Chaotic systems with pseudorandom number generate to protect the transmitted data of wireless network

Heyam A. Marzog, Marwa Jaleel Mohsin, Mohammed Azher Therib
Engineering Technical College/ Najaf, Al-Furat Al-Awsat Technical University, AL-Najaf, Iraq

Article Info

Article history:

Received Oct 12, 2020
Revised Dec 15, 2020
Accepted Dec 28, 2020

Keywords:

Chaotic system
Encryption
GPRN
Pseudorandom number
Security

ABSTRACT

Communication techniques have witnessed rapid development in recent years, especially the internet and the mobile network, which led to rapid data transmission. The latest developments, in turn, have come out with advanced decisions to secure information from eavesdropping. Myriad in-depth studies in cryptography. It was implemented with the intention of proposing a revolutionary solution to protect data by encryption techniques, tend maps, and logistics. This work had proposed a new design to the generator of pseudo-random numbers (GPRN) which had utilized multi chaotic systems. Synchronization of Multi-parameters chaotic arises in many applications, in natural or industrial systems. Many methods have been introduced for using a chaotic system in the encryption of data. Analysis of security of chaotic system had been executed on key sensitivity and key space.

Corresponding Author:

Heyam A. Marzog
Engineering Technical College/Najaf
Al-Furat Al-Awsat Technical University
AL-Najaf 31001, Iraq
Email: heyam.marzog@atu.edu.iq

1. INTRODUCTION

The main challenges of this current study are to develop a system that can increase the security develop communication data among users. A main obstacle faced many algorithms, which used to encryption data as 3DES, AES and DES was the consumed time when encrypting large amount of data (e.g. video or image) through real time [1]. Eclectic encryption methods had been found appropriate measure to solve speed problem of cipher. Many factors had been known to affect the originality of cipher rudimentary and one of them is the sequence of random number, that was believed to be the most important and reliability among the other methods [2]. Random number sequences have enormous effect on many applications, as spread spectrums, signal processing, encryption, the simulations of random and gaming etc. The random numbers are classified into two types: true random number generator (TRNG), which depended on phenomena of physical and natural like quantum random process, noise of photon etc. and second classified pseudo-random number generator (PRNG). A pseudo-random number generated (PRNG) had explained the shape of the algorithm resolution that had been used for improving of security application. Reverse the first classified highlights the palpable matters, which lead to the weak implement attach to cipher [3]. Chaotic cipher had showed a rise in the attention towards amongst many researchers' during the previous decade due to its noticeable characteristics as the responding to different states and parameters of control, blend the data, behavior of pseudo random [4]. The chaos system had used in widely form to most science fields as engineering, medical also it is used in humanities. Chaos is physical phenomenon of nonlinear and has many definitions proposed but the most widely used are; Wiggins' chaos, Smale's chaos and Devaney's chaos which all these concentrates on chaos variance achievement [5].

Chaotic system is utilized widely range in the pseudorandom sequence generators design, although the achievement of pseudorandom sequence generators is influenced by the chaotic decadence in greatly form, which is produced by reliability of computation [6]. With the appearances of rapid computers, it become to discover the parameters completely for any system with purpose obtaining on these parameters which outcome required characteristics for these system [7]. Chaotic systems is enticed many researchers' concern which may assist one to realize the dynamics of the actual system through generating chaotic attractors [8].

Behavior of chaotic is existed in a lot of natural factors, as fluid flow, heartbeat irregularities, weather [9-11]. It also take place automatic in many systems with synthetic ingredients like traffic movement, market of the stock. Nowadays, the new technique has remarkable a rise of interest by the most people. It is making the life of person very easier. So the most people is utilized credit cards for their requirements of life as shopping, social networks for communications, internet banking for paying the bills, internet phone and of short message service (SMS) communication and soon. Generally, each of these activities need to protect by one of security ways [12, 13]. Communication systems are exposed to multiple noise hazards such as Gaussian noise, which comes from a natural source, also known as electronic noise because it comes from amplifiers, filters, and other , that affect the data within the network [14].

