results show that high level of the similarity exists between the stego-images and cover images and the same is for secret images and extracted image as represented also in In Histogram Analysis of secret images. These algorithms is performed by using MATLAB program.

Index Terms— Cryptography, hash-lsb, Image Encryption, RC4, pixel, shuffling, Security, stream cipher, Steganography.

I. INTRODUCTION

In recent trends of technology the challenge of improving Information security is important need when sending and receiving data in the fields of data communication and networks.to solve this problems there are several methods used to protect data from unauthorized access during transmission. Many techniques is used to protect the user data. The most efficient technique is using cryptography and steganography. Cryptography and Steganography are the master areas which take a shot at Information Hiding and Security.

In cryptography, encryption algorithm is the technique of converting transferred data into unrecognizable form to prevent unauthorized access to data unless knowing specific information about the used key. Decryption algorithm is used to reconstruct the original data.

Cryptography recently includes using advanced mathematical procedures in encryption and decryption techniques. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric [1]. In Symmetric-key Encryption using similar cryptographic key for both encryption and decryption. The used keys must to be similar or there can be a Some changes between the two keys .In asymmetric key encryption algorithms the keys used for encryption and decryption must be different.

Steganography is the technique that deals with hiding secret data in some cover media which may be image, audio, or video. The word steganography comes from the Greek “Seganos”, that mean covered or secret and “graphy” which mean writing or drawing [2].

In this paper, cryptography and steganography are used to ensure security of transmitted data. RC4 and pixel shuffling encryption algorithm is used to encrypt the secret image and Hash-LSB is embedded encrypted image into the selected Least significant bits of RGB image and then sent.in receiver side the image is reconstructed from stego RGB image and use RC4 and pixel shuffling decryption algorithms to obtain the original image.

II. PROPOSED METHODOLOGY

The security of data communication and especially images became a significant goal as the network is growing. The security of images is an important research field in different trends like data security, secure data transmission and copyright security. So, Image encryption algorithms and hiding algorithms should be designed to enhance the effectiveness of transmission and keep safety from attacks by the intruders. So, the proposed method can achieve the highest level of data integrity, confidentiality and security.

In this paper trying to verify the confidentiality of grayscale image that makes uses of pixel shuffling and RC4 stream cipher for cryptography and Hash-LSB for steganography. The main function of the pixel shuffling is that it involves no modification in the bit values and no expansion of pixels in the

978-1-5386-2962-8/17/$31.00 ©2017 IEEE

end of the encryption and the decryption procedure. Here, the pixel values are redesigned and combined moving from their particular positions and then the values are swapped to give the cipher image which become recognizable [3]. The objective of using RC4 stream cipher is to improve the confidentiality to encryption [4]. Then encrypted data as well as the cover image passed to the HASH LSB technique. HASH-LSB calculate the LSB pixel value to insert the message or file content into the cover image and finally stego-image will be created [2]. On the other hand adding pixel rearranging to the RC4 cipher will enhance the security of the combination. When we can implement this system then we can embed secret data easily in cover image without any noticeable change in original image. So intermediate person can't access to the secure data. This work is a novel concept, which combining the RC4 algorithm and pixel shuffling with H-LSB for grayscale image to improve security and privacy[1], [5]. The method effective quality is for the following reasons.

(i) The simplicity of RC4 and pixel shuffling algorithm

(ii) RC4 requires only byte-length manipulations so it is suitable for embedded systems,

(iii) Even though RC4 has vulnerabilities, we combined it with shuffling to make it almost impossible to break

(iv) In pixel shuffling all features of an image remain unchanged during the process of encryption and decryption.

v) HLSB use hash function to select insertion LSB bits, so is more efficient than simple LSB

The following diagrams in fig.1 describe the method of proposed system.

