scientific reports

OPEN

2D logistic map with unit transfer function and modulus operation based pseudorandom number generation for image encryption

Raiz Ahmad[1], Ghawar Said[2], Aymen Flah[3,4,5,6,7], Habib Kraiem[8], Claude Ziad El bayeh[9], Yousaf Hameed Khattak[1,10]✉ & Faisal Baig[1,10]

This study presents a novel approach to generating high-quality random numbers using a two-dimensional logistic map with a unit transfer function (2DLMUTF). The method is built upon the chaotic dynamics of the logistic map, where the parameter r governs the system's behavior, exhibiting chaotic nature in the range of 3.57 to 4. By applying a unit transfer function and modulus operation, the system's output is constrained within the [0, 1] range, altering the phase space dynamics compared to traditional 2D logistic maps. Numerical simulations in MATLAB, with parameters r_1=4, r_2=3.8, and initial seed values x_0=0.2350 and y_0=0.3500, were run for 10^6 iterations. Statistical testing using the NIST SP 800 – 22 test suite showed superior randomness, with the method passing all 15 tests. Additionally, uniformity, autocorrelation, cross-correlation, and entropy analyses confirmed the method's suitability for cryptographic applications. The generated random numbers were used to create substitution boxes (S-boxes) for image encryption, demonstrating strong encryption performance. Overall, 2DLMUTF offers a computationally efficient and secure solution for random number generation which is suitable for cryptographic and image encryption applications.

Keywords Encryption, Image cryptography, Chaotic map, Two-dimensional logistic map, Security analysis

Advancements in communication technologies and the widespread adoption of the internet have dramatically increased the exchange of multimedia data, encompassing audio, video, and digital images. This surge in multimedia content has consequently led to an escalating demand for efficient transmission bandwidth to accommodate the substantial volume of data being exchanged over the internet. As a result, multimedia communication has emerged as the preferred modality for data exchange, surpassing traditional text-based communication, owing to its intuitive and engaging nature. In contemporary society, multimedia communication applications are integral to a wide array of activities, including entertainment, social networking, teleconferencing, and online education. However, the growing reliance on multimedia data transmission has introduced significant challenges related to data processing, storage, and, most critically, the security of transmitted data. Ensuring the security of multimedia content during transmission is of paramount importance, given that such data often includes sensitive information such as trade secrets, personal details, and classified military intelligence[1].

The ubiquity of internet use for activities such as e-commerce, online shopping, banking, and email communication further magnifies the need for robust information security mechanisms. Due to the open and accessible nature of the internet, it remains susceptible to unauthorized access and malicious attacks. Cyber threats, including data breaches, eavesdropping, and unauthorized alterations, pose serious risks to the confidentiality, integrity, and authenticity of transmitted data. These challenges have prompted researchers to explore a

[1]Federal Urdu University of Arts, Science & Technology Islamabad, Islamabad, Pakistan. [2]Computer Science Department, Iqra University, Islamabad, Pakistan. [3]Processes, Energy, Environment, and Electrical Systems, National Engineering School of Gabès, University of Gabès, Gabès, Tunisia. [4]Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan. [5]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab 140401, India. [6]ENET Centre, VSB-Technical University of Ostrava, Ostrava, Czech Republic. [7]Jadara University Research Center, Jadara University, Irbid, Jordan. [8]Center for Scientific Research and Entrepreneurship, Northern Border University, 73213 Arar, Saudi Arabia. [9]College of Engineering and Technology, University of Doha for Science and Technology, Doha, Qatar. [10]School of Design Engineering, Universitat Politecnicia de Valencia, Valencia, Spain. ✉email: yousaf.hameedk@gmail.com

wide range of cryptographic techniques, including encryption, hashing, and random number generation, to safeguard data transmission[2]. Among these cryptographic techniques, random number generation (RNG) plays a fundamental role in ensuring secure key generation, encryption, and authentication processes. RNG is also widely utilized across diverse scientific and engineering fields, including stochastic simulations, game theory, and Monte Carlo simulations. RNG systems can generally be classified into two primary categories: Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs)[3–6]. PRNGs rely on deterministic mathematical algorithms to generate sequences of numbers that are statistically random, but which may be predictable if the algorithm and seed value are known. In contrast, TRNGs derive randomness from physical entropy sources, such as atmospheric or thermal noise, thereby guaranteeing greater unpredictability[7]. While TRNGs are widely regarded as more secure, their practical implementation is often limited by hardware constraints, which makes PRNGs a more viable alternative for many cryptographic applications. Common PRNG techniques include Linear Congruential Generators, the Mersenne Twister, and chaotic systems. Despite their widespread use, many PRNG methods are vulnerable to prediction attacks, which can compromise the security of the generated random sequences[8]. These vulnerabilities are often linked to the internal states of the PRNGs, which may expose patterns in the generated sequences. Consequently, researchers are exploring methods to improve the randomness and security of PRNGs, including approaches such as seed randomization, chaotic systems, and hybrid models.

In this research, we propose an innovative approach to random sequence generation based on a two-dimensional Logistic Map Unit Transfer Function (2DLMUTF). This method represents a modification of the traditional logistic map, wherein two distinct values for the parameter "r" are employed instead of the conventional single fixed value. By incorporating gene dominance principles, the selection of these values becomes dynamic at each iteration, enhancing both the security and randomness of the generated sequence. The key contributions of this research are as follows:

- Identification of a novel change in the local structure of the 2DLMUTF, which has not been previously reported in existing literature.
- Development of an enhanced 2DLMUTF model that incorporates two distinct values for the parameter "r".
- Introduction of a new method for random sequence generation, specifically designed for use in 2D cryptographic systems.
- Utilization of the generated sequence in an S-box within a 2D cryptographic system for enhanced encryption.
- As there are strong method to create strong S-box that has no-fixed points, reverse points and short period rings [Add references[9–11] but in this work our major focus is generation of highly random chaotic sequence which can be used for generation of S-box, so we only focused on nonlinearity, SAC, BIC, DP, and LP for analysis.
- Verification of the method through an image encryption case study, where the S-box derived from the proposed sequence was used to securely encrypt an image.

Literature review

The generation of secure, high-quality random numbers has long been a fundamental concern in cryptography. Pseudo-Random Number Generators (PRNGs) are crucial components of various cryptographic functions, including key generation, hashing, and challenge-response authentication. Their importance stems from their computational efficiency, which makes them ideal for use in systems requiring high-performance cryptography. Among the most widely used PRNGs are those based on Linear Feedback Shift Registers (LFSR), Linear Congruential Generators (LCG), and the Mersenne Twister algorithm[3,4]. LFSR-based PRNGs are popular due to their simplicity and efficiency. Their low resource requirements make them faster, cheaper, and easier to implement. However, despite these advantages, LFSR-based systems are highly susceptible to cryptanalysis. Their deterministic behavior makes them less secure in high-stakes cryptographic environments, where unpredictability is paramount[3,5].

The NIST SP800-22 test suite has become an industry standard for evaluating the statistical properties of pseudo-random number sequences generated by PRNGs. Many recent PRNG innovations have successfully passed the necessary tests, confirming their adequacy for cryptographic applications[5,7]. However, a central challenge in PRNG design is obscuring the sequentially generated numbers in such a way that they cannot be predicted. Various techniques, such as entropy initialization and reseeding, have been proposed to enhance the unpredictability of PRNGs[8,12]. In response to the limitations of traditional PRNGs, researchers have turned to chaotic systems, which offer a higher degree of randomness. Chaotic systems are known for their sensitivity to initial conditions, making them inherently unpredictable. Several chaotic systems have been studied for their potential use in cryptographic applications, including the Logistic map[18], Lorentz system[19–22], skew tent map[23,24], and Henon map[29]. Of these, the Logistic map has garnered significant attention due to its simplicity and ease of implementation[31]. Despite its popularity, the standard Logistic map has some inherent flaws, such as short periodicity and predictability, which necessitate modifications to enhance its security.

