Al-Qadisiyah Journal of Pure Science

Volume 26 | Number 1 Article 21

1-7-2021

True Random Number Generator Based on nondeterministic Device and Multi dimension Chaos Theory

Shireen Sabeeh
Computer Science Department, University of Technology, Baghdad, Iraq,
cs.16.128@student.uotechnology.edu.iq

Alaa Kadhim
Computer Science Department, University of Technology, Baghdad, Iraq, 110030@uotechnology.edu.iq

Ayad Al-Adhami
Computer Science Department, University of Technology, Baghdad, Iraq, 0010@uotechnology.edu.iq

Recommended Citation

Sabeeh, Shireen; Kadhim, Alaa; and Al-Adhami, Ayad (2021) "True Random Number Generator Based on nondeterministic Device and Multi dimension Chaos Theory," *Al-Qadisiyah Journal of Pure Science*: Vol. 26: No. 1, Article 21.
DOI: 10.29350/qjps.2021.26.1.1249
Available at: https://qjps.researchcommons.org/home/vol26/iss1/21

Al-Qadisiyah Journal of Pure Science
ISSN(Printed): 1997-2490 ISSN(Online): 2411-3514
DOI: /10.29350/jops.
http://qu.edu.iq/journalsc/index.php/JOPS

True Random Number Generator Based on nondeterministic Device and Multi dimension Chaos Theory

Authors Names

a.Shireen sabeeh

b.Alaa Kadhim

c. Ayad Al-Adhami

Article History

Received on:29/11/2020
Revised on:28/12/2020
Accepted on:4/1/ 2021

Keywords:

Chaotic system, Mouse Device, Cryptography, RNGs, NIST.

DOI: https://doi.org/10.29350/jops.2021.26. 1.1249

ABSTRACT

There have been strong links between chaotic theory and cryptographic theory for the last three decades. The characterization of behaviors of the Chaotic system, such as: highly responsive to initial states.These proposed generators suffer from minimal key space and those centered on a 1D chaotic map have limited capacity to produce entropy due to their limited number of exponents of Lyapunov (s). Random binary sequence generator producing sequence of bits has been proposed in this paper. The proposed system model consists of two parts that use mouse device data constructively as the basis for the theory of non-determinism and chaos. The chaos theory includes three forms with the mouse cursor coordinates while moving as the initial seeds in this proposed system (1D logistic chaotic system, 2D Hénon system and 3D chaotic system) and combines the values produced in the algorithm. With 1D, 2D Hénon, 3D chaotic maps, the mouse cursor coordinates are treated as an initial random number with post processing to increase the randomness and security of the keys. In the suggested research, there is high key space and a very long time. It is also evident that the developed keys have successful statistical features that require purely random binary sequences that are optimal for use in essential cryptography systems provided by evaluating the results of 16 NIST hardness tests (National Institute of Standards and Technology).

a. Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: cs.16.128@student.uotechnology.edu.iq.
b. Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: 110030@uotechnology.edu.iq.
c. Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: 10010@uotechnology.edu.iq.

1. Introduction

In recent applications of science and diverse technologies, such as modeling, sampling, numerical analysis, computer programming, decision making and recreation, random number generators (RNGs) have been widely used. [1][2]. RNGs are important for a variety of applications, including encryption, secure key generation, and gaming and Monte-Carlo calculations, because RNG collects randomness from different high-entropy input streams, and tries to produce yields that are in practice indistinguishable from really irregular streams [15]. Pseudo-random number generators (PRNGs) are used in most of these applications: deterministic algorithms implemented on a machine or dedicated hardware that produce a seemingly unpredictable sequence of bits that are statistically indistinguishable from a truly random sequence[4]. Although PRNGs are cost-effective and in most instances, active, [2], If one discovers the seed or internal state of the algorithm, they suffer from the limitation that the future (and in some cases past) series can be deterministically computed. The internal state can be inferred in weak PRNG algorithms by following a sufficiently long background of the bit sequence [13].It is important to separate random number generators into two categories: pseudo random-number and true random-number generators. Pseudo-random numbers are generated by deterministic algorithms from a normal short seed, and these are used in modern digital electronic information systems [3].Researchers have shown that there is a fascinating association between cryptography and chaos over the last three decades [19]. Chaotic systems are primarily used in the cryptographic random number generator [5,10,12] due to strong entropy and noise sources. In science and engineering, the applications of random numbers have an important role, since randomness is crucial for cryptography. Cryptography requires numbers which can't be guessed by aggressors. We can't allow equivalent use over and over again of the same numbers. We can't make equal use of the same numbers over and over again. In a very eccentric way, we need to generate these numbers so that aggressors can't find them out. For safe encryption, these random numbers are necessary [14]. In this paper, chaos based deterministic random generator systems are investigated. A novel design have been obtained by using chaotic systems and mouse device as entropy sources to designs a generator of random number. The mouse cursor coordinates are gathered as the user moves the mouse around the screen to generate a predefined number of values. The work proposed has high key space and a very long period of time. Statistical tests have been used to analyze the performance of new modified designs. Analysis result shows that outputs of this design are randomness and have been used as may application area such statistics, game theory, cryptography.

