Color Image Encryption using Random Password Seed and Linear Feed Back Shift Register

Suhad Latef, Najwan A. Hassan and Ban N. Dhannoon
Department of Computers, College of Science, Al-Nahrian University, Baghdad-Iraq.
E-mail: suhadlatef@yahoo.com, najtena2003@yahoo.com, dr-ban2001@yahoo.com.

Abstract

With the fast progress of electronic data exchange, information security was become more important in data storage and transmission. And because of widely use of images in industrial process, it is important to protect the confidential image data from unauthorized access. In this paper, a proposed seed was generate as a key to a *Linear Feed Back Shift Register (LFBSR)* which applied on the RGB color image (Bmp image) with random keys=2^{100}. The performance of this algorithm has been implemented on two types of Bmp image, the 8-bit Bmp image (palletized image) and 24-bit Bmp image.

Keywords: image encryption, decryption, linear feed back shift register.

1-Introduction

Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

Images are different from text. This means not all traditional cryptosystems are suitable to encrypt images directly. It is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Security is needed against two types of attacks, namely, casual listening (observers) or professional unauthorized recipients, termed as cryptanalysts. In the former case, the security is needed only in terms of hours while in the later it may be in terms of years. The duration roughly indicates the amount of time that is needed to analyze the information available in unintelligible form in the insecure channel without the knowledge of keys to derive the underlying information. The scenario where security is needed against casual listener (observer), the cryptographic structure should be as simple as possible in order to reduce the cost [1].

In order to transmit secret images to other people, a variety of encryption schemes have been proposed. The proposed scheme in the paper could be applied on 8-bit and 24-bit Bmp images.

2-Background

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images [2].

Image encryption techniques try to convert an image to another one that is hard to understand [2]. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of

image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption [3]. Mitra A *et al*. [4] have proposed a random combinational image encryption approach with bit, pixel and block permutations.

Zhi-Hong Guan *et al*. [5] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image.

Sinha A. and Singh K. [6] proposed an image encryption by using Fractional Fourier Transform (FRFT) and JigSaw Transform (JST) in image bit planes.

In the proposed algorithm 24-bit image the encryption is done on the three components color (Red, Green, and Blue) by generate pseudo random number for each color component using Linear Feed Back Shift Register (LFBSR). In the 8-bit Bmp images we could applied our algorithm either on the index value by generate one pseudo random number or on the palette table by generate three pseudo random numbers, one for each color component. The structure of the Bmp image (24-, and 8-bit image) has been described in the next section and how we applied our algorithm on it after we describe this algorithm.

3- Color Images

Color images can be modeled as three-bands each band could be considered as a monochrome image data, where each band of data corresponding to a different color. The actual information stored in the digital image data is the brightness information in each spectral band. When the image is displayed, the corresponding brightness information is displayed on the screen by picture elements that emit light energy corresponding to that particular color. Typical color images are represented as Red, Green, and Blue, or RGB images. The corresponding color image would have 24-bits/pixel; 8-bits for each of the three color bands (Red, Green, and Blue). Structure of bitmap image file consists of either 3 or 4 parts depending on its type as shown in the following diagram [7]:

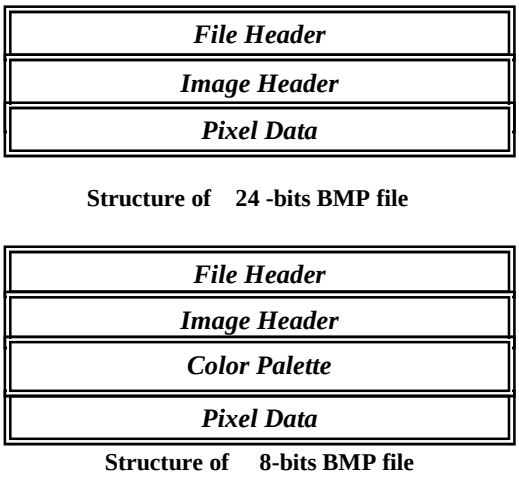

Fig.(1) structure of BMP file.

The first part is a header (file and image), this is followed by an information section, and if the image is indexed color then the palette follows. The last of all is the pixel data which is either index value (one byte) or three color band values (three bytes, one for Red, one for Green, and one for Blue). Information such as the image width and height, the type of compression, the number of colors is contained in the information header.

