

Efficient image encryption scheme using a nonlinear shift register and chaos

Hadjer Bourekouche *

LIST Laboratory

Department of Electrical Systems Engineering

Faculty of Technology

University M'Hamed BOUGARA of Boumerdes

Avenue of Independence

35000 Boumerdes

Algeria

Samia Belkacem [†]

LIMOSE Laboratory

Department of Electrical Systems Engineering

Faculty of Technology

University M'Hamed BOUGARA of Boumerdes

Avenue of Independence

35000 Boumerdes

Algeria

Noureddine Messaoudi [§]

LIST Laboratory

Department of Electrical Systems Engineering

Faculty of Technology

University M'Hamed BOUGARA of Boumerdes

Avenue of Independence

35000 Boumerdes

Algeria

* E-mail: h.bourekouche@univ-boumerdes.dz (Corresponding Author)

<https://orcid.org/0000-0003-3516-290X>

[†] E-mail: s.belkacem@univ-boumerdes.dz

<https://orcid.org/0000-0003-0912-3392>

[§] E-mail: n.messaoudi@univ-boumerdes.dz

<https://orcid.org/0000-0002-3406-4120>



Abstract

Powerful cryptographic systems require a qualified random number generator. This research purposes to provide a comprehensive comparative analysis done on several of the well-known pseudo-random number generators (PRNGs) regarding their efficiency and resilience against crypto-analytical threats. These generators consist of the basic 8-bit Non-Linear Feedback Shift Register (NLFSR), the logistic map (LM), and our proposed hybrid random number generator named NLFSR-LM, which combines through XOR operation the sequences of the NLFSR with the LM to achieve a high quality of randomness. The performance of the created generator is examined and subsequently compared according to statistical tests of randomness alongside cryptographic features in terms of key space, key sensitivity and resistance to numerous attacks. The proposed generator produced good results and exhibited several interesting properties, such as a high degree of security, a sufficiently large key space, and it provided better randomness than other frequently used PRNGs.

Subject Classification: (2010) 11T71, 68P25, 94A60, 68R01.

Keywords: Random number generator, NLFSR, Logistic map, NLFSR-LM, Image encryption.

1. Introduction

The security of images is a major issue in real-time applications[1]; therefore, applying cryptography is a direct way to hide image information by converting known images into unrecognized noise-like ones[2]. When designing encryption algorithms, the security level of the whole system is dependent significantly on the employed key's complexity[3], [4]. However, alternative techniques have been offered to make keys more secure and prevent any possible abuse, and other strategies are being developed for the same[5]. Therefore, random number generators (RNGs) utilized in cryptographic applications must fulfill strict security standards in order to be regarded as safe for usage[6]. In reality, utilizing weak random values allows an opponent to break the entire system[7].

Pseudorandom number generators which are mostly used in computer applications, are created using a mathematical formula in a predictable way. This is appropriate for many applications and sometimes even ideal[8].

With every new technique of designing random numbers, there is an improvement that is expected, existing pseudo-random number generator schemes exhibit drawbacks in different aspects. Researchers have used feedback shift registers (FSR) and chaos-based cryptosystems, among many other techniques, for many reasons. For instance, when dealing with multimedia data, chaos-based solutions are extremely successful [9], in general, chaos possesses three crucial dynamic features[10]: (1) the

sensitive dependency on initial conditions, (2) the semi-stochastic feature, and (3) ergodicity[11]. On the other hand, the generalized feedback shift register pseudorandom number approach offers significant benefits over all other pseudorandom number generators [12]; it generates multidimensional pseudorandom numbers with arbitrarily long period; it is portable and faster than other pseudorandom number generators.

In this study, the Non-Linear Feedback Shift Register (NLFSR) according to the logistic map (LM), which have been most often utilized in cryptographic applications, are selected to develop our suggested pseudo-number generator, termed NLFSR-LM. These generators are evaluated and compared according to various criteria, which consist of statistical randomness quality, and are subsequently employed for image cryptography.

Our paper is globally organized as follows: Section II introduces overviews of the logistic map (LM) with the NLFSR, and then the structure of the suggested generator (NLFSR-LM) is studied correspondingly. Section III presents approved tests for the randomness and key sensitivity of RNGs. Section IV demonstrates and discusses the use of the proposed RNG in image cryptography. Section V provide the results and assessment are provided in Section V. In Section VI, a comparative study of the performance of the three schemes is presented.

II. Background Information

In this part, we will present the pseudo-number generators that have been selected for comparison: the nonlinear feedback shift registers (NLFSR), the logistic map (LM), and our generator based on combining the NLFSR with the LM, termed the NLFSR-LM.

Logistic map (LM)

LM is one of the basic one-dimensional chaotic maps that is characterized by[13]: (1) simple structure, (2) easy implementation, and (3) moderate computing cost. It is commonly mentioned as an example of how complicated behavior may evolve from a basic deterministic dynamic system without any stochastic disruption[14]. However, the restricted chaotic range and nonuniform data distribution of the output chaotic sequences are drawbacks[15].

This map is written as:

$$\text{For } 0 < \mu \leq 4, X_n \in [0, 1] \quad X_{n+1} = \mathcal{L}(\mu, X_n) = \mu X_n (1 - X_n) \quad (1)$$

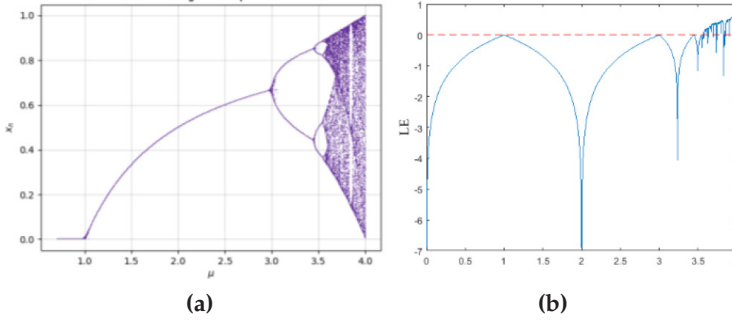


Figure 1

Logistic map: (a) BD; (b) LE.