2. Chaotic System

As stated before the principle of chaos is used to construct a random number generator with regard to the specifics of mouse motion[14]. As a nonlinear complex dynamic system, Chaos theory is well defined and is a branch of mathematics[15]. This dynamic system is highly dependent on the initial properties and The principal explanation for the utility of chaotic maps in the field of secure communications[17] is this property. The chaos theory would be used as chaotic mapping to create the pseudo-random number generator in order to generate the mutual key with chaotic properties. The numbers created by this generator will depend, as explained below on the logistic equation, the Hénon system equation and the 3D logistic map of chaos[9].

2.1. Chaos Logistic Equation: It is the one-dimensional recursive mapping[7], by generating pseudo-random numbers, that generates chaos in the system. The logistic equation model is given by the standard:

$$f(xi) = RXi(1 - Xi) \textbf{(1)}$$

Where X_i is called the iteration of X_0 (or population) and should by in subinterval [0, 1], and R is the growth rate of a population that takes any values between [1, 4], the output should lie between [0, 1].The map is chaotic when control parameter R ∈ [3.57, 4]. When R = 4,The performance of the map Xn+1 ∈ (0, 1) covers the entire process, which is evident in **Figure 1**. For the area R∈[3.57, 4] in **Figure 2**, the chaotic logistic map has a positive Lyapunov

representing the chaotic behavior. The exponent of Lyapunov calculates the quantitative orbit divergence that confirms the chaotic behavior [10].

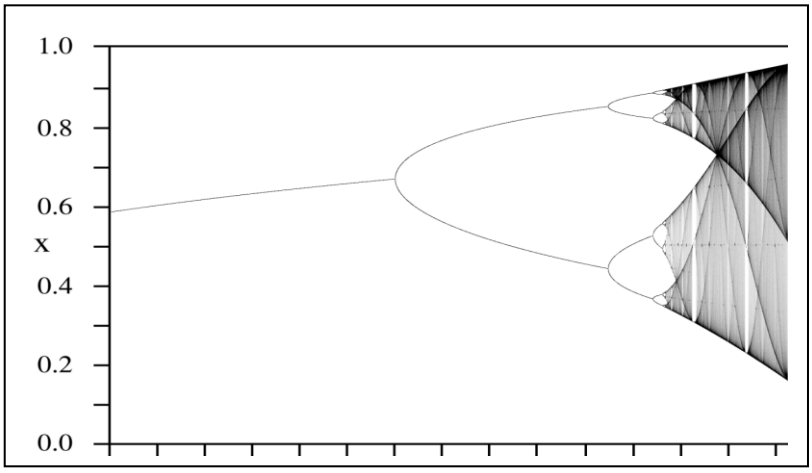

Fig.1-Logistic Map Bifurcation Diagram.**[11]

