EUROPEAN ACADEMIC RESEARCH
Vol. I, Issue 11/ February 2014

ISSN 2286-4822
www.euacademic.org

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

Encryption and Decryption Digital Image Using Confusion System

NOOR D. AL-SHAKARCHI
Computer Science Department, Science College
Karbala University, Karbala
Iraq

Abstract:

Cryptography is considered one of most important and widely methods to provide the secrecy, integrity, confidentiality and message recovery in all multimedia such as digital image and video. Cryptography aims to protect the content of digital image during transmission and to be able to recover its content in receiver's side with sufficient level of accuracy. The strength of encryption and decryption system increased with increasing the randomness and hiding the natural properties to encrypted image. In this research we presented a method to encrypt and decrypt the digital color image. This algorithm is designed and implemented to provide the secrecy, integrity and confidentiality during transmission of the image. This method is proposed depending on the randomness by using confusion algorithm. This confusion provides the system a confusion manner which is considered a very good feature of the encrypted system. The confusion system applies depending on random permutation to color image pixels and blocks. The randomization permutation provided by used pseudo random generation depending on Linear Feed-back Shift Register (LFSR) and Non-Linear Feed-back Shift Register (NLFSR) algorithms. This new proposed Encryption algorithm can ensure the loss of transmissions of images. The proposed encryption Algorithm in this study has been tested on some images and showed good results.

Key words: Encryption Algorithm, Decryption algorithm, LFSR Generator, NLFSR Generator, Confusion Algorithm, autocorrelation function.

1. Introduction:

With the wide development in communication process and fastening on multimedia data, the secrecy of information has become a central issue in data transmission. Particular multimedia application involves protecting its content to verify the security requirements, and that's done by using specifically designed encryption schemes. Digital image is one of most widely used multimedia in communication. Therefore it has become very important to protect the confidentiality of the image data to ensure it is not obtained illegally. Encryption is one way used to send data securely in open network, and regarding images, protection is achieved by converting the original formed image to deformed image.

In response to this need, there have been proposed several digital image encryption algorithms all working to protect the content of digital image, but some are unsafe. The encryption algorithm is used to transmit data in security manner in an open network. Each type of data has its own features, so one must use different techniques in order to fit the type of data (Ramchandra 2009).

Encryption technique must satisfy the digital image properties such as bulk capacity, high redundancy and high correlation among the pixels. Most encryption algorithms used are mainly with text data but these are not suitable for multimedia data such as digital image (Bibhudendra, Patra, and Panda 2010). Colors are analyzed to each pixel of digital color image by getting pixel from image and analyzing to three levels which represent the main color in image Red, Green and Blue. After getting the three colors levels in the image point (pixel) one can encrypt those values using encryption algorithms.

One of main natural image feature is the neighboring pixels that have approximate values (İsmet 2005). The proposed system divides the image into blocks and permutes those

positions and then apply another permutation in each block to be aimed to increase the entropy value. In other words, whenever there is an increased confusion in the cipher system, the entropy value increases also and then the cipher system has a high security.

In this research we present an algorithm which is proposed depending on the randomness by using the confusion algorithm. This confusion provides the system a confusion manner which is considered a very good feature of the encrypted system. The confusion system applies depending on the random permutation to color image pixels. The proposed algorithms provide the secrecy or privacy so no one can see or receive the image, only the authorized person, the integrity to ensure that the image has not been modified and confidentiality to ensure that the image is received at the right place during the transmission of the image. The most important point to be achieved in the case of the proposed algorithms is not to lose the image data during the decryption process, so that the decrypted image is similar to the original image.

The confusion system applies depending on random permutation to color image pixels and blocks. The randomization permutation is provided by used pseudo random generation depending on Linear Feed-back Shift Register (LFSR) and Non-Linear Feed-back Shift Register (NLFSR) algorithms.

