Digital Image Encryption using AES and Random Number Generator

Noor Kareem Jumaa
Computer Technology Engineering DEPT.
Al-Mansour University College
Baghdad, Iraq
noor.jumaa @muc.edu.iq

Abstract *In nowadays world of rapid evolution of exchanging digital data, data protection is required to protect data from the unauthorized parities. With the widely use of digital images of diverse fields, it is important to conserve the confidentiality of image's data form any without authorization access. In this paper the problem of secret key exchanging with the communicated parities had been solved by using a random number generator which based on Linear Feedback Shift Register (LFSR). The encryption/decryption is based on Advance Encryption Standard (AES) with the random key generator. Also, in this paper, both grayscale and colored RGB images have been encrypted/decrypted. The functionality of proposed system of this paper, is concerned with three features: First feature, is dealing with the obstetrics of truly random and secure encryption key while the second one deals with encrypting the plain or secret image using AES algorithm and the third concern is the extraction the original image by decrypting the encrypted or cipher one. "Mean Square Error (MSE)", "Peak Signal to Noise Ratio (PSNR)", "Normalized Correlation (NK)", and "Normalized Absolute Error (NAE)" are measured for both (original-encrypted) images and (original-decrypted) image in order to study and analyze the performance of the proposed system according to image quality features.*

Index Terms— AES, LFSR, secret key exchange, MSE, PSNR.

1. INTRODUCTION

'Encryption' is the transformation of a 'plain' message into a senseless form called a 'cipher' that cannot be read by any persons without decrypting the encrypted message. 'Decryption' is the opposite process of encryption which defined as the procedure of converting the encrypted message into its original plain form so, it can be read. [1]

With the technological evolution, data protection over Internet and other communication systems will be the great concern. 'Encryption' is a widespread technique to uphold the security of images. Video and image encryption have many applications in different fields including multimedia systems, internet communication, Tele-medicine, medical imaging, and military communication. [2]

Problems of image security arises due to the usage of computers, cell phones, mobile devices, and many other communication devices. Security of digital images encryption is based on two levels: "low-level security encryption" and "high-level security encryption". In "low-level security encryption", the encrypted image has low visual quality by compression with that of the original image, but the image contents still understandable and visible to the viewers. In 'high-level security', the content is totally scrambled and the image looks just like random noise. In this case, the image is not comprehensible absolutely to the viewers. [2, 3]

In this paper, grayscale images and RGB images have been encrypted/decrypted using AES cryptographic algorithm which is a symmetric key (secret key) algorithm which use the same key that used in encryption process to decrypt the cipher data.

With secret key cryptographic systems (also known as symmetric key cryptographic systems), the communicating parities (Alice and Bob) are using the same key to encrypt/ decrypt a message. One of the considerable problems with symmetric key cryptography is the 'logistical issue of how to get the key from one parity to the other without allowing access to an attacker'. [4, 5]

In this paper, the problem of secret key distribution is solved by using a random key generator (described later in section 3.1.3).

This paper is organized as follows. Section 2 shows a brief survey of the related works, Section 3 discuss the modeling of the proposed system details, section 4 contains the proposed cryptographic system for the grayscale image, section 5 presents the proposed cryptographic system for RGB image, section 6 contains the results and discussions, and the last section (section 7) concludes the paper.

2. Literature Review

In [3], the researcher uses the standard AES to encrypt/decrypt digital images in order to provide security to transmitted images over the communication media.
In [4], the researcher uses the AES to encrypt a plaintext message and hide the cipher text within grayscale image using the LSB steganography technique. Also, she uses the LFSR as a random pixeles generator.
In [6], the researchers proposed a cryptosystem algorithm for the coloured images. Their work inspected two encryption algorithms Huxia and PCACH and compared between these two algorithms.
In [7], the researcher encrypts a colored images using 3D Chaotic Map with AES key Dependent S-Box.

3. Modelling of Proposed System

The proposed system of this paper was modelled and designed within three concerns: secret key generation, image encryption, and image decryption which are discussed in the following sub sections.

3.1 Key Generation

One of the main concerns in symmetric cryptographic systems is how to share a truly random and secure key for both encryption and decryption processes in secure manner. in this paper, a symmetric random key has been generated using **LFSR** algorithm.
A sixteen-byte cryptographic key is generated randomly in order to be used later in AES encryption/decryption algorithms.

3.1.1 LFSR Random key generator

The words "random numbers" are in fact "pseudo random numbers"; since there were no truly random series but pseudo random series of numbers. Pseudo Random Numbers Generators (PRNG) are generated values in accord with several internal equations. The kind of the equations have a tendency to be such that the values are appeared to be random and possibly even pass many randomness statistical measures. Yet, all the pseudo-random number generators have a cycle. After a single cycle has been pass, some principal property of the numbers repeated in the same order as it appeared before. [4]
Linear Feedback Shift Register (LFSR) is a PRNG. LFSR is a feedback shift register and it is made up of two parts: [4, 10]

- Shift register
- Feedback function

Many types of feedback shift register (FSR) are available, the simplest kind of FSR is the linear feedback shift register (LFSR). Simply, the feedback function is the XOR of particular bits in the register that is list of these bits called a '**tap sequence',** Table 1 shows the relationship between the tap sequence bits and the maximal length of the generated sequence**.**
Only (2^n-1) state counter can be generated with n flip-flops. Normally, the 'all-zeros' state is not allowed because the counter is locked up. LFSR are generating pseudo random numbers within 'maximal-length polynomial' which performs the insurance (2^n-1) states with no repeated states have been generated. Typical LFSR is shown in Figure 1. The maximal-length sequence has the next properties: [4, 8]

1. "The number of ones in a sequence approximately equals the number of zeros".
2. "The statistical distribution of ones and zeros is well defined and always the same".

