KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

DOI: https://doi.org/10.32441/kjps.02.02.p12

Robust Digital Image Encryption Approach Based on Extended Large-Scale Randomization Key-Stream Generator

Raghad Zuhair Yousif [1],.Ayad Ghay Ismaeel[2]

[1,] Department of Applied Physics- Communication, Salahaddin University, Erbil, Iraq.

[2] President of Al-Kitab University-Altun Kupri-Kirkuk.

[1]Raghad.yousif@su.edu.krd, [2] dr.ayad.ghany.ismaeel@gmail.com

ABSTRACT

This paper presents a novel image encryption scheme based on extended large-scale randomization key-stream generator. The basic form of the key-stream generator is presented, and employed in digital image ciphering. The modification of the basic form also, presented, and gives encouraging results in image encryption as compared with classical non-linear stream cipher generators and the basic form. Pixel shuffling is performed via vertical and horizontal permutation. Shuffling is used to expand diffusion in the image and dissipate high correlation among image pixels the sequences generated from all presented generators are introduced to five well-known statistical tests of randomness to judge their randomness characteristic. The ciphered images are tested for their residual intelligibility subjectively. The measures applied to images ciphered by one of the classical key-stream cipher generators (Threshold generator) for the purpose of comparison with the presented key-stream algorithms. Experiments results show that the proposed algorithm achieves the image security. In order to evaluate performance, the proposed algorithm was measured through a series of tests. Experimental results illustrate that the proposed scheme shows a good resistance against brute-force and statistical attacks.

Keywords: image encryption, stream cipher, data security

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

نظام محكم لتشفير الصور الرقمية يعتمد على موسع مفتاح التوزيع العشوائي واسع النطاق

رغد زهير يوسف[1] .أياد غني اسماعيل[2]

[1] قسم الفيزياء التطبيقية– الاتصالات ، جامعة صلاح الدين ، أربيل ، العراق.

[2] رئيس جامعة الكتاب – ألتون كوبري – كركوك.العراق.

[1]Raghad.yousif@su.edu.krd, [2] dr.ayad.ghany.ismaeel@gmail.com

الملخص

تقدم هذه الورقة مخططا جديدا لتشفير الصور يقوم على تمديد المولد واسع النطاق العشوائي. لقد قدم الشكل الأساسي لمولد تيار المفتاح، واستخدم في التشفير الصورة الرقمية. تعديل الشكل الأساسي أيضا، قدم، واعطى نتائج مشجعة في تشفير الصور بالمقارنة مع مولدات الشفرات غير الخطية الكلاسيكية والشكل الأساسي. حيث تم تنفيذ خلط عناصر الصورة عن طريق التقليب الرأسي والأفقي. يتم استخدام المراوغة لتوسيع الانتشار في الصورة وتبديد الارتباط البيني بين عناصر الصور ت ايضا عرض المفتاح العشوائي من جميع المولدات المقدمة إلى خمسة اختبارات إحصائية معروفة من العشوائية للحكم على الخصائص العشوائية الخاصة بهم. وتوضح النتائج التجريبية أن الطريقة المقدمة، اظهرت مقاومة جيدة ضد القوة الغاشمة والهجمات الإحصائية.

الكلمات الدالة: تشفير الصور ، دفق التشفير ، أمن البيانات

INTRODUCTION

As computer –networks widely adapted by societies, network security issue becomes essential in this century. Many people need data privacy and feeling it is necessary when they sending or receiving information against unauthorized people [2]. Consequently, digital images represent one of the important information, transmitted through communication networks; hence there must be some techniques to conceal them. The most reliable way is by

employing ciphering algorithm to convert the digital image to unintelligible information. Image coding such as (Huffman code), can be also considered as one of the ways of image data concealment, but coding gives constant (codebook)[3], to each image to be ciphered. On other hand ciphering provides many cipher text to each image, through different transformation keys employing. Fortunately, security algorithms do not have to be expensive or complicated. Such as, stream cipher algorithms that will be focused during the work of this paper and will be applied for image ciphering because of such generators simplicity and perfection (close to one-time-pad) [2],[3],[4]and fast implementation of ciphering process .

2. Image Encryption Using Large–Scale Randomization Stream Cipher Scheme

The Large –Scale Randomization algorithm is composed of mainly two parts as shown in figure (1).

The driving sub-system. The non-linear combining subsystem.

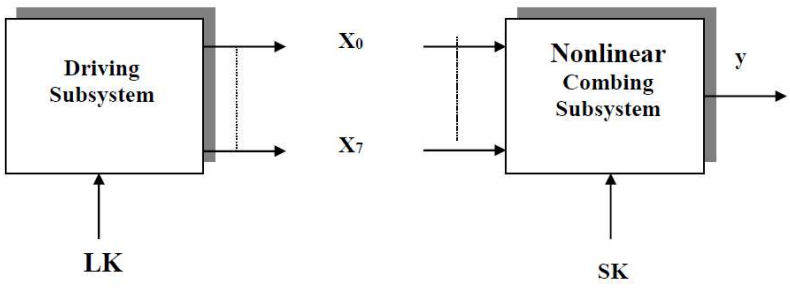

Figure (1) Block diagram of proposed stream cipher generator.