In which μ is a control parameter that decides whether chaotic variable X stabilizes at a constant value [14], and the initial value of the system is set to X_0 ($0 < X_0 < 1$) [16]. The relationship between μ and chaotic behavior is represented by the bifurcation diagram (BD) that provides details of the system dynamics as depicted in Figure 1 (a).

The behavior of the logistic map depends on μ , when $3.5699 < \mu < 4$, the system goes into chaos [16]. According to Figure 1 (b), the Lyapunov exponent (LE) of the logistic mapping is positive when $3 < \mu < 4$ [16], indicating that the system is in a chaotic state [17].

Note that the main flow generator's parameter interval must be guaranteed to be in a chaotic state.

Non-Linear Feedback Shift (NLFSR)

To create pseudo-random sequences for stream ciphers [18], Non-Linear Feedback Shift Registers [19] have been suggested as alternatives to Linear Feedback Shift Registers (LFSRs) [20]–[22]. As the LFSR is structurally a shift register with specific tap taken out and XOR-ed with n flip-flop and fed back to itself [23] via a linear Boolean function, the NLFSR is a generalization of a LFSR where the feedback function is any Boolean function f of n variables [20], [24], but the contents of n stages are calculated according to a non-linear function. To illustrate the principle of NLFSR, consider the feedback shift register (FSR) in Figure 2.

Where, f is the nonlinear feedback function represented as [25]:

$$f(x_i, x_{i+1}, x_{i+2}) = 1 \oplus x_i \oplus x_{i+2} \oplus x_{i+1}x_{i+2} \quad (2)$$

(x_0, x_1, x_2) are the initial fills.

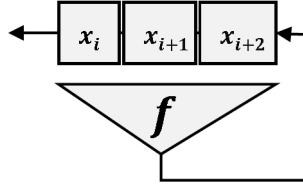


Figure 2

General diagram of the Feedback Shift register.

Proposed generator NLFSR-LM

Our proposed generator illustrated in Figure 3 comprises of two subsystems stated before; the first is based on the chaotic time series (logistic map (LM)) and the second is based on the Non-Linear Feedback Shift Registers (NLFSRs).

First, we employ a Fibonacci NLFSR that comprises of 8-bit shift registers with particular feedback functions. As a potential valid feedback polynomial for an 8-bit NLFSR is mentioned in [26], we choose f as:

$f = x_0 \oplus x_1 \oplus x_6 \oplus (x_1 \cdot x_2)$, where taps x_0, x_1, x_6 are XORed with x_1 and x_2 to get the output bit and feedback to the rightmost bit. The second task is to select the chaotic map with parameter μ that contributes to have an excellent chaotic behavior of the function. Because we are using the logistic map whose input and output value belong to the interval $[0,1]$.

The generated chaotic sequence X_{n+1} should be converted to an unsigned integer in the range of 0 to 255 by multiplying the sequence

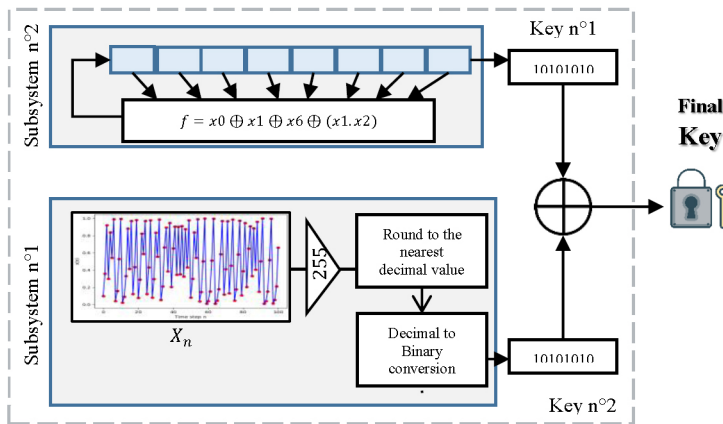


Figure 3

Proposed NLFSR-LM Key generator structure.

element X_{n+1} with 255, then round it to the nearest decimal value, to be converted then via a decimal to binary converter.

Finally, the XOR operation is applied on the sequences produced by the two subsystems to acquire the final sequence of key. The symbol $\oplus$ signifies addition modulo 2.

III. Evaluation and comparison of PRNGs

The security of an entire program is significantly affected by the used random numbers, therefore, it is important to guarantee the security of the generated numbers used in these applications [6].

In this part, we investigate and compare the randomness quality of the NLFSR, the logistic map, and our suggested combination NLFSR-LM generated sequences, via the National Institute of Standards and Technology (NIST) [27], [28], which has set rules for random number generation. Then, the key sensitivity of the suggested key sequence is assessed by the Pearson's correlation coefficient [29] and the Hamming distance.

NIST test of randomness

The 15 subtests that make up the NIST test can all be used to assess the unpredictability of the sequences. The test results primarily demonstrate the pros and cons of the pseudo-random sequence by examining the uniformity of the sequence [30] [31], in which the regularity of the sequence is represented by a probability value (P-value) [32].

The p-value of each subtest is compared with the significance level α , that is chosen by a tester [33] (for cryptography and in the case of NIST test suite version SP800-22, α is usually set to $\alpha = 0.01$ [33]). If the sequence has a P-value of $\geq \alpha$, then it is random; otherwise, it is not. The four alternative categories may be used to categorize the NIST tests. These tests include the frequency test (tests 1-4), the repetitive pattern test (tests 5-7), the pattern matching test (tests 8-12), and the random walk test (tests 13-15). The numerical values in Table I lead us to conclude that:

In the case of the sequence created by the basic NLFSR, 15 tests were done, and out of that, 10 have failed as the resultant P-values are considerably less than 0.01. Thus, the sequence generated cannot match the criterion of randomization for the secure method.