2. Related Work:

For a significant time, many researchers and scientists have worked with large efforts for the encryption and decryption of data using various methods. Most of these researches have been applied on digital images to securely transmit the image over the network. An unauthorized user will not be able to access the image data. Many methods have been used to achieve the purpose of image encryption, such as in 2012, when using the

classical cipher system with advanced Hill cipher to "develop a procedure for the encryption of an image by applying modern advanced Hill Cipher including a pair of involuntary matrices as multiplicands and a set of functions" (Samson 2012). Another work using diffusion concept by selective image encryption is based on chaos algorithm (Ismail and Diab 2010).

A proposed system was presented using randomly diffusion concept by using randomly permutation with LFSR and NLFSR generators.

These methods presented fast and randomly decrypted images so that we can recover the original image by a decryption process without distortion or loss data.

3. Digital Color Image Encryption and Decryption:

Encryption technique must satisfy the digital image properties such as bulk capacity, high redundancy and high correlation among the pixels. Most encryption algorithms are used mainly with text data but these are not suitable for multimedia data such as digital images.

The Figure 1 below shows the main algorithms implemented in this research:

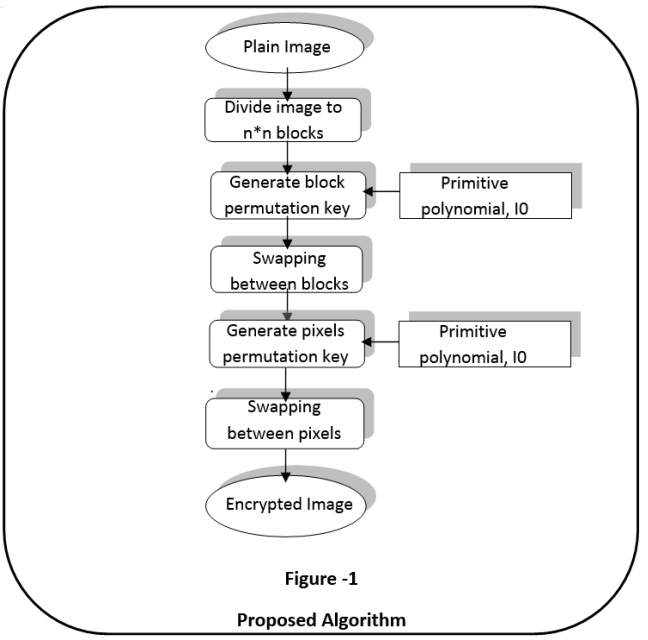


Figure -1

Proposed Algorithm

3.1. Confusion Cipher:

Another method proposed depending on the randomness is by using confusion algorithm. This confusion provides the system a confusion manner which is considered a very good feature of the encrypted system. The confusion system applies depending on random permutation to color image pixels and blocks. The randomization permutation is provided by used pseudo random generation depending on Linear Feed-back Shift Register (LFSR) and Non-Linear Feed-back Shift Register (NLFSR) algorithms.

3.1.1. Encryption and Decryption key generation:

The basic element in proposed cipher system is the encryption and decryption keys (permutation key) generators, which will generate the sequence, determine the permutation sequences to blocks in image and the permutation sequences to pixels in each block. The method most often used in hardware pseudo

generations is by means of the following recurrence relation:

$$X_i = \sum_{k=1}^{m} a_k \, x_{i-k} \qquad I = 0,1,2,3, \ldots, m \qquad \ldots\ldots\ldots (1)$$

Where i is a timing index, Xi €{ 0, 1} are output sequence digits. ak € {0, 1} are constant coefficients. And the summation is modulo-2 addition. With an appropriate choice of the {ak} coefficients, the generated sequence will have the maximal length of period (for a given m) and is called an M-sequence.

A major advantage of the maximal length M-sequence generation method is the simplicity of its implementation as Linear Feedback Shift Register (LFSR). It is simply implemented using m-bits shift registers, which consist of a register R= (r_m , r_{m-1}, ….. , r_1), and a tap T = (t_m , t_{m-1}, ….. , t1), where each r_i and t_i is one binary digit as illustrated in figure …… . At each step, bit ri is appended to the key stream, bits r_m, …, r1 are shifted to right, and a new bit is derived from T and inserted into the left end of the register R.

