ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

Color Images Encryption using Cipher System with different types of Random Number Generator

Najwan AH

Department of Computer Science, Al-Nahrian University, Baghdad, Iraq

ABSTRACT: Image encryption is a wide science in a nowadays and is used in research of information security, and a lot of image encryption algorithms have been introduced to protect the personal images from unauthorized access. The proposal algorithm generated random password seed which is used as a key to three types of Pseudo Random Number Generator; Linear Feed Back Shift Register, Non-Linear Feed Back Shift Register and BLUM BLUM SHUB. The algorithms are applied to the colour images with large random keys. The experimental results of comparisons between these algorithms, shows that BBS have better performance than LFBSR and NLFBSR.

KEYWORDS: Encryption; Decryption; Pseudo random number generator; Linear feedback shift register; Non-linear Feed Back Shift Register; BLUM BLUM SHUB.

I. INTRODUCTION

Communication is the activity of exchanging data and thoughts over network. Secure communication protecting these exchange of data from thieves (attackers). Which know them as professional unauthorized recipients or observers called as cryptanalysts [1]. The method which converting understandable data, for example, audio, images, text, video and etc. into another data that are hard to understand protect these data from thieves and that's called cryptography. The plaintext (original text) is converted into another data that are coded equivalent called cipher text by using encryption methods. The encryption methods deal with plaintext and secret key as an input and cipher text as the output. The only person how know the secret key is the sender and receiver [2].

Image is an important part of data and it's very important to protect these images from unauthorized access. Image encryption has many applications in internet communication, medical imaging, multimedia systems, telemedicine, military communication, etc. to secure these images data from attackers it must encrypt images data before transmitted or stored them through network. Images are unlike text. Means not all classical cryptosystems are acceptable to using to encrypt images straight. That's not good thought for two reasons. One of them the decrypted text must be exactly to original text, in image data that is not necessary because decryption image may contain small distrotion and that usually accepted. The second reason is that image size is always much bigger than text size and that's mean classical cryptosystems encrypt an image data but need much more time.

To Transmit encrypted images to any person in the network many encryption algorithms have been proposed. Techniques that use in this paper applied to Bmp images.

II. RELATED WORK

Shrija Somaraj, Mohammed Ali Hussain, [3] suggested two methods encrypt images. Both of these algorithms using an image as a key. Then an encrypted image is obtained by XORed Every pixel in the key image with the original image pixel.

Vishal Kapur, Surya Teja Paladi [4] proposed a straightforward and secure process to ensure images. Two pseudo random number generators used to process image encryption. One of them used algorithm of linear feedback shift register for the original image to swap rows. After that swapping the columns to produce an encrypted image. The second one, algorithm Blum Blum Shub used to exchange intensity for every pixel of the encrypted image that introduced a final encrypted image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

Arihant Kr. Banthia, Namita Tiwari [5] proposed two algorithms to image encryption. One of them encrypt image using algorithm linear generator to generate random numbers using as index to columns, rows and pixels of image shuffling. The second algorithm generates random number sequences by using logistic maps that are using as an index to columns, rows and pixels of image shuffling.
Suhad Latef, Ban N. Dhannoon [6] proposed new algorithm to encrypt RBG color images with large random keys and produced the new method to generate random password seed which used as initializing to the linear feedback shift register algorithm. This algorithm implemented on 8 and 24-bit Bmp image.

III. THE PROPOSED COLOR IMAGES ENCRYPTION

Here presented the approach for image encryption using Pseudo Random Number Generator (PRNG). Figure 1 shows proposed system as a block diagram. The secret key is sent to the receiver by secured channel. If the eavesdropper knows the secret key in any way, the algorithm of generating the password seed is hidden, and that is advantage offered by using such scheme. The eavesdropper could not be able to reproduce an image. The decrypted image could obtain as an original image by having a reverse method and the password seed only. pseudo random number generator is originated with starting random password seed then the number produced is converted into the index (0-255) using bits to byte converter and XORed with the original image generating an encrypted image, which is transmitted to intended users to decrypt it.

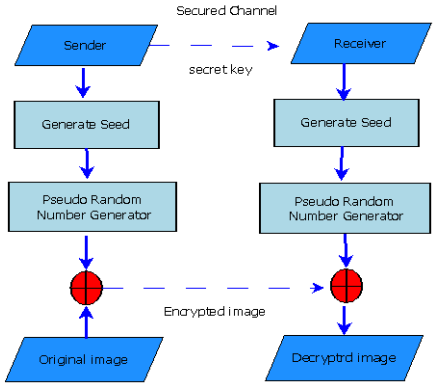

Figure 1: Block diagram of the proposed system.