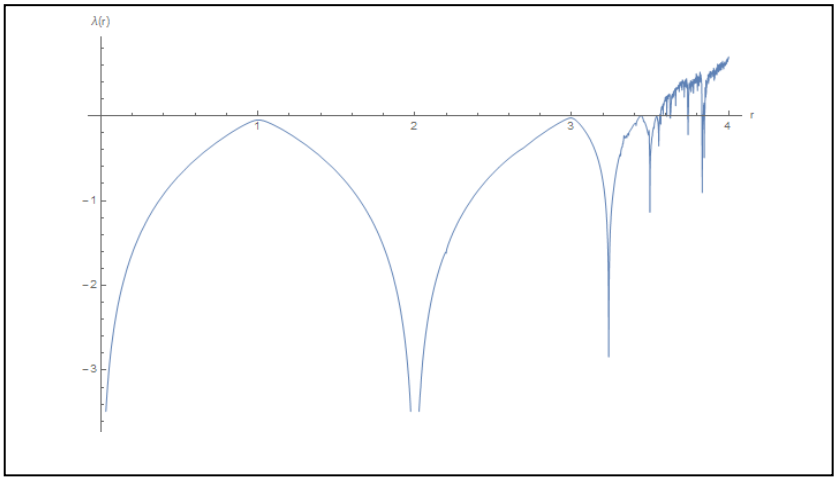

Fig.2-Logistic Map in Lyapunov Exponent. **[11]**

2.2. Hénon System: The Henon Method, which is a two-dimensional chaotic map, is the second mapping scheme that was used for the pseudo-random number generation. It is an iterative map as well. The equations reflect the initial conditions:

$$Xi = 1 - \alpha X^2_i + Yi \qquad (2)$$
$$Yi = \beta Xi$$

Where α and β have values 1.4 and 0.3respectively, which is evident in **Figure 3**[21]. The outputs of these functions are translated to 0,1 to form a binary sequence. Dependent upon the value of the threshold. The pseudo-random sequences generated have been shown to have fantastic statistical properties. The values obtained are deterministic in view of the initial state, but given their high susceptibility to the initial conditions offered, which are selected randomly in the range above,The iterative values become volatile, making them ideal for the shared binary key to be used as a random integer[22].

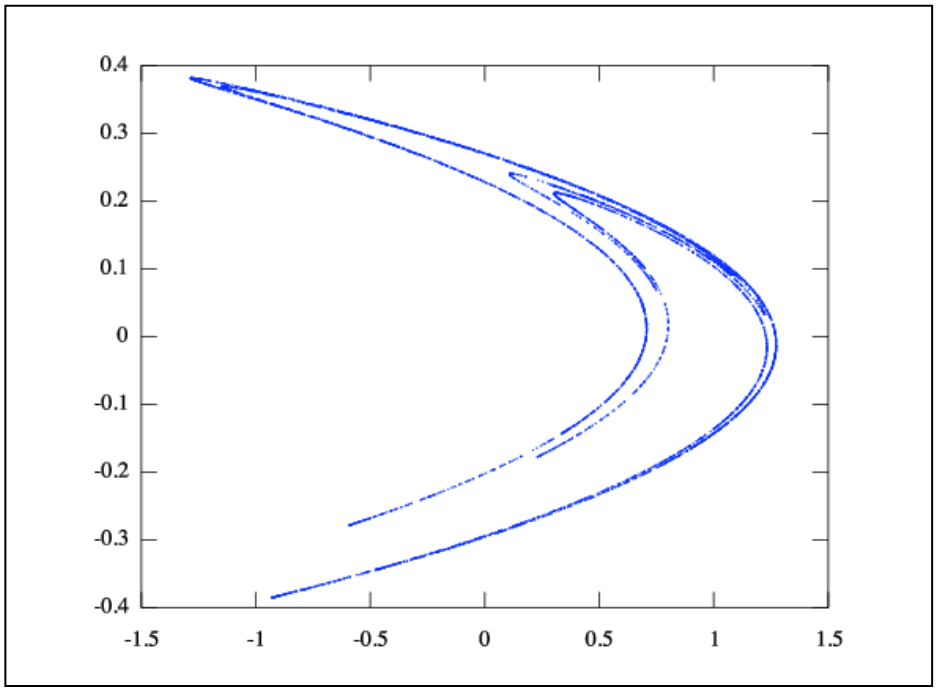

Fig.3-Bifurcation diagram for Hénon System**.[21]**

2.3. 3DLogistic Map: There are three simple variables (X), (Y) and (Z) in logistic equations and three control parameters, R, Q and k.

$$Xi+1 = R\,Xi\,(1-Xi) + Q\,Yi\,2\,Xi + K\,Zi\,3$$
$$Yi+1 = R\,Yi\,(1-Yi) + Q\,Zi\,2\,Yi + K\,Xi\,3 \qquad \textbf{(3)}$$
$$Zi+1 = R\,Z\,i(1-Zi) + Q\,Xi\,2\,Zi + K\,Yi\,3$$

When the control parameters have the following values of $3.53 < R < 3.81$, $0 < Q < 0.022$, $0 < K < 0.015$, the three simple state variables (X), (Y) and (Z) should be between [0, 1], the functional system becomes unstable.[12].

