Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 34, Issue 2, 2023 DOI: http://doi.org/10.23851/mjs.v34i2.1294

Research Article Open Access

Image Encryption Using New Non-Linear Stream Cipher Cryptosystem

Adnan M. Ali[1*], Faez H. Ali[1], Sabah M. Redha[2], Nurideen Abubakari[3]

[1]Department of Mathematics, Collage of Science, Mustansiriyah University, 10052 Baghdad, IRAQ.
[2]Statistics Department, Collage of Administration and Economics, University of Baghdad, Baghdad, IRAQ.
[3]Linn-Benton Community College Albany, Oregon, USA.

[*]Correspondent contact: dnan79816@gmail.com

Article Info

Received
08/12/2022

Accepted
08/03/2023

Published
30/06/2023

ABSTRACT

In this paper, we designed a new efficient stream cipher cryptosystem that depend on a chaotic map to encrypt (decrypt) different types of digital images. The designed encryption system passed all basic efficiency criteria (like Randomness, MSE, PSNR, Histogram Analysis, and Key Space) that were applied to the key extracted from the random generator as well as to the digital images after completing the encryption process.

KEYWORDS: Stream Cipher, Image Encryption, Chaotic Map, Randomness.

الخلاصة

في هذا البحث، تم تصميم نظام تشفير انسيابي جديد فعال اعتمد على الدالة الفوضوية من اجل تشفير (فك تشفير) أنواع مختلفة من الصور الرقمية. اجتاز نظام التشفير المصمم جميع مقاييس الكفاءة الأساسية (مثل العشوائية ومربع معدل الخطأ ونسبة قمة الاشارة للضوضاء وتحليل المدرج التكراري وفضاء المفتاح) التي تم تطبيقها على المفتاح المستخرج من المولد العشوائي وكذلك على الصور الرقمية بعد اتمام عملية التشفير.

INTRODUCTION

With the escalation of cybercrime, the need for this topic indicates the highest degree of attention, prompting it to continuously search for new ways and methods, and the winter of instructions. Data basically means protecting data from being used by authorized persons or used by attackers. Cryptography has uses in multiple and global domains and functions. Oad et al., (2014) [1] states that image encryption is the technique of converting an image from its current form (the original) to another form that is more difficult to understand (the cipher), while the reverse process of converting data from its ciphertext to plaintext is called decryption. Without knowing the secret key, an attacker cannot decrypt the encrypted message nor even know any part of its information [2]. The purpose of encryption is to provide a number of different security goals such as confidentiality, data integrity, non-repudiation, and access control. Among the previous studies and research related to our research, we mention the following: Yoon and Kim (2010) [3] developed a chaotic image cipher in which initially a small matrix was generated using the chaotic logistic map. The experimental results show that the proposed encryption scheme provides comparable security. Çavusoglu and Pehlivan (2017) [4], using a new chaotic system with algorithm is developed to encode digital images with a chaotic-based random number generator design with the help of the new chaotic system. The necessary analyzes were conducted on the proposed algorithm, which proved its efficiency and speed in encrypting secure images. Hussein et al., (2019) [5] introduced the logistic sine map to image encryption where an image encryption algorithm was proposed in which the image pixels were first shuffled using Arnold map. Hence a 256-bit key was generated using a 2D logistic sinusoidal map with a matching generator. Then the pixel values of the image were changed by XOR shuffling with the key to produce the encrypted image. The encrypted image was tested by several statistical measures. Ismail and Said, (2018) [6] designed a generic double-camber (DH) logistics map and the generic parameter added to the map provided more control over the extent of the chaos. The new map was analyzed and its fixed points and ranges of stability were studied. The S. Lyapunov method showed that the option of designing any specific map is possible by changing the global parameter that increases the randomness and controllability of the map. The DH map provided secure transmission of MRI and X-ray medical communications. According to security analyzes such as key sensitivity analysis, key space, histogram, correlation coefficient analysis, MAE, NPCR and UAC calculations, which highlighted the efficiency and robustness of the proposed system. Gad et al., (2021) [7] produce a brand-new chaotic logistic map that is fuzzy and multi-modular for image encryption. Chen *et al.*, (2022) [8] using improved Henon Map to Hybrid Domain Image Encryption Algorithm. In this paper we introduce a new efficient non-linear stream cipher cryptosystem based on stream cipher and chaotic system to encrypt (decrypt) several kinds of digital images.

MATERIALS AND METHODS

Golomb's concepts applied to the binary series have been expanded to include the possibility of applying them to a digital series consisting of 256 digits, where the series belongs to GF space (2). In this research, a hybrid encryption system was designed for the purpose of encoding different types of digital images, where this system consisted of four Crawler recorders of different lengths with a control unit for a rotating multiplication group with the reinforcement of this system with a logistical chaotic function whose parameters were carefully chosen in order for the output to be a digital series that is difficult to predict as the series has undergone resulting data is subjected to a series of standard statistical tests before being used as an encryption key. In order to highlight the strength of the designed algorithm, the encrypted images were subjected to a series of statistical analyzes related to the area of the chain, its cycle, and its complexity. According to those analyzes, it proved a high efficiency that enables it to withstand strongly against attempts to hack it.

Basic Concepts for Cryptography

The security is an important in protecting data against intruders. One of most important methods for ensuring data secrecy is cryptography [9]. The study of mathematics is known as cryptography, and it is used to both encrypt (encipher) and decrypt (decipher) information. The process of transforming data into something that appears random and meaningless is known as encryption. Decryption is the process of returning encoded data to its original format. Cryptography is broadly classified into two categories symmetric and asymmetric key cryptography (popularly key cryptography), (see Figure 1) [10].