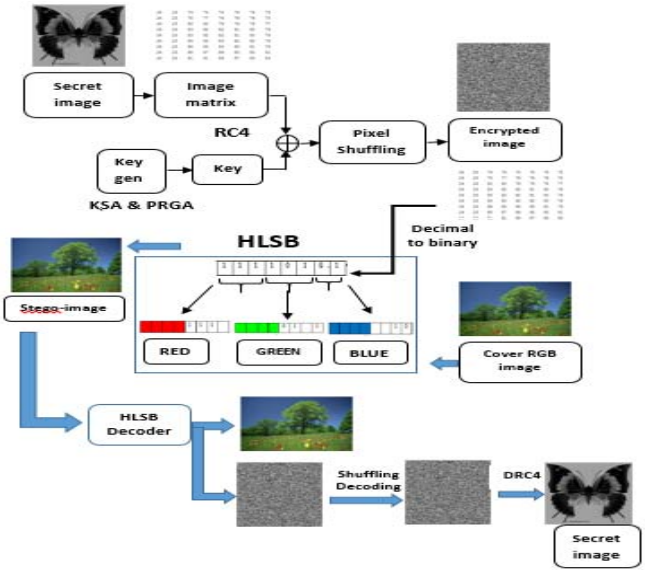

Fig.1.Proposed system encoder and decoder

A. RC4 stream cipher algorithm

In this paper, the RC4 encryption is characterize and executed. The RC4 is an abbreviation of "Rivest Cipher 4" or "Ron's Code 4"[6]. It uses a variable key length which can range between 1 to 256 bytes (8 to 2048 bits) and is utilized to instate a 256-byte state vector S. The key stream is totally independent of the used plaintext. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits that is XORed with plaintext to produce the ciphertext [7] as shown in fig.2.By applying the same method we again decrypt the encrypted image. After the end of this step we again got the original image back.

In RC4 encryption algorithm, the encryption process including two Algorithms, Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA) to produce the keystream of the stream cipher[8].

Algorithm 1.Key Scheduling Algorithm (KSA).

```
INPUT: K[$K_1$, $K_2$,…. $K_l$],m
OUTPUTS: S
    1. S[i]=i, for i=0,1,2,…,255
    2. j <—0
    3. For i <—0 to 255 $D_0$
        3.1 j<—(j+S[i]+K[i mod L]) mod 256
    4. Swap S[i] with S[j]
    5. Return (s)
```

Algorithm 2.Pseudo-Random Generation Algorithm (PRGA).

```
INPUT: State S
OUTPUT: Key sequence Kseq
    1. j <—0
    2. i <—0
    3. While not end of sequence $D_0$
        3.1. i <—(i+1) mod 256
        3.2. j <—(j+S[i]) mod 256
        3.3. Swap S[i] with S[j]
        3.4. Kseq <—S[(S[i]+ S[j]) mod 256]
    4. Return (Kseq)
```

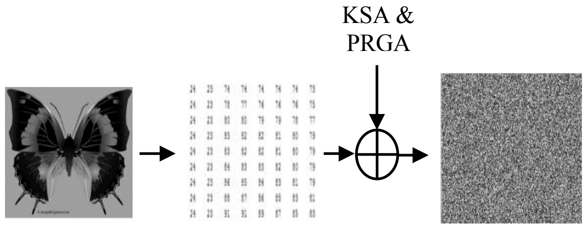

Fig.2.RC4 encryption algorithm

B. Image pixel shuffling technique

A technique of shuffling of the image pixel values has proven to be really effective in terms of the security analysis. The extra swapping of pixels in the image file after component shifting has increased the security of the image against all possible attacks available currently [1].

This paper manages a basic image encryption method using adjustment or rearranging of the image pixels. Initially we take a grayscale image of size N × N. In the straightforward mentation we took a 256 × 256 grayscale image and rearranged pixels in an arbitrary way and this random order used as the common key between the parties. Pixel shuffling consists of a permutation map that is applied to decrease adjacent pixels correlation. From the rearranged framework the scrambled image is as appeared in fig.3.