3.1 Generation of The Seed

The definition of the seed that is a number using to introduce pseudo random number generator. The seed is not necessary to be random if it used in pseudo random number generator. In field of computer security it is important to choose a good random seed. When a secret encryped key is pseudo randomly generated, having the seed allow to obtain a key. High entropy is necessary for selecting good random seed data. shared the same random seed, it becomes for all use it as the secret key, and when two or more systems using matching random seed and the same pseudo random number algorithms that can generate same nonrepeating sequences of numbers and that sequences can be used in the systems to remote synchronize, such as GPS satellites and receivers [7]. The first step in the proposed system is to generate the random password seed number from the secreted key which must be as large as possible to be hard for attacker to know it as shown in Figure 2.

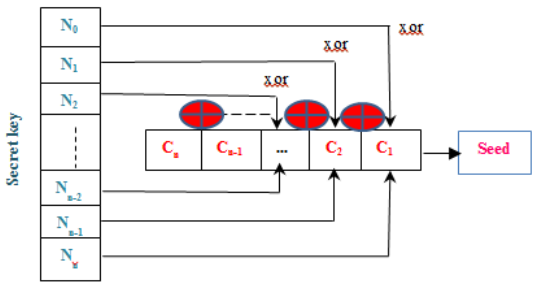

Figure 2: Seed Generation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

Equation (1) used in generating seed.

$$seed = C_1 \oplus C_2 \oplus C_3 \oplus \ldots \oplus C_{n-1} \oplus C_n$$
$$C_1 = (N_0 \oplus N_n)$$
$$C_2 = (N_1 \oplus N_{n-1})$$
$$\vdots$$
$$C_{\frac{n}{2}} = (N_{\frac{n}{2}} \oplus N_{\frac{n}{2}+2})$$

3.2 Pseudo Random Number Generator (PRNG)

It is uses one or more than one data to generates multi pseudo random numbers. PRNGs inputs are called seeds (Explained earlier)and this seed that is used should be unpredictable and random**.**PRNG outputs are usually inevitability functions of a seed, for example, randomness which are true random are limited to the generation of seed. The inevitability nature of a process drives to an expression "pseudo-random". While every pseudo-random sequence elements is consistent from pseudo random sequence seed, only a seed requires being saved if validation or reproduction of pseudo random sequences are required**.**Pseudo random numbers frequently appear more random than gained random numbers from real sources. If a pseudo random sequence is properly constructed, every value in the sequence is output from the prior value using transformations that appear to bring additional randomness[8].

3.2.1 Linear Feed Back Shift Register (LFBSR)

LFBSR is An efficient structure and very straightforward algorithm. Fig 3. shown an LFBSR is consists of registers, and every register contains an array of memory cells, in these cells feedback function and one binary value, feedback function consists of the XOR operator. Every new unit of time subsequent operations is performing[9].

a) The output is the content of the last memory cell.
b) The register is handled by the feedback function. Or can say, chosen memory cells are XORed between each other to generate one bit of feedback.
c) Every bit of the register developed one position, first bit received the result of feedback function and last bit being discarded.

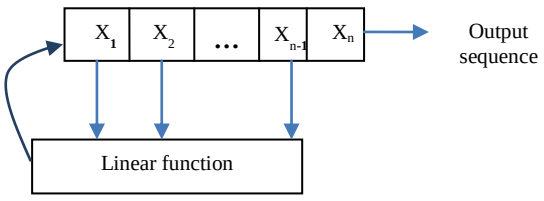

Figure 3: LFBSR.

The common form of n-stage LFBSR is shown in Figure 3, the feedback logic, in this case, can be written as in equation (2):

$$f(x_1, x_2, x_3, \ldots, x_n) = a_0 + a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \quad (2)$$

Where a's defines feedback tapings and can only take values of 1 or 0. The contents of the **a** determine the transition matrix which represents the autonomous behaviour of the Feed Back Shift Register (FBSR).