According to deriving sub-system design there are two forms for the presented key-stream generator that will be introduced in the next stage.

Basic Form of the Presented Algorithm

The deriving sub-system for the basic form of the presented algorithm consist of also Two parts as illustrated in figure (2). the first part is the deriving sub-system that involves single group of (LFSRs), this group is called choosing group that illustrated in figure (3).

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

These five bits generate an address to any cell in the g^ container that consist of 32 locations (Session-key). These contents should be selected randomly in other word the container should include random combination of ones and zeros. Ruppel key-stream generator can be used to generate this key.

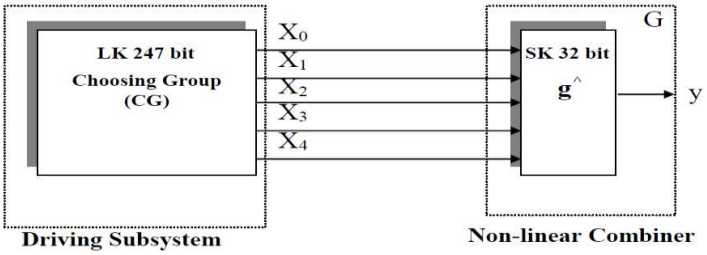

Figure (2) proposed system components

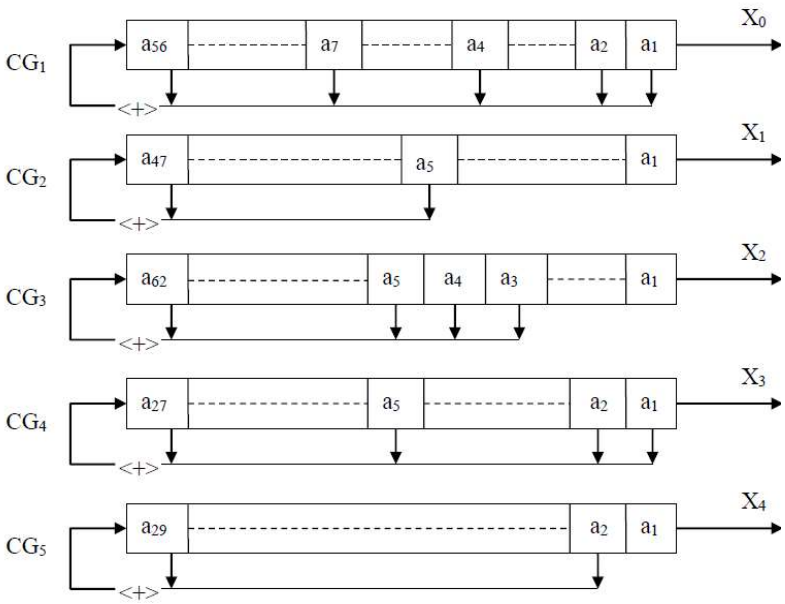

Figure (3) Driving subsystem (Basic form)

Developed Form of the Presented Algorithm

The developed form of the presented algorithm can be considered as an extended form of that presented previously. The extension here applied for driving sub-system and non-linear sub-system. The driving subsystem consists of three groups LFSRs:

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

1-Choosing group (CG): consists of five LFSRs (CG1 – CG5).

2-Rotation group (RG): consists of two LFSRs (RG1, RG2).

3- Directives registers (DR). The deriving sub-system is illustrated in figure (2).

Where, registers of each group have relatively different prime lengths. The content of each LFSR is filled with the sequence of bits derived from the secret key (LK) that will be discussed later. In the design of the non-linear combining sub-system (G) the following requirements have been considered [10],

(1) (G) must transfer the statistical properties of the periodic driving sequences to the generated running key in the sense that, when the input sequences have good properties, so is the output sequence.

(2) (G) must be maximizing the complexity of the running key relative to the complexities of the driving system generators. Linear methods to reliably predict future key stream digits

$$G: \text{Binary}^8 \rightarrow \text{Binary}$$

from any observed part of the key stream is made unfeasible. In the suggested stream cipher generator, the non-linear part assumed is a Boolean function (G) of type:

Which is given in the form:

$$y_j = (g^{\wedge}_j (X_{0}j,\ X_{1}j,\ X_{2j},\ X_{3j},\ X_{4j}, S^{\wedge}_j (X_{5j},\ X_{6j}), P^{\wedge}_j (\ X_{7j}\ )) <+> X_{4j} <+> X_{6j} <+> X_{7j}) \quad (1)$$

Where:

$$S^{\wedge}_j (X_{5j}, X_{6j}) = (X_{5j} + X_{6j}) << 1 \quad (2)$$

And:

$$P^{\wedge}_j (X_{7j}) = \begin{cases} \text{ROTR } (g^{\wedge}, S^{\wedge}) \text{ if } X_{7j} \neq 0 \\ \text{ROTL } (g^{\wedge}, S^{\wedge}) \text{ if } X_{7j} \equiv 0 \end{cases} \quad (3)$$

Where, yj is the output of the function at time j, (X_{0j}, …X_{7j}) are the output bits of the driving stage at time(j) g^j is a 5-bit combining function, it works as a 32-bit container whose contents are initialized by the secret session key (S_k).