The result of grayscale image (256 x 256) shuffling is as shown below

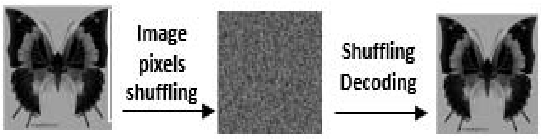

Fig.3. .shuffling encryption algorithm

C. Hash-LSB Techniques

Image steganography taking benefit of human eye constraint. It utilizes RGB image as the cover image for inserting secret image. The major attribute of a steganographic system is to be less distortive while expanding the extent of the secret image. This system is proposed to hide a grayscale secret image into a RGB cover image. A 3,3,2 LSB insertion method is used for color image steganography [2].

The hash based LSB technique is different from simple LSB technique on basis of hash function as hide eight bits of secret image in LSB positions of RGB pixels of cover image and the distribution sequence of bits is 3,3,2 respectively and in such a way that first 3 bits of the 8 bits secret image are inserted into R pixel and other 3 bits of secret image into G pixels and remaining 2 bits are inserted into B pixels [9]. These eight bits are embedded in a specific order based on the chromatic impact of blue color to the human eye is more than red and green colors [10]. In LSB insertion technique, when the binary representation of the secret data overwrite in the LSB of every byte in the cover file the amount of change happened in cover image will be negligible and not perceived to the human eye [9].

The insertion of secret data pixel (8-bit) is in the order (3,3,2) as shown in fig (4).The embed position of each pixel(8-bit) of secret image in the LSB of (red, green, blue) of cover image is as represented in x, Where x is LSB bit position per pixel

x=1 ,2 and 3 bits of red pixels,

x=1, 2 and 4 bits of green pixels,

x=3 and 4 bits of blue pixels.

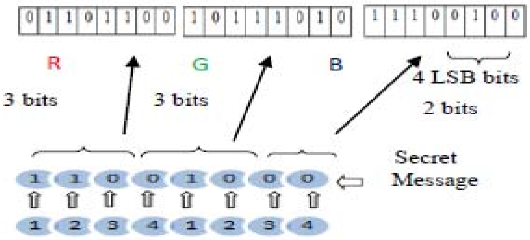

Fig.4. Distribution of Secret Message bits

To recognize the placements to conceal information in LSB of each RGB pixels of the cover image the following formula can be used:

$$P = H \% L \qquad (1)$$

Where, P is the LSB bit placement inside the pixel,
H demonstrate the position of any concealed picture pixels,
L is number of bits of LSB which is 4 for the present case.

HLSB Inserting proposed algorithm

1- Take encrypted image
2- Select a cover color image.
3- Take 4 LSB bits of every (Red, Green, and Blue) pixels of the cover image.
4- Embed 8 bits of encrypted image into the 4 LSB in pixels of cover image in the sequence of 3, 3, 2 respectively utilizing the hash function in eq 1.

HLSB Decoding Process

1-Obtain stego-image
2- Detect 4 LSB bits of each RGB pixels from stego-image.
3- Implement the hash function to acquire the placement of LSB of used image.
4- Recover the bits in sequence of 3, 3, and 2 respectively.
5- Finally read the secret image.

III. RESULT ANALYSIS

Based on the proposed algorithm, we have developed a system, which implements the proposed algorithms using MATLAB program. As a target measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and security quality (SQ) are studied.

$$\text{MSE}=\frac{1}{H*W}\sum_{1}^{H}(p(i,j)-S(i,j))^2 \qquad (2)$$

Where, MSE is Mean Square error, H and W are height and width and P(i,j) is original image and S(i,j) is (stego or reconstructed) image.

$$\text{PSNR} = 10 \log_{10}\frac{L^2}{MSE} \qquad (3)$$

Where, PSNR is peak signal to noise ratio, L is signal level for a used image it is taken as 255.

$$SQ=\frac{\sum_{i=0}^{255}(x(i)-x'(i))}{256} \quad (4)$$

Where SQ is security quality, X Is the original image histogram and X' is scrambled/encrypted image histogram.