The purpose to sum two maps of chaotic, the logistic map and tent map to obtain a good (PSR) which had high cipher features. A comprehensive security analysis test was performed as evidence of the suitability of the proposed PRNG for resistance to cyber-attacks in cipher. Several researches fulfilled in pseudo random number generation, focusing on the manipulation of chaotic maps for cryptographic aims. For instance, Parrek and Patidar modify the chaotic tent map and prove that the output sequence is completely fit 10. Lopez et al. embrace couple chaotic systems and perturbation, and select what is less important bits to suggest a pseudo random number generator for cryptographic aim [15]. Francois et al., in a similar study, integrate chaotic maps generated from an input premier vector to offer a new pseudo random number generator [16]. The statistical analysis of output sequence and the assessment of approaches in term of vulnerability to different attacks, have demonstrated the safety of the algorithm. Another research is done by J Szczepański and Z Kotulski, who manipulate discrete dynamical systems to create a pseudo random sequence and confirm the authenticity of generated sequence [17]. Yang, Liu and Tong Xiao suggest a new PRNG, which is supported by NIST test relied on a complicated number chaotic equation and haphazardness of generated sequence [18, 19]. M. Hamdi et al. offer a pseudo random sequence depended on chaotic maps and S-box table to create high-speed secure keys or random sequence with fixed security [20].

2. BASIC CONCEPTS

This section sheds light on the major concepts that are abstracted in this paper. It also examines the basic role of chaotic maps, which are utilized in the proposed algorithm.

2.1. The logistic map

Chaotic map is a recent concept in modern science and researchers prefer it because it involves operational simplicity, high speed, sensitivity to initial conditions, parameters of control, stability, ergodicity and the whole required characteristics in security systems design [21]. The logistic map was based on a single ingredient, which was performed by a particular mathematical mode to prove the employment of biological inhabitancy, PRNG and cryptographic implementation. Moreover, the mathematical simplicity supplied by the logistic map makes it a precious approach for examining new concepts in chaos theory and data security. The simplified mathematical formula is:

$$\text{Ni} +1 = \mu \,\text{Ni}\,(1 - \text{Ni}) \qquad (1)$$

Where Ni ∈ (0, 1) indicates the distinguished state, keeping the premier condition $N_0 \in (0, 1)$, while $\mu \in (3.999,4)$ symbolizes the control parameter and $n \geq 0$, is the number of iterations. To restrain digital downgrade and short period cycles, a 64-bit floating-point that affected 10-15 decimals is utilized. The Lyapunov exponent is a numerical approach that characterize chaos and orbital divergence once it has got a positive significance, which is valuable in proving the chaotic orbit in a logistic map. For fraction n_i*+1 =f(*n_i*)*, its Lyapunov exponent λ is defined as:

$$\lambda = \lim_{i\to\infty} \frac{1}{i} \sum_{j=0}^{i-1} ln|f'(n_i)| \qquad (2)$$

Where,

$$f'(n_i) = \frac{\delta Z(t)}{\delta Z_0}$$

A positive significance is granted to the function of chaotic behaviour that is measured quantitatively (i.e., $\lambda > 0$) by the Lyapunov exponent that is enumerated through the quantitative process with the exception that the system control parameter is modified from 3 to 4, with step 0.0001, as appeared in the Lyapunov exponent in Figure 1 which indicates Lyapunov classification. It can be noticed that the logistic map Lyapunov exponent started to expand to 0 at μ > 3.64 as appear Figure 1. Furthermore, when it was between intervals [3.999,4], all Lyapunov exponents are greater than 0 and became more fixed, while some values for limited points were below 0 when $\mu \in$ [3.64,3.9].