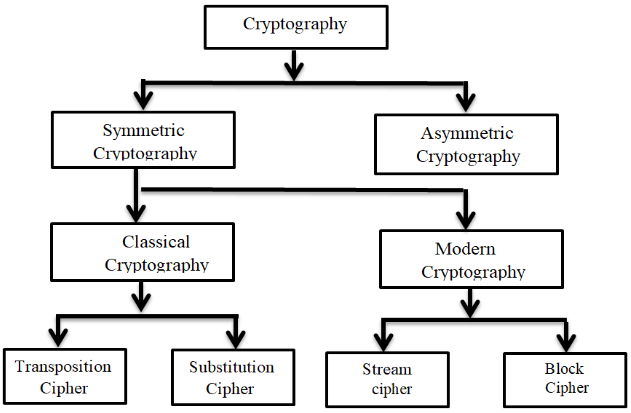


Figure 1. cryptography classification.

Symmetric and stream ciphers

The block ciphers can either have different keys for encryption and decryption, in which case they are known as public-key or asymmetric block ciphers, or they can have a single key for both encryption and decryption, in which case they are known as shared-key (also known as secret-key or symmetric). With a stream cipher, each binary digit in a data stream is encrypted one bit at a time using a cryptographic key and algorithm to create ciphertext. The one-time pad is the name of the key that is generally used with stream ciphers. A one-time pad is mathematically impossible to crack because it is always exactly the same size as the message it is encrypting. In a stream cipher, the cryptographic keys used to encrypt the binary image are randomly modified, resulting in a cipher image that is mathematically impossible to decipher. Additionally, every bit of key and every bit of data are encrypted. The benefit of employing a stream cipher is that it executes more quickly than block ciphers and requires less complicated hardware. Because the keys are changed, stream ciphers do not consistently output the same ciphertext even for repeating blocks of plaintext [11]. There is some hope for quick image encryption thanks to the exclusive or (XOR or) technique, which is easy to implement on hardware [12]. The linear feedback shift register (LFSR's) based pseudo exhaustive test pattern generator the reseeding and characteristic polynomial reprogramming techniques. A LFSR is made up of a shift register (R) that holds a series of bits and a feedback function (f) that is the bit sum (XOR) of a portion of the shift register's entries. The shift register has n memory stages or cells, labeled R_{n-1}, …, R_1, R_0, each holding one bit [13].

Chaos Theory

Mathematical study of chaos theory has applications in physics, economics, biology, and philosophy, among other fields of study. The butterfly effect—a property of dynamical systems that is very sensitive to beginning conditions—is a topic of study in the field of chaos theory. Long-term prediction is generally impossible for chaotic systems because even slight variations in the initial conditions result in drastically different results. There are two categories of chaotic maps: chaotic maps in one dimension and chaotic maps in greater dimensions. Chaotic maps are simple to construct, require little complexity, and are simple to use. In contrast, higher dimension chaotic maps feature at least two variables, better performance, and chaotic orbits that are more unpredicTable [14]. The chaotic maps refer to a set of quadratic functions defined on the unit interval, which are expensive to compute and challenging to implement in hardware, indicating that it is not real-time processing. The equation of logistic map proposed in [15] is:

$$x_{n+1} = r\, x_n\, (1 - x_n) \qquad (1)$$

where $\boldsymbol{r}$ is a control parameter (it is often referred to as the amplitude parameter), and ($n = 0, 1, 2, \ldots$) is the number of iteration and x_{n+1} is in interval [0,1]. A logistic map is a one-dimension discrete chaotic map. It was widely used in various fields, including economics, physics, and social sciences. Figure 2 shows the bifurcation diagram of the non-modular logistic map:

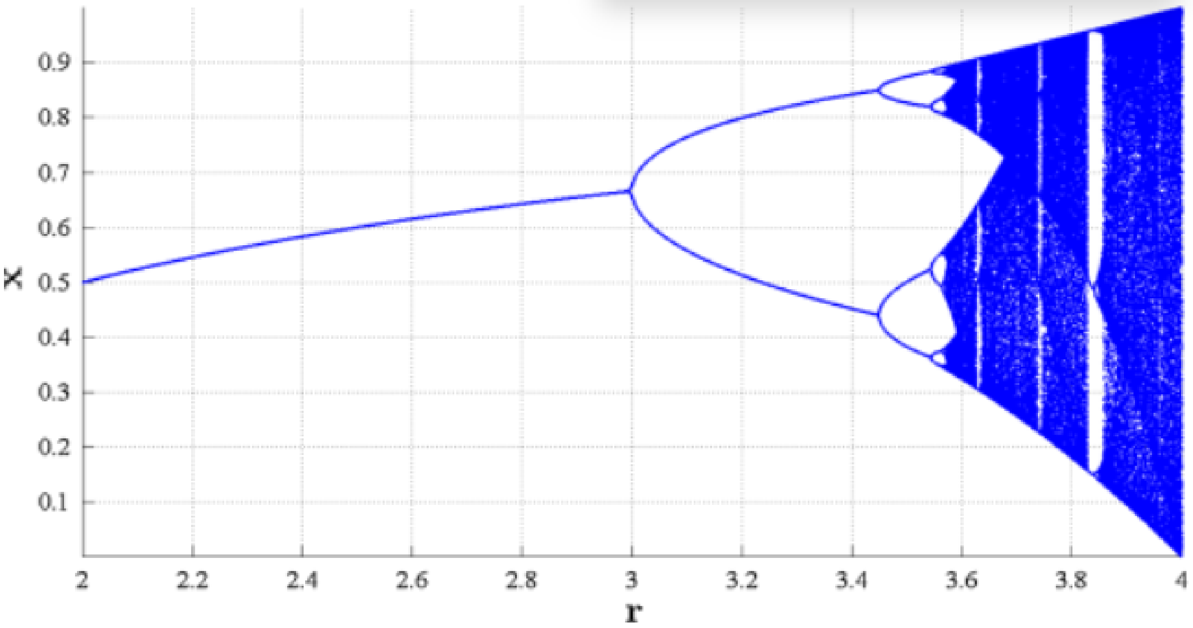


Figure 2. The bifurcation diagram of the one- dimensional logistic map.

