Robust and Secured Image Steganography using Improved LSB and RC4 Cryptography with Preprocessing Operation

Zahraa K. Taha, Mohammed Naser Alturfi, Baraa M. Albaker, Y. W. Abduljalel, H. A. Jasim, I. Majeed, A. J.Askir, A. A. Mhawish, R. R. Saady, M. A. Ahmed, A.S. Ali, M. G.Abbas

Abstract: ***The security of the transmitted data over the internet has become one of the challenges sharing with data communication over computer network. In this paper, a new stegnography system is developed using Improved Least Significant Bit (ILSB) with preprocessing operation for concealing data. The system mixes several technological rules to enhance the performance of concealing scheme. The original secret image is divided into several segments then rearranged to even and odd. Rivest Cipher 4 (RC4) algorithm is applied on preprocessed image before concealing it on the cover image using ILSB. The proposed systems are simulated using MATLAB software package. The experimental results show that our suggested method successes of concealing data according to PSNR ratio, correlation and elapsed time. Preprocessing operation provides flexibility and robustness to the overall system. Improved LSB is simple and strong method for concealing images. Finally, the proposed system is very active to hide the gray scale image inside the color image.***

Index Terms**:** ***Image Steganography; Cryptography; RC4 Algorithm; Concealing Data; Security of Data Transmission.***

I. INTRODUCTION

The rise of internet, everyone need to share and transfer information in safety path. Many insecure pathways have utilized for sharing and transferring data but at a specific level it's not reliable. Cryptography and steganography are two strategies that used to protect information from unauthorized persons [1].

Cryptography and stegnography are complementary to each other to provide more security, flexibility, robustness and more security. Cryptography is art of transformation data from readable to unreadable to protect them during transmission [2]. Steganography is the technique of hiding information in appropriate that message carrier (text, image, audio, or video) [3].

All of the existing methods of steganography focus on the embedding strategy and give no consideration to the pre-processing stages, such as encryption, as they depend heavily on the conventional encryption algorithms which obviously are not tailored to steganography applications where flexibility, robustness and security are required.

The objective of this study are proposing a new stream cipher for encrypting images that outperforms current solutions and that provides a more security, robustness and flexibility, and a new algorithm RC4-ILSB for protection secret image that is more accurate and faster than currently deployed techniques.

II. GENERAL MODEL OF THE PROPOSED SYSTEM

The general model of the proposed system is shown in Fig. 1. The following subsections explain briefly each stage in the figure.

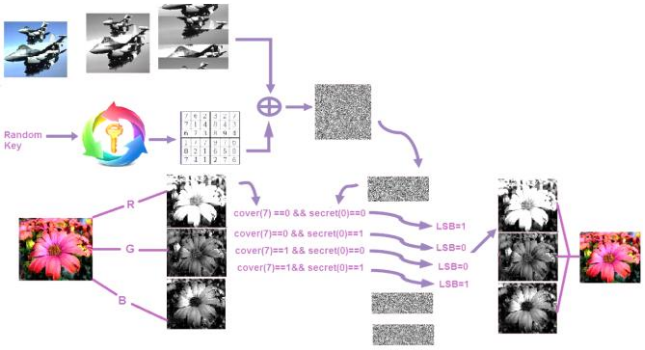


Fig.1: General Model of the Proposed System.

A. Preprocessing Unit

The preprocessing unit is proposed to give more security, reliability and robustness of the overall system. It employs both division and transposing for protect data from authorized person during transmission.

Revised Manuscript Received on September 22, 2019.

Zahraa K. Taha, College of Engineering, Al-Iraqia University, Baghdad, Iraq, eng_zahraataha@yahoo.com
Mohammed Naser Alturfi, College of Engineering, Al-Iraqia University, Baghdad, Iraq
Baraa M. Albaker, College of Engineering, Al-Iraqia University, Baghdad, Iraq
Y. W. Abduljalel, College of Engineering, Al-Iraqia University, Baghdad, Iraq
H. A. Jasim, College of Engineering, Al-Iraqia University, Baghdad, Iraq
I. Majeed, College of Engineering, Al-Iraqia University, Baghdad, Iraq
A. J.Askir, College of Engineering, Al-Iraqia University, Baghdad, Iraq
A. A. Mhawish, College of Engineering, Al-Iraqia University, Baghdad, Iraq
R. R. Saady, College of Engineering, Al-Iraqia University, Baghdad, Iraq
M. A. Ahmed, College of Engineering, Al-Iraqia University, Baghdad, Iraq
A.S. Ali College of Engineering, Al-Iraqia University, Baghdad, Iraq
M. G.Abbas, College of Engineering, Al-Iraqia University, Baghdad, Iraq.