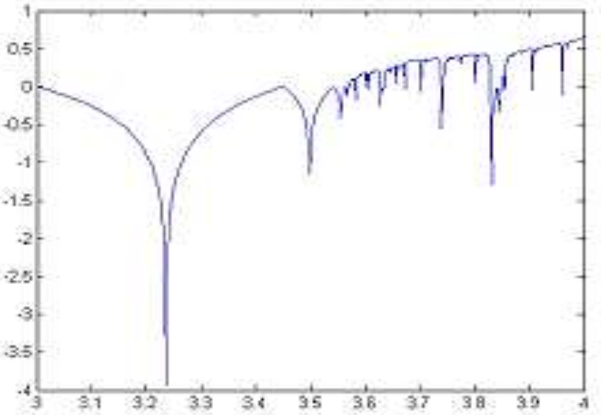

Figure 1. Lyapunov exponent of the logistic map

2.2. The tent map

The map of tent is ergodic and the interval has a stable density function [14]. It is regarded to be simple and of one-dimensional chaotic map, and so is recognized as:

$$M_{i+1} = \begin{cases} M_{i+1}\ if\ M_i < 0.5 \\ \omega(1 - M_i)\ otherwisex \end{cases} \tag{3}$$

Where $M_i \in$ [0, 1], $i \geq 0$ indicates the system parameter. This map modifies an interval [0, 1] against itself and contains only one control parameter ω, where $\omega \in$ [0, 2]. The set of exact values M_0, M_1... Mn form the system orbit, where M_0 is the premier value, and an orbit can be got for each M$_i$. In accord with the control parameter, different dynamical performances extending from prospective to disorder as appeared in (3). When the Lyapunov exponents in the interval [0, 1] are positive, that shows that the system is disordered and the signal is convenient in terms of traversal of the state, certainty and mixing. The chaotic generated sequence by mapping has tendency to cover a decent statistical asset. Furthermore, they have a custom of satisfied regular intervals under limited precession. The significance is classified into two scenarios as follow:

- The sequences show robust randomness, when the value of ω is small.
- Periodicity appears on sequences behaviour, that ω value becomes bigger.

3. PROPOSED ALGORITHM

The suggested algorithm includes three major steps:

Step 1. Initialization:

a) Input values for logistic map 0 in the range [0, 1], and μ = 3.99999988.

b) Input initial values for tent map $Y0$ in the range [0, 1], and ω = 1.99999988.

c) Both chaotic maps are restored for t times.

d) The output Xt and Y will be the input value to the next step.

Step 2. Chaotic Numbers Generating:

This step includes two points of chaotic systems, which are organized of logistic map (LM) and tent map (TM), to produce a sequence, which will be manipulated as a premier for each restoration between the points. In second phase, two new chaotic maps mentioned as tent map to logistic map (TLM) and logistic map to tent map (LTM) are used and restored by values produced by the first phase. LTM manipulated the premier value from Logistic map (first phase) according to (3). While, TLM is filled with the premier value from the tent map (first phase) using (1). As appeared in Figure 2. This stage works as follows:

a) set both chaotic maps (first phase) with the last Nt and Mt, which have been generated by stage.

b) set both new chaotic maps (second phase) with the last Nt and Mt, which have been generated by step (1).

c) produce the output by restoring both phases, which indicated as A, B, C, and D. 4. Transform produced sequences into bytes in the range [0,255], by (4):

$$Byte\ (A) = Round\ (A\times\ 255) \tag{4}$$

After that, each byte will be supplied into the next stage as explained in Figure 3.

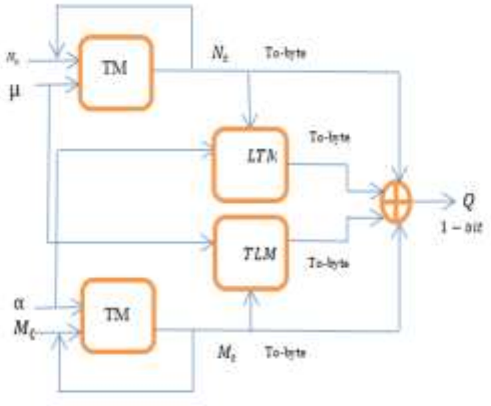

Figure 2. The chassis of proposed cha otic

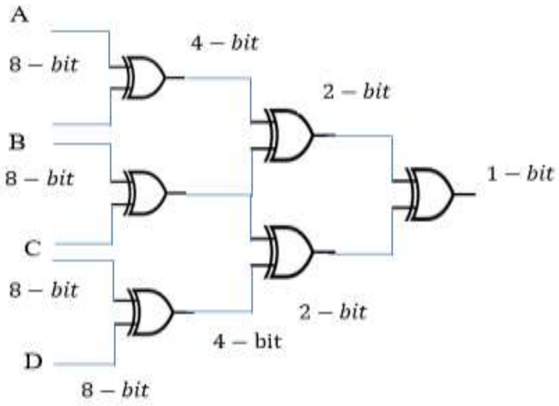

Figure 3. The operating of XOR

XOR phase 1: This phase XORed is only specific 4 bits of the sequence for all bytes (A, B, C, D). An example might be claimed is described in Table 1. This processing is similar the decimation-in frequency of signal processing.