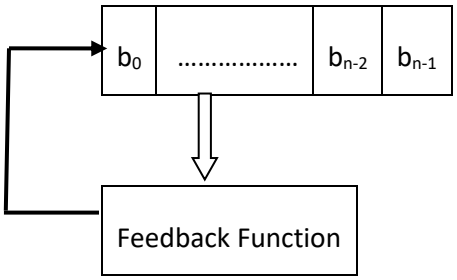


Fig. 1 Typical LFSR.

Table 1. Taps for maximal length LFSRs with 2 to 32 bits.

# of Bits	Length of Loop	Taps
2	3 *	[0,1]
3	7 *	[0,2]
4	15	[0,3]
5	31 *	[1,4]
6	63	[0,5]
7	127 *	[0,6]
8	255	[1,2,3,7]
9	511	[3,8]
10	1,023	[2,9]
11	2,047	[1,10]
12	4,095	[0,3,5,11]
13	8,191	[0,2,3,12]
14	16,383	[0,2,4,13]
15	32,767	[0,14]
16	65,535	[1,2,4,15]
17	131,071 *	[2,16]
18	262,143	[6,17]
19	524,287 *	[0,1,4,18]
20	1,048,575	[2,19]
21	2,097,151	[1,20]
22	4,194,303	[0,21]
23	8,388,607	[4,22]
24	16,777,215	[0,2,3,23]
25	33,554,431	[2,24]
26	67,108,863	[0,1,5,25]
27	134,217,727	[0,1,4,26]
28	268,435,455	[2,27]
29	536,870,911	[1,28]
30	1,073,741,823	[0,3,5,29]
31	2,147,483,647 *	[2,30]
32	4,294,967,295	[1,5,6,31]

3.1.2 Implementation and Results of LFSR

In this research, LFSR with 5 bits loops has been implanted which generate 2^5-1 random states (i.e. 31 random states). The first 16 random states are selected as a 16 bytes secret key of the encryption/decryption processes.

Note that 4 bits loop LFSR cannot be used because the random states that are generated are 2^4-1 state which equal to 15 states and the AES algorithm required 16 bytes thus, the 5 bits loop LFSR is used as a random secret key generator.

Figure 2 shows the flowchart of 5 bits LFSR

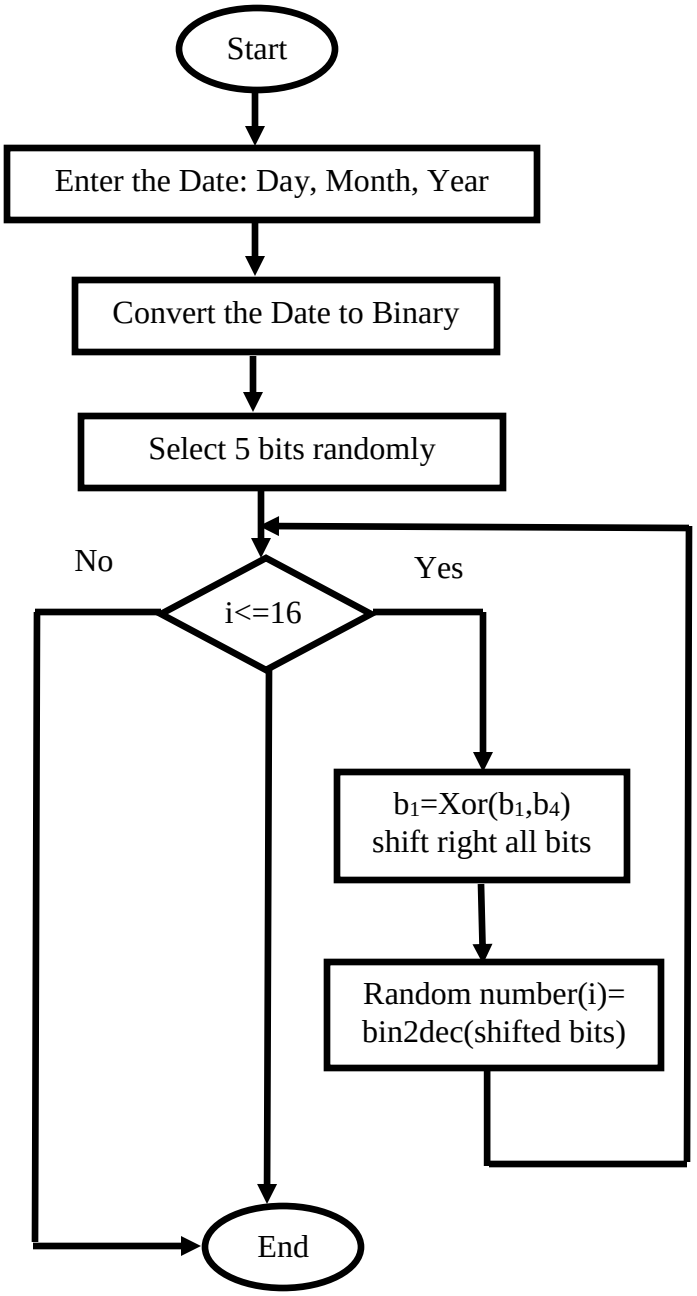


Fig. 2 Five bit LFSR flowchart.