Sequences generated by using a simple chaotic map, such as a logistic map (LM), are not highly random and provide less security, because 10 out

Table I
NIST test suite.

n	Test	Proposed (LM-NLFSR)		NLFSR		Logistic Map(LM)	
		P-value	Pass/ Fail	P-value	Pass/ Fail	P-value	Pass/ Fail
1	Frequency Test (Monobit)	0.76415	Pass	2.14427 e-10	Fail	7.17529e-05	Fail
2	Frequency Test within a Block	0.37932	Pass	0.99999	Pass	3.47372e-10	Fail
3	Run Test	0.55484	Pass	0.0	Fail	4.00730e-121	Fail
4	Longest Run of Ones in a Block	0.12164	Pass	3.55113 e-08	Fail	1.32771e-91	Fail
5	Binary Matrix Rank Test	0.69244	Pass	0.405550	Pass	0.69244	Pass
6	Discrete Fourier Transform Test	0.77602	Pass	2.67766 e-47	Fail	0.22926	Pass
7	Non-Overlapping Template Matching Test	0.94259	Pass	3.81760 e-14	Fail	8.69254e-41	Fail
8	Overlapping Template Matching Test	0.17493	Pass	8.05656 e-08	Fail	2.79215e-35	Fail
9	Maurer's Universal Statistical test	-1.0	Fail	-1.0	Fail	-1.0	Fail
10	Linear Complexity Test	0.86082	Pass	0.64701	Pass	0.59279	Pass
11	Serial test	0.08374	Pass	0.08374	Pass	9.02224e-09	Fail
12	Approximate Entropy Test	0.14597	Pass	0.0	Fail	3.67830e-63	Pass
13	Cummulative Sums (Forward) Test	0.82356	Pass	3.52703 e-10	Fail	0.00012	Fail
14	Cummulative Sums (Reverse) Test	0.88208	Pass	3.30387 e-10	Fail	6.49393e-05	Fail
15	Random Excursions Test	0.46045	Pass	0.71348	Pass	0.18615	Pass

of 15 tests failed, this suggests that employing logistic chaotic maps to generate key sequences does not provide a high degree of security for cryptographic applications.

The sequence generated by the suggested NLFSR-LM generator has desired randomness properties, by passing at least 14 out of 15 tests of the NIST suite, as all the p-values are considerably greater than 0.01, which indicates the supply of high randomness from the provided method.

Key sensitivity analyses of the NLFSR-LM

The sensitivity of the produced keys is guaranteed by testing the correlation between the generated sequences of keys [34], it has two ways: the Pearson's correlation coefficient [35] and the hamming distance [34].

Pearson's correlation coefficient

The strength of the linear link between two sets of data is statistically measured using Pearson's correlation coefficient [36]. Where $\text{str} = [x_1, \dots, x_n]$ and $\text{str1} = [y_1, \dots, y_n]$ [34].

The Pearson's correlation coefficient is given by:

$$R_{(\text{str}, \text{str1})} = \frac{\sum_{i=0}^{n-1} (x_i - \bar{x}) \cdot (y_i - \bar{y})}{[\sum_{i=0}^{n-1} (x_i - \bar{x})^2]^{1/2} \cdot [\sum_{i=0}^{n-1} (y_i - \bar{y})^2]^{1/2}} \quad (3)$$

$\bar{x}$, $\bar{y}$ mentioned by equation (4) represents the mean values of Str and Str1.

$$\begin{cases} \bar{x} = \sum_{i=0}^{n-1} \frac{x_i}{n} \\ \bar{y} = \sum_{i=0}^{n-1} \frac{y_i}{n} \end{cases} \quad (4)$$

Hamming distance

Based on studying the bits of the sequences directly, we determine the average Hamming distance [37] by calculating the number of distinct bits between two binary sequences that have the same length m [38]. Consequently, the following equation provides the Hamming distance for two binary sequences [39]:

$$d(s_1^b, s_2^b) = \sum_{j=0}^{m-1} (x_j \oplus y_j) \quad (5)$$

Where x_j , y_j are the elements of s_1^b , s_2^b .

In our test, three primary binary keystream sequences K1, K2, and K3 produced by our suggested NLFSR-LM are formed from slightly different initial values:

K_1 is produced using the following initial values:

$$\mu_0 = 3.999000000000011, X_0 = 0.100000000000011, \text{NLFSR} = 10101101$$

K_2 is produced using the following initial values:

$$\mu_0 = 3.999000000000099, X_0 = 0.100000000000099, \text{NLFSR} = 10101100$$

K_3 is produced using the following initial values:

$$\mu_0 = 3.999000000000059, X_0 = 0.100000000000067, \text{NLFSR} = 10101001$$

Correlation results explained by Pearson's correlation coefficients and Hamming distance [37] of three key sequences generated by NLFSR-LM were constructed as described in TABLE II. Basically, if two sequences have a Pearson correlation and hamming distance of 1 or of -1 , this implies that one set of the sequences is redundant.

In our case, the connection between K1, K2, and K3 assigns a value between 1 and -1 , implying that the three sets of keys were uncorrelated; the three key sequences do not have the same information content. Thus, the proposed NLFSR-LM benefice an extreme sensitive to the system parameter with initial conditions (keys), and a capability of generating a large and uncorrelated number of key sequences that exceed 520×10^3 bits for each iteration.

Table II
Pearson's correlation and the hamming distance results.

	K1 vs K2	K1 vs K3	K2 vs K3
Pearson's correlation coefficients	-0,0038	0,0043	0,00043
Hamming distance	0.9933	0.99581	0.9959

IV. Image encryption and decryption scheme based on the NLFSR, LM, and NLFSR-LM generators

In this section, three key sequences are employed for image encryption and decryption. Here, we utilize the most simple and appropriate scheme for basic encryption and decryption which is the exclusive OR (XOR) operation [40]. This method is predicated on the idea that by performing an XOR operation on two numbers A and B, C will be produced. The same

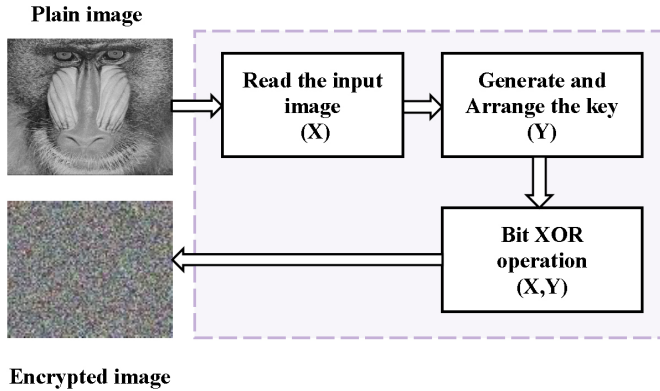


Figure 4
Image encryption procedure.

manner when performing XOR operation on the Key and B, then C is returned to A. The XOR approach has various advantages over other simple encryption techniques, including a fast and simple algorithm, and the ability to completely achieve lossless reduction by encrypting the image's gray value [40].