The secret image of size (256x256) is converted into a gray scale ,which is a white and black image. The gray scale is represented by numbers from 0 to 255, where 0 represents black and 255 is white. The gray scale secret image is divided (silted) according to the proposed preprocessing as shown in Fig. 2. The block is re-arranged to even and odd.

This process generates cipher image is more reliable because the transmitter and receiver only knows how to preprocessed the original image which the objector does not know the mathematical sequence that utilized in this process.

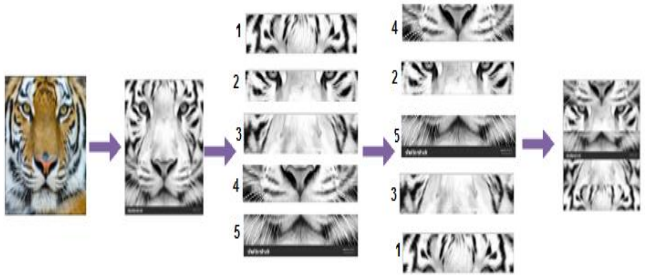


Fig. 2: Preprocessing of secret image.

B. Cryptography process

RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security. It is variable key size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. It is remarkably simply and quite easy to explain. A variable-length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with elements S[0], S [1], …, S[255] [4-6].

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 (See Algorithms 1 and 2, and Fig. 3 below).

Algorithm 1.Key Scheduling Algorithm (KSA)

INPUT: K[K_1, K_2,…. K_I],m

Initialized the state vector S and temporary vector T. S is initialized so the S[i] = i,

and T is initialized so it is the key K (repeated as necessary).

OUTPUTS: S

1. S[i]=i, for i=0,1,2,…,255
2. j = 0 ;
3. For i ⟵0 to 255 Do
   j = (j+ S[i]+ T[i]) mod 256
4. Swap(S[i] , 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 (true) {
   i = (i+1) mod 256;
   j = (j + S[i]) mod 256;
   Swap(S[i] , S[j]);
   t = S[(S[i]+ S[j]) mod 256];
   Kseq=S [t];
4. Return (Kseq)

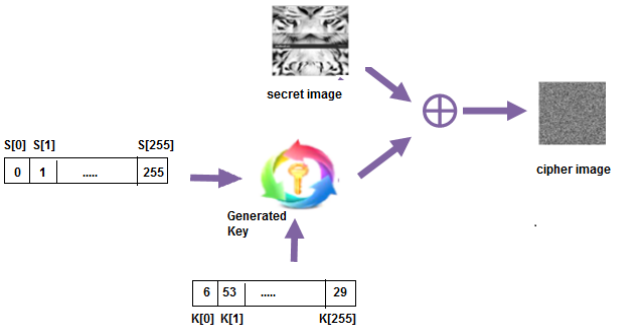


Fig. 3: Original image after RC4 encryption algorithm

C. Steganography process

The steganography or embedded process has proven to be really effective in terms of the robustness analysis of the whole proposed systems [2, 3, 7]. In LSB Algorithm, the cipher image is directly distributed on each least significant bit of the cover image. but in Improved LSB, it is not directly distributed. Second least significant bit and the information bit are used to embedded process. The embedded process is achieved according to four rules, is shown in table 1.

Table 1: Operation for Improved LSB

7^{th} least significant bit of image	Bit of information to be hidden	Resultant Least Significant bit to be replaced
0	0	1
0	1	0
1	0	0
1	1	1

These operations are used for both to hide and to extract the information. Steps used in proposed Improved LSB (Hiding process):

1. Obtain the value 7^{th} LSB of each pixel of cover image.
2. The cipher image is converted to binary value.
3. With the help of rules in table 1, perform the process between the value 7^{th} LSB and binary bits of cipher.
4. Replaced the value of LSB of the cover image with result of the step 3

The cover image is (512x512) color image and the cipher image is 256 gray scale. The cipher image is divided into three parts and each parts is embedded into red, green and blue of the cover image respectively as shown in Fig. 4. The 8 bits of the ciphered image in the first part are distributed over the red of the cover image.

The 8 bits of the ciphered image in the second part are distributed over the green of the cover image. The 8 bits of the ciphered image in the third part are distributed over the blue of the cover image. This process continuous until all bits in each part are hidden completely.