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

The input to the function is three groups, where the first group (i.e. X_{0j}, X_{1j}, …X_{4j}) is considered as address, to a certain location (cell) in the container. The second group (X_{5j}, X_{6j}) pass through the operator ($\hat{S}$), whose output will specify the amount of rotation (i.e. the bits length of the rotation). Finally, (X_{7j}) bit which is pushed to the operator (P^) whose output bit will specify the direction of the rotation. The importance of the ($\hat{S}$) and (P^) functions is to increase the immunity that will be illustrated. Figure (4) shows the complete structure of previously presented scheme.

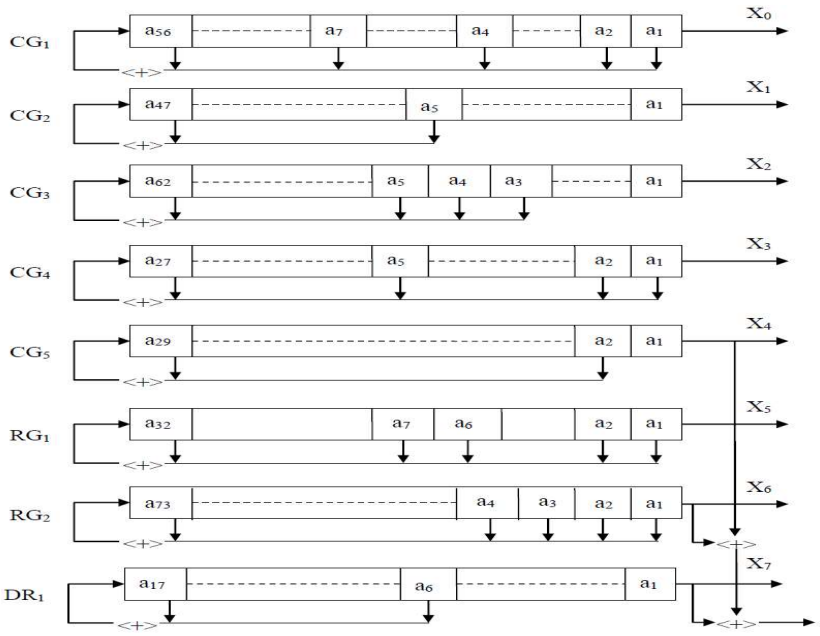

Figure (4) proposed system internal structure

Key Structure

Two different secret keys are involved with the suggested generator these keys are: Session key (SK): 32 bits that should be generated randomly (by the user) with correlation rate equal (0.5). The random generator selected to construct this key is the Reuppel-generator. The value of this generator initial key is: (1011,0101,1100,0100,0110,1101,0111,1010) b (0Xb5C46d7A) H. Linear key (LK): (343) bits are used to initialize the contents of LFSRs with the driving subsystem. Three keys are used; thus, the adopted three keys contain different levels of redundancies, and randomness

which will be considered as a weak randomness (key 1) to the good randomness (key 3). Figure (5) below shows Complete system components