In Figure 4 we illustrate the encryption process. After reading the input image (X) of size $(n \times m)$ to be encrypted, we arrange the key (Y) according to the image dimension in the Row Major Order, where the elements of the binary vector of random numbers are arranged sequentially row-wise, which means filling all the indices of the first row and then moving to the next row in order to produce the key's matrix of size $(n \times m)$. Later, the input image and cipher matrix of the previously generated key are combined using the bitwise XOR operation.

As is the usual protocol, the decryption process reverses the encryption operation and restores the original data. The bitwise XOR operation with the same arranged key matrix used for encryption is used to decode the cipher image in our proposed scheme.

V. Experimental tests and security analysis

An effective image encryption technique can withstand numerous regularly used attacks, such as the brute-force attack [41] and differential attack [42]. This part includes thorough numbers, tables, and explanations to assess the performance and compare the NLFSR, the LM, and the proposed algorithm. This article used MATLAB R2018a to run a simulation

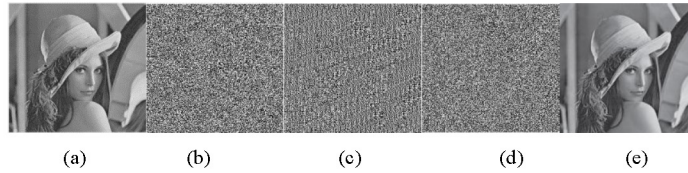


Figure 5

Image encryption and decryption results: (a) Plain-image; (b) NLFSR-LM encrypted image; (c) NLFSR encrypted image; (d) LM encrypted image; (e) NLFSR-LM decrypted image.

experiment on a PC with a Pentium (R) Dual Core T4500 CPU running at 2.30 GHz and 2 GB of RAM under Microsoft Windows 7.

Encryption and decryption experiments

Using the right created keys and the suitable initial values, in this subsection, we describe the encryption and decryption outcomes. $X_0 = 0.1$ is the initial value of the chaotic map along with μ which represent the control parameter and it is selected to be in the chaotic interval; $\mu = 3.999$. The initial state of the NLFSR is chosen to be [10101101].

Figure 5 shows the encryption-decryption results using the three sequences of keys generated by the NLFSR, LM and our combination NLFSR-LM. It may be reached at a conclusion from the figures that:

The plain image is successfully encrypted into a noise-like secret image in the three circumstances where, we can see the primitive information is totally destroyed, which results in enhanced privacy protection. Meanwhile, we employ the right keys for decryption, and the results are presented in Fig. 5(e), the original images are correctly recovered, revealing that our encryption process is reversible. Overall, this experiment indicates that our encryption system works legitimately in all three cases.

Histogram

A crucial statistical component of an image is its histogram, which is used to describe the spread of pixels in the image [43], [44]. Figure 6 shows the plain-image and equivalent cipher-images for the three schemes and their histograms. From the presented figures, it may be seen that:

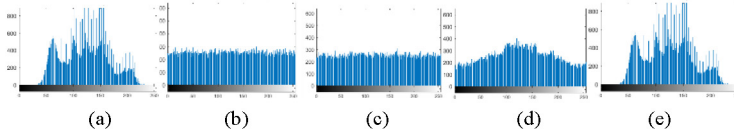


Figure 6

Histogram plot of: (a) Plain-image; (b) NLFSR-LM encrypted image; (c) NLFSR encrypted image; (d) LM encrypted image; (e) NLFSR-LM decrypted image.

The histograms of the encrypted images are radically different from those of the original images. The histogram of the encrypted image employing the LM method is not flat, which indicates that the distribution of pixel values is not uniform, thus resulting in the leakage of some statistical information.

The histograms of encrypted images employing the NLFSR and the proposed NLFSR-LM are flat and evenly distributed. It signifies that the distribution of pixel values is uniformly distributed, this illustrates the resistance of the two encryption methods to statistical attacks.

Entropy

The information entropy measures the quantity of information in an image [45]. It is computed as follows [46]:

$$P(m) = -\sum_{i=0}^{255} P(m_i) \log_2(m_i) \quad (6)$$

Where m is the image, and $P(m_i)$ is the probability of m_i gray value in the image [46]. For a 256-gray-level image, an optimal Shannon entropy value is 8.

Table III

Entropy score values.

	Original	Encrypted (LM- NLFSR)	Encrypted (NLFSR)	Encrypted (LM)	Decrypted (LM-NLFSR)
Entropy	7.2432	7.9970	7.9956	7.9593	7.3224

By using the three schemes as depicted in Table III, the information entropies values of encrypted Lena images using the NLFSR and the proposed NLFSR-LM have assumed values varying from 7.995 to 7.997.

This indicates that the encrypted images are relatively close to a random source, and that these two approaches are resistant to an entropy attack.