4-The Proposed Image Encryption System Using LFBSR

Here presentations of image encryption approach using LFBSR. The block diagram of the proposed method is shown in Fig.(2). The password seed is also sent to destination via secured communication channel. The advantage offered by such a scheme is that even if the secret key is known to the attacker somehow but the process of generating the random password seed is unknown, then the attacker will not be able to extract the image. The decrypted image can be obtained as original image by having a reverse method and the password seed only.

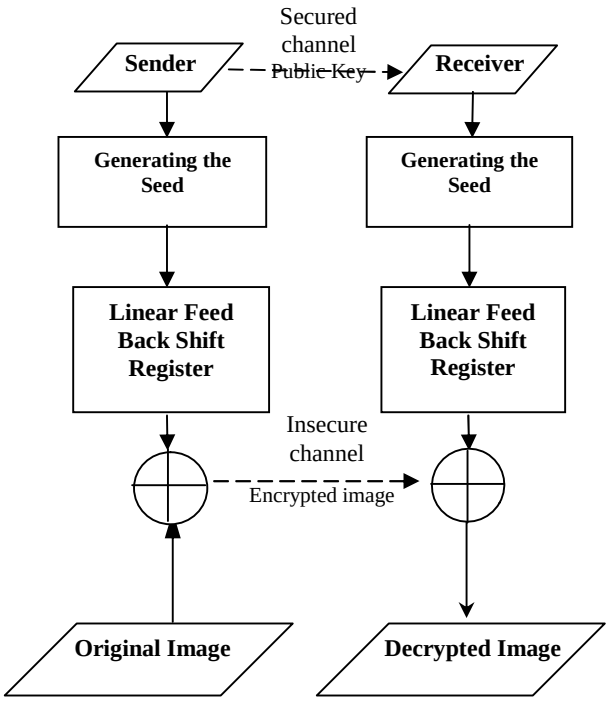

Fig.(2) the block diagram of proposed system.

4-1 Generation of the Seed

The first state in the proposed system is to generate the random password seed number from the secrete key as shown in Fig (3).

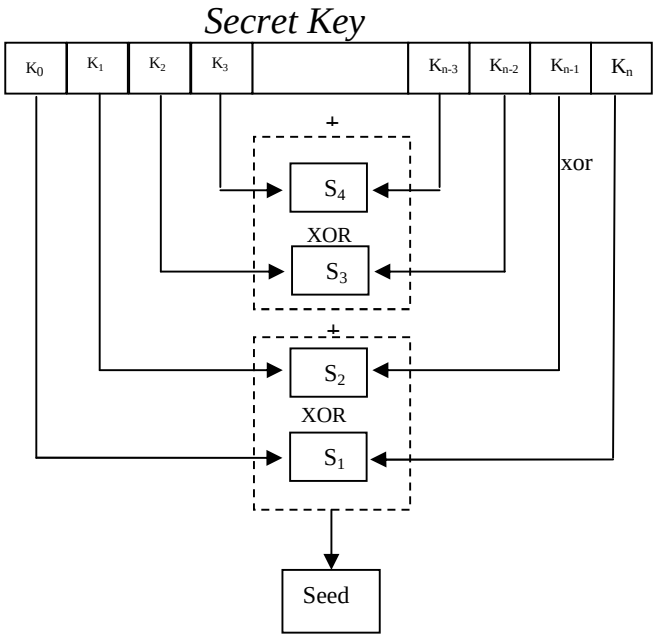

Fig.(3) Generation of seed.

Where

$Seed = S_1 \oplus S_2 + S_3 \oplus S_4 + ... + S_{n-1} \oplus S_n$ …(1)

$S_1 = (K_0 \oplus K_n)$

$S_2 = (K_1 \oplus K_{n-1})$

M

$S_{n/2} = (K_{n/2} \oplus K_{n/2+1})$

4-2 Pseudo Random Number Generator (PRNG)

A pseudo random process is a process that appears random. Pseudo random sequences typically exhibit statistical randomness while being generated by an entirely deterministic causal process. Such a process is easier to produce than a genuine random one, and has the benefit that it can be used again and again to produce exactly the same sequence of numbers, useful for testing and fixing software.

The use of pseudo random number generators is insecure. Where random values are required in cryptography, the goal is to make a message as hard to attack as possible, by eliminating or obscuring the parameters used to encrypt the message from the message itself or from the context in which it is carried. Pseudo random sequences are deterministic and reproducible. [8]

4-2 Linear Feed Back Shift Register (LFBSR)

A very simple and efficient construct is given by linear feedback shift registers (LFBSRs). A LFBSR is composed of a register, which is an array of memory cells, each capable of storing one binary value, and a feedback function, which consists in the XOR operator applied to selected cells of the register [9].