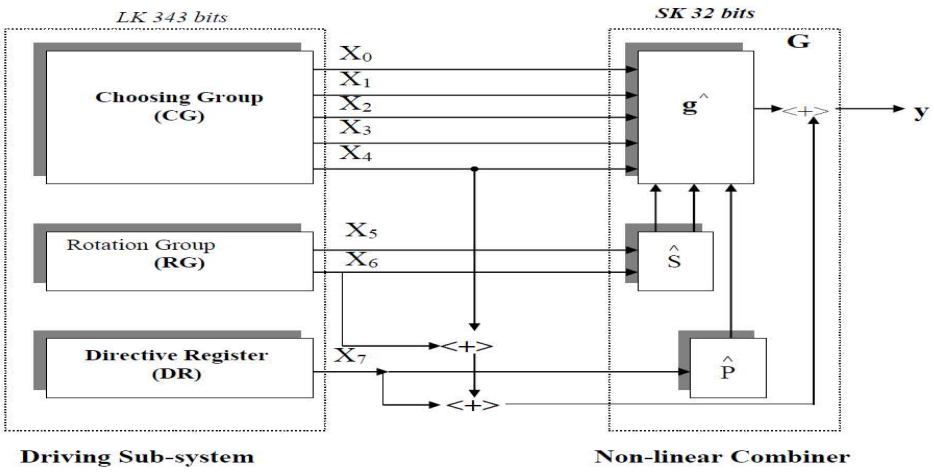

Figure (5) Complete system components

Initialization and Operation

The initialization operation is done by first loading the (LK) (343) bit, to initialize the registers starting from (CG1…CG5) then RG1, RG2, and finally DR receptively. The operation of bits stream generation is started by producing five bits from CG as an address to the session key that is resident in the (g^) container, and then the content of (g^) will be rotated before producing its value. The rotation operation depends on the output of the function (Ŝ) which decide how many positions can be rotated, but the direction of rotation decided by direction operation (P^) (when(X_{j7}=0) to be rotated container content (g^) right and when (X_{7j} =1) the content is rotated to the left). The output bit of generator produced by XORing of the output of (g^) function and output of three registers (CG5, RG2, and DR). XORed together. This operation can be repeated to generate a key sequence [7]. The outline of generator operations can be shown in the following pseudo code, which written in C++ notation:

Step1: Input = SK, LK, no. of cycles.

Step2: Initial LFSRs with LK.

Initial ($g^{\wedge}$) with SK.

Step3: I=1

Step4: If I>no. of cycles then go to step 12.

Step5: Shifting of LFSRs, and producing $X_0, X_1, \ldots, X_7$.

Step6: Address = 0.

Step7: For j=0; j <5 ; j ++

Address = Address $\oplus$ X_j << j

End for.

Step8: No. of rotations = X_5+X_6 << 1;

Step9: For K = 0; K < no. of rotations; K ++

IF X_7 = = 0 the rotate ($g^{\wedge}$) to the left

Else

Rotate ($g^{\wedge}$) to the right

End for

Step10: Output = ($g^{\wedge}$[Address] + X_4 +X_6 +X_7) mod (2);

Step11: I = I+1, Goto step 4.

Step12: Stop

Expected Sequence Period

The architecture of this algorithm is chosen so that the size of period (L) is such that the system is computationally secure against linearization attacking i.e. L $\cong 2^{343}$. This value is derived by the fact that the period (Li) of the sub-generators (i) is given by:

$$L = \prod_{i=1}^{N} L \qquad \ldots(4)$$

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Where N = number of sub-generators. Then it can be show that, the period of sub-generators: $L_1 = \prod_{i=1}^{8} (2^{Li} - 1) \approx 2^{343}$ **bits**

On the other hand, the period of the non-linear part is the period of three functions (g^), (S^), (P^) which can be computed as:

$$L_2 = \prod_{i=1}^{3} 2^{Li} = 2^1 * 2^2 * 2^{32} = 2^{35} \quad \textbf{bits}$$

Therefore, the overall period (L) of the system becomes :

$$L_T = (L_1) * (L_2) \approx 2^{378} \quad \textbf{bits.}$$

The size of period makes attack becomes unfeasible and suitable for huge data (such as image information) ciphering the different (LFSRs)[5].One of the classical Non-linear stream cipher generators is threshold generator in which the combination function checks the majority of ones ,thus if more than half the output bits from each sub-generator(X1,X2,X3…).Includes '1'more than '0' then the output of generator is '0'.The output of generator can be written as[1]:

$$y=(X_1<*>X_2)<+>(X_1<*>X_3)<+>(X_2<*>X_3) \quad \ldots(5)$$

Where y is the output of generator and <*>denotes logical AND.

3. Image Ciphering by Presented Algorithm

To cipher digital images by the proposed algorithm .The following procedure must be followed .If M represents whole image pixel values M is divided in to successive parts mij ,i.e.,m11 ,m12 ,…..mn1 n2 where 1<i , j < n1 , n2 ,then if m11 ,m12 ,…..mn1 n2 ∈M ,and mij stands for one image data pixel (8-bit for gray-scale images) with in a set of whole images pixels M .The encryption engine enciphers mij (8-bit) at a time with the Key-stream element kl (where kl ∈K) , kl is the entire Key-Stream and 1< l < n1n2 . The process of encryption is as follows [2]:

Equation (a):

$T_k(M) : M \rightarrow C = t_{k1}(m_{11})\ t_{k2}(m_{12}) \ldots\ldots\ldots t_{kl}(m_{n1\ n2})$.

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Where $T_k(M)$ and $t_{kl}(m_{n1n2})$ are the encryption of whole message and a single pixel in image respectively .

Equation (b):

$$T_k^{-1}(C) : C \rightarrow M : t_k^{-1}(c_{11})t_k^{-1}(c_{12}).....t_k^{-1}(c_{n1n2}) .$$

Where and $T_k^{-1}(C)$ and $t_k^{-1}(c_{n1n2})$ are the encryption of whole message and a single pixel in image respectively. Equation (a) is applied to each pixel in image frame in row-wise manner, until the final row in image. Then the same key-stream is applied to the previously resulted image frame in column- wise to deals with image data as a two-dimensional message. The same procedure is applied by equation (b) to decipher the images and reconstruct the original image without loss in image quality (recovered image). Image encryption scheme illustrated in figure (5).