XOR phase 2: This phase is specific 2 sequence bits for all bytes (AB, BC). An example might be claimed is depicted in Table 2.

XOR phase 3: This is specific 2 sequence bits for all bytes (ABC, BCD). We can give simple example is depicted in Table 3.

XOR phase 4: The output which is produced from the former phase, is XORed to generate one bit only, as it is shown in the next Equation:

Table 1. This phase XORed is only specific 4 bits of the sequence for all bytes (A, B, C, D)

A	B	AB
1	3	1
3	1	2
2	4	3
4	2	4

Table 2. This phase is specific 2 sequence bits for all bytes (AB, BC)

AB	BC	AB BC
1	3	1
3	1	2

Table 3. This is specific 2 sequence bits for all bytes (ABC, BCD)

ABC	BCD	ABC BCD
1	3	1
3	1	2

$$G = (ABCD)_{1^{st}bit}\ (ABCD)_{2^{nd}bit} \tag{5}$$

The output to one iteration where G ∈ {0,1}.

4. SECURITY ANALYSIS

The strength of the pseudo random number generator against different attacks must be examined before it is utilized in cryptography. The key space and the key sensitivity are both produced as security demands on systems of the cryptographic.

4.1. Analysis of key space

A key space size should contain more than 2^{100} potential keys. If the key space is tiny, an attacker tried to brute-force the system. However, the sequence generated by the suggested system relies on premier state M_0, N_0 and the control parameter μ. It shows that the suggested scheme includes 2^{192} from two phases that each one of them includes two chaotic maps. This shows that all generated keys are regarded as strong.

4.2. Analysis of key sensitivity

An algorithm of producing PRNG ought to be subtle to the tiniest changes in the produced keys. In order to test the sensitivity of the proposed algorithm, the following test cases have been manipulated to prove the sensitivity numbers are produced and compared with the original case. Figure 3 shows the first 20 numbers of each case as shown in Tables 4. and 5.
Case 1: Both $X0$ and $Y0$ equal 0.123456889,
Case 2: $X0$ is changed from 0.123456889 to $X0 + 2{-}48$,
Case 3: $Y0$ is changed from 0.123456889 to $Y0 + 2{-}48$,
Case 4: $X0$ and $Y0$are changed from 0.123456889 to $0 + 2{-}44$and $Y0 + 2{-}45$.

Table 4. Case 1 and case 2 analysis of key security

Case1		Case 2	
element	Bit integer	element	Bit integer
0.96	101.474	9.92E-01	8.96E+01
1.984	214.853	1.98E+00	3.85E+01
3.008	199.56	2.98E+00	1.98E+01
4	52.7211	4.00E+00	1.21E+02
4.992	230.159	4.99E+00	1.42E+02
5.984	6.23583	5.98E+00	5.50E+01
6.976	96.9388	6.98E+00	1.14E+02
8	69.7279	7.97E+00	1.22E+02
8.992	227.324	8.99E+00	2.52E+02
9.984	165.533	1.00E+01	3.17E+01
11.008	120.181	1.10E+01	1.45E+02
12	65.1927	1.20E+01	1.11E+02
12.992	143991	1.30E+01	2.49E+01
13.984	180.272	1.40E+01	6.69E+01
15.008	30.0454	1.50E+01	2.45E+02
16	44.7846	1.60E+01	7.60E+01
17.024	212.018	1.70E+01	8.73E+01
17.984	198.98	1.80E+01	2.45E+02
19.008	198.98	1.90E+01	2.10E+02
20	179.705	2.00E+01	2.22E+02