The proposed 1-dimentional logistic map with triple parameters is represented as follows [16]:

$$x_{n+1} = a x_n (\alpha - x_n)^{\beta} \qquad (2)$$

where $a = 1.5, \alpha = 3, \beta = 0.5$, and $0 < x_0 < 3$, $n = 0,1,2, \ldots$.

Multiplicative cyclic group (MCG)

Basic Concept of MCG [17]

- Let $\langle G,* \rangle$ be a group which is called Multiplicative Cyclic Group (MCG). The set G has order $p-1$ where p is prime number, let $\alpha_i \in G$ be an element which is be called a generator element if and only if $\delta_i = f(\alpha_i, i, p) = \alpha_i \ (mod\, p), 1 \leq i \leq p-1,\ \forall \delta_i \in G$. If $(k, p-1) = 1$ then δ_k is another generator. Its cleat that f is one to one and onto function. As known, there are $g(p) = \Phi(p-1)$ generators, where Φ is called the Euler function.

- The sequence $S = \{s_k\}_{k=1}^{p-1}$, $0 \leq s_k \leq m-1$, $m \geq 2$, s.t. $s_k = (m \cdot \delta_k)\ div\ p$, $k = 1, \ldots, p-1$, (div gives the quotient number of division procedure) can be generated from only one generator element α where $\delta_k = f(\alpha, k, p)$ is any element can be found in G. It's obvious, that the period $P(S)$ of S equal to $p-1$.
- The sequence S, can be generated by using two generators of MCG. Such that let $\alpha_t, \alpha_r \in G$ be two generators with $\alpha_t \neq \alpha_r$ and let $x = f(\alpha_t, j, p)$ and $y = f(\alpha_r, x, p)$, $1 \leq j, x \leq p-1$, so we can find another the function h which is a compound function of the function f such that:

$y = f(\alpha_t, f(\alpha_r, j, p), p) = h(\alpha_t, \alpha_r, jp)$, where $h: G \rightarrow G$. It's not hard to prove that the function h is one to one and onto function.

- Now we can construct an MCG unit (MCGU) which can be responsible for generating the sequence S. The MCGU is a function of five independent variables, where p is a prime number, α_t andα_r be two generators of MCG, and m is the digit value of the sequence S s.t. $S = MCGU(p, \alpha_t, \alpha_r, \gamma, m)$, where $1 \leq \gamma \leq p-1$ is an arbitrarily chosen start point.
- The MCGU algorithm steps illustrated in Algorithm 1.

Algorithm 1: MCGU Algorithm

```
INPUT: READ ($p$ , $\alpha_t$ , $\alpha_r$ , $\gamma$ , $m$ , $L$);
$i \leftarrow \gamma - 1$ ; $j \leftarrow 0$ ;
REPEAT
    $i \leftarrow i\ (mod(p-1)) + 1$ ;
    $j \leftarrow j + 1$;
    $y \leftarrow h(\alpha_t, \alpha_r, j, p)$ ;
    $s_k \leftarrow (m \cdot y)\ div\ p$;
UNTIL $j = L$;
OUTPUT: The final output sequence of MCGU
  $S \leftarrow \{s_1, s_2, \ldots, s_L\}$ ;
END.
```

Efficiency Criteria Calculations of MCGU [17,18]

- General Complexity $(GC(S))$: Let's choose prime number p so we have $g(p) = \phi(p-1)$ ways to choose the generator α to establish the set $A(p)$, so there are $P_2^{g(p)}$ (permutation 2 generators from the total numbers of generators of MCGU) ways to choose two different generators from the set $A(p)$, and $p-1$ ways to choose γ then: $GC(S) = \phi(p-1) * P_2^{g(p)} * (p-1)$.
- Periodicity $(P(S))$: the period of S when choosing two different generator elements is $p-1$, since we have $P_2^{g(p)}$generators then the period S which is generated from the MCGU is: $P(S) = P_2^{g(p)} * (p-1)$.
- Randomness: Since the MCGU generates all the elements of G Whether we depend on one or two generator elements, and the generated element converted to an element in the sequence S so we expect to obtain a good randomness sequence.
- Linear Complexity $((LC))$: Ali and Ghazi (2009) [18] proved in their paper that the high LC of MCGU, that's done because of the high nonlinearity of all the used parts of the MCG unit.

Efficiency Criteria for Images Encryption

Efficiency metrics are among the basic methods used to measure the performance of the algorithms used. In the following, we present some properties for efficiency Criteria for image encryption.

Standard Randomness Tests

Any key generator can't be used as a cryptographic system unless its output sequences pass all the randomness tests. As known, there is a binary randomness tests can be used to test the output sequences of any stream cipher cryptosystem. But it prefers to use the generalization of the binary randomness tests when the key generator output is not binary. When the keygenerator is proposed to encrypt/decrypt digital images, this mean the output must be bytes, so we can use the randomness tests which is worked in the filed GF(2^8). Three basic 256-randomness tests should be applied to the key generators with digital values, the most important tests are the frequency, Run and auto-correlation tests. These tests are depending on chi-square distribution since it considered a statistical experiment [19]. For 256-Digital Frequency Test (256DFT), suppose we have the sample n_i which considered the observed number of occurrences of the digit i of the sequence S, where $i = 0,1, \ldots, 255$, and the expected number of occurrences of digit i is $E^F = \frac{L}{256}$, then the statistic value T^F of 256DFT is calculated as follows:

$$T^F = \sum_{i=0}^{255} \frac{\left(n_i - E^F\right)^2}{E^F} = \sum_{i=0}^{255} \frac{(n_i - L/256)^2}{L/256} = \frac{256}{L} \sum_{i=0}^{255} (n_i - L/256)^2 \tag{3}$$

With freedom degree $\upsilon = 255$.

For 256-Digital Run Test (256DRN), Let R_{ij} be the observed number of runs with type i runs with length j, and let E_j^R be the expected number of runs with length j, then, the statistic value T_i^R of 256DRT is calculated as follows (* Adnan M. Ali *et al.*, 2023):

$$T^R = \sum_{i=0}^{255} T_i^R \tag{4}$$

With T_0 freedom degree $\upsilon_i = 256(M_i - 1)$, where

$$T_i^R = \sum_{j=0}^{M_i} \frac{\left(R_{ij} - E_j^R\right)^2}{E_j^R} = \sum_{j=0}^{M_i} \frac{\left(R_{ij} - 255^2 L/256^{j+2}\right)^2}{255^2 L/256^{j+2}}$$

M_i is maximum length of run i.