The cyclic properties of sequence generator are defined by a characteristic polynomial (Goran and Denić, 2011)

$$_{\varphi} = \sum_{k=1}^{m} a_k \, x_{i-k} \qquad \ldots\ldots\ldots\ldots\ldots (2)$$

$a_0 = a_m = 1$ and akj € {0, 1} with j = 1, 2, ……, m-1.

In other words, for any m-stage register with feedback constant c0, c1, …, cn-1, the characteristic polynomial is $f(x) = c_0x^0 + c_1x^1 + \ldots + c_{m-1}x^{m-1} + x$.

The periodic of the sequence generated by the circuit depends on whether polynomial $_{\varphi}(x)$ is primitive and irreducible. Maximal length sequence with period $(2^m - 1)$ is generated only in the case when the characteristic generating polynomial $_{\varphi}(x)$ is primitive and irreducible; that's shown in Figure 2.

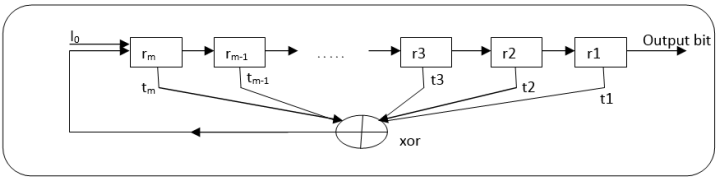


Figure -2 M-sequence Generation (LFSR)

3.3.2 Linear Shift Registers: (Goran and Denić 2011, Serberry and Pieprzyk 1989, Schneier 1996)

A feedback shift register is an implementation of the key stream generator. It is made up of two parts: a shift registers and a feedback functions. The shift register is a sequence of bits. Each time a bit is needed; all the bits in the register are shifted 1 bit to the right. The new left-most bit is computed as a function of the other bits in the register. The output of the shift register is one bit. The simplest kind of feedback shift register is a linear feedback shift register (LFSR) the feedback function is simply the XOR function.

Three parameters: initial state, primitive polynomial, and the length of the register affect the output stream of the linear shift register. For each linear shift register there exists a linear equivalence, which is defined as the length of the smallest linear shift register which can be used to generate the sequence.

3.3.2.1 Register Stages:

Shift registers consist of finite length of binary memory, called stages, for m-binary memory, called m-stages shift register, and in any given time the contents of the register, called state. The register could be in one of 2m states. Zero state is ignored because it causes endless sequence of zeros, thus, we are left with 2^{m-1} state. A next state depends on the feedback function (the mixer).

To achieve maxim length of 2m-1 stages of LFSR, the tap sequence must cause the register to cycle through 2m-1 non

zero bit sequence before repeating. This will happen if the polynomial formed from the elements in the tap sequence is primitive.

3.3.2.2 Primitive polynomial:

When talking about the polynomials, the term prime is replaced by irreducible. Primitive polynomial of degree n is defined as an irreducible polynomial that divides $x^{2n-1} + 1$, but not $x^d + 1$ for any d that divides 2^n-1. A polynomial is irreducible if it cannot be expressed as the product of two other polynomials (except 1 and itself). In another meaning maximal length sequences with period 2^n-1 are generated only in the case when the characteristic (generating) polynomial $\varphi(x)$ is primitive, irreducible, and the initial state of the register must be other than zero.

3.3.3 Non Linear Shift Register: (Serberry and Pieprzyk 1989, Schneier 1996, Stalling 2005)

Linear feedback shift registers are unsafe because they have relatively small linear complexity, and hence a relatively small fragment of the key (LFSR sequence) can be used to obtain the entire sequence by solving a set of linear equation. To increase the linear complexity of LFSR, one or more output sequence of LFSR's are combined with some nonlinear function to produce relatively high linear complexity.