To address these limitations, a number of modifications have been proposed. Li et al.[36] introduced a reseeding technique to extend the periodicity of the Logistic map by introducing small perturbations. Murillo-Escobar et al.[37] enhanced the randomness of the Logistic map by incorporating multiplication and modulo operations. Liu et al.[38] developed a time-varying Logistic map that dynamically alters the system's parameter 'r', making it more resistant to phase space reconstruction attacks. These innovations have significantly improved the security and applicability of chaotic maps in PRNGs. Recent research continues to explore the use of chaotic systems for PRNG design, with various chaotic maps being investigated for their potential to improve randomness and security. Chaotic maps, such as the Logistic map, Lorentz system, skew tent map, sawtooth map, quantum chaotic map, and Henon map, are among the most studied due to their highly unpredictable behavior and sensitivity to initial conditions[19–31]. The Logistic map, in particular, has been extensively researched due to its one-dimensional nature, which makes it easier to implement in practical systems. Several improvements have been proposed to address the inherent limitations of the traditional Logistic map. Li et al.[36] enhanced the periodicity of the Logistic map with reseeding techniques, while Murillo-Escobar et al.[37] improved its randomness using multiplication and modulo operations. Liu et al.[38] proposed a non-stationary, time-varying Logistic map that mitigates vulnerabilities to phase space reconstruction attacks. These advancements have made chaotic maps a more viable option for secure PRNGs. Non-degenerate chaotic mappings are mathematical models that exhibit complex, unpredictable behavior while maintaining a well-defined structure. Unlike degenerate mappings, they do not simplify into fixed points or periodic cycles, making them ideal for modeling systems with sensitive dependence on initial conditions. These mappings are increasingly used in fields like cryptography and nonlinear dynamics, and they hold potential for applications in energy systems[39,40].

Building on these previous advancements, we introduce a two-dimensional extension of the Logistic map that dynamically selects “r” values based on gene dominance principles. This novel approach increases the complexity and unpredictability of the random sequences generated, making them more suitable for cryptographic applications. In the following sections, we provide a detailed explanation of the proposed methodology, its implementation, and its security analysis.

Proposed methodology

The larger information proportion precisely the transmission bandwidth expansion and multimedia data comprising of audios, videos and digital images exchanged on internet with the rapid communication technologies and internet development. Now a days mostly people choose to share or communicate information or data with others by means of multimedia information rather than the classical means of communication due to its intuition and vividness. In routine daily life, the usage of broad multimedia communication applications creates terrific convenience. Meanwhile data storing, processing, and transmitting of information are the raised series of problems. One of them is the data security during the information transmission on a common medium or channels because the multimedia data contains the trade secret, personal privacy and even in military[1]. In current scenario the Information security has become an important issue due to the use of internet in daily routine like in e-commerce, e-shopping, e-mailing and online banking. The circulation of information can be interrupted by the other users because of the fact that an internet is an open channel[2]. To resolve these types of problems due to information loss, random number sequences are used. The random bits or numbers sequence plays a significant role is numerous scientific fields like stochastic simulations, cryptography, gaming theory and also in Monte Carlo Simulations. Pseudo Random Number Generators (PRNGs) and True Random Number Generators are the two primary categories into which RNGs research is typically categorized in the literature[3–6] (TRNGs). The PRNGs typically use algebraic or mathematical formulas to generate deterministic, periodic sequences of numbers. This long and well-known sequence pattern is typical. The initial state, sometimes referred to as seed, entirely determines the generated sequence[5]. Furthermore, perfect knowledge of the generator mechanism and a few recently generated numbers can be used to determine or predict the next generated number. As a result, PRNGs are sometimes referred to as deterministic random number generators[3,4]. PRNGs can be easily constructed from a Linear Feedback Shift Register (LFSR) by carefully selecting the XOR tap[3]. In general, PRNGs solutions are usually fast, simple, cheap, and hardware independent[4]. The statistical tests mentioned in NIST (National Institute of Standards and Technology) test suits 800 – 22 used to determine the quality of random numbers for cryptographic applications are mostly passed by recent PRNGs solutions[5,7]. According to the NIST test guide document, if a sequence is properly constructed, a few PRNG solutions can exhibit excellent statistical properties. Random numbers with a higher degree of disorder are useful in the generation of keys for symmetric cryptography, hashing initialization vector and salt, and challenge-response nonce. Random number generators must have the following characteristics:

- The key space has a uniform distribution of all possible numbers. The calculated key space of proposed method is 197 bits.
- The current number generated is independent of the previously generated sequence.

A source of entropy is required to generate a random number sequence. Entropy must be truly random, as in atmospheric noise, thermal noise, and so on[8,12]. True random number generator implementations are impractical for many applications. This resulted in the widespread use of deterministic algorithms to generate random-like (pseudo) number sequences with the aforementioned properties[13,14]. These deterministic algorithms’ implementations are efficient and platform agnostic. The question of selecting good quality seeds was then posed to researchers, and various techniques were proposed to effectively garner the seeds for good results[15–17].

Researchers began to concentrate on software-based random number generation. Many concepts were proposed using mathematical systems such as de Burjin sequences, Linear Congruential Generators, Mersenne Twister, and so on. These systems are vulnerable to being more predictable even when only one element of the sequence is exposed. Later developments aimed at harnessing the random behavior of chaotic systems. Dynamic systems that exhibit chaotic behavior and are reactive to minor changes in initial parameters are a good candidate for Pseudo Random Number Generators (PRNG). Researchers from all over the world devised methods for using various chaotic systems, such as the Logistic map[18], Lorentz chaotic system[19–22], skew tent map[23,24], saw tooth map[25], quantum chaotic map[26–28], Henon map[29], and zigzag map[30], to generate random numbers and encrypt digital images.

Because of their simple formulation defined in one-dimension, logistic maps were the most common of all chaotic maps in use[31]. Later on, a variety of solutions were proposed to overcome the disadvantages of the Logistic map, which are cryptanalyzed in[32–35]. Li et al. proposed a reseeding technique using the Logistic map to extend the generator's periodicity in[36]. The reseeding technique employs small perturbations on a regular basis to eliminate the low period and improve randomness. They also improved the period selection to reseed the generator, and their hardware implementation demonstrated a throughput of 250 Mbit/s. Murillo-Escobar et al.[37] enhanced the performance of the Logistic map by incorporating a multiplication and modulo 1 operation. The modified logistic map's histograms and Lyapunov exponents (LE) outperform the conventional logistic map. Their results improved significantly in terms of statistical tests and security analysis. Liu et al.[38] created a non-stationary time-varying Logistic map by continuously varying the chaotic system's parameter 'r'. This non-stationary logistic map is resistant to phase space reconstruction attacks. The value of 'r' is chosen at random from the range [3.5699, 4]. Recently constructed hyper chaotic maps suffer from ergodicity in phase space because of weak LE and poor randomness and there is direct correlation in LE and randomness of chaotic maps[39]. A positive LE can help us leverage better randomness as proposed in this work.

In this paper to use a one-dimensional logistics chaotic map to generate a new two-dimensional sequence using the unit transfer function given in Eqs. 5 and 6. The two-dimensional (2D) Logistic Map has long been used to generate random numbers. A 2D Logistic map is a two-dimensional extension of a traditional Logistic map that adds another dimension to make the system more complex. The parameter 'r' in a 2D logistic map determines the chaotic system's behavior. Instead of a single 'r' value, this paper proposes two 'r' values, with the 'r' value to be used determined by gene dominance at each iteration.

Two-dimensional logistic map based on unit transfer function (2DLMUTF)

Equation 1 represent a logistic chaotic map with parameter 'r' determine the nature of system. When value of 'r' is in range of 3.57 to 4 logistic map exhibits chaotic nature.