3.2.2 Nonlinear Feed Back Shift Register (NLFBSR)

NLFBSR is a mechanism for generating binary sequences as shown in Figure 4 NLFBSRs generates an excellent pseudo random binary pattern. If this register is stored with any inputted initial value, a clock pulse is the only signal needed for binary pattern generation. In binary sequence, a bit is generated With every clock pulse [10].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

The general structure of the combinational feedback function is given by the equation (3)

$$f(x_1, x_2, x_3, ..., x_n) = a_0 + a_1x_1 + a_2x_2 + ... + a_nx_n + a_{n+1}x_1x_2 + a_{n+2}x_1x_3 + ... + a_{2n-1}x_1x_n + a_{2n}x_1x_2....x_n \quad (3)$$

Where the **a**'s =0 or 1. Hence there are 2^{2^n} possible feedback functions for **n**-stage FBSR. Only $\mathbf{2^n}$ of these functions are linear. Also, there are $2^{2^n} - 2^{2^n-n-1}$ FBSRs that have cyclic behaviour.

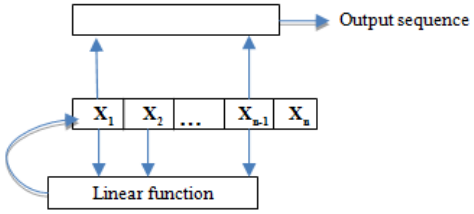

Figure 4: NLFBSR.

3.2.3 Blum Blum Shub Generator (BBS)

A common way to generate confident pseudo random number is recognized as Blum, Blum, and Shub generator, which is the name of its developers. BBS has possibly the powerful public evidence of its cryptographic strength. To produce any set of random numbers these steps should be followed[11].

Step 1, two huge prime numbers are chosen, a and b, these two numbers have the remainder of 3 while divided by 4. This can be written as in equation (4):

$$a \equiv b \equiv 3 (\text{mod } 4) \quad (4)$$

That means (a mod 4) = (b mod 4) =3.

Step 2, random number w is chosen, such that w is prime to **m**; this is equivalent to say that neither **a** nor **b** is an item of w, after that BBS generator generates a sequence of bits $\mathbf{V_i}$ as show to the following algorithm:

Y0=W2 mod m

For j=1 to α
Yj= (Yj-1)2 mod m
Vj=Yj mod 2

3.3 Comparisons between Encrypted Images

The comparison between encrypted images that used three different algorithms using four methods: histogram, time to encrypt the image, means square error, peak signal to noise ratio and randomness test.

3.3.1 Histogram Analysis

The image histogram is a frequently used method of test in data mining applications and image processing. The histograms have many advantages one of them its show the shape of the division for a huge set of information. Therefore, image histogram provides a clear representation of the way in which pixels in the image are divided by graphing histogram to a number of pixels at every colour density grade. It is necessary to make sure that the encryption image and original images possess various statistics. The histogram examination shows the ways divided pixels in an image by plotting number of pixels for every density grade[12].

3.3.2 Mean Square Error (MSE)

Is one of many ways to quantify the difference between values implied by the estimator and the true values of the quantity being estimated. MSE is a danger function, corresponding to the expected value of the squared error loss or quadratic loss. It could define the MSE easily for two m*n black and white images X & Z the consideration that one of images is approximated noisy for other images. equation (5) defined MSE [13].

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[X(i,j) - Z(i,j)]^2 \quad (5)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

Where i and j are position of a pixel for m×n image, X (i, j) is a reference or original image and Z (i, j) is a modified or distorted image. When X (i, j) = Z (i, j) then MSE is zero.

3.3.3 Peak Signal to Noise Ratio (PSNR)

Is an engineering expression for a proportion between maximum potential powers for any signal with the damaging power noise that influences precision for its performance. Because several signals must have very broad dynamic range, equation (6) defined the PSNR as [14].

$$PSNR = 10.\log_{10}\left(\frac{\max_1 2}{MSE}\right) \qquad (6)$$

Where $\max_1$ is the maximum pixel amount for any image.

3.3.3 Randomness Test Measures:

Let $r=r_0, r_1, r_{2,\ldots,} r_{n-1}$ is a sequence of length n and this sequence is binary. The randomness degree of the ciphered result was investigated using the following statistical tests [15]:

a) Frequency test

This test examines a numbers of 1's and 0's in {r} sequence are roughly equal.

b) Serial test

This test examines a number of existences of *11*, *10*, *01*, and *00* as subsequences of $\{r\}$ that are roughly equal to the random sequence as expected.

c) Poker test

The sequence $\{r\}$ is divided into non-overlapped parts of length y. This test examines whether length y sequences appear roughly equal number of times in a sequence $\{r\}$.

d) Run test

This test examines number of runs for a different length in sequence {r} is predictable for random sequence.

e) Autocorrelation test

This test examines the degree of correlations may found between the parts of sequence $\{r\}$ and the shifted versions of it.