3.3.3.1 Non Linear Feedback Shift Register system:

This is one in which the key generator is a shift register with nonlinear feedback function, as illustrated in Figure-3. In this type, one LFSR is used with n- stages and non- linear feedback function.

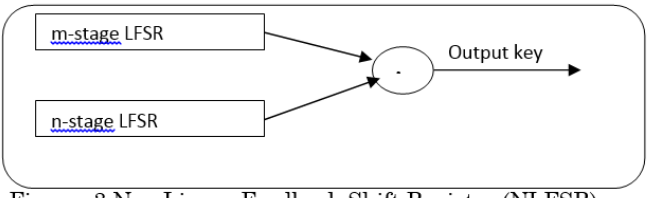


Figure -3 Non Linear Feedback Shift Register (NLFSR)

In this research we used these generators to produce the blocks encryption and decryption keys (block permutation keys); these keys determine the order of blocks (division the original image to blocks), which gives the pseudo random permutation to blocks. Another generation is used to produce the pixel encryption and decryption keys (pixel permutation keys); these keys determine the order of pixels in each block, which gives the pseudo random permutation to pixels. The randomness presented during confusion cipher system gives a harder task to the cryptanalyst.

4. The proposed system:

In order to protect data and images during communication, a cipher system is used to achieve the characteristic of encryption process. These characteristic are:

a. Protect the content of transmission data and images from anyone unauthorized.
b. Protect the transmission data and images from any modification.
c. Verify the transmission of data and images from actual sender.

In this research we present an algorithm to encrypt and decrypt digit color image. The method presented depends on the randomness by using the confusion algorithm. This confusion provides the system a confusion manner which is considered a very good feature of the encrypted system. The confusion system applies depending on random permutation to color image pixels and blocks. The randomization permutation is

provided by used pseudo random generation depending on Linear Feed-back Shift Register (LFSR) and Non-Linear Feed-back Shift Register (NLFSR) algorithms.

4.1 Confusion Cipher System:

The confusion system applies depending on random permutation to color image pixels and blocks. The randomization permutation is provided by used pseudo random generation depending on Linear Feed-back Shift Register (LFSR) and Non-Linear Feed-back Shift Register (NLFSR) algorithms.

- ✓ **The main steps of proposed encryption algorithm are:**

Step1: Read plaintext image.

Step2: Divide the image into blocks of size n*n such as 8*8.

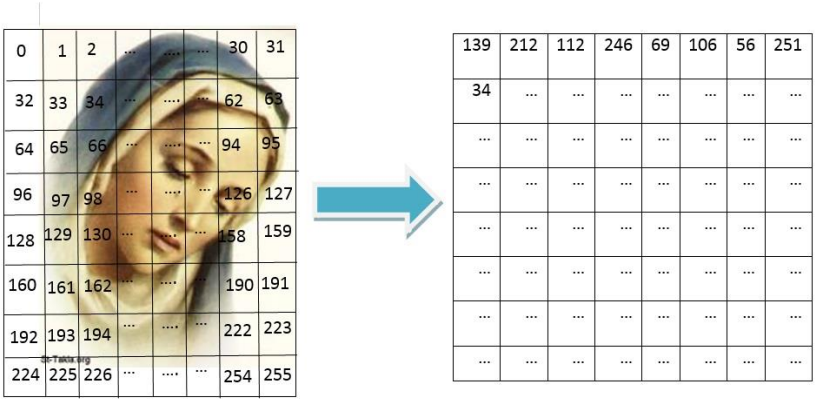
Step3: Applying LFSR with primitive polynomial to generate pseudo random sequence using as key permutation to blocks image pseudo randomly. The order of blocks represent blocks key and shared between the encryption and the deception process (side). One example used in this research - we apply LFSR with primitive polynomial $T(x) = x^5+x^3+x^2+x+1$; and initial value such as I0 = 01011 to produce the pseudo random sequence, such as:

b_1b_2 ..... b_{10}

1101 0001	00101011	00001110	01101111	101 00010	01010110	.....
139	212	112	246	69	106	

Then after we captured each d bits (according to number of images blocks) we used d=8 bits and converted each 10bits block to decimal number representing the blocks order used to permutation blocks (rearrange blocks).