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

$$y_{n+1} = ry_n(1 - y_n) \tag{2}$$

Similarly, Equation for two-dimensional logistic map is given as[41]

$$x_{n+1} = r\,(3y_n + 1)\,x_n\,(1 - x_n) \tag{3}$$

$$y_{n+1} = r(3x_{n+1} + 1)y_n(1 - y_n) \tag{4}$$

Now to derive two-dimensional logistic chaotic map with unit transfer function what we have done is divide Eqs. 1 and 2 with each other and apply modulus to the Equation with unit one. The new form of these Equation is shown in Eqs. 5 and 6.

$$x_{n+1} = mod\left(\frac{r_1 + x_n(1 - x_n)}{y_n(1 - y_n)}\,,\,1\right) \tag{5}$$

$$y_{n+1} = mod\,\left(\frac{r_{2+}y_n(1 - y_n)}{x_n(1 - x_{n+1})}\,,\,1\right) \tag{6}$$

in our case $r_2 = r_1 - 0.2$

The new form is called the unit transfer function (UTF), as defined in Eqs. 5 and 6, UTF introduces a non-linear transformation to the 2D logistic map through modulus operation. This modulus operation, applied with unit one, constrains the output of the map within the range of [0, 1], which alters the phase space dynamics compared to the standard 2D logistic map. From Lyapunov exponent analysis it was found that with the variation in values for control parameters, the system exhibits different behaviors as shown in Fig. 1.

1. $r\ (-0.04,\ 0.03)$, (0.18,0.23), system was unstable
2. $r\,(-2.7, -4)$ (2.7,4) , system exhibits chaotic behavior.

Two-dimensional logistic maps with unit transfer function were implemented in MATLAB 2018a with initial seed value ($x_0,\ y_0$) taken as 0.2350 and 0.3500 with $r_1 = 4$ and $r_2 = 3.8$. Then sequence was run for a given number of iterations 10^6. The point plot between $(x_{n+1},\ y_{n+1})$generated sequence from Eqs. 3–6 is shown in Fig. 2 below. Figure 2a shows the generated sequence from Eqs. 3 and 4, whereas results drawn in Fig. 2b show the results for 2DLMUTF and results in Fig. 2b clearly show that sequence generated with Eqs. 5 and 6 is well distributed across entire plane.

The generated sequence was converted into a binary sequence by using simple median formula as given in Eq. 7 below.

$$Bin_X = \left\{ \begin{array}{c} 1\,if\;x \geq \;mean\;\,(x) \\ 0\,otherwise \end{array} \right. \tag{7}$$

Experimental analysis

Statistical testing of proposed random number generator

The generated random bit sequence was tested using NIST SP 800 – 22 test suite. 100 sequences were generated with slight variation in initial conditions with length of each sequence greater than or equal to 10^6 bits. NIST SP 800 – 22 test suite consists of 15 statistical tests that were run on these sequences and each test return a 'p' value

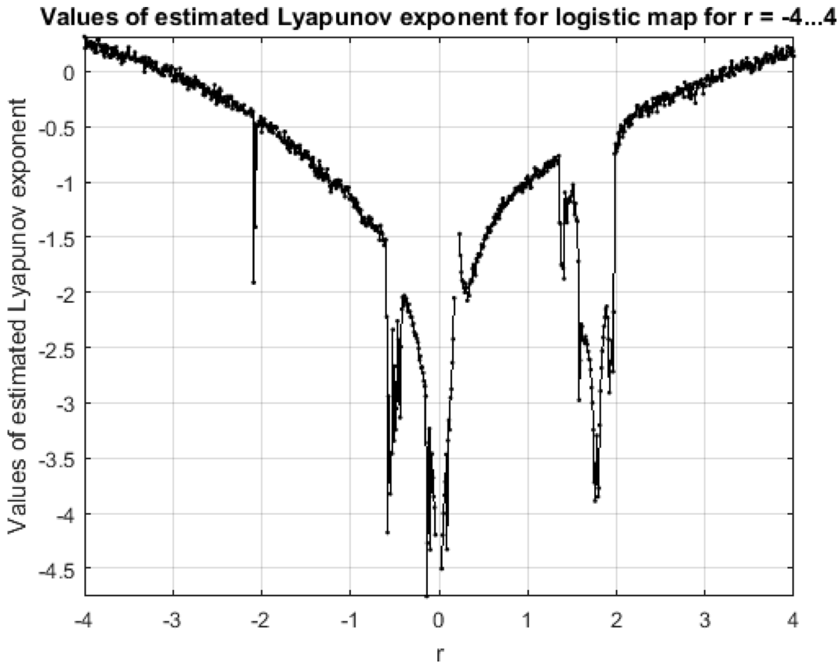

Fig. 1. Lyapunov exponent for two-dimensional logistic map with unit transfer function.

that is ranging from 0.01 to 1. A higher number close to unity means that sequence is perfectly random. The sequence will pass the test if returned p-value is greater than 0.01. Table 1 compares the proportion of passing sequences (out of 1000) to the test results of various Logistic Map implementations. According to Table 1, some of the maps have very low P-values for frequency, block-frequency, runs, longest runs, FFT, universal, approximate entropy, random excursions, serial test, and linear complexity. The proposed 2DLMUTF has a higher P-Value in these tests than other existing maps and passes all 15 statistical tests.

Security analysis

Uniformity

Uniformity test used to find the number of ones and zeros in generated bit sequence from 2DLMUTF with unit transfer function. The generated bit sequence must possess balance because uneven distribution of bit sequence will lead to non-uniform sequence. Uniformity for the generated sequence was calculated with the formula given in Eq. 8. In Equation below S_0 are the number of '0', S_1 are the number of '1' in the sequence and N is the total length of sequence.

$$\epsilon = \frac{|S_0 - S_1|}{N} \tag{8}$$

Figure 3 shows the results for a bit uniformity test under different length of sequence. Ideally this should be zero to achieve equilibrium. The drawn results show that when the length of sequence is increased good equilibrium is achieved for generated test sequence. whereas results in Fig. 4 show the distribution of '0' and '1' of sequence size 100 and length 16.

Autocorrelation

To find out the similarity between two same generated sequences auto correlation function was used. Autocorrelation was measured between the original and shifted version of generated sequence. Formula for auto correlation is written in Eq. 9 below.

$$AC = \frac{|A - D|}{N} \tag{9}$$

'AC' Auto correlation function. 'A' is the number of similar bits between original and shifter version of sequence. 'D' difference between bits for original and shifter version of sequence. 'N' length of sequence.

Figure 5 shows the result for auto correlation for generated sequence logistic unit transfer function with bits shifted by 0 to 250-bit positions on both sides and results clearly depict a good pseudo random number.

Cross correlation

It is a degree to measure the change in output sequence of a PRNG with respect to its initial condition. When cross correlation is equal to '0' its means generated sequence are completely unrelated. Unrelated sequences with respect to change in initial condition of logistic unit transfer function will help the PRNG to with stand against