Anti-Differential Attack

To evaluate the sensitivity of the ciphertext image to the plain-image, we use the number of pixels changes rate (NPCR) [47], the number average changing intensity (UACI) and the peak signal-to-noise ratio (PSNR) [47] in equations (7), (8) and (9) respectively [46]:

$$NPCR = \frac{\sum_{i=1}^H \sum_{j=1}^W \sum_{k=1}^L D(i, j, k)}{M.N} \times 100\% \quad (7)$$

$$D(i, j, k) = \begin{cases} 0 & C1(i, j, k) = C2(i, j, k) \\ 1 & C1(i, j, k) \neq C2(i, j, k) \end{cases}$$

$$UACI = \frac{1}{255.M.N} \left[\sum_{i=1}^H \sum_{j=1}^W \sum_{k=1}^L \frac{|C1(i, j, k) - C2(i, j, k)|}{2^Q - 1} \right] \times 100\% \quad (8)$$

Where C1 and C2 are two ciphertext images encrypted using only slightly different images [46].

$$PSNR = 20 \log_{10} \left(\frac{255}{\sqrt{MSE}} \right) \quad (9)$$

$$MSE = \frac{1}{W.H.L} \sum_{i=1}^H \sum_{j=1}^W \sum_{k=1}^L [I(i, j, k) - K(i, j, k)]^2 \quad (10)$$

MSE is the mean squared error [48]. I, and K are the pixel positions, whereas i, j, and k are the pixel values of the original and encrypted images [48], respectively.

Table IV
NPCR, UACI, MSE and PSNR values.

	NPCR	UACI	MSE	PSNR(dB)
Encrypted (LM-NLFSR)	0.996231	0.278690	7.229+03	45.10937
Encrypted (NLFSR)	-	0.282059	6.39e+03	44.94362
Encrypted (LM)	0.990203	0.246942	7.36e+03	46.19030

A comparison of the NPCR, UACI, and PSNR for the proposed scheme and the NLFSR scheme, according to the LM scheme, is shown in

Table IV, demonstrating that the suggested confidentiality scheme is more resilient in repelling differential attacks.

Correlation coefficient analysis

Due to a correlation value mainly close to 1, one pixel of an original image is often highly associated with nearby pixels [13] in the three directions: horizontal (H), diagonal (D), and vertical (V) directions [49]. Thus, an effective encryption technique should be able to disrupt the associations between nearby pixels.

Table V

Horizontal, vertical, and diagonal corr values of 2048 pairs of original, encrypted and decrypted image.

	Original	Encrypted	Encrypted (NLFSR)	Encrypted (LM)	Decrypted (LM-NLFSR)
H	0.9438	0.0019	-0.2007	-0.0222	0.9346
V	0.9700	-0.0133	0.0029	-0.0166	0.9675
D	0.9152	-0.0205	0.0678	0.0003	0.9125

The correlation between the neighboring pixels in three directions; horizontal, vertical, and diagonal are reported in Table V according to

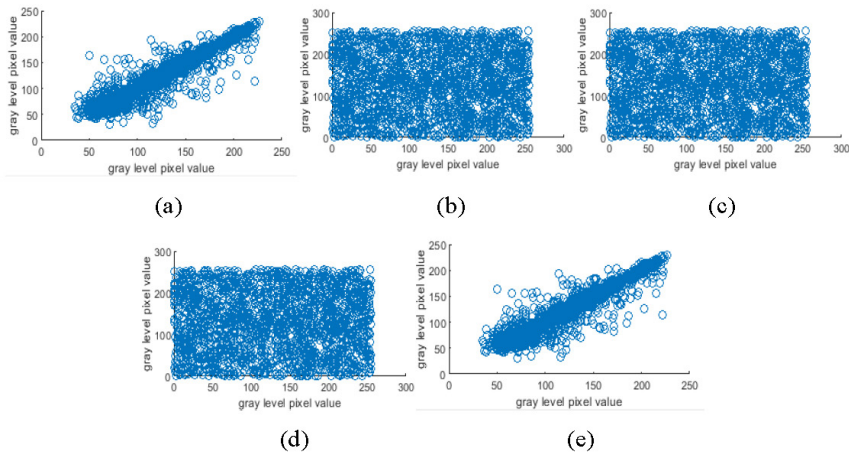


Figure 7

Correlation results: (a) Plain-image; (b) NLFSR-LM encrypted image; (c) NLFSR encrypted image; (d) LM encrypted image; (e) NLFSR-LM decrypted image.

Figure 7; it is clear that the correlations between pixels in the cipher image using the NLFSR-LM scheme are significantly minimized compared to those obtained using only the NLFSR or only the logistic map (the values are very close to the 0 value), so the proposed algorithm successfully destroys the related coefficient.

Key sensitivity

A reliable test to measure the strength of an encryption cryptosystem for digital images is key sensitivity against even a tiny change in a single key [50]. The parameters and initial values used to assess the key sensitivity of our proposed cryptosystem are listed in Table VI.

Even with a minor variation in the single parameter μ between the encryption right key (K1) and wrong key (K2) for the identical image, we noticed a difference in the resultant pixel-to-pixel difference $|E_1 - E_2|$ [51] as shown in Figure 8.

Key space

To evaluate the cipher’s security, a brute-force assault, known as a chosen-plaintext attack, is used. Since the approach uses double precision floating point numbers in representing real numbers on computers, the

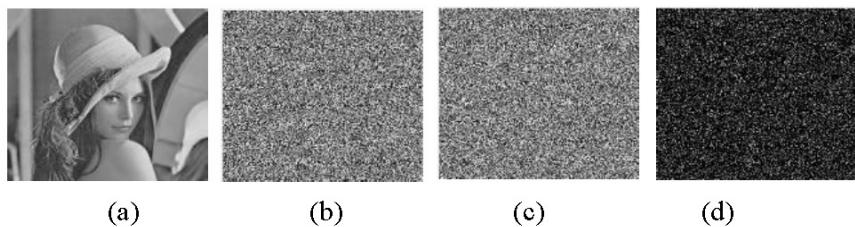


Figure 8

Key sensitivity analysis :(a) Original image, (b) Encrypted image with correct key E1, (c) Encrypted image with wrong key E2, (d): Pixel-to-pixel difference $|E_1 - E_2|$.

Table VI

Parameters and initial values used as K1 and K2.

	μ	X_0	NLFSR Initial state
K1	3.999	0.1	10101101
K2	3.9990000000000001	0.1	10101101

cost to estimate μ is 10^{-15} , in accordance with IEEE-754 standards [52]. The total number of keys used as a component of the key generator system is represented by the key space employed in the proposed work. For our scheme, we have:

The 8-bit NLFSR generated sequences are $\text{key1} = (2^8 - 1) \approx 255$. Thus, total key-space of the NLFSR is 2^8 .