Step4: Rearrange the blocks according to permutation key. Such as:



0	1	2	...	...	30	31
32	33	34	...	...	62	63
64	65	66	...	...	94	95
96	97	98	...	...	126	127
128	129	130	...	...	158	159
160	161	162	...	...	190	191
192	193	194	...	...	222	223
224	225	226	...	...	254	255

139	212	112	246	69	106	56	251
34	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...

Step5: Get blocks orderly.

Step6: For each block generates the permutation key pseudo randomly also by using NLFSR generator to plan the confusion process in blocks pixels. This key represents the permutation key and is shared also between the encryption and decryption process. The NLFSR generator generates pseudo random sequence and represents the location number of pixels used to swap with order pixel in same block.

Practically that's done in this research by using NLFSR generator using 2LFSR. First LFSR used primitive polynomial $T(x) = x^4 + x + 1$ and initial value $I_0 = 1001$. Second LFSR used primitive polynomial $T(x) = x^3 + x + 1$ and initial value $I_0 = 100$. The outputs of these two LFSRs xore to produce the output sequence, such as:

101010	111001	111111	001010	000001	.....
42	57	63	10	1	

Then after we captured each d bits (according to size of image blocks) we used d=6 bits because the size of each block in this research is 8*8, which means that each block contained 64 pixels(0 – 63) and converted each 6bits block to decimal number representing the pixels locations order used in swapping.

Step7: Rearrange pixels in the selected block according to pixel permutation key generate in step 6**.** Pixel permutation key

determine the location of pixel to swapping with plain pixel of selected block, such as:

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

42	57	63	10	1	22	51	9
34	17	6	37	26	50	15	30
3	21	0	31	52	46	4	43
8	23	33	19	38	55	24	60
14	27	2	44	40	25	58	36
37	16	48	54	32	7	47	18
28	59	35	13	61	45	56	49
11	20	41	53	5	39	29	12

Step8: Repeat steps (5, 6, 7) to all blocks of plain image.
Step9: Print the ciphered image.

- ✓ **Decryption Algorithm Steps**

On the receiver's side, for the decryption of the ciphered image, the following steps represent this algorithm:
Step1: Read the ciphered image.
Step2: Divide the image into blocks of size n*n such as 8*8.
Step3: Apply LFSR with primitive polynomial to generate pseudo random sequence using as key permutation to blocks image pseudo randomly. The order of blocks represent blocks key and are shared between the encryption and the decryption process (side). For the example used in encryption process in research we apply LFSR with primitive polynomial $T(x) = x^5+x^3+x^2+x+1$ and the initial value such as I0 = 01011 to produce the pseudo random sequence, such as:

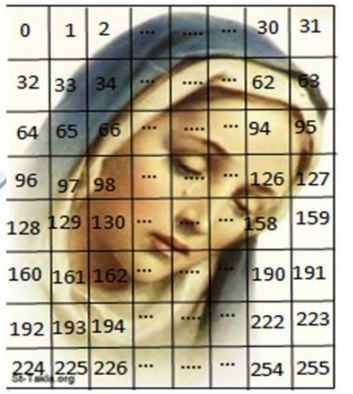
b_1b_2 ..... b_{10}

1101 0001	00101011	00001110	01101111	101 00010	01010110	.....
139	212	112	246	69	106	

Then after we captured each d bits (according to number of images blocks) we used d=8 bits and converted each 10bits block to decimal number representing the blocks order used to permutation blocks (rearrange blocks).

Step4: Retrieve the blocks according to permutation key such as:

139	212	112	246	69	106	56	251
34	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…



Step5: Get blocks orderly.