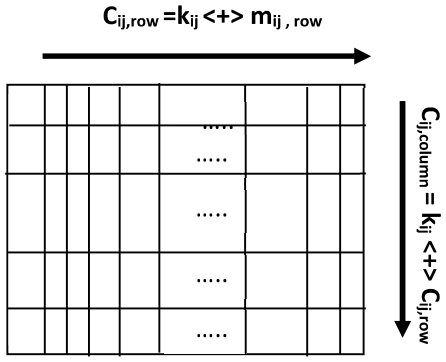

Figure (5) Image ciphering scheme

4. Residual Intelligibility and Regularity of Digital image

When ciphering systems are constructed, there must be some techniques to show the amount of residual intelligibility in ciphered images, and the quality of the reconstructed images. The ciphered image must be considered nearly as a white noise (chaotic) with low residual intelligibility and low quality, on other side the reconstructed (deciphered) image, must give high intelligibility and high quality with high level of regularity.

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Subjective Fidelity Criteria

Human are good at identifying geometric objects (such as circles, rectangles, triangles, and lines) and shapes in general. Images, which contain-mostly recognizable shapes, are called regular images. If an image is not regular, i.e. does not contain identifiable objects or patterns, or its too chaotic (such as white noise), it is difficult for humans to compare or recall it [9]. Thus, for image ciphering systems it is suitable that the ciphered image To have bad subjective quality, (low visual quality), and the deciphered image to have high visual quality. The histogram of an image is a plot of gray-level values, versus the number of pixels at that value. The shape of histogram provides information about the nature of image. The histogram measures are statistically based features, where the histogram is used as model of the probability distribution of gray levels. The first order histogram probability P(g) can be defined as:

$$\mathbf{P(g) = \frac{N(g)}{Mp}} \qquad \ldots(6)$$

(Mp) is the number of pixels in the image or sub-image, and N(g) is the number of pixels at gray level g. The statistical measure based on histogram probability used to measure image regularity is the entropy which is a measure of randomness achieving is highest value when all gray levels of image are equal so, it is given by [10]:

$$\mathbf{H = -\sum_{g=0}^{N_L-1} P(g) \log_2[P(g)]} \qquad \ldots(7)$$

As, the pixel values in the image are distributed among more gray levels, the entropy increase [5]. Hence, the ciphered image must have maximum entropy, but the deciphered image must have less amount of entropy (flat histogram distribution).

Objective Fidelity Criteria

The objective fidelity criteria provide equations that can be used to measure the amount of error in the reconstructed (deciphered) images or to measure the amount of error between pure image and ciphered image. Commonly used objective measures are the root-mean-square error (erms), and the peak signal-to-noise ratio (PSNR) [10]. The root-mean-square

error is found by taking the square root of the total error divided by the total number of pixels in the image of size (N×N):

$$e_{rms} = \sqrt{\frac{1}{N^2}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[\hat{I}(x,y) - I(x,y)]^2} \quad \ldots(8)$$

Hence, the smaller the value of erms metrics, the better the deciphered image represents the original image and the larger the value of error metrics. The better the ciphered image conceal pure image information. Alternatively, with (PSNR) metrics, a larger number implies a better deciphered image, and smaller number implies better image concealment of original image is obtained. the peak signal–to–noise ratio, is defined as:

$$PSNR = 10\log_{10}\frac{(N_L - 1)^2}{\frac{1}{N^2}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[\hat{I}(x,y) - I(x,y)]^2} \quad \ldots(9)$$

Where NL = number of gray levels (for 8-bits NL = 256) . Also, as a useful indicator for intelligibility losses in deciphered or residual intelligibility in ciphered image, because all pixel in spectral domain represents a contribution of all image pixels in spatial domain [10]. The spectral signal–to–noise ratio for the digital image can be defined as:

$$SSNR = 10\log_{10}\frac{\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}|If(u,v)|^2}{\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}|If(u,v) - \hat{I}f(u,v)|^2} \quad \ldots(10)$$

Where If(u,v) is the two-dimensional Discrete Fourier Transform (2DDFT) of original image and I^f (u,v) is the (2DDFT) for ciphered image equation (19) is defined in [8] for one-dimensional discrete signal as a scrambled signal quality measure as:

$$SNR = 10\log_{10}\frac{\sum_{u=1}^{N}|If(u)|^2}{\sum_{u=1}^{N}|If(u) - \hat{I}f(u)|^2} \quad \ldots(11)$$

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Similarity Measure

The most common form of the similarity measure can be interpreted in two given matrices A_{ij} and B_{ij} .The inner product can be defined as $\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}b_{ij}$ Alternatively; each element in the matrix is subtracted from the image mean value as illustrated below:

$$\left(a_{ij} = a_{ij} - \sum_{g=0}^{N_L} g \times p(g)\right)_{i=0,j=0}^{i=N,j=N} \quad \text{...(12)}$$

$$\left(b_{ij} = b_{ij} - \sum_{g=0}^{N_L} g \times p(g)\right)_{i=0,j=0}^{i=N,j=N}$$

Then, the similarity test finally is given by (after normalization) [5]:

$$\text{CORR2}\ (A_{ij}, B_{ij}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}b_{ij}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} b_{ij}^2}} \quad \ldots(14)$$

By considering Aij and Bij as two image matrices. The similarity measure shows the amount of correlation between Aij and Bij. Therefore, when the similarity between the ciphered image and the original image, is small, then good concealment to the original image is obtained. The similarity between any two-image matrices gives its maximum value of (1) if the two images are perfectly similar.