2.4. Mouse Movement

As we discussed earlier, different nondeterministic source methods will produce a true random number. It is possible to regard the mouse system as a random source[24]. There are two dimensions of the operation of a mouse unit on the screen, the X-axis and Y-axis corresponding to the coordinates of the mouse cursor on a surface at a given point. The motion of the mouse cursor in the graphical movement is perceived. These values can be obtained and stored for further work as the user pushes the mouse over the screen. When the user tries to shift the mouse cursor around the web page, different numbers are created each time. It is hard for the consumer to replicate the same moving sequence. These generated numbers can be treated as a random number series[25].There are of course, a vast range of choices for random number generation, such as thermal noise, ambient noise, radioactive decay and even coin-tossing. But for everyday consumers, these approaches are either too costly or too slow. These approaches

require additional electronic equipment in most situations, which make their implementations not so universal. Mouse movement, on the other hand, is a cheap, easy and universal technique for PC users to produce random numbers. The pace is also appropriate, and no extra protection device has to be bought by consumers. Moreover, it will be more rewarding for consumers to be able to monitor security on their own[8]. They knew nothing about the random number to be made, even the hackers stole the hidden key of the customer. The action of the mouse then seems a safe choice[27].

3.Proposed System

The proposed system is designed to generate an alternate method that seeded chaotic maps. The proposed system consists of two components, mouse movement and chaos theory, **Figure 4**and **Figure5** illustrates the idea of the proposed system. The first part of the proposed random bits generator, Which is related to the mouse device or non-deterministic device, requires the computer user to move mouse cursor, then generating coordinates x and y and The generated coordinates are used as the initial parameter to seed the chaotic equation which are collected by moving the cursor over the screen.These values represent the coordinates of mouse movement(X, Y). The generated coordinate create two sequences with different values of the same duration (N), the first sequence for the X-axis (called Xn) and the second sequence for the Y-axis (called Xn), as the cursor travels across the screen (called Yn).These sequences will be the primary parameter and prerequisite to the chaos equation the proposed system The X-axis values are processed to float numbers between [0, 1], and the Y-axis also processed to float numbers between [1, 4]. To increase the security of proposed generator, we applied (1D chaotic system, Hénon System, 1D chaotic system) When movement as the initial seeds, with the coordinates of the mouse cursor and combines the values produced in the algorithmic process. The mouse cursor coordinates are treated with 1D, Hénon, 3D chaotic maps as an initial random number with post processing to improve the randomness of the keys [14]. For the proposed system it will be strong against differential cryptanalysis for the following reasons, The key is generated from merging of mouse movement and chaos theory, which includes the equations of 1D logistic map, Hénonmap and 3D logistic map to increase the complexity and randomness of the generated keys. It is impossible to repeat the movement of the mouse and get the same results, and here lies the strength of the proposed system. Chaos theory is used in a very complicated way, which makes it difficult for the attacker.

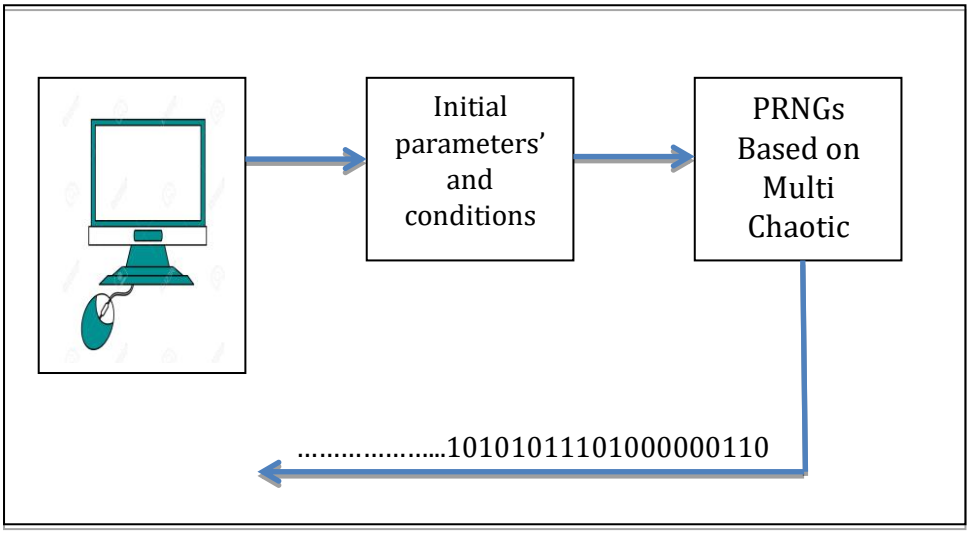

Fig .4- Proposed System Structure.