The precision of the initial condition X_0 variation along with bifurcation parameter is 10^{-15} . The key-space for X_0 is $\text{key2} \approx 10^{15}$ and for the bifurcation parameter is $\text{key3} \approx 10^{15}$.

The iterations number $n = 65536$, so the iteration number is $\text{key4} \approx 65.10^3$. Thus, total key-space of the LM is 2^{118} .

Finally, the total key-space of the NLFSR-LM is $\approx 255 \times 65 \times 10^3 \times 10^{15} \times 10^{15} \approx 10^{37}$ which is roughly equal to 2^{126} .

To fend against brute force attacks, the key space of the image encryption technique should be greater than 2^{100} [53]. Consequently, compared with existing systems, the proposed algorithm has a vast key space to fend against brute-force attacks.

VI. Comparative analysis

Here, we briefly compare our proposed NLFSR-LM generator with the currently available NLFSR and LM RNGs, and subsequently, its application to image encryption. First, a statistical randomness test is done to assess the quality of the random numbers generated by the three types of generators. The satisfactory findings from the NIST tests reveal that the random bit sequence of our evolutionary random bit sequence generator (NLFSR-LM) has higher statistical quality and does not have any statistical defects. It also offers important benefits in that it prevents data loss, which is a key problem when taking into account the challenges and costs of producing random numbers in contrast to the NLFSR and LM generators, which proved that it does not meet the randomness level requirements for cryptographic applications.

The second part of our comparison study focuses on the application of the three number generators in image encryption, where a comparative analysis is performed among the tested parameters presented in Section V. It can be noticed that:

- The correlation tested in three directions between the neighboring pixels obtained from the three techniques is similar to the previously released scheme, demonstrating that the suggested NLFSR-LM,

NLFSR, and even LM image encryption techniques may effectively reduce the adjacent pixel's correlations in the encrypted images. Behind the histogram plot, which is found to be flat and uniformly distributed in the case of NLFSR and NLFSR-LM, the statistical analysis reveals that the scheme protects the image from any form of statistical attack.

- The image encrypted with the proposed NLFSR-LM scheme attains maximum information entropy in form of a random pixel value distribution, making it nearly impossible to obtain visual information from encrypted images, which makes it secure against entropy attacks.
- The values of NPCR, UACI, and PSNR of the suggested technique are close to the theoretical values in request, which proves to be exceedingly sensitive for our scheme for resisting differential attacks.
- Sensitivity to secure key changes of the proposed NLFSR-LM algorithm is high in both encryption and decryption phases, and its key space is much larger than that of only NLFSR or only LM. This advantage supports system's qualification in resisting different brute-force attacks.

Table VII
comparative analysis.

	Evaluation parameters	Proposed NLFSR-LM	NLFSR	LM
RNG	NIST Pass/Fail	Pass	Fail	Fail
	Randomness conclusion	Random	Not random	Not random
	Efficiency	Excellent	Poor	Poor
RNG applied in image encryption	Resistance to statistical attack	High	High	Less
	Resistance to entropy attack	High	High	Medium
	Resistance to differential attacks	High	High	Medium
	Key space	2^{126}	2^8	2^{118}
	Key sensitivity	High	Less	High
	Resistance to Brute force attack break	High	Less	High
	Security	High	Less	Less

Finally, from the findings reported in Table VII, it is evident that the security analyses and experimental results indicate the efficacy of the proposed method.

VII. Conclusion

This study aimed to provide an efficient design of a binary sequence generator termed NLFSR-LM and then compare it with the current random number generators in the literature, as well as the NLFSR and the logistic map (LM). These generators are utilized for producing sequences of keys whose features are gauged by utilizing NIST SP 800-22 r1a for use in image encryption. The findings were also compared to those of the NLFSR and LM encryption methods to assess the strength of our proposed NLFSR-LM cryptosystem. The encryption system using the XOR algorithm was assessed using several statistical tests. The acquired findings revealed a considerable increase in system efficiency and resistance against several types of cryptographic analysis challenges compared with prior image encryption techniques based on comparable algorithms. Overall, our proposed scheme meets a high level of security which enables it to be applied to secure medical image storage and transmission.

Acknowledgement

We appreciate the useful comments provided by the anonymous reviewers.

Declaration of interests

The authors declare that they have no known contending monetary interests or individual connections that might have seemed to impact the work revealed in this paper.

References

- [1] G. Lokeshwari, S. Udaya Kumar, and S. Susarla, "Experimental analysis of image encryption using elgamal and block-substitution method for color images," *J. Inf. Optim. Sci.*, vol. 38, no. 5, pp. 745–757, Jul. 2017, doi: 10.1080/02522667.2016.1251026.