Statistical Tests of Randomness

Numerous statistical tests can be applied to a sequence. In the current work, five particular tests will be described and some remarks about their usefulness will be presented to give an indication of their usefulness. The five tests are:

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Frequency Test

This is perhaps the most obvious test in comparison with other tests, occurred in the sequence and it is applied to ensure that there is roughly the same number of '0s' and '1s'. Let n0 zeros and n1 ones be in a sample of (nt = n0 + n1) bits. Then[6] :

$$\chi^2 = (n_0 - n_1)^2/n_t \quad \ldots(15)$$

Clearly if n0 = n1 then $\chi^2 = 0$. To decide if the value obtained is good enough for the sequence to pass, the value of test can be compared with a table of χ^2 distribution (Appendix (B)), for one degree of freedom (DOF). It is obvious that the value of χ^2 for 5% significant level is (3.84). So, simply, if the test value is no greater than (3.84) the sequence passes, otherwise it is rejected.

Serial Test

The serial test is used to check that the number of bit transitions of the binary sections (01,10,00,11) in the stream of length nt are occurred roughly (the same number of times). If a sample passes this test it suggests that each bit is independent of its predecessors. If n00 represents the frequency of the section 00, n_{01} the frequency of the section 01, n10 is the frequency of the section 10, and n11 is the frequency of the section 11, then the following equations will always hold

$$n00 + n01 = n1 \text{ or } n1\text{-}1 \quad \ldots(16)$$

$$n10 + n11 = n1 \text{ or } n1\text{-}1 \quad \ldots(17)$$

$$n10 - n01 = 0 \text{ or } 1 \quad \ldots(18)$$

$$n00 + n01 + n10 + n11 = nt\text{-}1 \quad \ldots(19)$$

(Note the (–1) occur because for a section of length L there are only L-1 transitions).

Ideally:

$$n01 = n10 = n00 = n11 \approx \frac{n_t - 1}{4}$$

as showed by [12], and,[30],[31] ,hence the serial test ST is given by:

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

$$S_T = \frac{4}{n_t - 1} \sum_{i=0}^{1} \sum_{j=0}^{1} (n_{ij})^2 - \frac{2}{n_t} \sum_{i=0}^{1} (n_i)^2 + 1 \qquad \ldots(20)$$

Is approximately, distributed with two degrees of freedom. From χ^2 distribution table. Thus, the value of χ^2 corresponding to a 5% significant level is 5.99. It is becoming clear that for this test any sequence for which the value is greater than 5.99 must be rejected.

Auto-correlation Test

If the binary stream to be tested is $x_1, x_2, x_3, \ldots x_{n_t}$ then:

$$A_c(d) = \sum_{i=1}^{n_t - d} x_i * x_{i+d} \qquad 0 \le d < n_t\text{-}1 \qquad \ldots \quad (25)$$

$$A_c(0) = \sum_{i=1}^{n_t} (x_i)^2 = \sum_{i=1}^{n_t} x_i^2 = n_1$$

If the stream contains n0 of '0s' n1 of '1s', then the expected value for A (d) where $d \neq 0$ is:

$$\mu = \frac{n_1^2 (n_t - d)}{n_t^2} \qquad \ldots(26)$$

The test will be successful if $\chi^2 \le 3.841$ for all d, where χ^2 can be calculated as follows:

$$\chi^2 = \frac{(A_c(d) - \mu)^2}{\mu} \qquad \ldots(27)$$

This test enables to decide whether the sequence under test is believed to have 'random' distribution or not [8] [9]

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

The Run Test

For this test, the sequence is divided into runs of zeros and ones, a run of zeros is defined as a consecutive string of zeros preceded and followed by ones a run of ones is defined similarly.

The (i) successive 0-bits preceded and followed by a '1' are called a 0-run of length (i):

$$\underbrace{10000001}_{\text{Length -i}}$$

The successive 1-bits preceded and followed by a '0' are called a 1-run of length i:

$$\underbrace{01111110}_{\text{Length -i}}$$

For example, the sequence 011000101101 contains:

3 of 0-runs of length 1

1 of 0-runs of length 3

2 of 1-runs of length 1

2 of 1-runs of length 2

n0i = number of 0-runs of length i.

n1i = number of 1-runs of length i.