Suppose that the date is 20/12/2017, convert the date to binary:

Day=$(20)_D$=$(10100)_B$

Month=$(12)_D$ =$(1100)_B$

Year=$(2017)_D$ =$(11111100001)_B$

Randomly select 5 bits from day, month, and year bits

day	month	year
10100	1100	11111100001
Initial state= year(11) month(4) day(1) day(3) day(5)= 10110		

Figure 3 below shows the circuit diagram of 5 bit LFSR and Figure 4 shows the generation process.

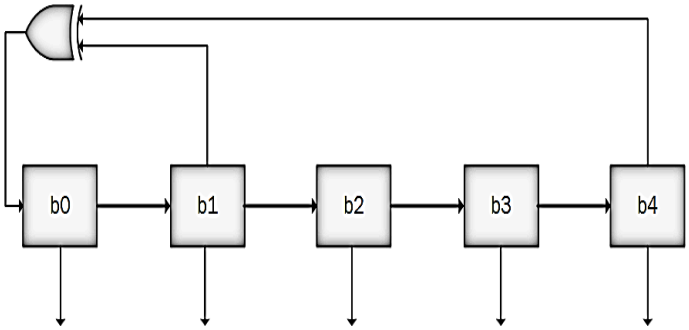
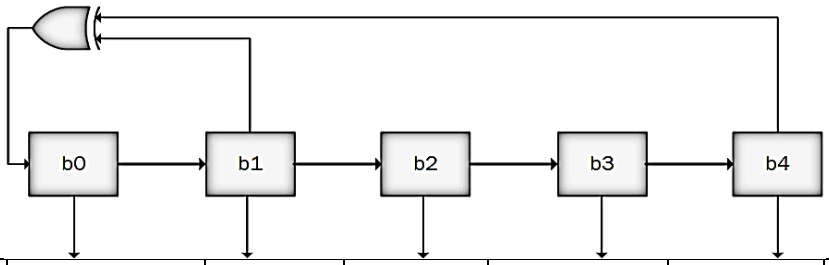


Fig. 3 Five bit LFSR circuit diagram.



	b_1	b_2	b_3	b_4	b_5	Random number
Initial state	1	0	1	1	0	
Loop 1	Xor(1,1)=0	1	0	1	1	11
Loop 2	Xor(0,1)=1	0	1	0	1	21
Loop 3	Xor(1,0)=1	1	0	1	0	26
Loop 4	Xor(1,1)=0	1	1	0	1	13
Loop 5	Xor(0,0)=0	0	1	1	0	6
Loop 6	Xor(0,1)=1	0	0	1	1	19
Loop 7	Xor(1,1)=0	1	0	0	1	9
Loop 8	Xor(0,0)=0	0	1	0	0	4
Loop 9	Xor(0,0)=0	0	0	1	0	2
Loop 10	Xor(0,1)=1	0	0	0	1	17
Loop 11	Xor(1,0)=1	1	0	0	0	24
Loop 12	Xor(1,0)=1	1	1	0	0	28
Loop 13	Xor(1,0)=1	1	1	1	0	30
Loop 14	Xor(1,1)=0	1	1	1	1	15
Loop 15	Xor(0,1)=1	0	1	1	1	23
Loop 16	Xor(1,1)=0	1	0	1	1	13

Fig. 4 Random Number Generator

Thus, the encryption/decryption key is:
11 21 26 13 6 19 9 4 2 17 24 28
30 15 23 13

3.1.3 Sharing of Secret Key

With secret key cryptographic systems (also known as symmetric key cryptographic systems), the communicating parities (Alice and Bob) are using the same key to encrypt/ decrypt a message. One of the considerable problems with symmetric key cryptography is the "logistical issue of how to get the key of one parity to the other without allowing access to an attacker".[4, 5]

In this paper, the problem of secret key distribution is solved by using the present date of each day as an initial state of the random key generator. In this approach, the communicating parities need to know the algorithm which used to generate the key which is 5 bits LFSR and the initial bits. For example, Alice can simply call Bob or text him and say 'year(11) month(4) day(1) day (3) day(5)'. Then Bob uses these bits as initial state to the LFSR algorithm and he got the secret key.

The scenario of this paper is based on the following assumptions:

1. Both Alice and Bob are knowing the encryption/decryption algorithm.
2. Both Alice and Bob are knowing the algorithm of secret key generator.
3. Alice and Bob only share the initial state which present the date of sending/receiving the encrypted image. Figure 5 below shows the communication between Alice and Bob to share the secret key.