A. *In sender side*

1. Reading the grayscale secret image and RGB cover image, the following images will be used.

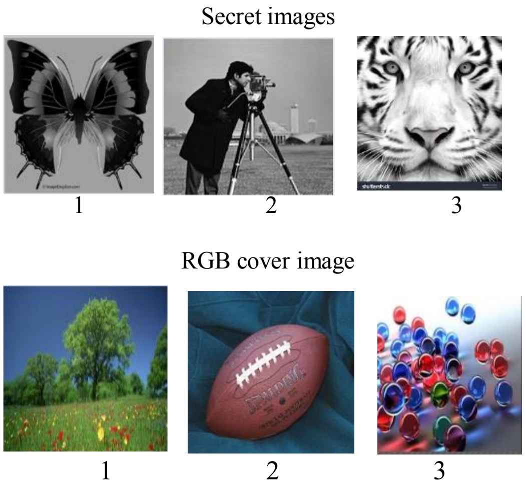

Fig.5.Secret and RGB cover images

2. Encrypt secret image sing RC4 and pixel shuffling
3- Embed 8 bits of encrypted image into 4 bits of LSB of RGB pixels in the sequence of 3, 3, and 2 respectively

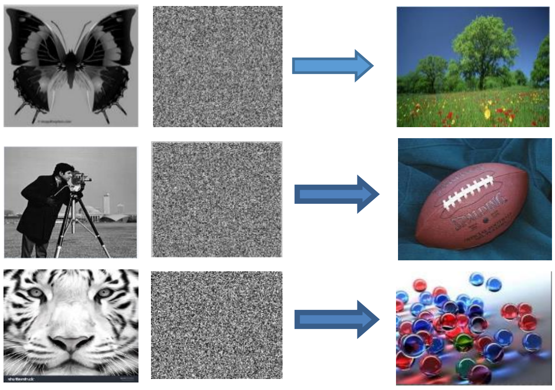

Fig.6.Image Encryption phase

B. *In receiver side*

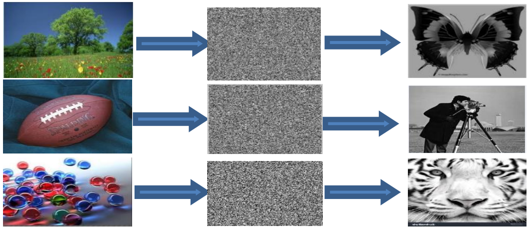

Fig.7. Image Decryption phase

In Histogram Analysis, The statistical features of images are presented using histogram that plots the occurrences frequency of image pixel value, this analysis is done to compare original and encrypted images where there should be no similarities between original image and encrypted image histograms.

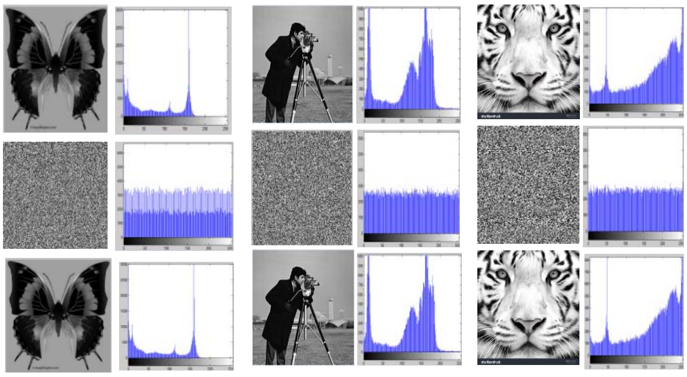

Fig.8. Histogram analysis of secret images

In above all images shows that the cover image and stego-image does not change, fig.6. Demonstrates the cover image object while applying the Shuffling and RC4 with HASH LSB technique.

We can embed the secured secret image into that cover image. When we can compared cover image and stego-images we can realize that both images are same.
So it is clear that we can embed the image, file or message in to the cover image by using Image Steganography method for more security and authentication.
In this section, both peak signal to noise ratio, mean square error and security quality are calculated for proposed system. The measures is shown in table 1 for secret images and table 2 for cover images

The results that are obtained from the two objective tests prove that the coded system is more secure than uncoded system since the values approaches one for secret images and for stego-images with high PSNR values. This means that high level of the similarity exists between the stego-images and cover images and the same is for secret images and extracted ones.