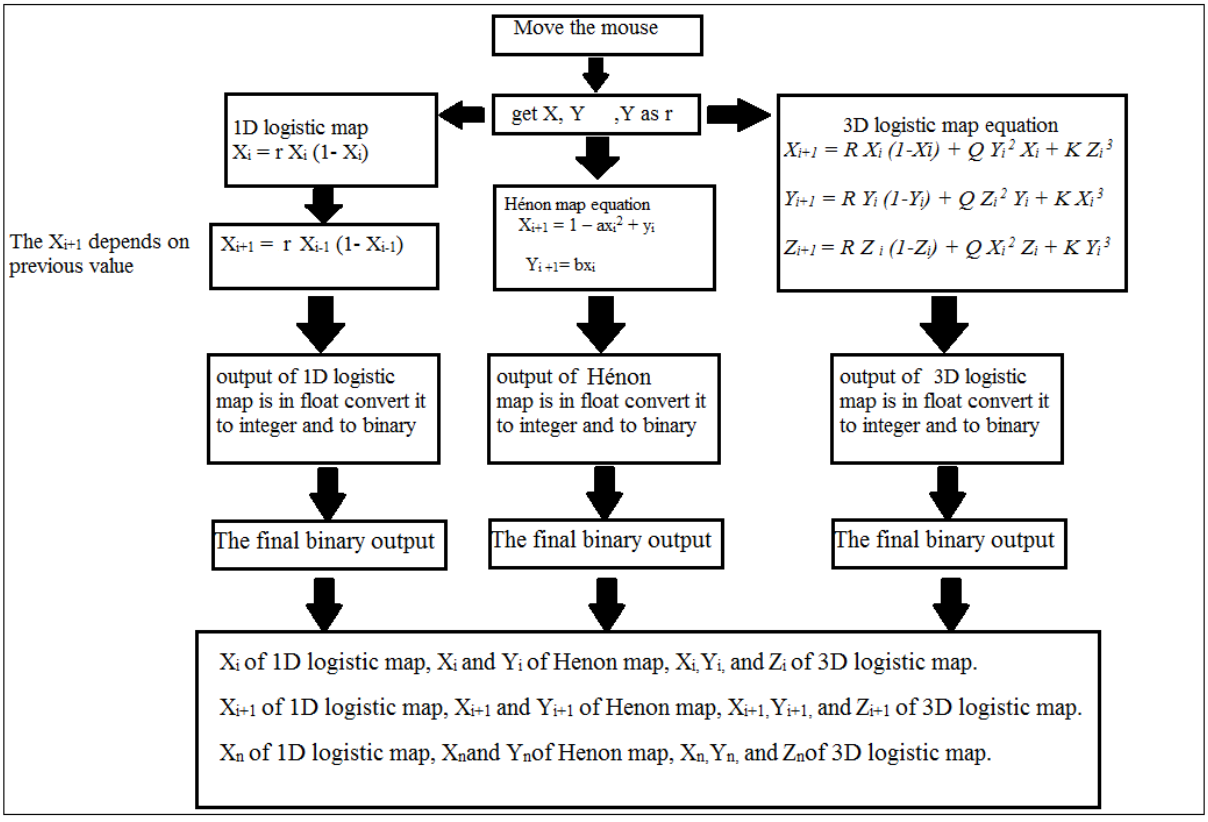

Fig.5-Initial values and condition parameters for system.

3.1. Set initial values and condition parameter in proposal System:-

1- For **1D** logistic map equation produces only outputs (X) in question 1

- X_0 initial value: is the first value from X_i coordinates (Array_X) after processed it.
- *R* condition value: is the first value from Y_i coordinates (Array_Y) after processed it. The output of X_i will be the initial parameter for the X_{i+1} and *r* still the same condition value in all iterations.

2- For **2D**Hénon System equation produce two outputs (X, Y) in equation 2

- X_0 initial value: is the second value of X_i coordinates (Array_X) after processed it.
- Y_0 initial value: is the third (the second value using in above step) value of X_i coordinates (Array_X) after processed it.
- a= 1.4 and b = 0.3 condition parameter are still the same values in all iterations .The outputs of X_i and Y_i will be the initial values for(second iteration) the X_{i+1} and Y_{i+1}.