Table 5. Case 3 and case 4 analysis of key security

Case 3		Case 4	
element	Bit integer	element	Bit integer
1.02E+00	1.17E+02	9.92E-01	8.96E+01
2.01E+00	8.62E+01	1.98E+00	3.85E+01
3.02E+00	4.02E+02	3.03E+00	1.98E+01
4.03E+00	1.46E+02	4.05E+00	1.21E+02
4.98E+00	9.86E+01	4.99E+00	1.42E+02
5.96E+00	4.81E+01	5.98E+00	5.50E+01
6.98E+00	6.63E+01	6.98E+00	1.14E+02
8.00E+00	7.65E+01	8.00E+00	1.22E+02
8.99E+00	3.97E+01	8.96E+00	2.52E+02
9.98E+00	9.52E+01	9.98E+00	3.17E+01
1.10E+01	2.18E+02	1.10E+01	1.45E+02
1.20E+01	2.04E+02	1.22E+01	1.11E+02
1.30E+01	3.57E+01	1.30E+01	2.49E+01
1.46E+01	8.90E+01	1.40E+01	6.69E+01
1.50E+01	9.98E+01	1.50E+01	2.45E+02
1.60E+01	1.97E+02	1.60E+01	7.60E+01
1.70E+01	1.39E+02	1.70E+01	8.73E+01
1.80E+01	4.65E+01	1.80E+01	2.45E+02
1.90E+01	9.58E+01	1.90E+01	2.10E+02
2.00E+01	5.33E+01	2.00E+01	2.22E+02

Figures 4-7, explain four cases of key sensitivity, the first few bits have closely valued so these values give the same shape, after these bits note the values will change by the proposed algorithm, which is high security of key sensitivity. In order to increase the security increase elements. The more elements, the greater the number of bits, which results in greater data security, and the more elements, the more random, providing a stronger way to encryption of the data.