Each new unit of time, the following operations is performing:

1. The content of the last memory cell is output.
2. The register is processed through the feedback function. In other words, selected memory cells are XORed together to produce one bit of feedback.
3. Each element of the register advances one position, the last element being discarded, and the first bit receive the result of the feedback function.

The proposed Pseudo Random Number Generator (PRNG) using LFBSRs. A PRNG contains ***n*** shift registers and is initiated with a starting seed, which is usually transmitted through a secured channel for intended users only. The outputs of the shift registers are multiplied with the coefficients (C_{n-1}, C_{n-2},….,C_1,C_0) of a primitive polynomial with respect to mod-2 operation. The resultant

output obtained by the modulo operation is then feed back to the first shift register. The shift register output values are converted into index (0-255) using bits to byte converter. The general structure of such a PRNG is shown in Fig.(4). [10].

For **n**-stage LFBSR, the number of maximal length sequence is obtained by deleting the nonprimitive polynomials from the number of irreducible polynomials of degree **n** which is given by the formula:

$$f(x) = j\left(\frac{2^n - 1}{n}\right) \quad \text{.....(2)}$$

Where j is the Euler function for $2 \le n \le 100$ [11].

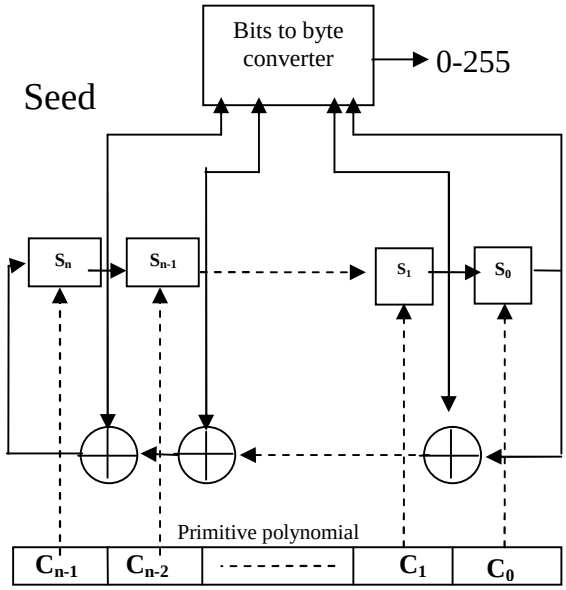

Fig.(4) Structure of a general pseudo random Number generator [4].

Maximal length sequence with period 2^n-1 are generated only in the case when the characteristic polynomial **(x)** is primitive, where **n** is the number of bits and **φ(x)** is the polynomials that have maximum sequence it have primitive polynomial up to degree **n**=100 [12].

Algorithm (1) shows the steps to generate random number using Linear Feed Back Shift Register.

Algorithm (1) Linear Feedback Shift Register

```
Input:
      Size: size of sequence
      Seq: sequence of binary bits
 Output: Random numbers which are
sequence of binary bits
begin
 count=1
 Feedback=0
  Loop for count<= Size
     feedback=feedback+poly*seq[count]
     Where poly is primitive polynomial
     Inc (count)
     Seq_Output[count]=feedback
  End loop count
End
```

5-Expermintal Results and analysis

The proposed system has been implemented using *Visual Basic* and tested several test images.

5-1 Applied LFBSR on 24-bit Bmp image The 24-bit Bmp image is represented as 1-byte for each of the three color bands (Red, Green, and Blue). Thus the LFBSR algorithm is performed to generate pseudo random number ranged from 0 to 255 to encrypt each color band.

5-2 Applied LFBSR on 8-bit Bmp image (on palette) The 8-bit Bmp image is indexed color image, this mean we have a palette table of 256 indexes. Each index refers to three color bands (pixel value) (Red, Green, and Blue). Here, the LFBSR has been performed on a palette table, this mean the encryption was performed on palette table by generate a pseudo random number for each color band that specific index referred to.

5-3 Applied LFBSR on 8-bit Bmp image (on index value) another approach to encrypt the palletized image in this paper is to perform the LFBSR on the index value. The LFBSR will generate one pseudo random number for each index value which refers to three color bands (pixel value).

Below are some experiment applied on standard Lena 24-bit and Horse 8-bit.