3- For **3D** logistic map equation produces three outputs (X, Y, and Z): on equation 3

- X_0 is the fourth value of X coordinates (Array_X) after processed it.

- Y_0 is the fifth value of X coordinates (Array_X) after processed it.
- Z_0 is the sixth value of X coordinates (Array_X) after processed it.
- And the condition parameter 3.53 <*R*< 3.81, so it is the second value of Y coordinates (Array_Y) after processed it.
- 0 <*Q*< 0.022, so it is the seventh value of X coordinates (Array_X) after processed it.
- 0 <*K*<0.015,so it is the eighth value of X coordinates (Array_X) after

The values of (*R, Q, and K*) are still the same in all iterations. The outputs of X_i, Y_i, Z_i will be the initial condition for the X_{i+1} Y_{i+1} Z_{i+1}.All equations will iterations that depend on the number of iterations (n) which user have been input it but must be less than the length of mouse movement. All outputs must be between [0, 1].

3.2. For more explanation let's take this algorithm of our generator processes:

Algorithm(1): Proposal System PRNGs

Input: Coordinates of Mouse Movement.

Output: Random Binary Sequences.

Begin

Step1: Initial values and condition as a,b,Q,K,R parameter for chaos equations in system.

Step2: Generate two Xi and Yi sequences when a user moves the mouse device, And save these sequences in two arrays, the first one for X values called (Array_X), and the second one for Y values called (Array_Y)

Step 3: Convert X_i to float numbers, to be values between [0, 1], as initial values.

The procedure is applied for each X:

```
If 500≥ Xi ≥0 then
X1=Xi+100//
X= Xi / X1
Else If 1000≥ Xi ≥500 then
X1=Xi+200
X= Xi / X1
Else If Xi>1000 then
X1=Xi+300
X= Xi / X1
End if.
```

Step 4: Do some operations as explain below on Y_i, to be values between [1, 4] and use in equation (1)as condition parameter.

```
r = Mid(Y, 1, 1)
If r >= 0 And r <= 2 Then
```

```
r = (r + 9) / 3.
ElseIf r = 3 Then
r = (r + 8) / 3
        ElseIf r = 4 OR r = 9 Then
r = (r + 1) / 3
        ElseIf r = 5 Then
r = (r + 3) / 3
        ElseIf r = 6 Then
r = (6 + 2) / 3
        ElseIf r = 7 And r = 8 Then
r = (r + 0) / 3
End If
```

Step 5: X_i, Y_i values are initial conditions to equation (1), (2) and (3) And the output of equation (1), (2), (3) will be the second initial conditions and so on.

Step 6: After we gain the output of equations, convert each one of the output from float to integer and finally to binary.

Step 7: make a combination between the outputs of three equations.

To make the combination between the outputs and generate huge sequences of binary must applied the following mechanism:

X_i of 1D logistic map, X_i and Y_i of 2D Hénon map ,X_i, Y_i and Z_i of 3D logistic map.

$X_{i+1}$of 1D logistic map, $X_{i+1}$and $Y_{i+1}$of 2D Hénon map, X_{i+1}, $Y_{i+1}$and Z_{i+1} of 3D logistic map.

1D logistic map, X_n and Y_n of 2D Hénon map,X_n,Y_n and Z_n of 3D logistic map.

Step 8: Save the binary sequence in a file.

End

4. Experiment Result and Discussion

The National Institute for Standard Technology issues statistics for research. There are 16 tests involved and a certain sub-test is involved in each test. In the bit sequence of the input and random generator of the bit sequence cryptography program, these checks concentrate on non-randomness. The NIST is designed to measure the randomness of (arbitrarily long) binary sequences generated on the basis of hardware or software by cryptographic random or pseudorandom number generators.Numerous chaotic systems have been used to create pseudo-random number sequences (PRGS). To test the proposed method, NIST 800-22 is being used. An actual estimation of the chaotic sequence's randomness is given by NIST 800-22[16], which involves several statistical tests. Each test needs a p-value, which from many sides can discover the non-random regions of a binary sequence. Table 1 lists the NIST-800-22 sequence results when the generated binary sequences are 1, 000, 000

bits in length. Table 2 lists NIST-800-22 sequence results when the generated binary sequences are 2, 000, 000 bits in length. All statistical tests are passed using the selected parameters and conditions.