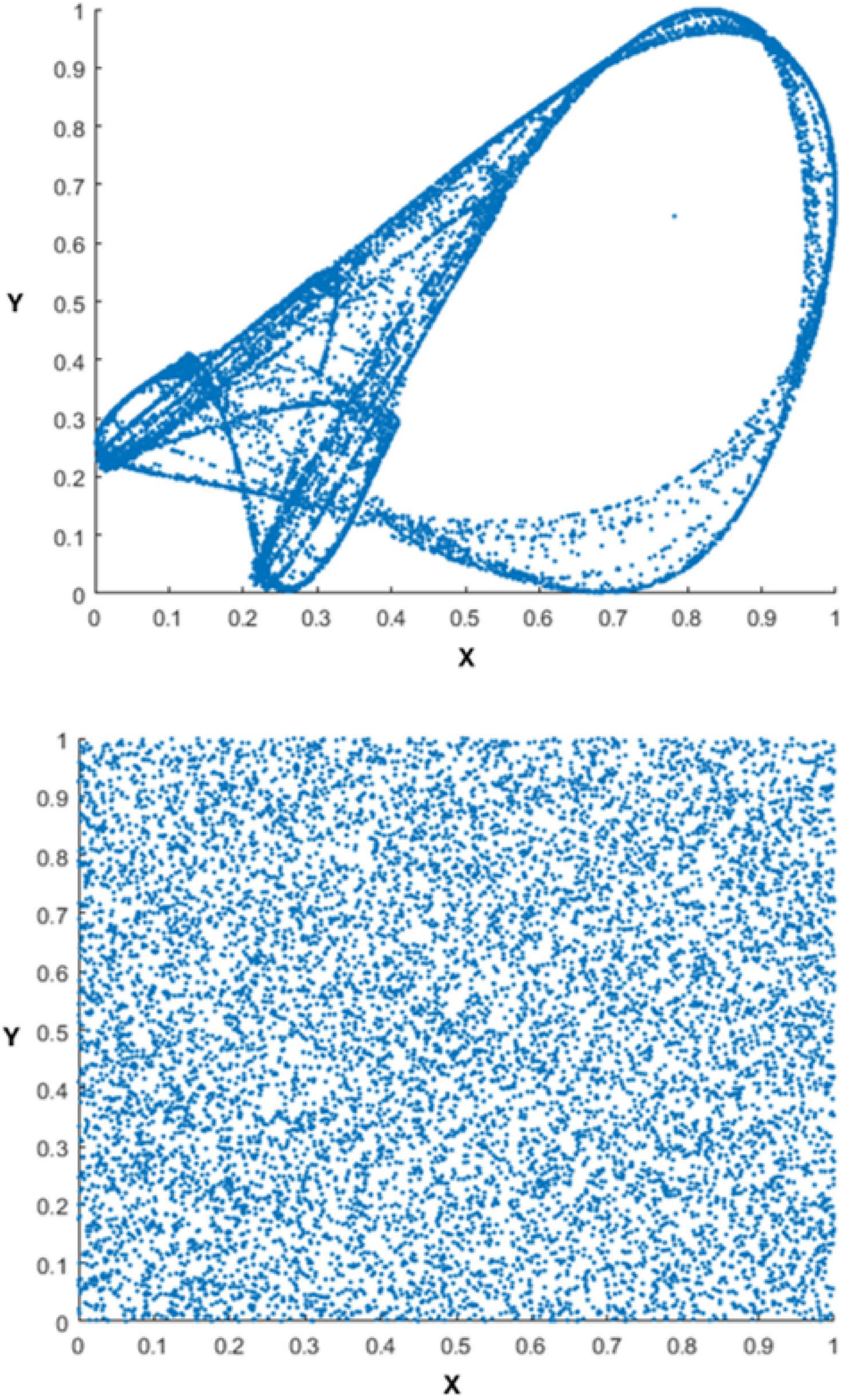

Fig. 2. Two-dimensional logistic map. Two-dimensional logistic map with unit transfer function.

differential attack. The following are the initial conditions that were used to check the cross correlation of the generated sequence.

Sequences Y_1, $Y2_2$, $Y2_3$ are generated by slightly varying the X_0 and Y_0 as

$$Y_1 : X_0 = 0.1678322;\ Y_0 = 0.218460$$

	Logistic map with additional input[43] *P*-value	Non-stationary logistic map[38] *P*-value	Digitalized modified logistic map[44] *P*-value	PRNG from chaotic logistic map[34] *P*-value	PRNG from mutual coupled 2D logistic map[45] *P*-value	Proposed 2DLMGD *P*-value[42]	Proposed technique
Frequency	0.5171	0.6298	0.0061	0.6355	0.4216	0.3461	0.9869
Block frequency	0.1586	0.5621	0.3371	0.4568	0.3324	0.6497	0.6884
Cumulative sums(forward)	0.2147	0.7939	0.4626	0.2655	0.2149	0.2648	0.383331
Cumulative sums(reverse)	0.5351	–	–	0.5585	–	0.6587	0.3723
Runs	0.2753	0.2113	0.1283	0.9673	0.2487	0.8431	0.535966
Longest-runs	0.6699	0.8906	0.8881	0.0123	0.2567	0.8712	0.622422
Rank	0.1546	0.3274	0.4685	0.5749	0.193	0.1045	0.574491
FFT	0.7967	0.6073	0.1626	0.0001	0.41	0.8421	0.156734
Overlapping templates*	0.2757	0.4848	0.8043	0.3795	0.3177	0.4679	0.546487
Non-periodic templates	0.2262	–	0.4970	0.3521	–	0.1246	0.70946
Universal	0.0849	0.8795	0.3241	0.4038	0.4102	0.1002	0.691846
Approximate entropy	0.0147	0.5549	0.4846	0.906	0.3497	0.0846	0.614823
Random-excursions *	0.7653	0.9742	0.1473	0.0158	0.3014	0.8318	0.5412
Random-excursions variant *	0.2686	0.5033	0.0013	0.5707	0.2987	0.3479	0.3780
Serial 1	0.3613	0.9005	0.2881	0.9329	0.2419	0.4399	0.885531
Serial 2	0.0365	–	–	–	–	0.1484	0.978562
Linear complexity	0.1478	0.6337	0.0083	0.1252	0.5167	0.3464	0.76795

Table 1. NIST SP 800 – 22 statistical test results.

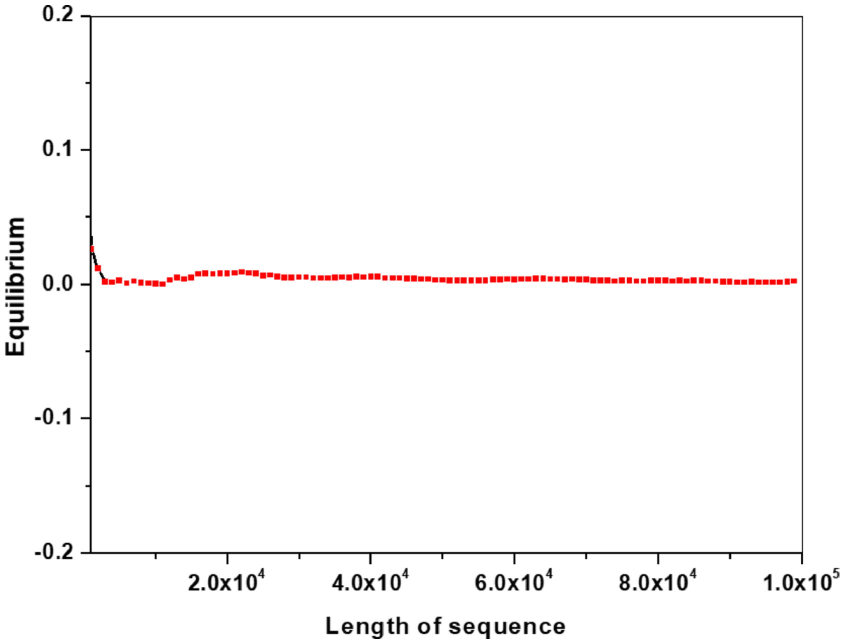

Fig. 3. Bit uniformity results.

$$Y_2 : X_0 = 0.0.1674804; Y_0 = 0.218460$$

$$Y_3 : X_0 = 0.167832; Y_0 = 0.0.2182617$$

The degree of cross correlation was measured using the same formula given in Eq. 9. but here it was measured first between sequence Y1, Y2 and then Y2, Y3. Results for cross correlation are shown in Fig. 6 below and these are well aligned with literature.