In Experiment 1 shown in Fig.(5), the results of 24-*bit BMP* using linear feedback shift

register. Here, the encrypted image appears as a random noisy image as shown in (b). The decrypted image is shown in (c), The histograms of original & encrypted images are shown in Fig.(5) (d) and (f). In the histogram of the encrypted image the nearly uniform random distribution of color image is achieved where the received (decrypted) image is totally noisy.

Experiment 1:

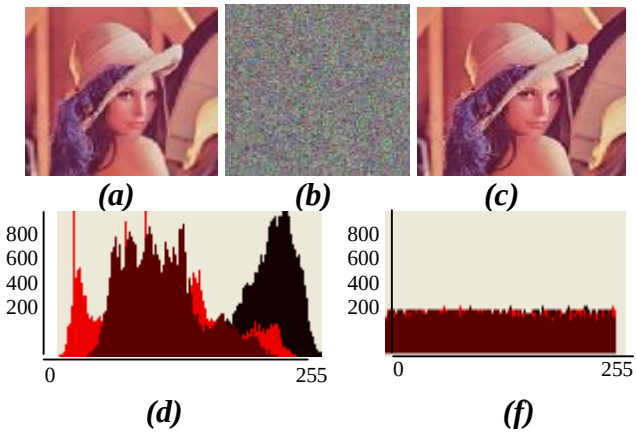

Fig.(5) Results of 24-bit BMP image of Lena. (a) Original image. (b) Encrypted image. (c) Decrypted image.(d) Histograms of Original image. (f) Histograms of encrypted image.

In Experiment 2 shown below, the system was applied of 8-*bit BMP* image. In (b), the encrypted image on palate appears as a random noisy image. Also in (c) the encrypted image on index appear as random as noise image.

Experiment 2:

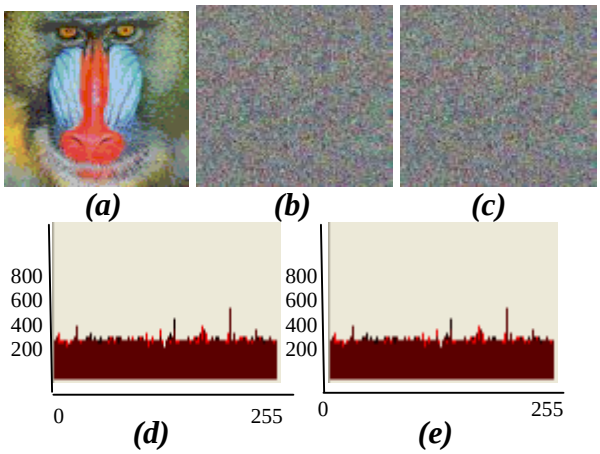

Fig.(6) Results of 8-bit BMP image of Baboon (a) Original image (b) Encrypted image (palate) (c) Encrypted image (index) (d) histogram of encrypted image (palette) (e) histogram of encrypted image(index).

6-System Evaluation

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

6-1 Image encryption and decryption time in seconds, objective fidelity criteria Mean Square Error (MSE) for traditional encryption image using Random Number (RND) function of Visual Basic and encryption image using the proposed random number are shown in Fig.7(a) the time of proposed and tradition shows in Fig.7(b). Where the y-axis in both figures is the types of images define in Table (1).

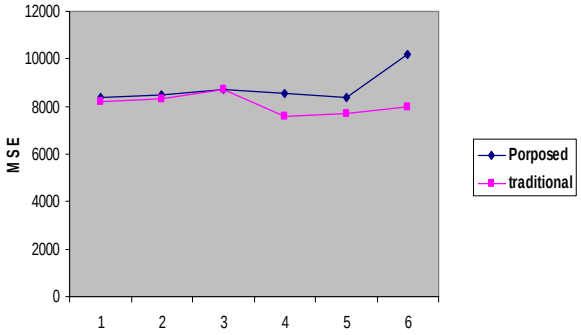

Fig.7(a) The effect of proposed and tradition in MSE.

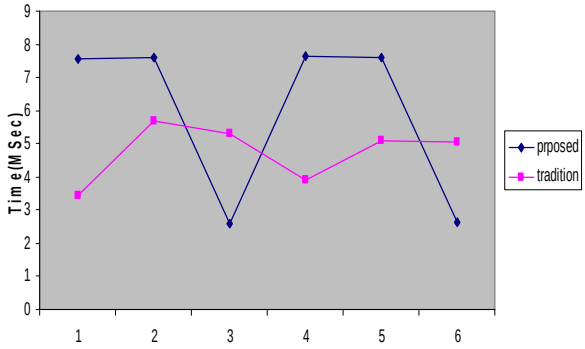

Fig.7(b) The effect of proposed and tradition on time.