Table (1): NIST-800-22 tests results of the first binary sequence

#	NIST Tests	P-value	Result
1	Frequency Test (Monobit)	0.7724232578210854	Random
2	Frequency Test within a Block	0.59087965644187018	Random
3	Run Test	0.41549365854192	Random
4	Longest Run of Ones in a Block	0.8533896842044	Random
5	Binary Matrix Rank	0.73790847701231	Random
6	Discrete Fourier Transform	0.582615010182692532	Random
7	Non-Overlapping Template	0.5522441657574574	Random
8	Overlapping Template Matching	0.6506924233408542	Random
9	Maurer's Universal Statistical	0.7821289360025	Random
10	Linear Complexity	0.5815389143005239	Random
11	Serial test	0.735919824982495095	Random
12	Approximate Entropy	0.56159493146891897	Random
13	Cumulative Sums (Forward)	0.8516336860902045	Random
14	Cumulative Sums (Reverse)	0.6265901830808537	Random
15	Random Excursions	0.71640747043379938	Random
16	Random Excursions Variant	0.8406715769752813	Random

Table (2): NIST-800-22 tests results of the second binary sequence

#	NIST Tests	P-value	Result
1	Frequency Test (Monobit)	0.877364097566463	Random
2	Frequency Test within a Block	0.69418701648085796	Random
3	Run Test	0.71648420449377	Random
4	Longest Run of Ones in a Block	0.8533896658541	Random
5	Binary Matrix Rank	0.879477073023101	Random
6	Discrete Fourier Transform	0.98822615032233408	Random
7	Non-Overlapping Template	0.7665011216575074	Random
8	Overlapping Template Matching	0.8507401692554292	Random
9	Maurer's Universal Statistical	0.782125002916808	Random
10	Linear Complexity	0.810850254289360	Random

11	Serial test	0.8815498205234950	Random
12	Approximate Entropy	0.7359198914300523	Random
13	Cumulative Sums (Forward)	0.66159242325782	Random
14	Cumulative Sums (Reverse)	0.73798516084770	Random
15	Random Excursions	0.859063511653762	Random
16	Random Excursions Variant	0.92847070943694923	Random

5. Security Discussion and key Space analysis

The secret key must be very sensitive to its variance in order to show the security of the encryption algorithm and the length of the key space should also be greater than 2^{128} in order to prevent brute force attack [12][16][17]. The main space and its effects of variation are shown by security analysis. For an encryption algorithm, security keys are very important for the security of cipher media from various attacks and brute force attacks. In the proposal system when any fraction adjustment in any state of parameters or initials will produce more total differences from the first in other sequences, for that the system is responsive in any change values. The initial value (1D, 2D and 3D) of the three maps and their parameters are also taken as a hidden key for the method of encryption/decryption.Initial conditions and parameters are X_0, Y_0, Z_0,R, andQ as hidden keys, and the total key space is about 10^{84} if the accuracy is 10^{-14}, which is greater than 2^{128} to prevent attacks by brute force.

6. Conclusion

This paper presents the findings of research on the implementation of pseudo-random bit generators based on a turbulent structure of nonlinear dynamics. Several solutions, using different numerical accuracy and different arithmetic operation implementations, have been investigated. Centered on a nonlinear dynamic chaotic system, new random number generator architecture has been suggested. In the suggested method, recurring key problems are solved. In order to replicate the same numbers for the same person, the architecture uses mouse interface gestures as a source of initial random numbers of three chaotic forms. Second, three chaotic keys are used to improve the complexity and randomness of the keys produced. The motivation of this proposed strategy is to take advantage of disorderly behavior and the ease of using the mouse. Eventually, a large amount of random binary sequences are produced that have maximum periods. These binary sequences are tested. The results of these tests ensure that random binary sequences are the appropriate characteristics of generated binary sequences and can therefore be used efficiently in the design of cryptography systems. The results of the second stage NIST randomness tests of the proposed pseudo-random bit generators (PRBGs) are presented, showing strong cryptographic properties of the PRBGs presented. The generators listed in this paper can be used in stable, real-time digital signal transmission, including audio-video applications, for key generation in stream ciphers.

References

[1] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, "A New S-Box Generation Algorithm Based on Multistability Behavior of a Plasma Perturbation Model," IEEE Access, vol. 7, pp. 124914–124924, 2019.

[2] A. K. F and H. I. Mhaibes, "A Low-Cost True Random Bits Generator Based on Chaotic System and Light Nature," vol. 13, no. 5, pp. 2141–2146, 2018.