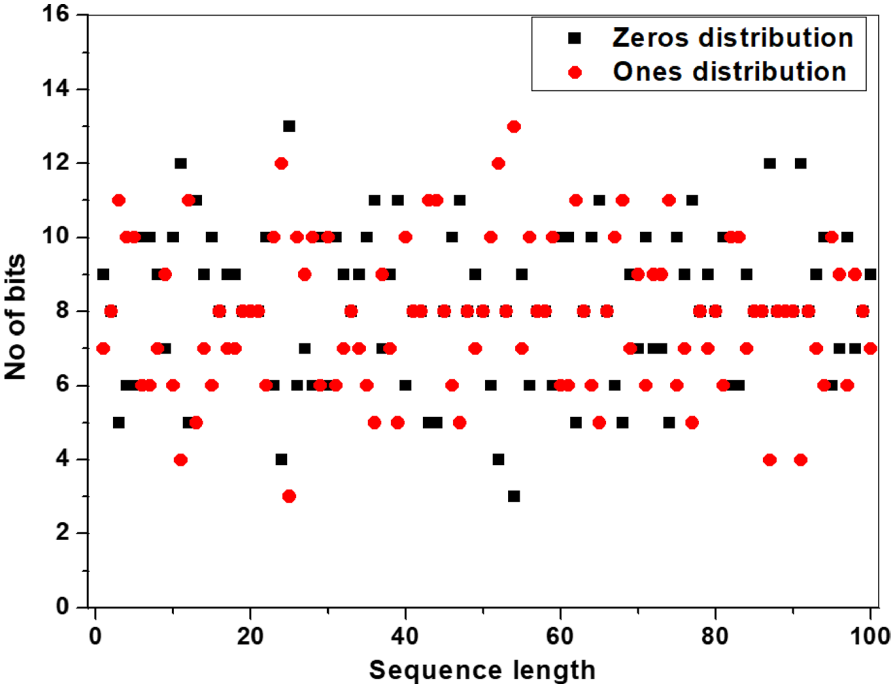

Fig. 4. Distribution of '0' and '1'.

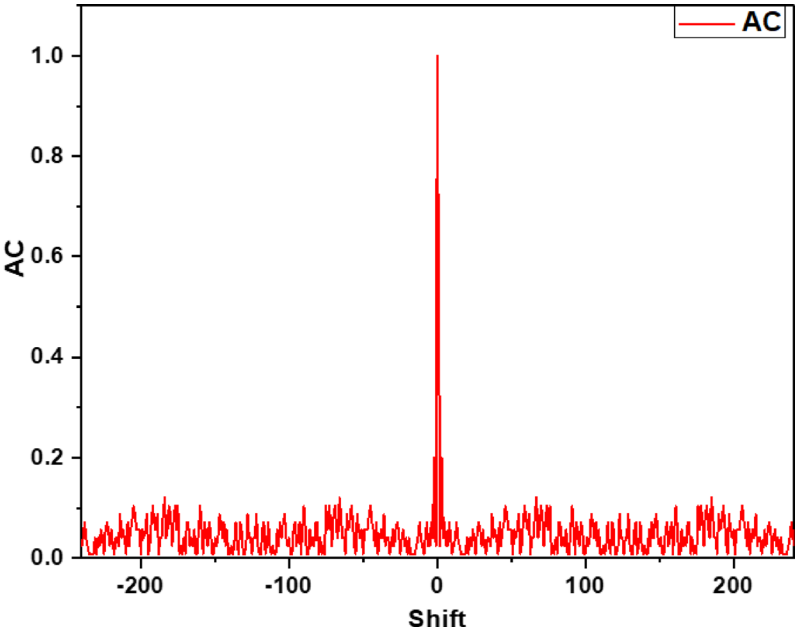

Fig. 5. Autocorrelation for 2DLMUTF sequence.

Entropy analysis

Entropy is the measure of disorder or unpredictability of a random number. A PRNG having a sequence 'S' with length of 'L' with 'n' number of bits has a key space of 2^n. So, entropy of a PRNG with size of each sequence 'n ' is given in Eq. 10.

$$H\left(S\right)=\sum_{i=0}^{2^n-1}p\left(s_i\right)\log_2 p\left(s_i\right) \tag{10}$$

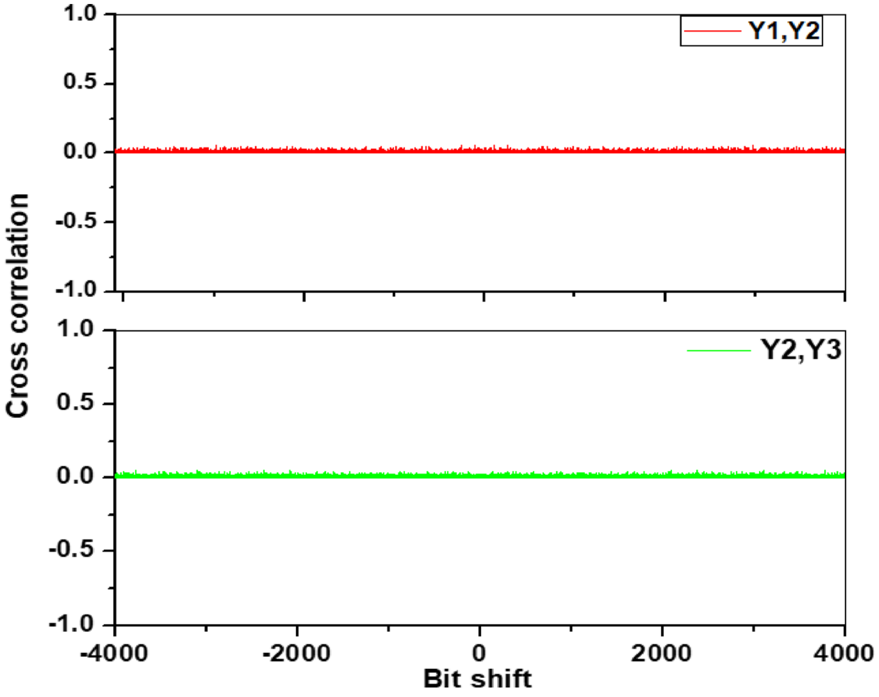

Fig. 6. Cross correlation results for 2DLMUTF.

First generate sequence Y1 with initial condition given above
Size = L*n;
y1 = y1(1: size) > = mean (y1(1: size)); % Eq. 7
y3 = reshape (y1, L, n);
y4 = Entropy(y3);

Table 2. Algorithm for measuring entropy of sequence.

Sequence length (L)	8-bit sequence (n)	16- bit sequence (n)
1000	7.9971	15.9900
2000	7.9993	15.9973
3000	7.9989	15.9966
4000	7.9984	15.9972
5000	7.9987	15.9976
6000	7.9978	15.9968

Table 3. Entropy of a PRNG with 8- and 16-bit sequence.

Entropy was measured by first generating the binary sequence with size equal to ‘$L \times n$’. After that sequence was reshaped into desired bit sequence ordered and entropy was measured. Algorithm for measuring entropy is shown in Table 2.

Results of entropy are drawn in Table 3, and from Table 3 it is found that entropy is close to ‘n’ for all iterations.

Histogram

Histogram is the graphical representation of probability of a PRNG that generates numbers in key space. And classically histogram of a good PRNG will show uniformity in entire key space. Figure 7 shows the results for histogram of a 16-bit key and hence the key space is from 0 to 65,535(2^0 to 2^{16}-1). The Histogram in Fig. 7 shows the almost equal distribution of generated random numbers.

Image cryptography

The random numbers generated were further used to create substitution boxes (S-box) for image cryptography as shown in Table 4. S-Box is generated using the chaotic values from the (**2DLMUTF**) as follows.

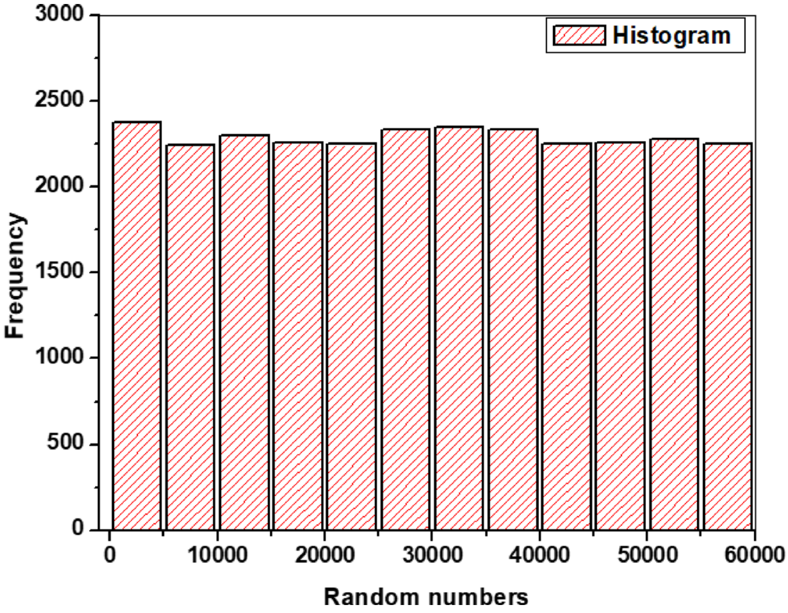

Fig. 7. Histogram of random number with 16-bit length for 2DLMUTF.