Table I.MSE, PSNR, SQ and Elapsed time for secret images

Images	MSE	PSNR	Security quality	Time
secret 1	0	infinity	0	709 s
secret 2	0	infinity	0	7.17 s
secret 3	0	infinity	0	7.07 s

Table II.MSE, PSNR and Elapsed time for cover images

Images	MSE	PSNR	Time
cover 1	0.0305	63.2944	7.09 s
cover 2	0.0306	63.2746	7.17 s
cover 3	0.0313	63.1807	7.07 s

IV. CONCLUSION

In this paper, a cryptography and steganography algorithms proposed to increase security and authentication of data transmitted in a network environment. The proposed system is one of the best ways of hiding the secret of data transferred between sender and receiver from intruders in unsecured networks. The Cryptography techniques RC4 & Shuffling cipher algorithm has been implemented to encrypt the secret image(jpg, png, gif, bmp) before embedding it in the RGB cover image(jpg, png, gif, bmp) with the goal that it is difficult to intruder to detect the encryption. Image encryption using RC4 and Shuffling encryption has a considerable security quality factor which implies the intensity distributions for the original images and mutilated image are distinctive. When we consider the encrypted image histogram we notice that they have a uniform distribution. The Hash based Least Significant Bit (H-LSB) steganography has been implemented for embedding encrypt image into cover image. The proposed HLSB technique is the development of an enhanced steganography by concealing data in an image with less variety in image bits have been made which makes proposed algorithm secure & more effective and can have the authentication module beeline with encryption techniques.

To evaluate this system we tested a number of images to be encrypted and hidden with the proposed algorithms. According to the tested we found that the system has provide a high security and easy way to encrypt, embedding and decrypt secret image without effecting the quality of images(secret or cover) as appeared in measurements of (MSE , PSNR and security quality) . Hence this system is very efficient to hide grayscale image inside other RGB image and can be developed to hide color image in other color image as future consideration.

REFERENCES

[1] Q. Kester, “A cryptographic Image Encryption technique based on the RGB PIXEL shuffling A cryptographic Image Encryption technique based on the RGB PIXEL shuffling”, International Journal of Advanced Research in Computer Engineering & Technology, vol. 2,no.2 pp.848-854, January 2013.

[2] P. Sahute, S. Waghamare, S. Patil, and A. Diwate, “ Secure Messaging Using Image Stegnography”, International Journal of Modern Trends in Engineering and Research,vol.2,no.3, pp. 598–608, March 2015.

[3] N. Agarwal and P. Agarwal, “An Efficient Shuffling Technique on RGB Pixels for Image Encryption”, MIT International Journal of Computer Science & Information Technology, vol. 3, no. 2, pp. 77–81, August 2013.

[4] K. Hamdnaalla, A. Wahaballa, and O. Wahballa, “Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms”,International Journal of Video & Image Processing and Network Security, vol.13, no. 04,August 2013.

[5] N. G. A. P. H. Saptarini, Y. A. Sir, “Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map”, Information Systems International Conference ,December, pp. 2–4, December 2013.

[6] http://en.wikipedia.org/wiki/RC4 accessed at 25 January 2013.

[7] A. Mousa and A. Hamad, “Evaluation of the RC4 Algorithm for Data Encryption,” no. 1, pp. 44–56, June 2006.

[8] B. H. Kamble, “Robustness of RC4 against Differential attack” ,International Journal of computer science and application, vol. 1, no. 4, pp. 661–665, June 2012.

[9] A. M. Abdullah, “New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm”, International Journal of Computer Applications, vol. 143, no. 4, pp. 11–17, June 2016.

[10] P. R. Deshmukh and B. Rahangdale, “Hash Based Least Significant Bit Technique For Video Steganography”, Int. Journal of Engineering Research and Applications, vol. 4, no. 1, pp. 44–49, January 2014.