And with each test it has P-value for it. The P-value is "the probability (under the null hypothesis of randomness) that the chosen test statistic will assume values that are equal to or worse than the observed test statistic value when considering the null hypothesis" [8].

IV. EXPERIMENTAL ANALYSIS AND RESULTS

Visual Basic.NET has been implemented to the proposed system using with several test images. The 24-bit Bmp image is represented as 1-byte for each of the three colour bands (Red, Green, and Blue). Thus the LFBSR, NLFBSR and BBS algorithms are performed for generating pseudo random number that is ranged from 0 to 255 for encryption every colour band. Below are some experiment applied on standard Lena 24-bit and Horse 24-bit.

Experiment 1 had shown in Figure 5 the results of BMP Lena image with 24-bit depth using Pseudo Random Number Generator. Here, (a) the original Lena image (b) encryption image that shows as a random noisy image (c) shown the decryption image (d) histogram of original Lena image, while histogram for encryption image is shown in (e).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

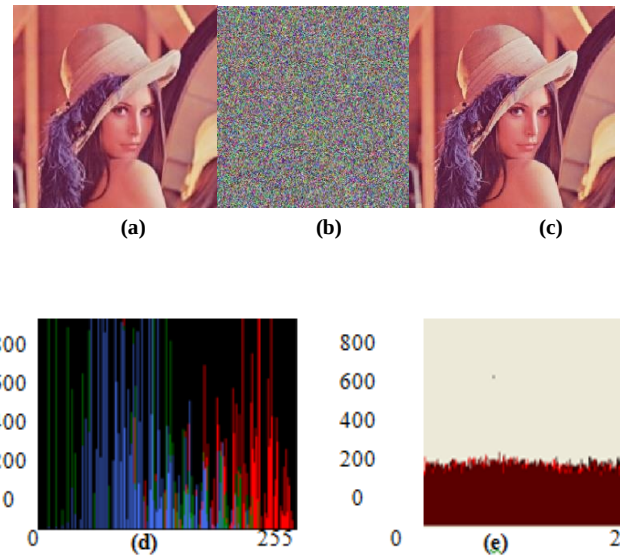

Figure 5: Results of 24-bit BMP image Lena.

Experiment 2 shown in Figure. 6 the result of BMP horse image with 24-bit depth using Pseudo Random Number Generator. (a) The original image, where the encryption image is shown in (b), decrypted image is shown in (c), histogram of original horse image is shown in (d), while histogram of encryption image is shown in (e)

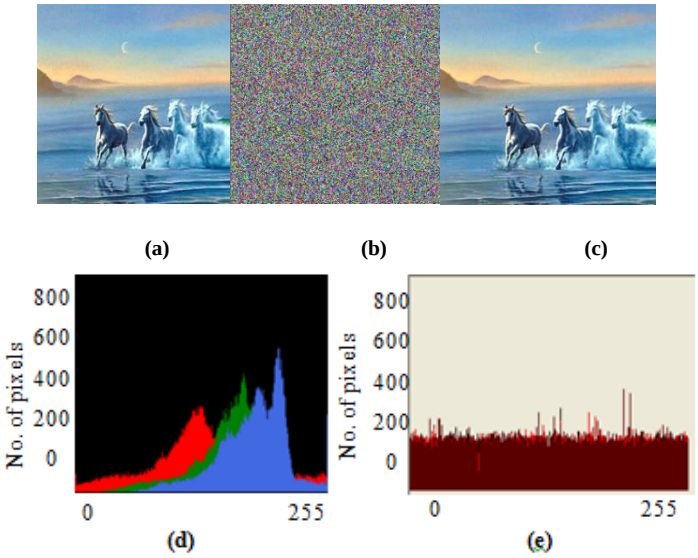

Figure 6: Results of 24-bit BMP image of Horse.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

Table 1and 2, the tests result of LFBSR, NLFBSR and BBS algorithms have been applied to Lena image and Horse image in PSNR and encryption/decryption time.

Algorithm	PSNR	Time Encryption/ Decryption in second
LFBSR	7.9714	7.563
NLFBSR	7.9665	8.993
BBS	7.9662	4.521

Table 1: Lena Image result.

Algorithm	PSNR	Time Encryption/ Decryption in second
LFBSR	7.9680	7.763
NLFBSR	7.9631	9.324
BBS	7.9620	4.689

Table 2: Image horse result.

In Table 3, the five randomness tests have been applied on two ciphered images (Lena & Horse), Statistical analysis has been performed on the proposed image encryption algorithms LFBSR, NLFBSR and BBS and P-values for each randomness statistical tests (<=), as shown in the table.