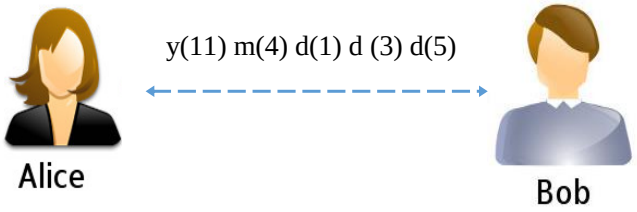


Fig. 5 Sharing of Secret Key.

3.2 Advance Encryption Standard (AES)

The Rijndael offering for AES is to defined a cipher in which length of the block and length of the key independently can specify to be 128, 192, or 256 bits. Based on the size of the used key size, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. Rijndael was designed to consume the following characteristics: [9, 10]

- "Resistance against all known attacks"
- "Speed and code compactness on a wide range of platforms"
- "Design simplicity"

"Image encryption" is the conversion of original image (plain image) into encrypted image (cipher image). Each round consists of the following stages for image encryption process as shown in Figure 6: [3, 9, 10]

- 'SubstituteBytes'
- 'ShiftRow'
- 'MixColumns'
- 'AddRoundKey'

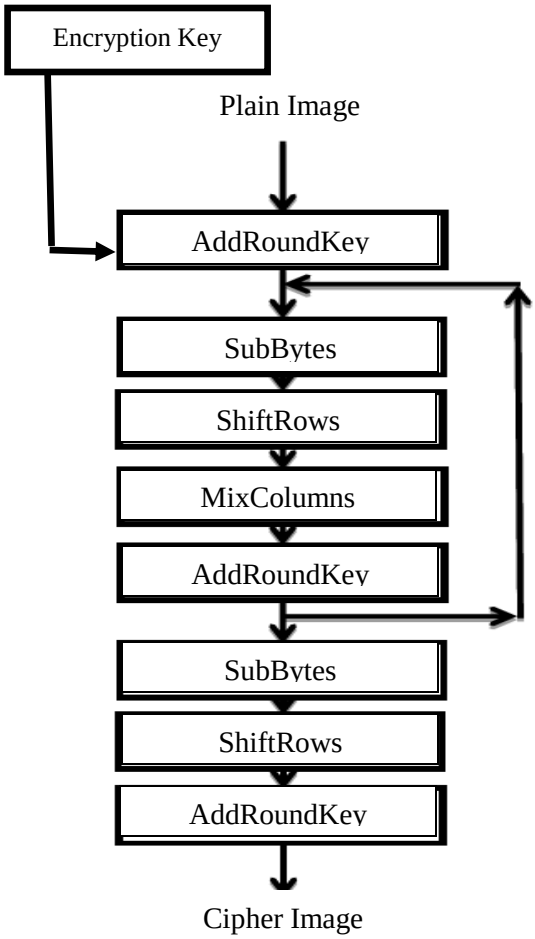


Fig. 6 AES Image Encryption Flowchart.

The details of the round stage are available at [9, 10].

In this paper AES with key size of 128 bits is used.

The reverse of "encryption" is called "decryption". Decryption means the conversion of cipher image into original plain image. Each round consists of the following stages for image decryption process as shown in Figure 6: [3, 10]

- "AddRoundKey"
- "InverseShiftRow"
- "InverseSubstituteByte"
- "InverseMixColumns"

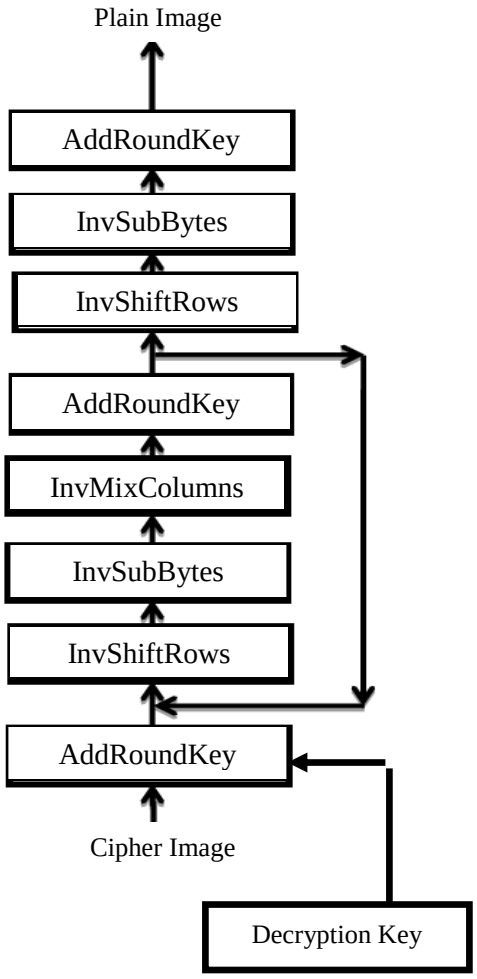


Fig. 7 AES Image Decryption Flowchart.

4. Proposed Cryptographic System for Grayscale Images

For the grayscale images, the encryption system can be described by the following structure shown in Figure 8 while the decryption system shown in Figure 9.

The plain image entered to the AES cryptographic system as an input simultaneously with the 128 bits key which is generated by the LFSR random key generator.