For 256-Digital Auto-Correlation Test (256DACT), let $n_0(\tau)$ denotes the number of similar digits in S after shifting it by τ, and $n_1(\tau)$ denotes the number of distinct digits in S after shifting it by τ respectively, where $\tau = 1,2,\dots,L-1$, While the expected number of similarity and difference respectively are:

$$E_0^A(\tau) = \frac{L-\tau}{256} \text{ and } E_1^A(\tau) = \frac{255(L-\tau)}{256} \tag{5}$$

$$T^A(\tau) = \sum_{i=0}^{1} \frac{\left(n_i(\tau) - E_i^A(\tau)\right)^2}{E_i^A(\tau)} = \frac{\left(n_0(\tau) - \frac{L-\tau}{256}\right)^2}{\frac{L-\tau}{256}} + \frac{\left(n_1(\tau) - \frac{255(L-\tau)}{256}\right)^2}{\frac{255(L-\tau)}{256}} \tag{6}$$

with freedom degree $\upsilon = 1$.

Key Space Analysis

To counter brute force attacks, we should expand the key space of the algorithm as much as possible. The key space of a secure encryption algorithm should be larger than 2^{100} [20].

Peak Signal–To-Noise Ratio and Mean Square Error

The quantitively measure to compute the error between the original plain image and the encrypted (decrypted) data is the Mean Square Error (MSE) which will be computed as [7]:

$$MSE(y) = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (P(i,j) - y(i,j))^2 \tag{7}$$

Where $P(i,j)$ is the pixel value in the plane image at pixel point (i,j) and $y(i,j)$ express the compared encrypted $(y(i,j) = E(i,j))$ or decrypted $(y(i,j) = D(i,j))$ images respectively and i,j are the pixels of $W \times H$ images. MSE must be equal zero when $P(i,j) = D(i,j), \forall i,j$ and has high value when $P(i,j)$is compared to $E(i,j)$. The similarity between original and encrypted image can be measured by PSNR. High PSNR means a high correlation between original and received image, and can be defined as:

$$PSNR = 10log10 \frac{W * H * (2^N - 1)^2}{\sum_{i=1}^{W} \sum_{j=1}^{H} [P(i,j) - C(i,j)]^2} \tag{8}$$

A good encryption represents the low value of PSNR.

Histogram Analysis

An image-histogram explicates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. In order to have an idealistic ciphered image in histogram's sight of view, the histogram of the image must have parallel distribution of pixels with the color intensity value. If the histogram of a cipher image is flat, information of the plain image is excellently hidden.

Proposed Image Stream Cipher Cryptosystem

In this section, firstly, we propose new Image Encryption/ Decryption Key Generator (IEDKG) to encrypt/decrypt the image files. The IEDKG is a part of Efficient Image Stream Cryptosystem (EISC) which is hybrid system consisting from two types of cryptosystems, these cryptosystems are: Stream Cipher and Chaotic system. The IEDKG is designed to generate byte-keys to be xored with plain bytes. In this subsection we will detail the most important parts of IEDKG.

Initialization of IEDKG

The initial key of IEDKG consists of three sub-keys. These sub-keys are as follows:

1. The first sub-key called Basic key (BK) is changed with each image and requires an essential private key consisting of (20) ASCII

CODE (8 bits) characters which are converted to binary to fill the LFSR's of the IEDKG.

2. The second sub-key is the initial value of the chaotic system. This key is considered as initial value x_0 of the chaotic system which consists of real number with accuracy for 16 digits. This sub-key is changed with each image.
3. For MCGU, we need prime number q, generators (α_1 and α_2) and start point γ. This sub-key is changed daily.

These three sub-keys must be transmitted over a secure channel.

IEDKG Components

1. LFSR'S unit (LFSRU): this unit consist of 4 LFSR will the following details:

a. LFSR1: has characteristic polynomial $x^{29} + x^2 + 1 \in GF(2)$ with period: $L_1 = 2^{29} - 1$.

b. LFSR2: has characteristic polynomial $x^{43} + x^2 + 1 \in GF(2)$ with period: $L_2 = 2^{43} - 1$.

c. LFSR3: has characteristic polynomial $x^{39} + x^3 + 1 \in GF(2)$ with period: $L_3 = 2^{39} - 1$.

d. LFSR4: has characteristic polynomial $x^{31} + x^3 + 1 \in GF(2)$ with period: $L_4 = 2^{43} - 1$.

$$P\,(G) = \text{L.C.M}\,(L_1, L_2, L_3, L_4) = \Pi_{i=1}^{4} L_i \quad (9)$$

2. Ram Unit (RAMU): Consists of 256 random and different bytes.
3. Control LFSR (CLFSR): has characteristic polynomial $x^{23} + x^2 + 1 \in GF(2)$.
4. Chaotic Map (1-Dimension with Triple-Parameters) (CM1DTP): using relation (2) to generate bytes $BP1$:

$$B1 = BP1_k\ XOR\ KB_j \quad (10)$$

The IEDKG algorithm steps are illustrated in Algorithm 2.