- [2] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019, doi: 10.1016/j.ins.2018.12.048.
- [3] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ELYazeed, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," *Signal Process.*, vol. 167, p. 107280, Feb. 2020, doi: 10.1016/j.sigpro.2019.107280.
- [4] I. Meraouche, S. Dutta, H. Tan, and K. Sakurai, "Tree Parity Machine-Based Symmetric Encryption: A Hybrid Approach," in *Mathematics and Computing*, B. Rushi Kumar, S. Ponnusamy, D. Giri, B. Thuraisingham, C. W. Clifton, and B. Carminati, Eds., in Springer Proceedings in Mathematics & Statistics. Singapore: Springer Nature, 2022, pp. 61–73. doi: 10.1007/978-981-19-9307-7_6.
- [5] A. Ramesh and A. Jain, "Hybrid image encryption using Pseudo Random Number Generators, and transposition and substitution techniques," in 2015 International Conference on Trends in Automation, Communications and Computing Technology (I-TACT-15), Dec. 2015, pp. 1–6. doi: 10.1109/ITACT.2015.7492652.
- [6] S. Yakut, T. Tuncer, and A. B. Ozer, "Secure and Efficient Hybrid Random Number Generator Based on Sponge Constructions for Cryptographic Applications," *Elektron. Ir Elektrotechnika*, vol. 25, no. 4, Art. no. 4, Aug. 2019, doi: 10.5755/j01.eie.25.4.23969.
- [7] A. Doğanaksoy, F. Sulak, M. Uğuz, O. Şeker, and Z. Akcengiz, "New Statistical Randomness Tests Based on Length of Runs," *Math. Probl. Eng.*, vol. 2015, p. e626408, Apr. 2015, doi: 10.1155/2015/626408.
- [8] J. Łukasiewicz, A brief overview of pseudo-random number generators and testing of our own simple generator. 2021. doi: 10.13140/RG.2.2.12598.22089/1.
- [9] S. Kumar, P. K. Srivastava, G. K. Srivastava, P. Singhal, D. Singh, and D. Goyal, "Chaos based image encryption security in cloud computing," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1041–1051, May 2022, doi: 10.1080/09720529.2022.2075085.
- [10] M. S. Tavazoei and M. Haeri, "Comparison of different one-dimensional maps as chaotic search pattern in chaos optimization algorithms," *Appl. Math. Comput.*, vol. 187, no. 2, pp. 1076–1085, Apr. 2007, doi: 10.1016/j.amc.2006.09.087.

- [11] Y. He, J. Zhou, N. Lu, H. Qin, and Y. Lu, "Differential evolution algorithm combined with chaotic pattern search," *Kybernetika*, vol. 46, no. 4, pp. 684–696, 2010.
- [12] T. G. Lewis and W. H. Payne, "Generalized Feedback Shift Register Pseudorandom Number Algorithm," *J. ACM*, vol. 20, no. 3, pp. 456–468, Jul. 1973, doi: 10.1145/321765.321777.
- [13] M. Essaid, I. Akharraz, A. Saaidi, and et A. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–187, Aug. 2019, doi: 10.1016/j.jisa.2019.05.006.
- [14] Y.-Y. He, J.-Z. Zhou, X.-Q. Xiang, H. Chen, and H. Qin, "Comparison of different chaotic maps in particle swarm optimization algorithm for long-term cascaded hydroelectric system scheduling," *Chaos Solitons Fractals*, vol. 42, no. 5, pp. 3169–3176, 2009.
- [15] S. Kamal, M. Darwish, and K. Hosny, "Chaotic Maps for Image Encryption: An Assessment Study," 2020. doi: 10.1007/978-3-030-38700-6_2.
- [16] L. Wang and H. Cheng, "Pseudo-Random Number Generator Based on Logistic Chaotic System," *Entropy*, vol. 21, no. 10, p. 960, Sep. 2019, doi: 10.3390/e21100960.
- [17] E. Fatemi-Behbahani, K. Ansari-Asl, and E. Farshidi, "A New Approach to Analysis and Design of Chaos-Based Random Number Generators Using Algorithmic Converter," *Circuits Syst. Signal Process.*, vol. 35, no. 11, pp. 3830–3846, Nov. 2016, doi: 10.1007/s00034-016-0248-0.
- [18] E. Dubrova, "How to speed-up your NLFSR-based stream cipher," in *Automation & Test in Europe Conference & Exhibition 2009 Design*, Apr. 2009, pp. 878–881. doi: 10.1109/DATE.2009.5090786.
- [19] S. A. Mehdi and A. Kadhim, "Image Encryption Algorithm Based on a New Five Dimensional Hyperchaotic System and Sudoku Matrix," *Proc. Fluids Eng. Conf.*, Jan. 2021.
- [20] L. Tawalbeh, W. Kanakri, and L. Al-Ebbini, "Efficient Random Number Generators (RNG) based on Nonlinear Feedback Shift Registers (NLFSR)," Dec. 2009.
- [21] E. Dubrova, M. Teslenko, and H. Tenhunen, "On Analysis and Synthesis of (n,k)-Non-Linear Feedback Shift Registers," presented at the

- Proceedings -Design, Automation and Test in Europe, DATE, Mar. 2008, pp. 1286–1291. doi: 10.1145/1403375.1403686.
- [22] E. Dubrova, “An equivalence preserving transformation from the Fibonacci to the Galois NLFSRs.” arXiv, Jan. 30, 2008. doi: 10.48550/arXiv.0801.4079.
- [23] R. Oommen, M. K. George, and S. Joseph, “Study and Analysis of Various LFSR Architectures,” 2018 Int. Conf. Circuits Syst. Digit. Enterp. Technol. ICCSDET, pp. 1–6, Dec. 2018, doi: 10.1109/ICCSDET.2018.8821227.
- [24] A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, “Areas of Application for Nonlinear Shift Registers in PRS Generators,” in *Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies*, A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, Eds., in Studies in Systems, Decision and Control. , Cham: Springer International Publishing, 2022, pp. 295–318. doi: 10.1007/978-3-030-79770-6_12.
- [25] “5 stream ciphers.” Accessed: May 28, 2023. [Online]. Available: <https://www.slideshare.net/harishsahu96558/5-stream-ciphers>
- [26] E. Dubrova, “A List of Maximum Period NLFSRs.” 2012. Accessed: May 28, 2023. [Online]. Available: <https://eprint.iacr.org/2012/166>
- [27] A. D. Hina, “Generation and statistical analysis of chaos-based pseudorandom sequences,” doctoral, Universiti Putra Malaysia, 2019. Accessed: May 28, 2023. [Online]. Available: <http://psasir.upm.edu.my/id/eprint/84993/>
- [28] J. S. Teh, M. Alawida, and Y. Sii, “Implementation and Practical Problems of Chaos-based Cryptography Revisited,” *J. Inf. Secur. Appl.*, vol. 50, Nov. 2019, doi: 10.1016/j.jisa.2019.102421.
- [29] S. Thamir, M. Kadhim, and A. Badr, “Novel Method to Choose a Certain Wind Turbine for Al. Hai Site in Iraq,” 2022, pp. 479–489. doi: 10.1007/978-981-19-0825-5_52.
- [30] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, “A new image encryption scheme based on coupling map lattices with mixed multi-chaos,” *Sci. Rep.*, vol. 10, no. 1, Art. no. 1, Jun. 2020, doi: 10.1038/s41598-020-66486-9.
- [31] R. Stepień and J. Walczak, “Statistical analysis of the LFSR generators in the NIST STS test suite,” *Comput. Appl. Electr. Eng.*, vol. Vol. 11, 2013, Accessed: Jan. 22, 2023. [Online]. Available: <http://yadda.icm>.