The plain image is broking to block each with 16 bytes size. Each block is entered to the AES cryptographic system, encrypted using the 16 bytes (128 bits) generated from the LFSR, and a cipher image is generated.

Each cipher block of 16 bytes sized are collecting together to form the cipher image which is not understandable image of the viewer.

The whole proposed cryptographic system was implemented using Matlab2017a and a Dell (Inspiron N4050) computer with Intel Core i5 CPU and 64 bit Windows10 OS.

The decryption process is the reverse of encryption process.

he

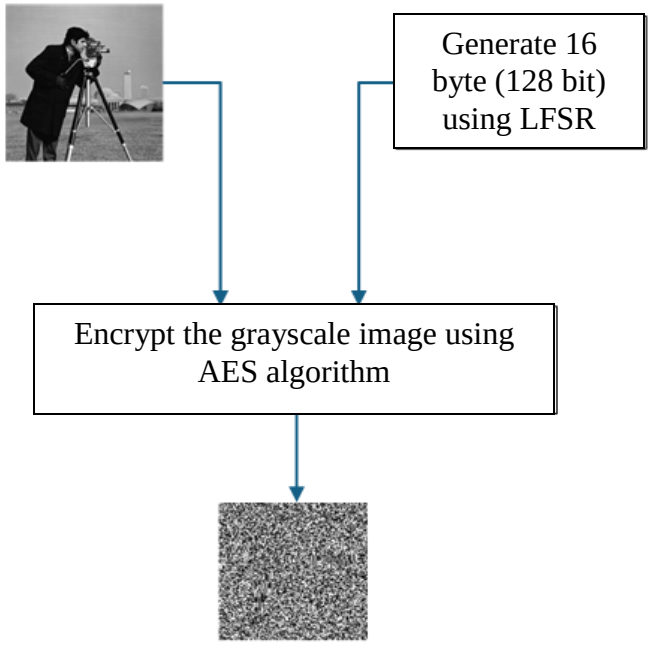


Fig. 8 Structure of the Encryption System for Grayscale image.

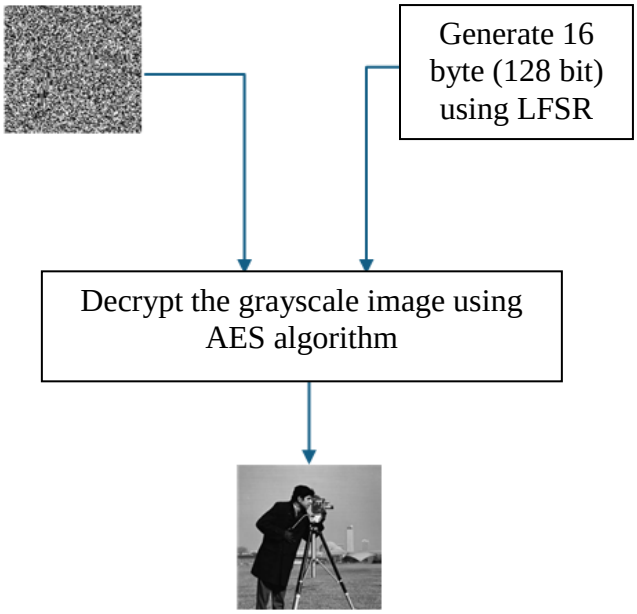


Fig. 9 Structure of the Decryption System for Grayscale image.

5. Proposed Cryptographic System for Colored Images

The encryption system for colored images is illustrated with Figure 10 and the decryption system is shown in Figure 11.

The plain image (RGB image) is broken to its monochrome images i.e. the three images (R image, G image, and B image) each monochrome image are entered to the AES cryptographic system as an input simultaneously with the 128 bits key which is generated by the LFSR random key generator.

Each monochrome plain image is broking to block each with 16 bytes size. Each block is entered to the AES cryptographic system, encrypted using the 16 bytes (128 bits) generated from the LFSR, and a cipher image is generated.

Each cipher block of 16 bytes sized are collecting together to form the cipher image which is not understandable image of the viewer.

Three monochrome cipher images are generated (R cipher image, G cipher image, and B cipher image), collecting the three monochrome cipher images, the cipher RGB image is prepared. Reverse of the encryption is the decryption process which extracts the decrypted image of the encrypted image. The same key is used in both encryption and decryption processes.