Algorithm 2: IEDKG Algorithm

```
Input: BK (20 chrs), $x_0$ and image input
       (plain/cipher), with length L bytes;
1.  Converting BK characters to binary form.
2.  Fill LFSRU, CLFSR and generate RAMU from CM.
3.  FOR k ← 1:L/4
4.      Move CLFSR one step to obtain CBi, i ← 1,2,3,4.
        IF CBi = 1 THEN
5.          Move LFSRi one step
        ELSE No Move.
6.      LFSRU Generate AD1.
7.      Shift AD1 two steps for (3) times to generate $AD_j$, j ← 2,3,4.
8.      RBj ← RAMU(ADj).
9.      MCGU moves to generate $MB_j$.
10.     $KB_j$ ← $RB_j$ XOR $MB_j$.
11.     $C_j$ ← $KB_j$ XOR $P_j$ (or $P_j$ = $KB_j$ XOR $C_j$);
12. END {FOR k}.
13. OUTPUT: Image (cipher/plain);
14. END {Algorithm}
```

Note: The IEDKG is considered a nonlinear system because of two reasons; first is the RAMU which is hard to be analyzed and the random move of each LFSR of LFSRU which are controlled by the output of CLFSR. The block diagram of IEDKG is shown in Figure 3.

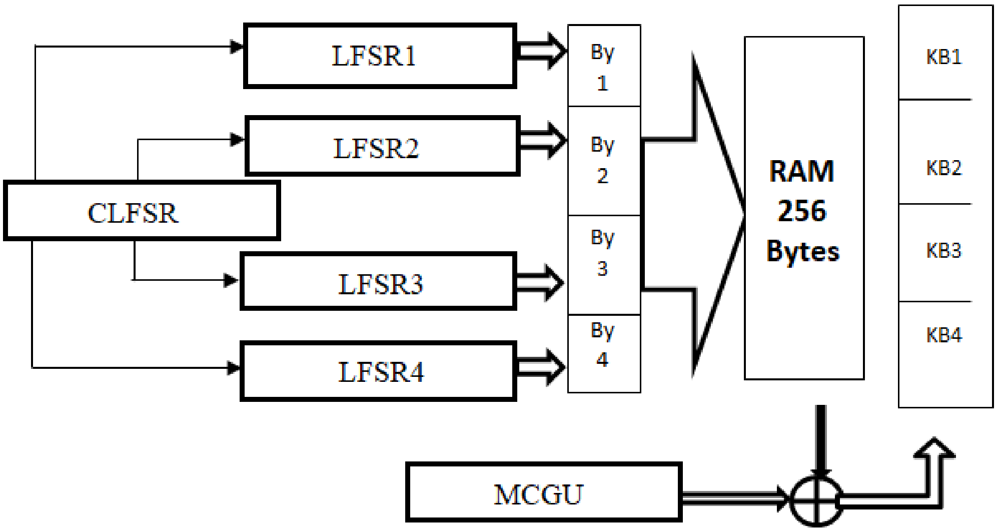


Figure 3. The block diagram of IEDKG.

IMPLEMENTATION OF EFFICIENCY CRITERIA ON IEDKG

Standard Randomness Tests Using 256-Digital Tests

We will review the results of output keys from IEDKG for various issues with different lengths with different key management as shown in Table 1.

Table 1. various issuses with different lengths with different key management.

Is.	L	BK	MCG q=10993	Chaotic map initial
1	10000	189 150 63 170 22 160 169 187 228 251 197 149 237 148 5 31 220 124 216 54	$\alpha_1 = 7$ $\alpha_2 = 10$	x$_0$=0.9421
2	25000	141 161 9 157 93 13 125 50 32 53 38 49 11 162 72 138 178 128 137 114	$\alpha_1 = 10$ $\alpha_2 = 13$	x$_0$=0.1769
3	50000	32 126 218 223 69 54 145 164 107 53 242 21 27 37 43 159 147 14 238 186	$\alpha_1 = 7$ $\alpha_2 = 13$	x$_0$=0.7961

For Frequency and Run tests, Table (2) shows the T value compared with T$_0$ with freedom degree and the finally the discussion for randomness.

Table 2. Frequency and run tests.

Test	Issue	T	T$_0$	υ	Discission
Freq,	1	264.013	288.016	255	Pass
	2	238.303			Pass
	3	261.084			Pass
Run	1	535.106	559.408	512	Pass
	2	551.964			Pass
	3	557.256			Pass

For Auto-correlation tests, Table 3 shows the number of fails for 100 shifting (τ), and the ratio of pass with average, maximum and minimum of difference between T value and T$_0$==3.841 with freedom degree υ=1.

Table 3. Auto-correlation tests.

Is.	Fail	Ratio of Pass	Average Difference	Maximum Difference	Minimum Difference
1	3	97%	2.611	3.344	2.423
2	3	97%	2.206	3.364	0.410
3	4	96%	1.438	2.548	0.104

MSE and PSNR

In this section we will introduce (4) images chosen as secret images to be tested for the proposed encryption system, the images are described as in Figure 2. The information of these images is as shown Table 4. In Table 5 we calculate the MSE and PSNR for the (4) images.

Histogram Analysis

In Figure 3 we will show the histogram analysis for the (4) images. Histogram (a) shows the distribution of bytes of the plain or origin image, histogram (b) shows the distribution of bytes of keys of the IEDKG system, while histogram (c) shows the distribution of bytes of encrypted image using the IEDKG system.