The expected number of runs of length i (both 0-runs and 1-runs T0, T1) is :

$$T_0 = \sum_{i=1}^{k_f} \frac{\left(n_{0i} - \frac{n_t}{2^i}\right)^2}{\frac{n_t}{2^i}} \qquad \ldots(28)$$

$$T_1 = \sum_{i=1}^{k_f} \frac{\left(n_{1i} - \frac{n_t}{2^i}\right)^2}{\frac{n_t}{2^i}} \qquad \ldots(29)$$

Which is approximately χ^2 distribution with (kf -1) degree of freedom.

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Results and conclusions

The results for Image regularity and residual intelligibility are all illustrated in Table (1) for the image beach. The ciphered images are all shown in figure (6)

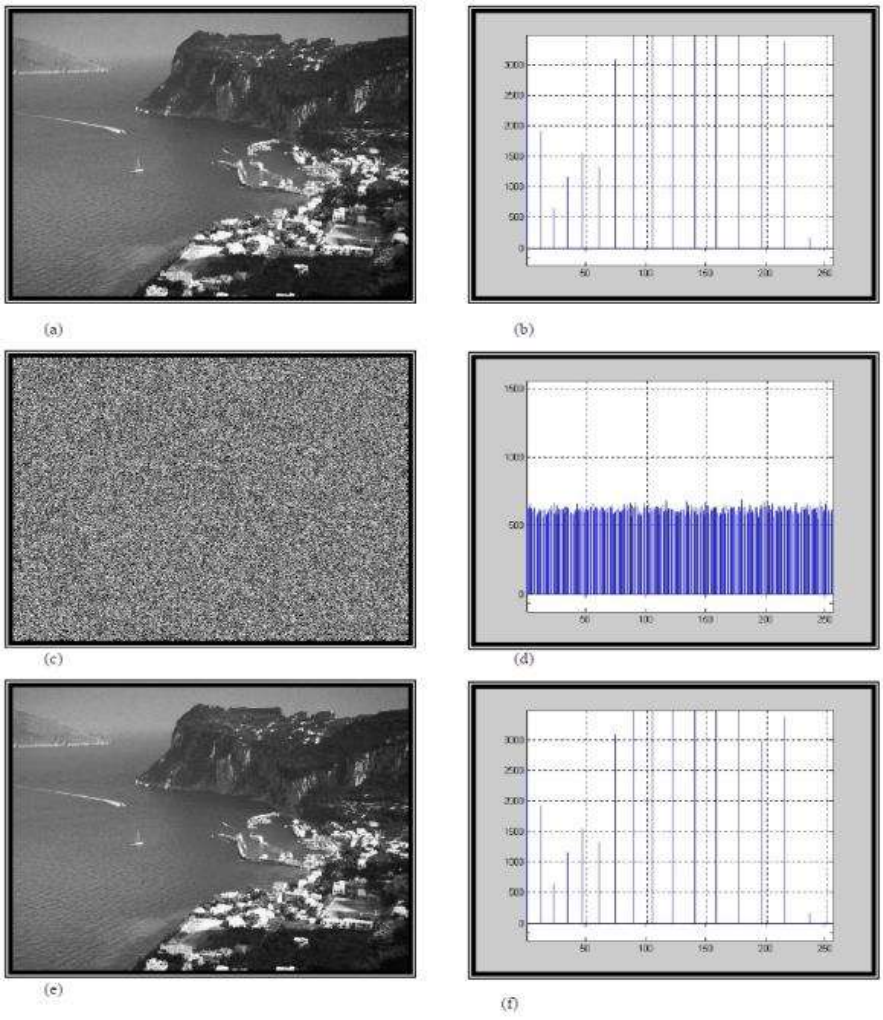

Figure:(6) Image called beach ciphered using presented algorithm
(a)&(b): original image with histogram
(c)&(d): ciphered image from preseuted Algorithm with histogram.
(e)&(f): deciphered image with histogram.

for the proposed non-linear key-stream generator and traditional Non-linear key-stream generator which is called Threshold generator for sake of comparison. The results of testing randomness of LFSRs are shown by tables (2) and table (3) below

Table (1) Regularity and Residual Ineligibility Measures for ciphered images

Image name	Entropy of pure image	Entropy	Similarity	SSNR (dB)	PSNR (dB)	e_{RMS}
The results of residual intelligibility for presented stream cipher generator						
Beach	7.4504	7.9023	-0.0431	0.6225	1.9258	204.367
The results of residual intelligibility for Threshold stream cipher generator						
Beach	7.0144	7.4289	0.4843	5.3219	7.1756	118.017

The requirements of the proposed algorithm are:

Both the sender and receivers need to have the identical functioning programs for enciphering and deciphering.

(2) The receivers must have obtained the randomization key string K(l) and the scheme description before the receipt of ciphertext from the senders. Therefore, a good key exchange protocol, like Diffie-Hellman scheme, must be performed. This may have employed in future as further development for the presented algorithm.