Step6: For each block one generates the permutation key pseudo randomly also by using NLFSR generator to plan the confusion in the retrieving process of pixels in blocks. The NLFSR generator generates pseudo random sequence, it represents the location number of pixel used to swap and retrieve the original (plain) pixel in same block.

Practically that's done in this research by using the same NLFSR generator used in encryption process. First LFSR used primitive polynomial $T(x) = x^4 + x + 1$ and initial value $I_0 = 1001$. Second LFSR used primitive polynomial $T(x) = x^3 + x + 1$ and initial value $I_0 = 100$. The outputs of these two LFSRs xore to produce the output sequence, such as:

101010	111001	111111	001010	000001	…….
42	57	63	10	1	

Then after we captured each d bits (according to size of image blocks) we used d=6 bits because the size of each block in this research is 8*8, that meaning that each block contained 64 pixels(0 – 63) and converted each 6bits block to decimal number representing the pixels locations order used in swapping.

Step7: arrange pixels in the selected block according to pixel

permutation key generated in step 6. Pixel permutation key determines the location of pixel to re-swapping with cipher pixel of selected block, such as:

42	57	63	10	1	22	51	9
34	17	6	37	26	50	15	30
3	21	0	31	52	46	4	43
8	23	33	19	38	55	24	60
14	27	2	44	40	25	58	36
37	16	48	54	32	7	47	18
28	59	35	13	61	45	56	49
11	20	41	53	5	39	29	12

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Step8: repeat steps (5, 6 and 7) to all blocks of plain image.
Step9: print the cipher image.

Figure 4 below shows the image before and after the Encryption process using confusion way:

a b c

Figure -4

a- original (plain) image b- Encryption image c- Decryption image

Figure 5 below shows the image before and after Encryption process using confusion way:

Figure -5
a- original (plain) image b- Encryption image c- Decryption image

5. Security of Proposed Cryptographic System:

The cryptosystem security depends on the difficulty associated with inverting encryption system. The encryption algorithm will be available for all to study and examine. The correlation and entropy are a measure of security, this protection is evaluated by the uncertainty facing an opponent in determining the permissible keys. The cryptosystem is toward to a lower correlation and a higher entropy value when compared to using the proposed algorithm, as improving the security level of the encrypted images. There are two main keys to increase the entropy: the block permutation key and the pixels permutation key.

The unicity distance U is defined as "a point that may be reached by the cryptanalyst at which a unique solution is possible" (Serberry and Pieprzyk 1989, Stalling 2005, Beker and Piper 1982).

The proposed system is designed according to the diffusion and confusion (Samir, Das, Mukherjee and Ganguly 2008; Jawad 2012). The idea of diffusion is to spread the statistics of the plain (origin) space into statistical structure which involves long combinations of the items in the cryptogram, and therefore spreads the correlations and dependencies of the plain as feasible so as to maximize the unicity distance. The concept of confusion is to make the relation between a cryptogram and the corresponding key a

complex one in order to whitening any indirection to the key as having come from any particular area of the key space.

The security of the proposed system can be evolved using several ways. Some of these ways are:

- ✓ **Histogram:** histogram is one of the security measure criteria used to evaluate the proposed system. We represent the histogram to the original image and compare it with the histogram of the ciphered image.

The histogram is represented by counting the frequency to each color number in image, and saving these frequency counters in **CountColor** matrix. Then we plot from X-axis (which represents color numbers) to Y-axis (which represents frequencies number). The equation done to each color as:

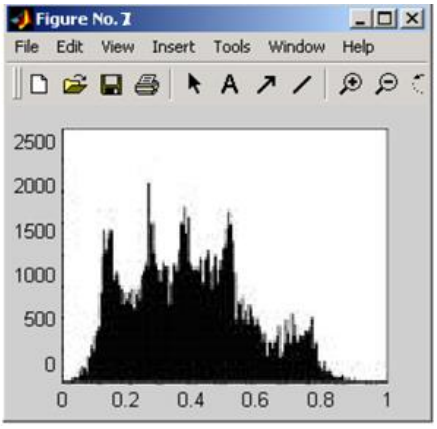
CountColor(Buff(i)) + = 1 .....(3)
CountColor(Buff(i+1)) + =1 .....(4)
CountColor(Buff(i+2)) + = 1 .....(5)