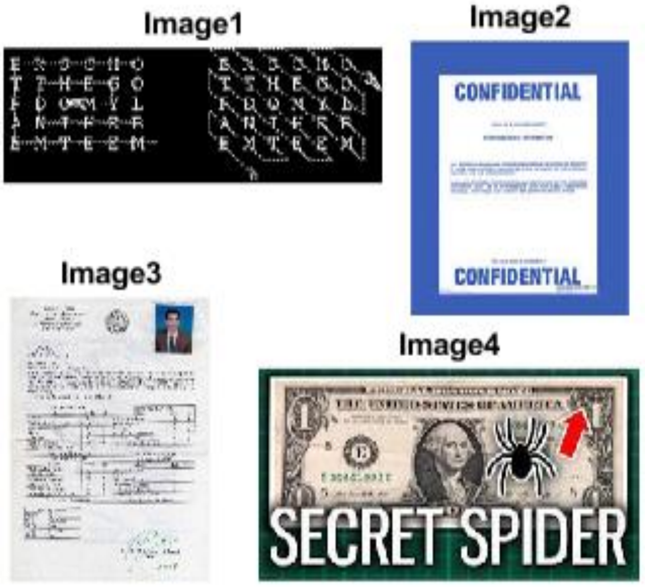


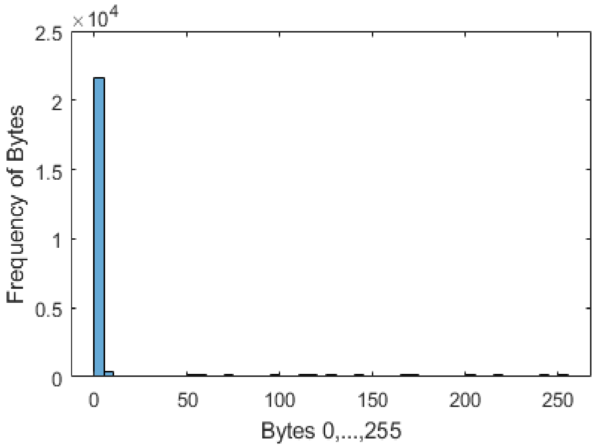
Figure 2. The four secret images.

Table 4. The information of the (4) tested images

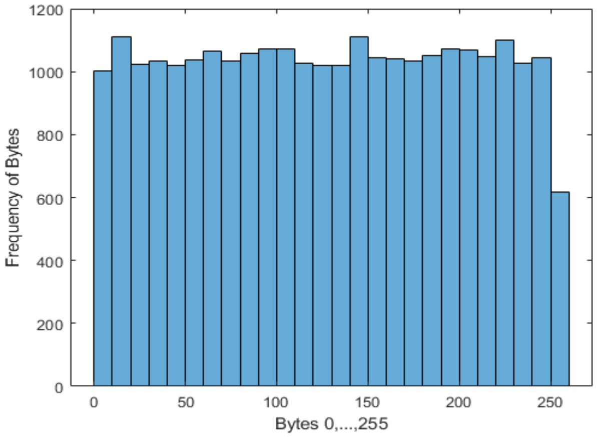
Image	Hight	Width	Size/b.	Description
Image 1	98	274	26852	Encrypted Text
Image 2	229	175	40075	Confidential Document
Image 3	306	214	65484	Certification Document
Image 4	168	300	50400	Paper Currency

Table 5. MSE and PSNR for the (4) images.

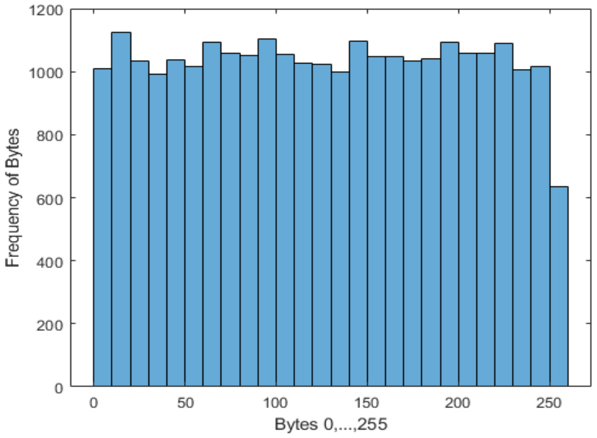
Image	MSE		PSNR
	MSE(E)	MSE(D)	
Image 1	19676.0848	0.0	5.2254
Image 2	14315.1373	0.0	6.6110
Image 3	14580.3871	0.0	6.5272
Image 4	12806.3756	0.0	7.1070