[3] A. Uchida et al., "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics, 2008.

[4] A. T. Sadeeq, A. K. Farhan, and S. A. Hassan, "A Proposed Public Key Encryption Based on Hybrid Chaotic Maps," Qalaai Zanist J., vol. 2, no. 2, pp. 64–71, 2017.

[5] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," Entropy, vol. 21, no. 10, pp. 1–14, 2019.

[6] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "A new technique for ultrafast physical random number generation using optical chaos," in Semiconductor Lasers and Laser Dynamics VII, 2016.

[7] A. M. Ali and A. K. Farhan, "A New Approach For Expansion the Throughput Capacity of the Quick Response Code," in 2019 First International Conference of Computer and Applied Sciences (CAS), 2019, pp. 226–231.

[8] A. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms," in 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), 2016, pp. 1–6.

[9] A. Kadhim F. and H. Emad M., "Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers," Diyala J. Pure Sci., vol. 13, no. 3, pp. 24–39, 2017.

[10] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," Chaos, Solitons and Fractals, 2009.

[11] A. T. Sadiq, A. K. Farhan, and S. A. Hassan, "A proposal to improve RC4 algorithm based on hybrid chaotic maps," J. Adv. Comput. Sci. Technol. Res., vol. 6, no. 4, pp. 74–81, 2016.

[12] B,jone "3D Chaotic Functions for Image Encryption," Int. J. Comput. Sci. Issues, 2012.

[13] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," Opt. Express, 2010.

[14] F. Özkaynak, "Cryptographically secure random number generator with chaotic additional input," Nonlinear Dyn., 2014.

[15] Farhan, Alaa K., and M. A. A. J. Ali. "Database protection system depend on modified hash function." Conference of Cihan University-Erbil on Communication Engineering and Computer Science. 2017.

[16] F. Alaa Kadhim, G. H. Abdul-Majeed, and R. S. Ali, “Enhancement CAST block algorithm to encrypt big data,” 2017 Annu. Conf. New Trends Inf. Commun. Technol. Appl. NTICT 2017, no. 0, pp. 80–85, 2017.

[17] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, “A new hyperchaotic map and its application for image encryption,” Eur. Phys. J. Plus, 2018.

[18] J. Purswani, R. Rajagopal, R. Khandelwal, and A. Singh, “Chaos theory on generative adversarial networks for encryption and decryption of data,” in Advances in Intelligent Systems and Computing, 2020.

[19] L. Zhao, X. Liao, D. Xiao, T. Xiang, Q. Zhou, and S. Duan, “True random number generation from mobile telephone photo based on chaotic cryptography,” Chaos, Solitons and Fractals, 2009.

[20] M. Peters, T. Giesbrecht, M. Jelicic, and H. Merckelbach, “The random number generation task: Psychometric properties and normative data of an executive function task in a mixed sample,” J. Int. Neuropsychol. Soc., 2007.

[21] M. Abutaha, S. El Assad, O. Jallouli, A. Queudet, and O. Deforges, “Design of a pseudo-chaotic number generator as a random number generator,” in IEEE International Conference on Communications, 2016.

[22] M. Li, M. Xu, J. Luo, and H. Fan, “Cryptanalysis of an Image Encryption Using 2D Henon-Sine Map and DNA Approach,” IEEE Access, 2019.

[23] M. A. Flierl, P. F. Stahel, K. M. Beauchamp, S. J. Morgan, W. R. Smith, and E. Shohami, “Mouse closed head injury model induced by a weight-drop device,” Nat. Protoc., 2009.

[24] N. A. Hamid, S. Safei, S. D. M. Satar, S. Chuprat, and R. Ahmad, “Mouse movement behavioral biometric systems,” in Proceedings - 2011 International Conference on User Science and Engineering, i-USEr 2011, 2011.

[25] Rahma, Abdul Monem S., Suhad M. Kadhem, and Alaa Kadhim Farhan. "Finding the Relevance Degree between an English Text and its Title." Engineering and Technology Journal 30.9 (2012): 1625-1640.

[26] S. El Assad and M. Farajallah, “A new chaos-based image encryption system,” Signal Process. Image Commun., 2016.

[27] S. M. Cho, E. Hong, and S. H. Seo, “Random Number Generator Using Sensors for Drone,” IEEE Access, 2020.

[28] Y. G. Yang and Q. Q. Zhao, “Novel pseudo-random number generator based on quantum random walks,” Sci. Rep., 2016.