The average of image colors is computed according to the following equation:

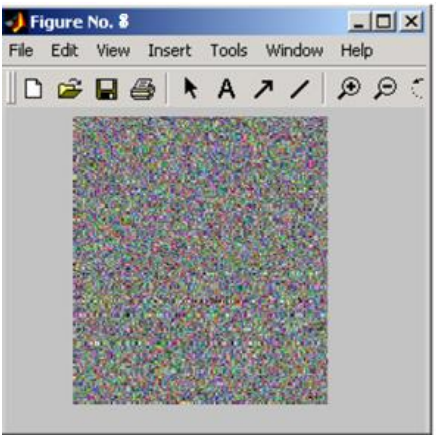
Average = (Buff(i) + Buff(i+ 1) + Buff(i+2)) / 3 .....(6)
CountColor (Average) + = 1 .....(7)

Figures 6, 7, 8, 9 represent the histogram comparison with first example and Figure 7 represents the histogram comparison with second example of proposed system.

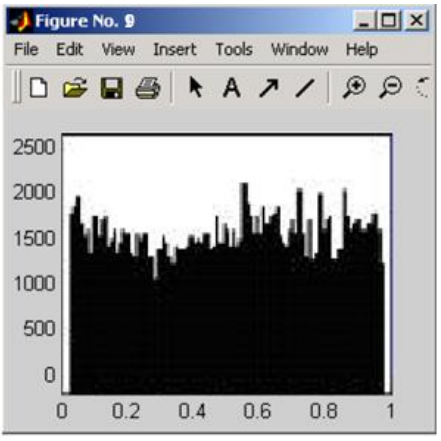
Figures (6)
The original image



Figures (7)
The grayscale histogram of original image



Figures (8)
The cipher image (Encrypted image)



Figures (9)
The grayscale histogram of cipher image

We can see from the above figures that the histogram of encrypted image (cipher image) is uniform and fairly regular, and is significantly different from the original image. Therefore it can't give any note or signal to statistical cryptanalysis and breaking the cipher system. Moreover, there is no loss of image quality after performing encryption and decryption of the original image.

✓ **Randomness and pseudo randomness:**

The second criterion is testing the randomly and pseudo

randomly to cipher (encrypted) image so that if a cryptanalyst intercepts a part of the sequence, and has no information on how to predict what comes next, the sequence is called pseudo-random sequence. Whenever randomness increases the system becomes more secret and the cryptanalysis is hard. Many methods are used to compute the randomness and determine its degree (pseudo randomly degree). The most famous are five statistical tests and autocorrelation function. We used autocorrelation function. It is a mathematical tool for finding repeating patterns. In statistics, the autocorrelation of a random process describes the correlation between values of the process at different times, as a function of the two times or of the time lag (David, 2004); as evaluation proposed system after converting encrypted image to binary image, then deals with it as sequence of binary bits. For example, to part binary image:

$$A(d) = \sum_{i=1}^{n-d} a_i * a_{i+d} \qquad 0 \le a \le n-1$$

$$\mu = \frac{n_1^2 (n-d)+1}{n^2}$$

$$x^2 = \frac{(A(d) - \mu)^2}{\mu} \qquad x^2 \leq 3.841 \text{ for all d.}$$

example:-
when d =1

$$\mu = \frac{(16)^2\,(31\text{-}1)}{(31)^2} = 7.99$$

d =2 $\mu = 7.72$
d = 3 $\mu = 7.45$
d=1

0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0
1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	
0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0	0	0	0	= 8