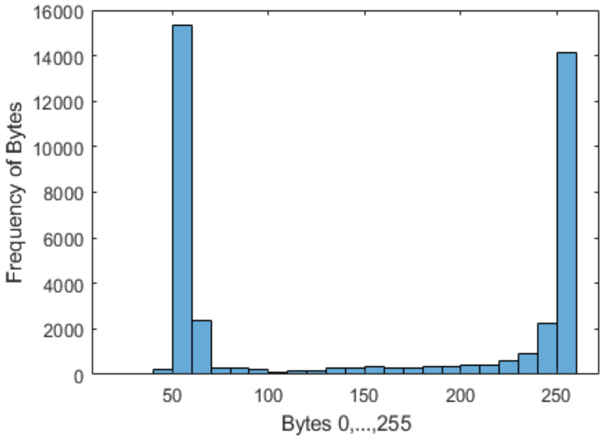
1a



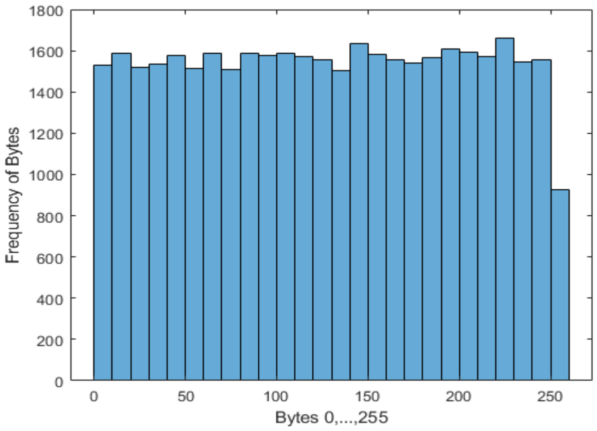
1b



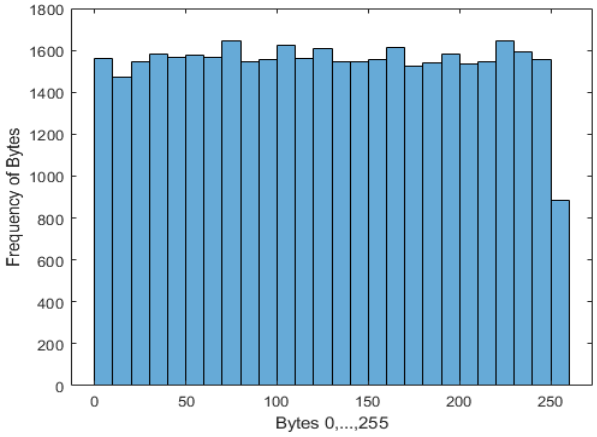
1c



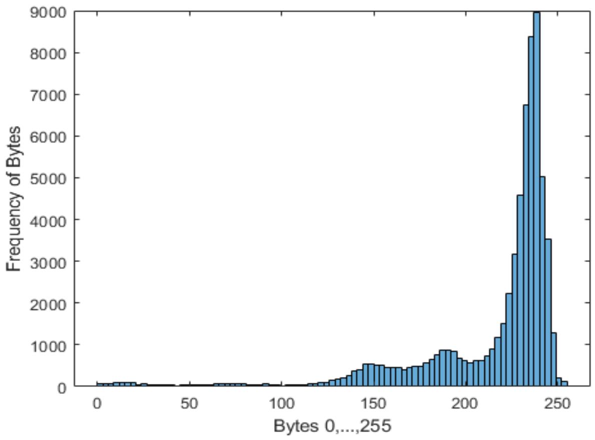
2a



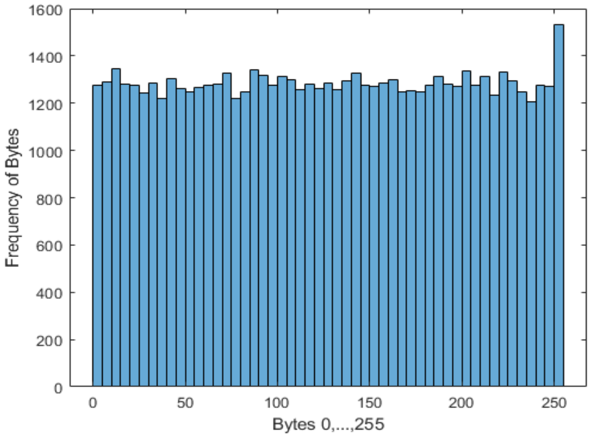
2b



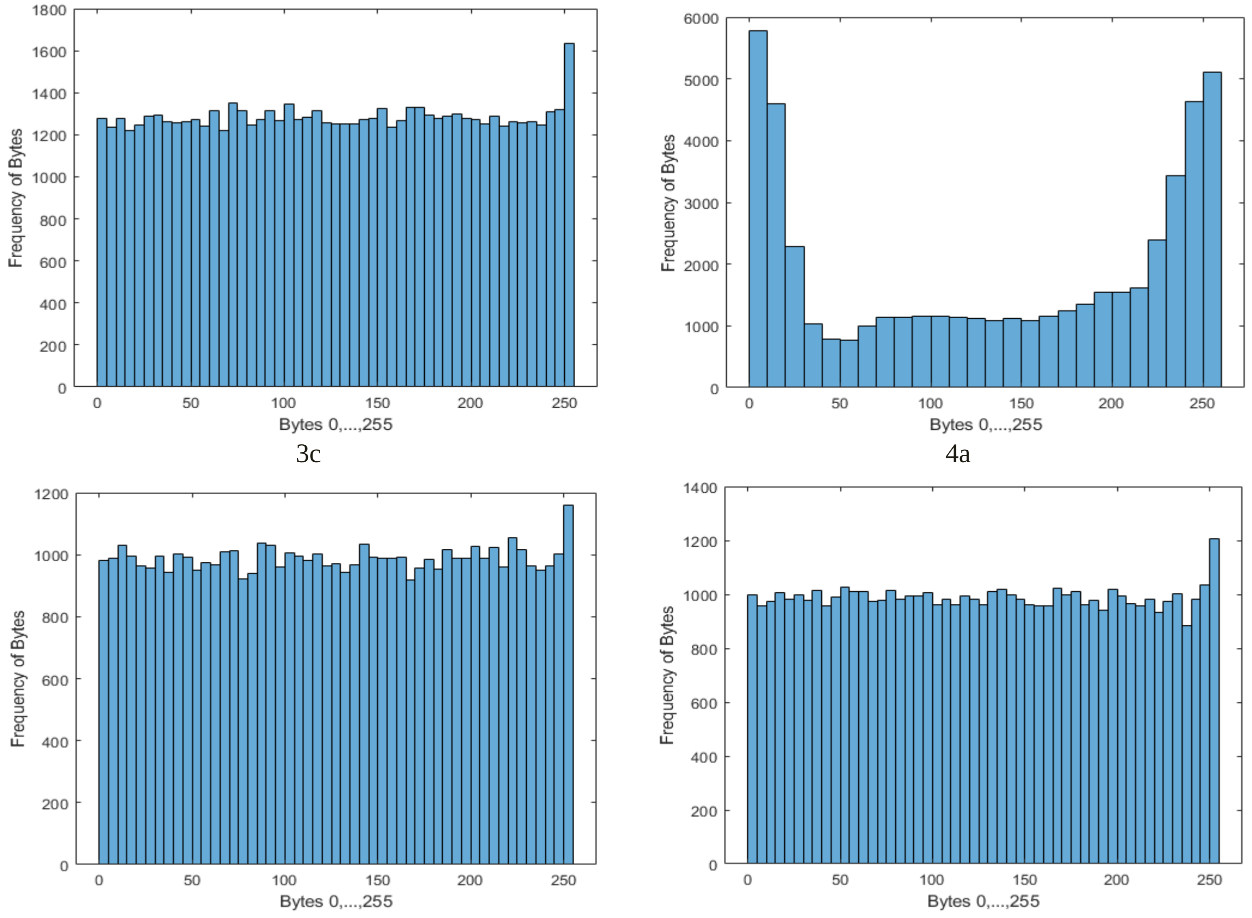
2c



3a



3b



3c 4a

4b 4c

Figure 3. Histogram for (4) images: (a) Plain, (b) Key and (c) Cipher.

Key Space

The size of Key space (or it can be called the general complexity) for the proposed cryptosystem can be calculated as follows:

1. For the LFSRU and CLFSR, and since we have 20 characters, then the general complexity is 2^{160}.
2. For the used CM we have the real value x_0 with 16 digits, so the GC is $10^{16} \approx 2^{53}$.
3. For MCGU, we have: $GC(MSCU) = \phi(q-1) * P_2^{g(q)} * (q-1)$.