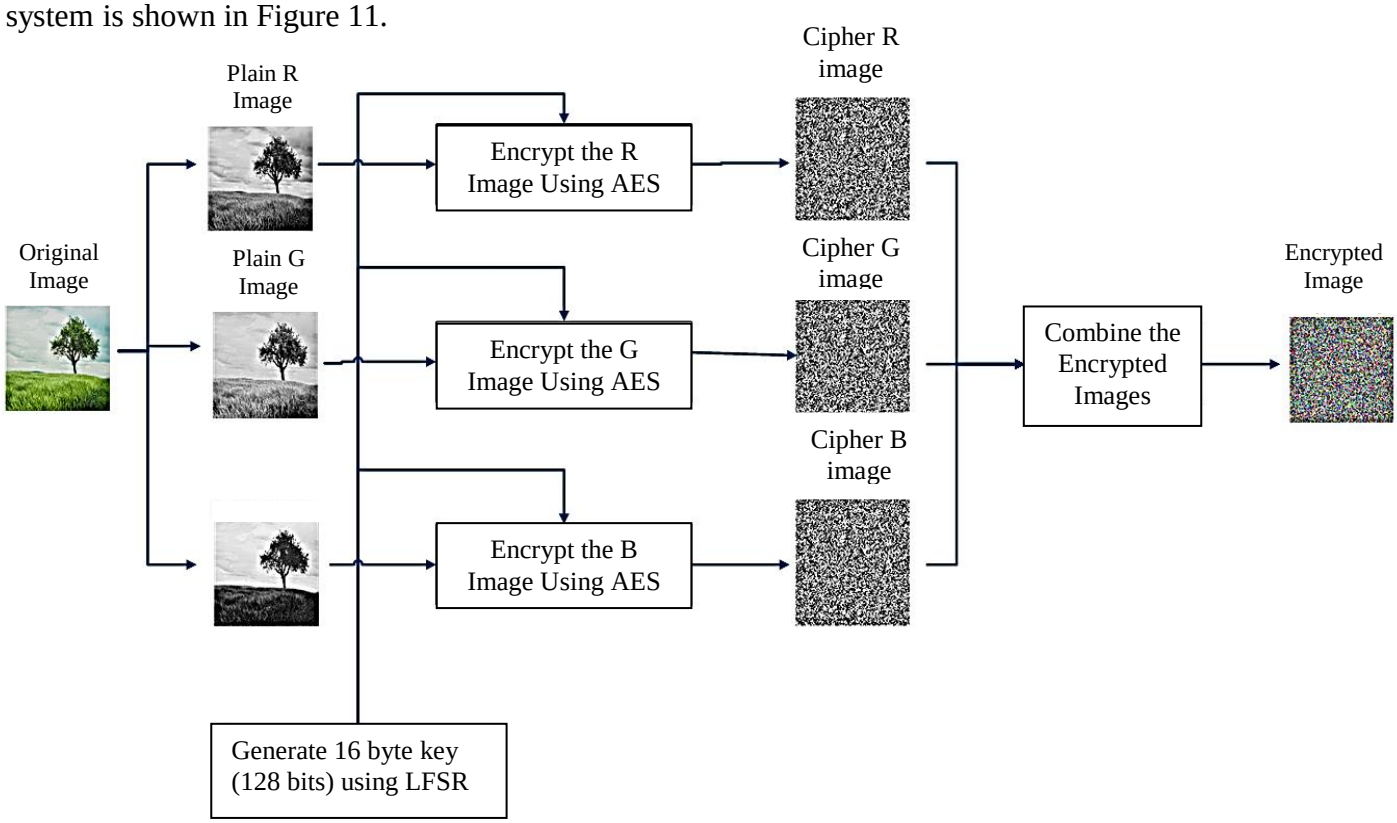


Fig. 10 Structure of the Encryption System for RGB images.