(And) or (multiplication) operation
A(1) =8

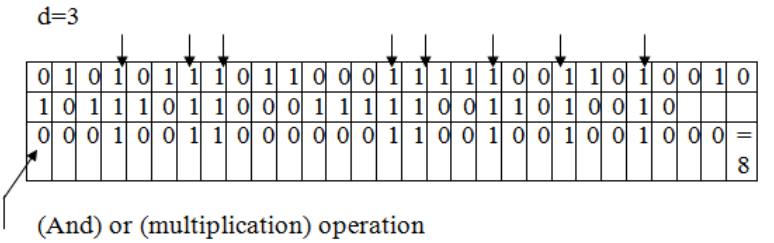
$$x^2 = \frac{(8 - 7.99)^2}{7{,}99} = 0.000125 \leq 3.841 \rightarrow \text{pass}$$

d=2

0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0
0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0		
0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	0	= 8

(And) or (multiplication) operation
A(2) =8

$$x^2 = \frac{(8 - 7.72)^2}{7{,}72} = 0.0101 \leq 3.841 \rightarrow \text{pass}$$



(And) or (multiplication) operation

A(3) =8

$$x^2 = \frac{(8 - 7.45)^2}{7,45} = 1.487 \quad \leq 3.841 \rightarrow \text{pass}$$

6. Conclusion:

The main points we could determine in this research:

1- The project provided high protection for the image data from illegal steals.
2- Speed of the algorithm in image encryption and decryption processes.
3- Obtained encryption and decryption algorithm which is characterized by accuracy and safety.
4- Despite the relative complexity of the algorithm, the decryption process does not involve any loss or modification of image data.
5- The number of blocks and pixels determined by the polynomial used in LFSR and NLFSR key generators. That provides pseudo random keys.

BIBLIOGRAPHY:

Beker, H. and F. Piper. 1982. "Cipher Systems, The Protection of Communications." London: Northwood Books.

Bibhudendra, S., S. K. Patra, and G. Panda. 2010. "Image Encryption Using Advanced Hill Cipher Algorithm." *ACEEE International Journal on Signal and Image Processing* 1(1).

Goran, I. and D.B. Denić. 2011. "Generation and Application of Pseudo Random Sequences for Random Testing." *Facta universitatis*, Series: Automatic Control and Robotics 10(1): 51 - 58.

Jawad, F. 2012. "Efficiency analysis and security evaluation of image encryption schemes." *International journal of video& image processing and network security. IJVIPNS-IJENS* 12(4).

Ismail, M., and H. Diab. 2010 "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps." *International Journal of Network Security* 11(1): 1-10.

İsmet, I. 2005. "Analysis and Comparison of Image Encryption Algorithm." *International Journal of Information Technology* 1(2).

Ramchandra, P. 2009. "Encrypting Informative Image by Key Image using Hill Cipher Technique." *International Journal of Recent Trends in Engineering* 1(1).

Rubin, D. M. 2004. "A Simple Autocorrelation Algorithm for Determining Grain Size from Digital Images of Sediment." *Journal of Sedimentary Research* 74(1):160.

Samir, D., P. Das, S. Mukherjee and D. Ganguly. 2008. "A Secure Scheme for Image Transformation." IEEE SNPD 490-493.

Samson, V. U. 2012. "Cryptography Of A Gray Level Image And A Color Image Using Modern Advanced Hill Cipher Including A Pair Of Involuntary Matrices as Multiplicand And Involving A Set Of Functions." *International Journal of Engineering Science and Technology (IJEST)* 4(7).

Schneier, B. 1996. *Applied Cryptography, Protocols, Algorithms, and Source Codes in C.* Second Edition. John Wiley & Sons.

Serberry, J. and J. Pieprzyk. 1989. *Cryptography. An Introduction to Computer Security*. Prentice Hall.

Stalling, William. 2005. *Cryptography and Network Security Principle and Practices.* Fourth Edition. Prentice Hall.