Labels	0 × 00	0 × 01	0 × 02	0 × 03	0 × 04	0 × 05	0 × 06	0 × 07	0 × 08	0 × 09	0 × 0 A	0 × 0B	0 × 0 C	0 × 0D	0 × 0E	0 × 0 F
0 × 00	68	12	22	51	3	7D	4 A	A7	95	28	36	78	6 F	A5	AB	31
0 × 01	1B	F3	46	10	F2	7 C	FA	F0	93	84	63	7	FD	3 A	CB	94
0 × 02	A	16	A2	5E	DE	CD	32	82	2 A	81	7B	8B	B5	D0	AE	2E
0 × 03	C4	53	70	6D	D1	E5	E1	5 A	B2	A0	C8	E2	76	26	B4	45
0 × 04	F	A9	9	D5	B6	18	C5	92	BC	CA	E0	47	5D	64	F9	6
0 × 05	E9	EE	A8	6 C	2 F	D7	50	59	E3	CF	D	D9	A1	B8	D3	D2
0 × 06	7 F	6B	DD	3 C	4 C	DC	E7	79	3D	B9	2 C	EA	C6	BA	B7	D4
0 × 07	30	90	37	2	44	C2	9 A	33	75	6E	14	55	9B	40	98	9D
0 × 08	73	D6	4 F	CC	1	CE	AC	1D	65	52	C3	97	4E	8	FF	88
0 × 09	1E	B	1 C	23	C9	6 A	42	9 C	F6	69	AD	60	9 F	54	8D	41
0 × 0 A	E6	5 F	A3	D8	85	29	A4	71	77	35	B1	3B	32	61	8E	1 F
0 × 0B	EF	E4	5 C	58	43	67	91	27	62	25	86	FE	FC	83	AA	FB
0 × 0 C	E8	49	0	E	4B	4D	8 A	48	F8	B3	9E	C7	F1	13	1 A	38
0 × 0D	3E	C0	AF	2D	3 F	DB	BB	7 A	11	F7	7E	72	DA	8 F	5	BD
0 × 0E	DF	BF	F5	80	8 C	15	19	ED	C1	4	74	39	17	21	34	96
0 × 0 F	99	89	56	EC	87	EB	5B	A6	66	F4	B0	24	BE	2B	57	C

Table 4. S-box from two-dimensional logistic map with unit transfer function.

- The first PRNG sequence was generated from modulus operation.
- Then this sequence was converted into binary numbers by simply applying a threshold to the sequences. Example is let's suppose we get a value of 0.80 for the sequence and as this if greater than the values of 0.5 we convert this in Boolean expression 1.
- Next step is to covert this Boolean array is converted into 8-bit decimal numbers.
- Unique 256 numbers were selected from the sequence. There is a detailed literature available about how to generate a strong S-box[46–48] but as our main focus is to develop S-box for low computing devices with small number of computation so we simply rely of sequence generation.

With every iteration of PRNG's unique 256 numbers were selected and then subjected to different tests. The effect on non-linearity and other paraments like BIC, SAC, LP, and DP on newly developed S-box is given in Table 5.

In the next step after S-box we apply cyclic substitution to the image by replacing images with the S-box values. The method was adopted from our previous work[49]. The results for image encryption were evaluated on our random grayscale images, with an image size of 256×256. The result for image encryption of our random is shown in Fig. 8. From Fig. 8, it is clearly visible that the proposed algorithm shows a flat histogram

Analysis	Min value	Max value	Average	Differential approximation probability	Linear approximation probability
Non-linearity	104.0	110.0	106	–	–
SAC	0.4063	0.6250	0.5012	–	–
BIC	100.000	–	104.286	–	–
DP	–	–	–	0.0468	–
LP	–	–	–	–	0.125

Table 5. S-box analysis results.

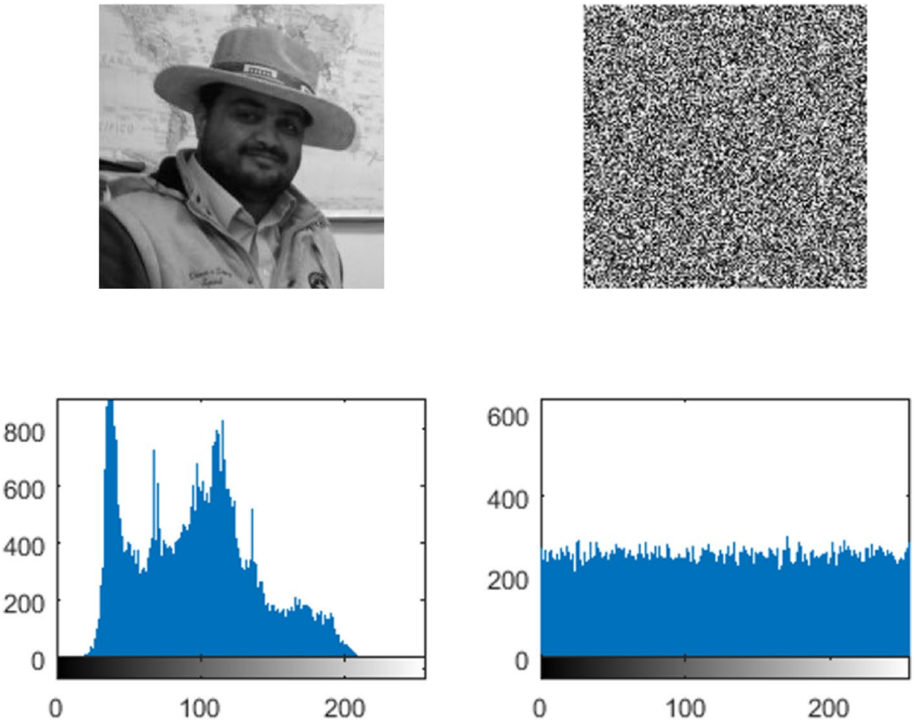

Fig. 8. Histogram analysis of proposed algorithm for our image.

for encrypted image. The visual demonstration of the flat histogram shows the strength of the proposed random numbers generated s-box encryption scheme for image dataset. The result of the proposed algorithm was further extended by applying known image encryption statistical method as described below.