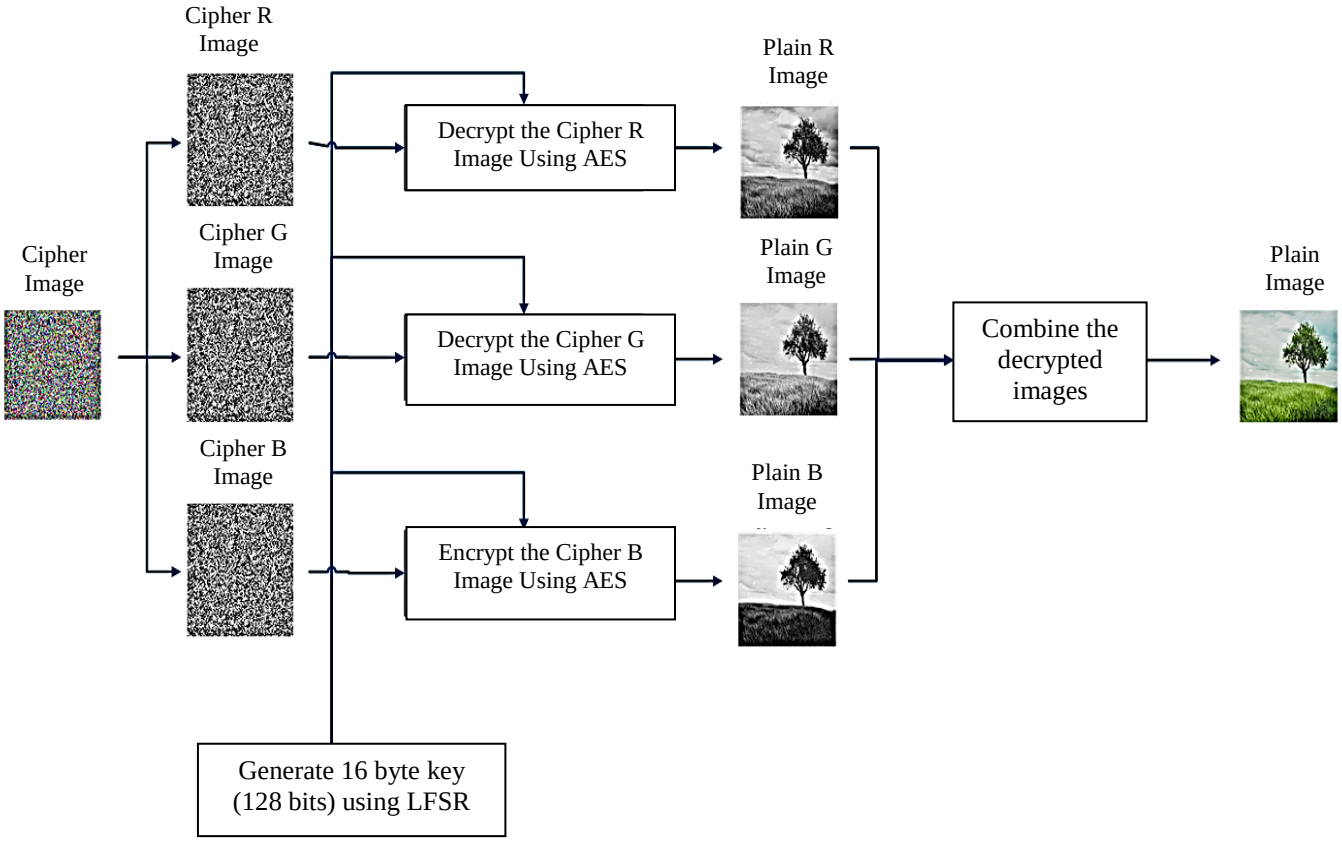


Fig. 11 Structure of the Decryption System for RGB images.

6. Results and Discussions

The obtained results are image quality results and vision results. Image quality is evaluated by calculating the following parameters:

1. **Mean Square Error (MSE):** "MSE is the measurement of average of the square of the difference between the intensities of the stego image and the cover image". [11]

$$MSE = \frac{1}{MN} \sum_{1}^{M} \sum_{1}^{N} (f(i,j) - \bar{f}(i,j))^2 \quad (1)$$

In this paper, MSE has been measured between the plain image and encrypted image also between the plain image and decrypted image.
MSE is one of the most used quality parameter followed by the PSNR.

2. **Peak Signal to Noise Ratio (PSNR):** "The PSNR depicts the measure of reconstruction of the compressed image. This metric is used for discriminating between the cover and stego image". [11]

$$PSNR = \frac{10Log255^2}{MSE} \quad (2)$$

3. **Normalized Correlation (NK):** **"**Normalized Correlation measures the similarity between the two images", [11] i.e. the plain image and the encrypted image. Larger values of NK point to poorer quality of image.

$$NK = \frac{\sum_{1}^{M}\sum_{1}^{N}[f(i,j).\bar{f}(i,j)]}{\sum_{1}^{M}\sum_{1}^{N}(f(i,j))^2} \qquad (3)$$

4. **Normalized Absolute Error (NAE): "**is the measure of how distant is the modified image from the original image with the value of zero being the perfect fit". [11]

$$NAE = \frac{\sum_{1}^{M}\sum_{1}^{N}|[f(i,j).\bar{f}(i,j)]|}{\sum_{1}^{M}\sum_{1}^{N}|f(i,j)|} \qquad (4)$$

Table 2 shows the measurements of image quality parameters for the grayscale images of the plain images and encrypted images while Table 3 shows the same measurements of plain images and decrypted images.

Table 4 shows the measurements of image quality parameters for an RGB image between the plain images and encrypted images while Table 5 shows the same measurements of plain images and decrypted images.

Table 2. (Plain-Encrypted) Grayscale Image Evaluation.

Image	MSE	PSNR	NK	NAE
Greens.png	8.33	-39.2065	0.8707	126.9997
Camera man.bmp	9.34	-39.7055	0.8452	128.0013
Lena.bmp	7.79	-38.9165	0.9018	127.9110

Table 3. (Plain-Decrypted) Grayscale

Image	MSE	PSNR	NK	NAE
Greens.png 4	0	inf	1	145.8623
Camera man.bmp	0	inf	1	151.4510
Lena.bmp	0	inf	1	141.8335

Image Evaluation.

Table 4. (Plain-Encrypted) RGB Image Evaluation.

Image	MSE	PSNR	NK	NAE
R	8.6100	-39.3501	74.5533	127.0654
G	9.346	-39.7064	85.5370	127.5645
B	1.113	-40.4681	65.9847	127.6868

Table 5. (Plain-Encrypted) RGB Image Evaluation

Image	MSE	PSNR	NK	NAE
R	0	Inf	1	167.0314
G	0	Inf	1	182.3906
B	0	Inf	1	173.7477

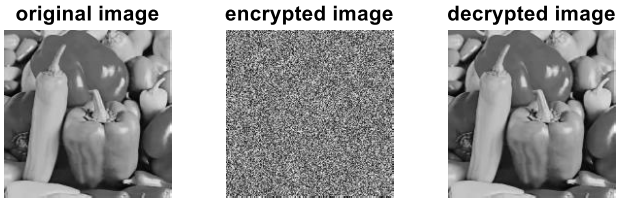


Fig. 12 Greens Image Vision Results.