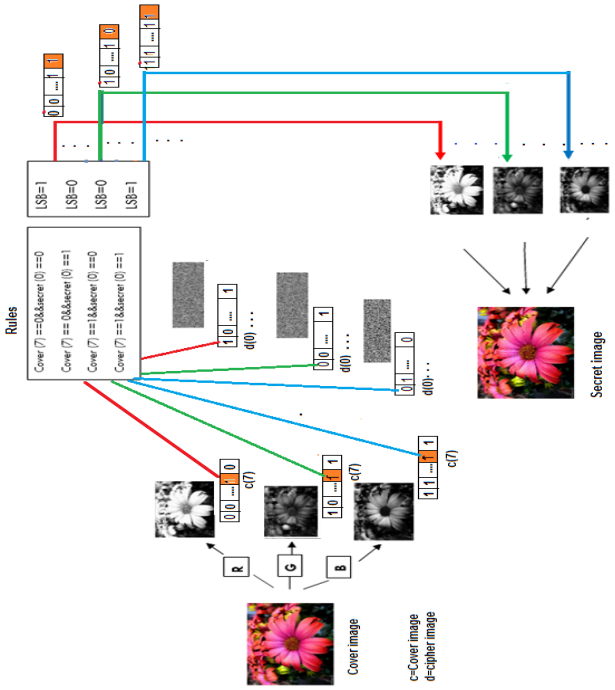


Fig. 4: Embedded process

An easy way to comply with the paper formatting requirements is to use this document as a template and simply type your text into it.

D. Extraction Process

To return the embedded images, three things must be sent. First the stego image is sent through a secret channel. While the second, the same secret keys that generate by running the KSA and PRGA and third is number of segmentation, arranging, and sorting process.

The coefficient that contains the secret image is converted to binary values. Perform the operation between 7th LSB and LSB binary bit according rules in table 1 then find result value of LSB. This process continuous until all bits in each bytes are extracted completely. The cipher image is obtained at the end of this process. This image is decoded by XOR secret keys that generate by running the KSA and PRGA to obtain the processed image. Finally the original secret image is completely return as depected in Fig. 5 and 6.

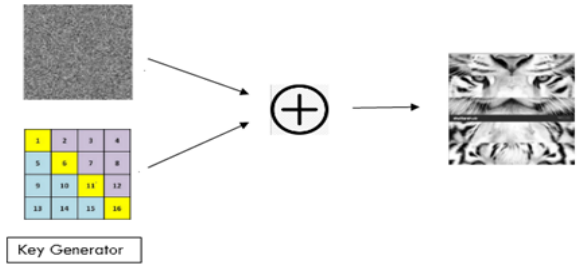


Fig. 5: Decryption

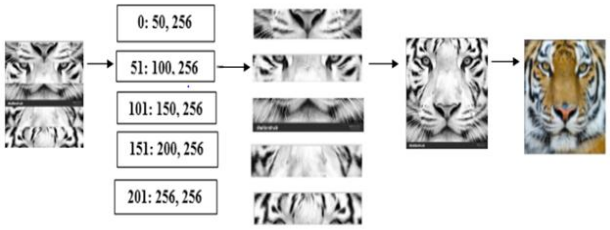


Fig. 6: Reproduction and original image extraction

III. TESTING AND PERFORMANCE EVALUATION

In this section, the performance of our proposed framework is demonstrated. Different factors are used to determine the performance. The Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) have been computed [Heba].

$$PSNR=10\log_{10}(s^2/MSE) \quad (1)$$

where

$$S^2=\frac{1}{m*n}\sum_{i=1}^{m}\sum_{i=1}^{n} J^2(i,j) \quad (2)$$

And the Mean Square Error (MSE) defined as:

$$MES=\frac{1}{m*n}\sum_{i=1}^{m}\sum_{i=1}^{n}[\,J(i,j)-j^1(i,j)\,]^2 \quad (3)$$

Where j^1 represents the pixel in the stego imag (the result of the steganography system)

Table 2 shows the results are obtained from objective test to the proposal method. The group from cover and secret images are tested as shown in Fig. 7.

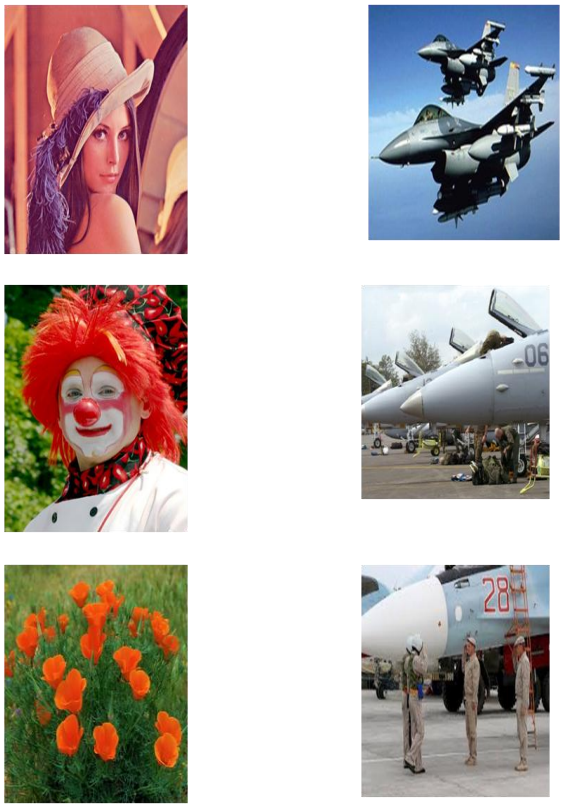
Note that the correlation of the all testes are equal unity in the receiver; this means the reconstructed images are the same as the original images.