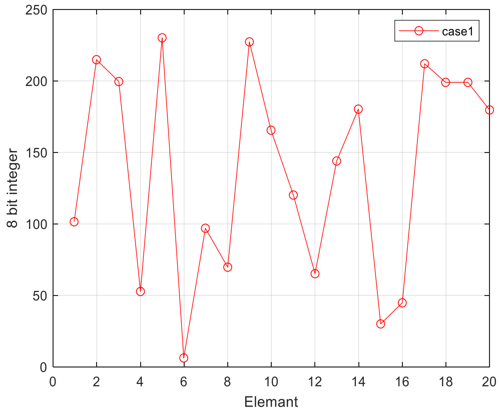

Figure 4. Case 1 of key sensitivity analysis

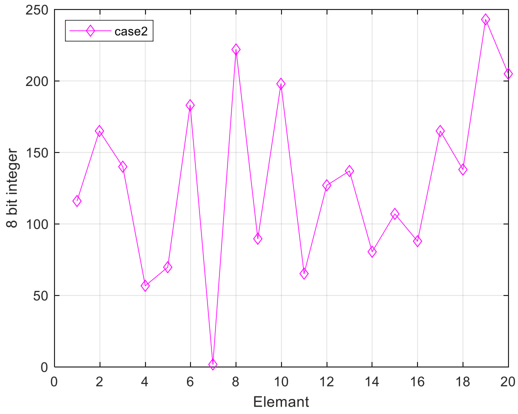

Figure 5. Case 2 of key sensitivity analysis

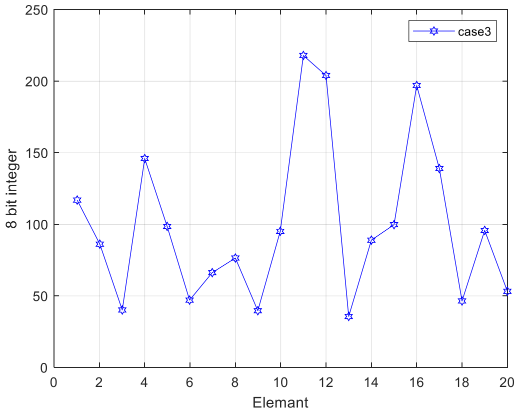

Figure 6. Case 3 of key sensitivity analysis

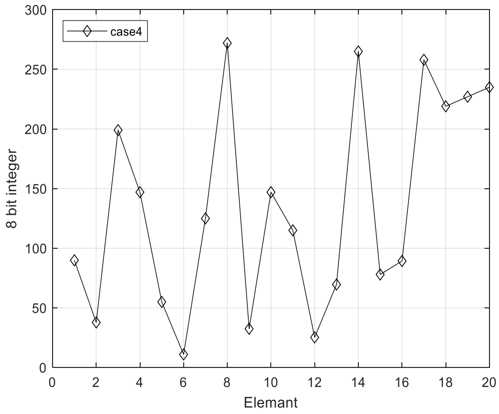

Figure 7. Case 4 of key sensitivity analysis

5. STATISTICAL TESTS

A statistical test is providing a technique for taking accuracy decisions about a process. The purpose is to limit if whether there are sufficient proofs to "refuse" a guess or assumption about the process. A called this assumption is the null supposition [22-24]. A pseudo-random number generators with chaotic system are used to create new developed algorithm to issue security which result random, so randomness a sequence of random bit can be given exegesis for the outcome of the fluctuations of coin an equitable “fair” with sides it which are categorized “0” and “1,” and each side possess precisely a probability ½ of making a “0” or “1” [25]. Moreover, the outcome of preceding coin does not affect on coin faces in future due to the fluctuations are separated of each other, these are required many statistically tests which designed to discover the randomly features [26-28]. To execute these tests of generate pseudo-random number, many options exist but NIST suite is representing the perfectly choose which it convenient to PRNG algorithm. A NIST suite consists 16 tests, which is depending to platform or devices to construct random number generator or cryptographic pseudo lead to develop a long binary sequences randomness [29-31]. This test can be classified to two categories as test of parameterized and Non-parameterized:

a) The Non-parameterized
- The frequency test is generally on proportion of the zeros and ones inside the entire sequence. It must be the ratio of the zeros to ones in a specific sequence is as expected of a real randomized sequence proximately, which proximity equal to ½.
- The cumulative sums test: The test of cumulative sums is determining the sequence partial sum that is very small or very large of cumulative sum of randomness sequence, which is expected. The sequence is adjusted digital [1, +1].
- Run test: this test is aimed to known the runs of 1s and 0s frequencies of different lengths if would be within randomness range.

- The ones longest run in a block test: it is focus on the blocks of ones ’longest run in M-bit.
- The Test of discrete fourier transform (DFTT): The aim of this test is detecting the periodic characteristics like the repeated nearness of maximum modes in a tested so it is on maximum altitude in sequence of DFT.
- The test of binary matrix rank: this test is applied to know if the string n-bit has repeated models via completely sequence it. The concatenation of n-bit is sequentially split into N disassemble lumps and it is attempt to showing linear dependence among its substring’s constant length substrings of each block.
- The test of Lempel-Ziv compression: this test focus on varian the models of inside the sequence of the accumulative number of different models inside the sequence. It determines the scope a its sequence during test which can be compressed it.
- The test Random Excursions purpose to see if the visits number to sums of a specific accumulative situation inside a period falls into a classify that is random sequence expected.

b) The Parameterized Tests
- Tests of frequency inside a block: it is testing the ratio of ones in n-bit of the series which determine if one’s frequency is close to (1/2) M, so this test aims to ensure that the frequencies 1 and 0 are distributed evenly across the entire n-bit sequence.
- The test of Maurer’s universal: this test examines the number of bits between identical models which is based on length of pressed sequence. The main purpose is ensuring the capability to press the information without losing for good data.
- The approximate entropy test: the test is focused on interference model for n-bits via entire sequence. In addition, it is comparing between two neighbouring frequencies or sequent block length versus predictable results for randomized sequence.
- The non-overlapping template matching test: this one concentrate on form matching in non-verlapping method, its appearance for occurrences of previously determined bit-chain and to know if the occurrences numbers are inside the statistical boundary of a sequence under the randomness supposition. It is employing n-bit window is to search for particular m-bit model. If the model is found, the window is reset to the next bit of the found model whilst the window slides in magnitude one-bit position when the model is not found.
- The overlapping template matching test: it is focusing on the occurrence frequency of previously determined chain objectives. The interference and non-interference template identical tests are utilized an n-bit at searching for a specific bit model. The difference between interference and non-interference models are that in a state which a model is found, the test of overlapping model will slide one bit only and the search is continue.
- The serial test: the main important of the serial test is determine the potential interference frequency for all n-bit models via the complete sequence, and it depend on the variation of each of all counts which one is examine to know if the sequence can be random or not.
- The linear complexity test: - this test examines the length of LFSR (linear feedback shift register) and locate if the sequence of bit from the LFSR length is random or not. The sequence of bit is random from that a longer LFSR is obtained, while the shorter LFSR refer to non-randomness.