Image	algorithm	Frequency test <= 3.841	Serial test <=5.991	Poker test <=43.77	Run test <=33.29	Auto-corr. test <=3.841
Lena 24-bit	**LFBSR**	3.619	5.924	40.798	33.09	2.1208
	NLFBSR	2.074	5.586	36.54	30.99	1.389
	BBS	3.394	5.068	38.074	31.177	1.138
Horse 24-bit	**LFBSR**	3.47	4.42	42.39	31.56	1.237
	NLFBSR	3.418	5.25	39.089	32.2	1.309
	BBS	2.315	5.307	35.026	33.068	1.035

TABLE 3: Randomness tests

V. SYSTEM EVALUATION

Many measures could be used to assess the performance of any developed system. In this paper, the evaluation is based on it.

5.1 Histogram of Encrypted Images

Calculate the histogram for two selected colour images of size 256*256 (Lena image and horse image). The histogram of encrypted images for both example shown in Fig (5.e) and Fig (6.e) that encrypted images are different and relatively uniform from original images.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 5, Issue 5, May2017

5.2 Image Encryption and Decryption Time in Seconds

As shown in Tables I and II, the time of encryption or decryption image for both images using three algorithms show that BBS has the minimum time between other algorithms.

5.3 Mean Square Error and Peak Signal to Noise Ratio

From Tables I and II, the results of the three proposed algorithms in this paper show that BBS algorithm is more efficient since it gives high MSE and less PSNR.

VI. CONCLUSIONS

The conclusions that can be produced from this work are listed below :

1. In this paper, a simple to implement and effective methods have been proposed for an encrypted image using Linear Feedback Shift Register with maximum input length 100 bits. The register cycles through the maximum number of 2^{100}-1 which it is the output over more seed, Non-Linear Feedback Shift Register using two or more LFBSR which increase the security level and Blum Blum Shub using two large prime random number this make the algorithm is harder for eavesdroppers to know and make security high .
2. From the histogram results, it is observed that decrypted images for colour images are totally lossless, thereby increasing a level of security significantly.
3. Experimentally with BBS algorithm, the encrypted image is more efficient than the encrypted image in LFBSR and NLFBSR since it gives high MSE and minimum encryption time.
4. From randomness statistical tests, since the *P-value* <= each states for the algorithms BBS, LFBSR and NLFBSR, then the sequence for all algorithms are random.

VII. REFERENCES

1. FA Behrouz, Data Communications and Networking, ed. 5. 2012: McGraw-Hill 2012.
2. PP Dang, PM Chau, Image Encryption for Secure Internet Multimedia Applications. IEEE Trans. Consumer Electronics 2000; 46:395-403.
3. S Shrija, HA Mohammed, Securing Medical Images by Image Encryption using Key Image. International Journal of Computer Applications 2014; 104: 30-34.
4. K Vishal, PT Surya, et al. Two Level Image Encryption using Pseudo Random Number Generators. International Journal of Computer Applications 2015; 115:1-4.
5. BK Arihant, T Namita, Image Encryption using Pseudo Random Number Generators. International Journal of Computer Applications 2013; 67:1-8.
6. L Suhad, HA Najwan, Color Image Encryption using Random Password Seed and Linear Feed Back Shift Register. Journal of Al-Nahrain University 2011; 14:186-192.
7. W Mark, Web's random numbers are too weak, researchers warn. Technology correspondent, BBC News in Las Vegas 2015.
8. R Andrew, S Juan, et al. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology Special Publication 2010; 131.
9. KE Donald, Pseudo randomness. The Art of Computer Programming 2009; 2.
10. K Choi, KCT Jung, The importance of PN Sequences in the Design of Spread Spectrum Systems. IEEE Trans. Commun 2001.
11. S William, Cryptography and Network Security: Principle and Practice, ed. 7th. 2017: Prentice Hall. 752.
12. QRS Gamil, TN Sanjay, Encrypting Image By Using Fuzzy Logic Algorithm. International Journal of Image Processing and Vision Sciences 2013; 2.
13. EL Lehmann, C George, Theory of Point Estimation ed. 2, New York: Springer 1998; 590.
14. G Mohammed, Q Huynh, Scope of validity of PSNR in image/video quality assessment. IEEE Xplore 2008; 44:800-801.
15.MJ Alfred, OVC Paul, et al. Handbook of Applied Cryptography, ed.5, CRC Press Inc. 2001; 816.