The outcomes that are gotten from the two objective tests demonstrate that the proposed system is more secure, robustness and flexibility. PSNR is high 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.

The secret image is concealed in the cover image using ILSB based on processed image and ciphering algorithm. This make information is more protection and safety. The mix of the steganography with the cryptography produces system with extra security. The intruder must know the used encoding algorithm, preprocessing operation, and the concealing algorithm. It is difficult for him to know this information because each of them transmitted through secure channel.

Table 2: PSNR and correlation results for the proposed system.

Groups	PSNR/db (Secret)	Correlation	PSNR/db (Stego)	Corr.	Elapsed Time/s
Group1	52.8979	0.9066	inf	1	16.85484
Group2	52.9179	0.9983	inf	1	16.22607
Group3	52.8998	0.8801	inf	1	16.29672



(a) (b)

Fig. 7: Group of the cover and secret images (a) Group of the used cover images (b) Group of the used secret images

IV. CONCLUSION

The paper presents a new method for enhancing security and authentication of data transmitted. The main focus of the paper is preprocessing and find new technique to conceal the information. Preprocessing has been applied to the original image and then encoded using RC4 before concealing it on the cover image. It is not easy to unauthorized-person to obtain original image without knowing number of segmentation and mathematical sequence used in the preprocessing method and the key streams in RC4. Moreover, Improved LSB has been added and executed for hiding encode image into cover image. Experimental results demonstrated the strength of our proposed method in hiding images in terms of PSN ratio and correlation. Preprocessing unit and ILSB added flexibility and robustness to the overall system to conceal images, especially the gray scale ones inside the color images.

REFERENCES

[1] Shinjit Kamal Borah and Surajit Borah, (2014), "Multilevel Encryption System Using RC4 and Steganography", *Research Journal of Information Technology, Vol. 6, pp. 399-405.*

[2] A. M. Abdullah (2016), "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.

[3] Ms.Vineeta Bassi (2014), "IMAGE STEGANOGRAPHY USING IMPROVED LSB AND EXOR ENCRYPTION ALGORITHM" MSc. *Dissertation in* Computer Science and Applications.

[4] K. Hamdnaalla, A. Wahaballa, and O. Wahballa (2013), "Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms", *International Journal of Video&Image Processing and Network Security*, Vol. 13, No. 04, pp.6-17.

[5] B. H. Kamble (2012), "Robustness of RC4 against Differential attack", *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 1, no. 4, pp. 661–665.

[6] Online site: https://www.geeksforgeeks.org/computer-network-rc4-encryption-algorithm/

[7] S. Rajendran and M. Doraipandian (2017), "Chaotic Map Based Random Image Steganography Using LSB Technique", *International Journal of Network Security*, vol. 19, no. 4, pp. 593–598.

AUTHORS PROFILE

I am **Zahraa K. Taha,** currently working with College of Engineering, Al-Iraqia University, Baghdad, Iraq. My area of interest operation management.eng_zahraataha@yahoo.com

My name is **Mohammed Naser Alturfi,** I am currently affiliated with College of Engineering, Al-Iraqia University, Baghdad, Iraq. My area of interest is operations.

I am Baraa **M. Albaker,** luckily, I relate to College of Engineering, Al-Iraqia University, Baghdad, Iraq.

My name is **Y. W. Abduljalel,** affiliated with College of Engineering, Al-Iraqia University, Baghdad, Iraq. I am interested with operations and technology.

My name is H. A. Jasim, my affiliation is with College of Engineering, Al-Iraqia University, Baghdad, Iraq

Majeed, College of Engineering, Al-Iraqia University, Baghdad, Iraq

J.Askir, College of Engineering, Al-Iraqia University, Baghdad, Iraq

A. Mhawish, College of Engineering, Al-Iraqia University, Baghdad, Iraq

R. R. Saady, College of Engineering, Al-Iraqia University, Baghdad, Iraq

M. A. Ahmed, College of Engineering, Al-Iraqia University, Baghdad, Iraq

A.S. Ali College of Engineering, Al-Iraqia University, Baghdad, Iraq

M. G.Abbas, College of Engineering, Al-Iraqia University, Baghdad, Iraq.