6-2 Histogram of encrypted images.

Several color images of size 256×256 that have different contents are selected and calculated their histogram. One typical example among them is shown in Fig.(5.f) and Fig.(6.e), one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original.

Table (1)
Image result.

	Image
1.	Lena 24-bit
2.	Lena 8-bit (palette)
3.	Lena 8-bit (index)
4.	Baboon 24-bit
5.	Baboon 8-bit (palette)
6.	Baboon 8-bit (index)

6-3 The randomness test measures applied on the produced cipher.

Five traditional randomness tests have been applied on the ciphered images, the result tests are shown in Table (2).

Table (2)
Image test.

Image	*Frequency test <= 3.841*	*Serial test <=5.991*	*Poker test <=43.77*	*Run test <=33.29*	*Auto-corr. Test <=3.841*
Lena 24-bit	1.246	3.246	7.465	7.667	0.04
Lena 8-bit (palette encryption)	2.393	4.402	5.230	25.427	0.389
Lena 8-bit (index encryption)	2.393	4.402	5.229	15.729	0.172
Baboon 24-bit	2.256	5.242	10.17	6.229	0.199
Baboon 8-bit (palette encryption)	2.687	25.446	10.78	45.750	0.73
Baboon 8-bit (index encryption)	1.131	4.273	7.532	9.559	0.469

7- Conclusions

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

1- A simple-to-implement method has been proposed in this paper for image encryption using proposed a random password seed number from the secrete key and a Linear Feed Back 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 a seed.
2- From the results, it is observed that decrypted images for all color images are totally lossless, thereby increasing level of security significantly.
3- Experimentally with 8-bit images, encrypt the index value is more effective than encrypt the palette table even more than encrypt the 24-bit image since it give us high MSE and minimum encryption time.

6-Refeneces

[1] P. P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications," IEEE Trans. Consumer Electronics, Vol. 46, No. 3, pp. 395-403, Aug. 2000.

[2] Li. Shujun, X. Zheng Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, page(s):708,711.

[3] S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," *Journal of Pattern Recognition Society*, Vol. 37, No. 4, pp.725– 737, 2004.

[4] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," *Journal of computer Science* Vol. 1, No. 1, p.127, 2006, Available: http://www.enformatika.org.

[5] G. Zhi-Hong, H. Fangjun, and G.Wenjie, "Chaos based image encryption algorithm," *Department of Electrical and computer Engineering*, University of Waterloo, ON N2L 3G1, Canada. Published by: *Elsevier*, 2005, pp. 153-157.

[6] A. Sinha, K. Singh, "Image encrypt ion by using fractional Fourier trans form and Jigsaw transform in image bit planes," Source: *optical engineering, spie-int society optical engineering*, vol. 44, No. 5, 2005, pp.15-18.

[7] John C. Russ, "Image Processing handbook", CRC Press, fifth edition, 2006.

[8] Donald E. Knuth, "Pseudo randomness", The Art of Computer Programming, Vol., March 2009.

[9] L. T.Wang and E. J. McCluskey, "Linear Feedback Shift Register Design Using Cyclic Codes", IEEE Trans. Computers, Vol. 37, No. 10, 1988.
[10] A. Fuster and L. J. Garcia, "An efficient algorithm to generate binary sequences for cryptographic purposes", Theoretical Computer Science, 2001.
[11] K. Choi, K. Cheun, and T. Jung, "The importance of PN Sequences in the Design of Spread Spectrum Systems" IEEE Trans. Commun., 2001.
[12] Roy Ward, Tim Molteno, "Table of Linear Feedback Shift Registers", October 26, 2007.

الخلاصة:

مع التطور الكبير لطرق نقل المعلومات الالكترونية، امنية المعلومات اصبحت مهمة جداً في خزن البيانات ونقلها وبسبب الاستخدام الواسع للصور في المجالات الصناعية من المهم حماية هذة الصور من الاشخاص غير المخولين. في هذا البحث اقترح توليد مفتاح باستخدام طريقه توليد الارقام شبه العشوائيه الخطيه حيث استخدمت على الصور الملونه من نوع BMP مع مفتاح عشوائي يصل الى 2^{100} لتشفير هذة الصور. الخوارزمية المقترحة طبقت على نوعين من الصور من نوع BMP وهي الـ 8 بت والـ24 بت.