Statistical analysis

Statistical analysis consists of number of parameters which are used to study the strenght of enctyption algorithm. These parameters are correlation, contrast, homogeneity, energy and entropy. They help in evaluating an encypted and plain image quantitative quality vice. These standard tests are well described in literature and are given as

$$\left.\begin{array}{r} Correlation = \sum{}_{i,j} \frac{(i-\mu\ i)(j-\mu\ j)p(i,j)}{\sigma\ _i \sigma\ _j} \\ Contrast = \sum{}_{i,j} |i-j|^2\, p\,(i,j) \\ Homogeneity = \sum{}_{i,j} \frac{p(i,j)}{1+|i-j|} \\ Energy = \sum{}_{i,j} p\,(i,\ j)^2 \\ Entropy = -\sum{}_{i,j} p(x_{i,j}),\ \log_2 P(x_{i,j}) \end{array}\right] \tag{11}$$

Where (i, j) are the indexed values of image pixels, μ is variance, σ is standard deviation, $P\,(x_i, j)$ probability of image pixel, $\mathrm{p}\,(\mathrm{i,j})$ values of image pixel at ith row and jth colomn. The image similarity is qunatified on the basis of correlation index ranging from [− 1, 1] and the positive value 1 shows the perfect correlation between two images. Contrast is a measure of images texture to identify an object in an image and the contrast of a constant image is 0 where as bigger value of contrast shows a disparity in pixels of an image. Homogenity and energy of an image is quantified with a value range of [0, 1] and a value nearer to '0' indicates a good encryption strength. Similarlly, entropy of an image is the degree of randomness of an image after encryption with decimal range of

Analysis	Images	Correlation	Entropy	Homogeneity	Contrast	Energy
AES [16-from other paper]	Baboon	0.0112	7.9973	0.2315	7.8651	0.0101
16	Baboon	0.0336	7.8815	0.3452	6.8815	0.0128
2D logistic chaotic map[59]	Baboon	– 0.0300	7.997	–	–	–
S-Box using 3D chaotic map[60]	Lena	–	7.9891	–	–	–
Proposed	Baboon	– 0.001	7.997	0.338	10.553	0.003
Proposed	Lena	– 0.006	7.985	0.340	10.490	0.003

Table 6. Statistical results for proposed algorithm for Gray image [256 × 256] with comparison to others

	NPCR (%)				UACI (%)			
Image	Proposed	[50]	AES[50]	[59]	Proposed	[50]	AES[50]	[59]
Our	99.6300	99.1369	99.6094	99.5510	33.29	33.15	33.39	32.8111
Baboon	99.6891	99.2589	99.6124	99.5450	33.36	33.45	33.44	33.8000

Table 7. Result comparison of NPCR and UACI.

[0,8], a value of 8 shows complete randomness of an image. So, grounded on statistical results for images of the proposed algorithm that are givnen in Table 6 shows a clear indication for the strength of proposed scheme.

Security analysis with UACI and NPCR analysis

Security/strength analysis of images encryption algorithm against differential attacks is described on the basis of two standard metrics which are well set in reserch community and these are Number of pixel change rate (NPCR) and Unified average change intensity (UACI). Mathematically these are defined as given in Eqs. 9 and 10.

$$NPCR = \frac{\sum_{i} D(i,j)}{N \times M} \times 100\% \tag{12}$$

$$UACI = \frac{1}{N \times M}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{13}$$

Desired minimum value for NPCR should be greater than 50% whereas for UACI should be around 33% to demonstrate strong avalanche effect. Results for NPCR and UACI is given in Table 7 below with comparison to well know AES encryption and with Lorenz systems S-box.

Conclusion

First, the 2D Logistic Map was presented and its characteristics were investigated for varying values of the determining parameter 'r'. The scatter plot continued to follow a predictable pattern. On the basis of control parameter r and unit transformation applied to equation, a novel two-dimensional logistics unit transfer function (2DLMUTF) based random numbers were obtained. The proposed generator was written in MATLAB 2018b and generates 16-bit random numbers. The NIST 800 – 22 Statistical Test Suite is used to statistically test the random sequences. The results of the tests show that the proposed 2DLMUTF has higher randomness in comparison to other known logistic map in literature. The security analysis of generated sequences also demonstrates that the proposed 2DLMUTF has high key sensitivity, higher equilibrium, optimal linear complexity, and even distribution of random sequences. The unit transformation Algorithm's simple conditional statements make it computationally cheap to combine with any cryptographic algorithm. The proposed novel 2DLMUTF algorithm can be fine-tuned to the application's needs. The primary benefit of the proposed algorithms is that the sequence 'Y' is completely hidden inside the generator and is not exposed as part of the output. As output, only the sequence 'X' is used. This feature ensures the 2DLMGD's forward secrecy, as knowing the current sequence makes computing the past sequences computationally impossible. The same random sequence was applied to image encryption, and it was found that results for image encryption are well aligned with the literature.

Data availability

All data generated or analyzed during this study are included in this published article.

Received: 20 March 2025; Accepted: 28 May 2025
Published online: 02 June 2025

References

1. Coddington, P. D. Analysis of random number generators using Monte Carlo simulation. *Int. J. Mod. Phys. C.* **5**, 547–560 (1994).
2. Karandikar, R. L. On the markov chain monte carlo (MCMC) method. *Sadhana-Acad. Proc. Eng. Sci.* **31**, 81–104 (2006).