- edu.pl/baztech/element/bwmeta1.element.baztech-6b8818c1-d909-4960-8c08-647e878b1531
- [32] R. I. Abdelfatah, "Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2020, doi: 10.1109/ACCESS.2019.2958336.
 - [33] M. Sýs, Z. Riha, V. Matyas, K. Marton, and A. Suciú, "On the interpretation of results from the NIST statistical test suite," vol. 18, pp. 18–32, Jan. 2015.
 - [34] A. S. Bader, S. Hameed, and M. A. A. K., "Key Generation based on Henon map and Lorenz system," *Al-Mustansiriyah J. Sci.*, vol. 31, no. 1, pp. 41–46, Mar. 2020, doi: 10.23851/mjs.v31i1.734.
 - [35] B. O. Al-Roithy and A. Gutub, "Remodeling randomness prioritization to boost-up security of RGB image encryption," *Multimed. Tools Appl.*, vol. 80, no. 18, pp. 28521–28581, Jul. 2021, doi: 10.1007/s11042-021-11051-3.
 - [36] M. M. Al-Mhadawi and A. A. Albahrani, "Hybrid Method as Pseudo-Random Bits Generator," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, Dec. 2019, pp. 250–255. doi: 10.1109/CAS47993.2019.9075715.
 - [37] M. J. Al-Muhammed and R. Abu Zitar, "Light and Secure Encryption Technique Based on Artificially Induced Chaos and Nature-Inspired Triggering Method," *Symmetry*, vol. 14, no. 2, Art. no. 2, Feb. 2022, doi: 10.3390/sym14020218.
 - [38] M. Elgamel and M. Bayoumi, "7 - Noise Analysis and Design in Deep Submicron Technology," in *The Electrical Engineering Handbook*, W.-K. Chen, Ed., Burlington: Academic Press, 2005, pp. 299–310. doi: 10.1016/B978-012170960-0/50024-4.
 - [39] O. Jallouli, S. E. Assad, and M. Chetto, "Robust Chaos-based Stream-Cipher for Secure Public Communication Channels," presented at the International Conference on Internet Technology and Secured Transactions, Dec. 2016, p. 23. doi: 10.1109/ICITST.2016.7856658.
 - [40] C. Chen, H. Zhang, and B. Wu, "Image Encryption Based on Arnol Transform and Fractional Chaotic," *Symmetry*, vol. 14, no. 1, Art. no. 1, Jan. 2022, doi: 10.3390/sym14010174.
 - [41] L. Bao, S. Yi, and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k,n) -Secret Image Sharing," *IEEE Trans.*

- Image Process.*, vol. 26, no. 12, pp. 5618–5631, Dec. 2017, doi: 10.1109/TIP.2017.2738561.
- [42] K. Hosny, *Multimedia Security Using Chaotic Maps: Principles and Methodologies*. 2020. doi: 10.1007/978-3-030-38700-6.
- [43] F. H. Abbood, “An Efficient Confusion-Diffusion Structure for Image Encryption Using Plain Image Related Henon Map,” *Int. J. Comput.*, Jan. 2020, Accessed: May 28, 2023. [Online]. Available: https://www.academia.edu/en/69454284/An_Efficient_Confusion_Diffusion_Structure_for_Image_Encryption_Using_Plain_Image_Related_Henon_Map
- [44] X. Wang, H. Zhao, and M. Wang, “A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices,” *Opt. Laser Technol.*, vol. 115, pp. 42–57, Jul. 2019, doi: 10.1016/j.optlastec.2019.02.009.
- [45] V. Himthani, V. S. Dhaka, M. Kaur, and P. Hemrajani, “V-Net architecture based advanced visually meaningful image encryption technique,” *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 7, pp. 2183–2194, Oct. 2022, doi: 10.1080/09720529.2022.2133255.
- [46] H. Zhong, G. Li, X. Xu, and X. Song, “Image Encryption Algorithm Based on a Novel Wide-Range Discrete Hyperchaotic Map,” *Mathematics*, vol. 10, no. 15, Art. no. 15, Jan. 2022, doi: 10.3390/math10152583.
- [47] “Compression-Based Cancelable Multi-Biometric System.” Accessed: May 28, 2023. [Online]. Available: <https://www.researchsquare.com>
- [48] M. Kumari and S. Gupta, “Performance comparison between Chaos and quantum-chaos based image encryption techniques,” *Multimed. Tools Appl.*, vol. 80, no. 24, pp. 33213–33255, Oct. 2021, doi: 10.1007/s11042-021-11178-3.
- [49] A. Alghafis, N. Munir, and M. Khan, “An encryption scheme based on chaotic Rabinovich-Fabrikant system and S8 confusion component,” *Multimed. Tools Appl.*, vol. 80, no. 5, pp. 7967–7985, Feb. 2021, doi: 10.1007/s11042-020-10142-x.
- [50] N. Nesa, T. Ghosh, and I. Banerjee, “Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map,” *J. Inf. Secur. Appl.*, vol. 47, pp. 320–328, Aug. 2019, doi: 10.1016/j.jisa.2019.05.017.

- [51] X. Wang, X. Zhu, and Y. Zhang, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018, doi: 10.1109/ACCESS.2018.2805847.
- [52] D. Lambic, "Cryptanalyzing a novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dyn.*, vol. 89, pp. 1–3, Aug. 2017, doi: 10.1007/s11071-017-3583-1.
- [53] S. J. Sheela, K. V. Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 25223–25251, Oct. 2018, doi: 10.1007/s11042-018-5782-2.

Received October, 2022