So, the general complexity for the proposed cryptosystem is:

$$GC(S) = 2^{213} * \phi(q-1) * P_2^{g(q)} * (q-1) \quad (11)$$

For example, if $q = 1009$, then $GC(MCGU) = 8.3227 \times 10^7$ which is approximately equal to $2^3 \times 2^{23} = 2^{26}$, then:

$$GC(LFSRU, CM, MCGU) \approx 2^{213+26} = 2^{239} \quad (12)$$

CONCLUSIONS

We design a new hybrid cryptosystem using three different approaches: stream, chaotic and MCG system. From the randomness tests, we proved the high randomness of the design cryptosystem since the output sequence passes all the randomness tests. (See, Table 1). The suggested cryptosystem has high periodicity (see relation (9)), and high complexity (see relation (10)). We suggested using four different images to apply the suitable tests on them using the proposed cryptosystem. (See, Figure 2 and Table 4). From Table 5, we proved that a good PSNR and MSE for the encrypted images. By applying the histogram test on the four images (see Figure 3), we see the efficiency of the design cryptosystem by comparing the histogram of the original image, output key and encrypted image for each tested image. We suggest using more tests for the encrypted images such as NIST and key sensitivity analysis. We suggested using the block cipher to encrypt the digital images as a hybrid with stream cryptosystem to increase the security of the cryptosystem.

Disclosure and Conflict of Interest: The authors declare that they have no conflicts of interest.

REFERENCES

[1] A. Oad, H. Yadav and A. Jain, "A Review: Image Encryption Techniques and its Terminologies," International Journal of Engineering and Advanced Technology (IJEAT), vol. 3, p. 2249 - 8958, 2014.

[2] J. P. Aumasson, "Serious cryptography: A practical introduction to modern encryption phone," 2017.

[3] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Communication in nonlinear science and numerical simulation, vol. 15, p. 3998 - 4006, 2010. https://doi.org/10.1016/j.cnsns.2010.01.041

[4] Ü. Çavusoglu and K. I. Pehlivan, "Secure image encryption algorithm design using a novel chaos based S-Box," vol. 95, pp. 92-101, 2017. https://doi.org/10.1016/j.chaos.2016.12.018

[5] H. H. Hussein, M. T. Elkandoz and W. Alexan, "Logistic sine map based image encryption," 2019.

[6] S. M. Ismail and L. A. Said, "Generalized double - humped logistic map based medical image encryption," Journal of advanced research, vol. 10, no. 85-98, 2018. https://doi.org/10.1016/j.jare.2018.01.009

[7] M. Gad, E. Hagras, H. Soliman and N. Hikal, "A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption," The International Arab Journal of Information Technology, vol. 18, no. 2, 2021. https://doi.org/10.34028/iajit/18/2/12

[8] Y. Chen, S. Xie and J. Zhang, "A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map," Entropy (Basel), vol. 24, no. 2, 287, 2022. https://doi.org/10.3390/e24020287

[9] Y. Allemami, M. Afendee and S. Atiewi, "Research on various cryptography techniques,," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 2S3, 2019. https://doi.org/10.35940/ijrte.B1069.0782S319

[10] F. H. Ali and M. G. Sabri, "Cryptanalysis of the Stream Cipher Systems Using the Genetic Algorithm," in Information Technology & National Security Conference, Al-Riyadh-KSA, 2007.

[11] R. J. Anderson, Security Engeneering: A Guide to Bulding Dependable Distributed System, Indianapolis, IN 46256: Wiley Publishing, Inc., 2008.

[12] L. Wu and H. Cai, "Novel stream ciphering algorithm for big data images Using Zeckendorf Representation," Hindawi Wireless Communications and Mobile Computing, Article, 2021. https://doi.org/10.1155/2021/4637876

[13] K. J. Lee and W. L. Wang, "A general structure of feedback shift registers for Built-In Self-Test," Journal information science and engineering, pp. 645-667, 1998.

[14] Z. Hua and Y. Zhou, "One - dimensional nonlinear model for producing chaos," IEEE transactions on circuits and systems, vol. 65, no. 1, pp. 235- 246, 2018. https://doi.org/10.1109/TCSI.2017.2717943

[15] N. A. Hikal and M. M. Eid, "A New Approach for Palmprint Image Encryption Based on Hybrid Chaotic Maps," Journal of King Saud University - Computer and Information Sciences, vol. 32, pp. 870-882, 2020. https://doi.org/10.1016/j.jksuci.2018.09.006

[16] A. A. Mohammed, Bifurcation analysis and design of classes of nonlinear dynamical systems with applications, Baghdad, Iraq: M. Sc. Thesis, Mustansiriyah university, College of Science, Mathematics Science department, 2019.

[17] F. H. Ali, "Use the Multiplicative Cyclic Group to Generate Pseudo Random Digital Sequences," Journal of Al-Rafidain University College for Sciences, vol. 20, pp. 122-135, 2006.

[18] F. H. Ali and A. G. Nasser, "High Efficient Sequences Generate from Developed MCG Generator," Journal of Al-Rafidian University College, vol. 21, no. 25, pp. 169-182, 2009.

[19] A. M. Ali, F. H. Ali and S. M. Redha, "Randomness of the Stream Cipher Digital Sequences in the Field GF(28)," Iraqi Journal of Sceince (Accepted), 2023.

[20] G. Ivarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," international journal of bifurcation and chaos, vol. 16, no. 3, p. 2129 - 2151, 2006. https://doi.org/10.1142/S0218127406015970

How to Cite

A. M. Ali, F. H. Ali, S. M. Redha, and N. . Abubakari, “Image Encryption Using New Non-Linear Stream Cipher Cryptosystem”, Al-Mustansiriyah Journal of Science, vol. 34, no. 2, pp. 103–112, Jun. 2023.