3. Lan, J., Goh, W. L., Kong, Z. H. & Yeo, K. S. A random number generator for low power cryptographic application. In *International SoC Design Conference*, pp. 328–331 (2010).
4. Seung-Il, K. et al. Cryptographic transistor for true random number generator with low power consumption. *Sci. Adv.* **10** (2024).
5. Shamir, A. On the generation of cryptographically strong pseudorandom sequences. *ACM Trans. Comput. Syst.* **1**, 38–44 (1983).
6. Zeng, K., Yang, C-H., Wei, D-Y. & Rao T 1991 pseudorandom bit generators in stream-cipher cryptography. *Computer* **24**: 8–17
7. Chernyaeva, A., Shirobokov, I. & Davydov, A. Game channels: State channels for the gambling industry with built-in PRNG. *J. Cryptol.* **362**. (2019).
8. Lydia, N. & Georgios, P. S. Blockchain state channels: A state of the Art. *IEEE* **9**, 160277–160298 (2021).
9. Hongjun, L., Abdurahman, K. & Chengbo, X. Cryptanalysis and constructing S-Box based on chaotic map and Backtracking. *Appl. Math. Comp.* **376**, 125153 (2020).
10. Yuanyuan, S., Hongjun, L. & Yuehui, C. Constructing keyed strong S-Box using an enhanced quadratic map. *Int. J. Bifur. Ch.* **31**, 2150146 (2021).
11. Ruoran, L., Hongjun, L. & Mengdi, Z. Cryptanalysis and construction of keyed strong S-Box based on random affine transformation matrix and 2D hyper chaotic map. *Exp. Syst. Appl.* **52**, 124238 (2024).
12. Brederlow, R., Prakash, R., Paulus, C. & Thewes, R. A low-power true random number generator using random telegraph noise of single oxide-traps. In *IEEE International Solid State Circuits Conference-Digest of Technical Papers*, pp 1666–1675 (2006).
13. Epstein, M., Hars, L., Krasinski, R. & Rosner, M. & Zheng, H. Design and implementation of a true random number generator based on digital circuit artifacts. In *International* (2003).
14. Workshop on. Cryptographic Hardware and Embedded Systems, pp. 152–165.
15. Huang, C-Y., Shen, W. C., Tseng, Y-H., King, Y-C. & Lin, C-J. A contact-resistive random-access-memory-based true random number generator. *IEEE Trans. Electron. Devices*. **33**, 1108–1110 (2012).
16. Bo, P., Qiqiao, W., Zhongqiang, W. & Jianguo, Y. *A RRAM-Based True Random Number Generator with 2T1R Architecture for Hardware Security Applications*141213 (Micromachines, 2023).
17. Eichenauer, J. & Lehn, J. A non-linear congruential pseudo random number generator. *Stat. Pap.* **27**, 315–326 (1986).
18. Jürgen, E., Jürgen, L. & Alev, T. A nonlinear congruential pseudorandom number generator with power of two Modulus. *Math. Comput.* **51**, 757–759 (1988).
19. Leeb, H. & Wegenkittl, S. Inversive and linear congruential pseudorandom number generators in empirical tests. *ACM Trans. Model. Comput. Simul.* **7**, 272–286 (1997).
20. Marsaglia, G. The structure of linear congruential sequences, Applications of number theory to numerical analysis, ed: Zaremba S, Canada: Elsevier. pp. 249–285 (1972).
21. Chen, X., Zhang, Y., Zhang, G. & Zhang, Y. Evaluation of ECG random number generator for wireless body sensor networks security. In *5th International Conference on BioMedical Engineering and Informatics*, pp. 1308–1311 (2012).
22. Hong, S. L. & Liu, C. Sensor-based random number generator seeding. *IEEE Access*. **3**, 562–568 (2015).
23. Li, C-Y., Chen, Y-H., Chang, T-Y., Deng, L-Y. & To, K. Period extension and randomness enhancement using highthroughput reseeding-mixing PRNG. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **20**, 385–389(2011)
24. Marsaglia, G. Seeds for random number generators. *Commun. ACM*. **46**, 90–93 (2003).
25. Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S. C. & Zhang, Y-T. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Trans. Biomed. Eng.* **65**, 2751–2759 (2018).
26. Araki, S., Miyazaki, T., Uehara, S. & Kakizaki, K. A study on precision of pseudorandom number generators using the logistic map. In *International Symposium on Information Theory and its Applications*, pp. 740–744 (**2012**).
27. Lynnyk, V., Sakamoto, N., Cˇelikovsky´ & S Pseudo random number generator based on the generalized Lorenz chaotic system. *IFAC-PapersOnLine* **48**, 257–261 (2015).
28. Pehlivan, I. & Uyarogˇlu Y 2007 simplified chaotic diffusionless Lorentz attractor and its application to secure communication systems. *IET Commun.* **1**, 1015–1022
29. Prasad, M. & Sudha, K. Chaos image encryption using pixel shuffling. In *International Conference on Computer Science, Engineering and Applications* pp. 169–179 (2011).
30. Singh, K. U. & Singhal, A. A color image watermarking scheme based on QR factorization, logistic and Lorentz chaotic maps. *Int. J. Recent. Innov. Trends Comput. Commun.* **5**, 291–296 (2017).
31. Eisencraft, M., Kato, D. M. & Monteiro, L. H. A. Spectral properties of chaotic signals generated by the skew tent map. *Signal. Process.* **90**, 385–390 (2010).
32. Palacios-Luengas, L., Pichardo-Me´ndez, J., Dı´az-Me´ndez, J., Rodrı´guez-Santos, F. & Va´zquez-Medina, R. PRNG based on skew tent map. *Arab. J. Sci. Eng.* **44**, 3817–3830 (2019)
33. Dastgheib, M. A. & Farhang, M. A digital pseudorandom number generator based on sawtooth chaotic map (2017).
34. with a guaranteed enhanced period. *Nonlinear Dyn.* **89**, 2957–2966
35. Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S-C. & Hassan, Z. Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **19**, 101–111 (2014).
36. El-Latif, A. A. A., Li, L., Wang, N., Han, Q. & Niu, X. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal. Process.* **93**, 2986–3000 (2013)
37. Seyedzadeh, S. M., Norouzi, B., Mosavi, M. R. & Mirzakuchaki, S. A novel color image encryption algorithm based on Spatial permutation and quantum chaotic map. *Nonlinear Dyn.* **81**, 511–529 (2015)
38. Suneel, M. Cryptographic pseudo-random sequences from the chaotic He´non map. *Sadhana-Acad. Proc. Eng. Sci.* 34, 689–701 (2009).
39. Ruoran, L., Hongjun, L. & Mengdi, Z. *Reveal the Correlation between Randomness and Lyapunov Exponent of n-dimensional non-degenerate Hyper Chaotic Map* 102071 (Integration93, 2023).
40. Fan, C. & Ding, Q. Dynamic analysis and geometric control of a novel parametrically controllable multi-scroll Conservative chaotic system. *Nonlinear Dyn.* **112**, 3935–3949 (2024).
41. Luo, Y., Xu, C. F. C. & Li, X. Design and FPGA implementation of a high-speed PRNG based on an n-D non-degenerate chaotic system. *Chaos, Solitons Fractals*,183, 114951 (2024).
42. Nejati, H., Beirami, A. & Ali, W. H. Discrete-time chaotic-map truly random number generators: Design, implementation, and variability analysis of the zigzag map. *Analog. Integr. Circuits Signal. Process.* **73**, 363–374 (2012).
43. Phatak, S. & Rao, S. S. Logistic map: A possible random-number generator. *Phys. Rev. E.* **51**, 3670 (1995).
44. Li, C. et al. On the security defects of an image encryption scheme. *Image Vis. Comput.* **27**, 1371–1381 (2009).
45. Li, C., Xie, T., Liu, Q. & Cheng, G. Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dyn.* **78**, 1545–1551 (2014).
46. Yuanyuan, S., Hongjun, L. & Mengdi, Z. Constructing keyed strong S-Box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation. *Integration* **88**, 269–277 (2023).
47. Mengdi, Z., Hongjun, L. & Yujun, N. Batch generating keyed strong S-Boxes with high nonlinearity using 2D hyper chaotic map. *Integration* **93**, 91–98 (2023).
48. Ruoran, L., Hongjun, L. & Mengdi, Z. Cryptanalysis and construction of keyed strong S-Box based on random affine transformation matrix and 2D hyper chaotic map. *Exp. Syst. Appl.* **252**, 124238 (2024).
49. Saira Beg, S., Faisal Baig, Y. H., Khattak, A., Anjum, A. & Khan Thermal image encryption based on laser diode feedback and 2D logistic chaotic map. *Multimed. Tools Appl.* **81**, 26403–26423 (2022).

50. Patidar, V., Sud, K. K. & Pareek, N. K. A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Acta Inform.* **33** (2009)
51. Pisarchik, A. N. & Zanin, M. Chaoticmapcryptographyand security. *Int. J. Comput. Res.* **19**, 49 (2012)
52. Li, C-Y., Chang, T-Y. & Huang, C-C. A nonlinear PRNG using digitized logistic map with self-reseeding method. In *Proceedings of 2010 International Symposium on VLSI Design, Automation and Test*, pp. 108–111 (2010).
53. Chen, S-L., Hwang, T. & Lin, W-W. Randomness enhancement using digitalized modified logistic map. *IEEE Trans. Circuits Syst. II Express Briefs*. **57**, 996–1000 (2010).
54. Murillo-Escobar, M., Cruz-Herna´ndez, C., Cardoza-Avendan˜o, L. & Me´ndez-Ramı´rez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dyn.* **87**, 407–425(2017)
55. Garcı´a-Martı´nez, M. & Campos-Canto´n, E. Pseudorandom bit generator based on multi-modal maps. *Nonlinear Dyn.* **82**, 2119–2131 (2015).
56. Liu, L., Miao, S., Hu, H. & Deng, Y. Pseudorandom bit generator based on non-stationary logistic maps. *IET Inf. Secur.* **10**, 87–94 (2016)
57. O¨ zkaynak, F. Cryptographically secure random number generator with chaotic additional input. *Nonlinear Dyn.* **78**, 2015–2020 (2014).
58. Huang, X., Liu, L., Li, X., Yu, M. & Wu, Z. A new twodimensional mutual coupled logistic map and its application for pseudorandom number generator. *Math. Probl. Eng.*, 1–10 (2019).
59. Asmaa Hasan Alrubaie, Maisa'a Abid Ali Khodher and Ahmed Talib Abdulameer. Image encryption based on 2DNA encoding and chaotic 2D logistic map. *J. Eng. Appl. Sci.* **2023**, 1–21 (2023).
60. Hongjun, L., Jian, L. & Chao, M. Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption. *Multimed. Tools Appl.* **82**, 23899–23914 (2022).

Acknowledgements

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number. NBU-FFR-2025-2484-05., also the authors declare that the article has been produced with the financial support of the European Union under the REFRESH – Research Excellence For Region Sustainability and High-tech Industries project number CZ.10.03.01/00/22_003/0000048 via the Operational Programme Just Transition and paper was supported by the following project TN02000025 National Centre for Energy II awarded to HK.

Author contributions

R.A. and G.S. conceptualized the study and designed the methodology. R.A., A.F., H.K., and C.Z.E. contributed to the theoretical framework and mathematical modeling. F.B. and Y.H.K. performed the simulations and statistical analysis. Y.H.K., G.S., and A.F. prepared the figures and tables. R.A., G.S., and Y.H.K. wrote the main manuscript text. H.K., C.Z.E. and F.B. reviewed and edited the manuscript for technical accuracy and clarity. All authors contributed to discussions, reviewed the manuscript, and approved the final version.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Y.H.K.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.