(3) The results of residual intelligibility that have been applied for image called Bridge and image called Fighter shows that the residual intelligibility for images ciphered by the presented algorithm is lower than the values obtained from the same images encrypted by Threshold non-linear stream cipher generator (see table (1)). Furthermore, the subjective quality for ciphered images by the presented algorithm is very close to the white noise (chaotic with flat histogram) as compared by the same results obtained from Threshold non-linear stream cipher generator.

(4) The correlation immunity of the presented generator with high period could be considered as the most important advantages of the presented algorithm. Finally, the simulation results show that the proposed algorithm achieves the image secrecy.

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Table (2) Statistical Tests of Randomness Results from classical method

Test		Key 1	Key 2	Key 3	Pass value
Frequency test		0.0269	0.3618	2.3687	must be ≤ 3.84
Run test	T_0	18.972	13.103	17.67	must be ≤ 22.362
	T_1	20.540	17.4062	15.8021	
Poker test $\beta = 5$		5.6026	5.1986	5.4849	must be ≤ 11.1
Serial test		0.84118	1.4497	3.6787	must be ≤ 5.99
Auto – Correlation test, for first ten bits	Shift 1	0.20334	0.2739	0.32610	must be ≤ 3.48
	Shift 2	0.69133	0.12747	0.08966	
	Shift 3	0.13613	0.06818	0.01968	
	Shift 4	0.04478	0.11389	1.21773	
	Shift 5	0.05576	0.60407	0.02818	
	Shift 6	0.45618	0.24653	0.2070	
	Shift 7	0.86701	0.54944	0.2762	
	Shift 8	0.7377	0.20560	0.38185	
	Shift 9	0.04525	0.33720	0.9558	
	Shift10	0.13753	2.27516	0.36748	
Maximum Auto – Corr. value		1.735	0.5251	0.8235	≤ 3.48

KJPS Al-Kitab Journal for Pure Science
Vol.2 (2), ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Table (3) Statistical Tests of Randomness Results from Large-Scale Randomization stream cipher scheme without ($\hat{S}, \hat{P}$)

Test		Key 1	Key 2	Key 3	Pass value
Frequency test		0.52711	0.05034	0.2586	must be ≤ 3.84
Run test	T0	*23.9218*	13.5559	15.8021	must be ≤ 22.362
	T1	20.8031	*38.9101*	7.27472	
Poker test $\beta = 5$		4.0218	3.627	7.747	must be ≤ 11.1
Serial test		0.3399	0.2567	0.50396	must be ≤ 5.99
Auto – Correlation test, for first ten bits	Shift 1	0.01522	0.4374	0.3217	must be ≤ 3.48
	Shift 2	0.8057	0.7043	1.23908	
	Shift 3	*3.8671*	3.5211	0.2597	
	Shift 4	0.2973	0.10312	*3.952*	
	Shift 5	0.01610	0.0064	4.1525	
	Shift 6	*4.47603*	3.215	0.8121	
	Shift 7	0.2735	*4.872*	0.33413	
	Shift 8	0.0058	0.0281	1.19559	
	Shift 9	*3.6902*	3.216	0.3979	
	Shift10	0.10022	0.04618	0.03205	
Maximum Auto – Corr .value		*4.482*	*8.2863*	2.61902	≤ 3.48

REFRENCES:

[1] B. Schneier, " Applied Cryptography ", NewYork, Wiley 1996.

[2] Tak-Ming Law,"Encryption Algorithm for Chinese Text Messages by Internal Code Structure", International Conference in Theory and Applications of Cryptography, Hong Kong University, 1999.pp246-250.

[3] W. Diffe, and M. E. Hellman, " Privacy and Authentication: An Introduction to Cryptography ", Proceeding of the IEEE, Vol.67. No.3, March 1979.pp 379-423

[4]Vera.S.Pless,"Encryption Schemes for Computer Confidentiality", IEEE Trans. On Computer, Vol. C-26, No.11, November 1977. pp. 1133-1136.

[5] J. C. A. Van Der Lubbe, " Basic Methods of Cryptography ", Cambridge University Press, 1998.

[6] T. Sigenthaler, " Correlation Immunity of Non-Linear Combining Function for Cryptographic Applications ", IEEE Trans. Info. Theory, Vol. IT-30, Sep. 1984, pp. 776-780.

[7] J. K. Ruben, "Analysis And Design of Large Scale Randomization Key-Stream Generator ", Springer-Verlage Proce. Eurocypt'97 ICTACT, May 11-15, 1998. pp 1229-1234.

[8] S. Sridhan, and E. Dawson, " Fast Fourier Transform Based Speech Encryption System ", IEE Proceeding, Vol. 138, No. 3, June 1991. pp 215-223.

[9] A. Perring, and D. Song, " Hash Visualization: A New Technique to Improve Real-World Security ", International Conference in Theory and Applications of Cryptography, Hong Kong University, 1999.pp131-138.

[10] E. U. Scotte, " Computer Vision and Image Processing: Practical Approach Using CVIP Tools ", Prentice-Hall, 1998.