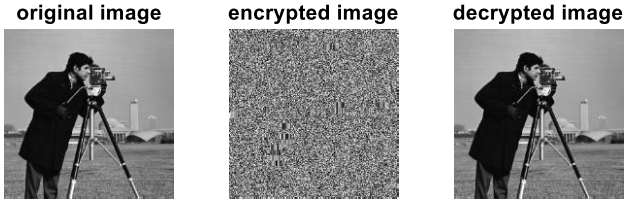


Fig. 13 Camera Man Image Vision Results.

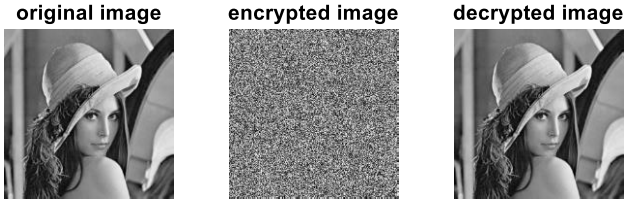


Fig. 14 Lena Image Vision Results.

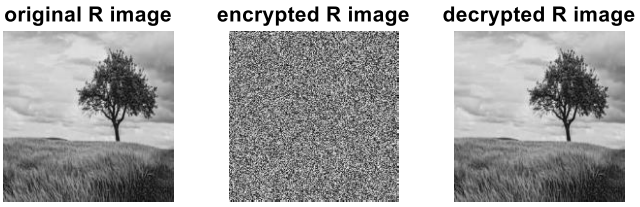


Fig. 15-a. R Image Vision Results

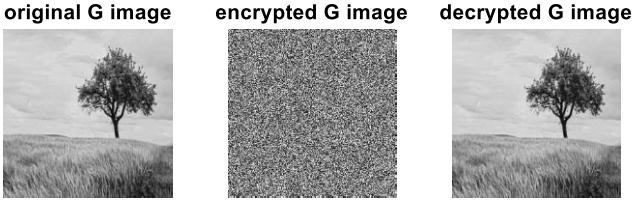


Fig. 15-b. B Image Vision Results

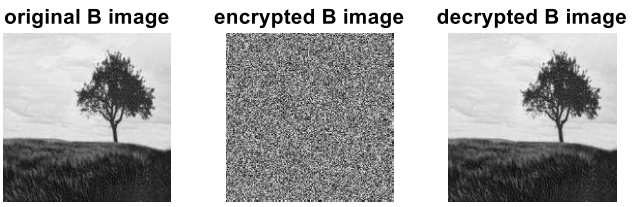


Fig. 15-c. B Image Vision Results.

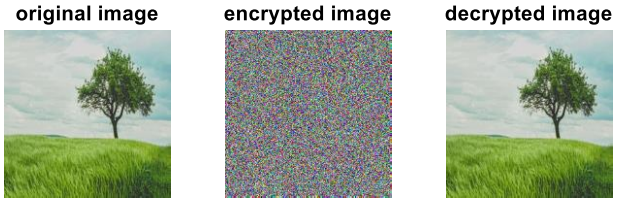


Fig. 15-d. RGB Image Vision Results.

7. Conclusions

The proposed system solves the problem of sharing the secret key by using a random number generator which used the sent date of the encrypted image as an initial state to the random number generator algorithm. The random number generated from the LFSR used as a secret key to encrypt the message at the sender side and to decrypt the message at the receiver side. Image quality parameters have been measured to evaluate the quality of a cipher (encrypted) images and quality of decrypted image. It should be noting that MSE between the plain (original) image the decrypted image is 0 which mean that quality of decrypted image is perfect since it matches the original image. Also (original-decrypted) NK proves the indication obtained from the MSE since it is 1.

References

[1] John Justin M and Manimurugan S, "A Survey on Various Encryption Techniques", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, 2012 .

[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", International Journal of Computer Science and Engineering, Volume 1 Number 1, 2007.

[3] Priya Deshmukh, " An image encryption and decryption using AES algorithm ", International Journal of Scientific & Engineering Research, Volume 7, Issue 2, 2016 .

[4] Noor Kareem Jumaa, "Hiding of Random Permutated Encrypted Text using LSB Steganography with Random Pixels Generator ", International Journal of Computer Applications (0975 – 8887), Volume 113, No. 13, 2015.

[5] IBM Knowledge Center, "Secret Key Cryptography", www.IBM.com.

[6] Osama Abu Zaid, Nawal El-Fishawy, and Elsayed Nigm, "Encryption Quality Measurement of a Proposed Cryptosystem Algorithm for the Colored Images Compared with Another Algorithm", The International Arab Journal of Information Technology", 2015.

[7] Ashwak Mahmood Alabaichi, "Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.10, 2016.

[8] Dr. Ashish Negi et al., "Cryptography Playfair Cipher using Linear Feedback Shift Register", IOSR Journal of Engineering, Vol. 2(5) pp: 1212-1216, ISSN: 2250-3021, 2012.

[9] William Stallings, "*Cryptography and Network Security* Principles and Practices", Fourth Edition, Prentice Hall, 2005.

[10] Sneha Ghoradka and Aparna Shinde, " Review on Image Encryption and Decryption using AES Algorithm ", International Journal of Computer Applications (0975 – 8887),National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015).

[11]Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique", International Journal of Computer Science and Business Informatics, ISSN: 1694-2108, Vol. 1, No. 1, 2013.