The base of NIST statistical tests is depend on premise testing completely as other statistical tests. A premise test is an operation of calculating the plausibility range for the merits of a particular population. The test of assumption in the current scenario is the definition of the specific sequence randomness of zeros and ones. A pertinent static randomness is utilized to determine the premise tests, which accept or reject. The possible values are distributed for this static when the randomness is assumed.

Mathematical techniques are utilized to define the indication allocation of theoretical of statistic under the null premise. By the generator of random number has given opportunity of producing sequence less randomness than current sequence, which determine by the p-value. The p-value of a test is 1, the randomness is perfect whilst p-value of zero is explain the sequence non-randomness. The passing ratio of a test is based on samples number of sequences of bit of a PRNG generator. The numerical analysis of the suggested PRBG include 3000 various series and each sequence possess 1,000,000 bits. The bit sequence of sample generated by PRNG are examined by NIST tests. A (alfa) is represented significance level of the test. The sequence is see randomized when the p-value is bigger or equal to α and accept the null premise, while the null premise is unacceptable and the sequence see non-randomized if the p-value is below α. An idealistic level of significance α is elected during the duration of (0.001 - 0.01). If ($\alpha = 0.01$), it meaning that (1%) of sequences is unacceptable; whilst the sequence is certainly random at ($\alpha \geq 0.01$). The NIST tests above-mentioned appears convergent results of the most researches. Consequently, at apply these tests; the results of NIST tests appear identical with previously researches.

6. CONCLUSION

This work is proposed algorithm using a pseudorandom number generator (PRNG) with logistic and tent of chaotic maps with high encryption. In addition, the operations of XOR and substitution were utilized through the number's generation. It was enhanced the security of pseudorandom number sequence in addition to minimize the interconnection between the values of two adjacent chaotic cases. The NIST suit were utilized to strictly test the sequences generated depend on the suggested system. The results were demonstrated that carry out the proposed PRNG was properly statistically. Nevertheless, the proposed algorithm of security was confirmed that the realization all the PRNG of required achievements and well randomness features against various attacks. The closely values of first few bits have given the same shape, then these bits note the values will be change by the proposed algorithm of new system, which is top security of key sensitivity. To increase the security increase elements.

REFERENCES

[1] W. K. Ahmed, M. N. Mohammed. and N. Sulaiman. "An Enhanced Encryption Algorithm for DB protection Based on Dynamic Key and Reverse String". *J. Eng. Appl. Sci.* vol. 12, no. 5, pp. 1186-1191, 2017.

[2] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system*", Chaos, Solitons and Fractals,* vol. 40, no. 5, pp. 2509-2519, 2009.

[3] Akhshani, A., *et-al*. "Pseudo random number generator based on quantum chaotic map". *Commun. Nonlinear Sci. Numer. Simul.,* vol. 19, no. 1, pp. 101-111, 2014.

[4] Marton, Kinga, A. Suciu, and I. Ignat, "Randomness in Digital Cryptography: A survey", *Romanian Journal of Information Science and Technology*, vol. 13, no. 3, pp. 219-240 13, 2010.

[5] X Huang, *et-al* "A New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics". *Hindawi Complexity,* 2019.

[6] Y. Zhao, *et-al* "A Self-perturbed Pseudo-random Sequence Generator Based on Hyper-chaos", *Chaos, Solitons & Fractals: X,* vol. 4, p. 100023, 2019.

[7] S. Jafari, J. C. Sprott, M. Molaie. "A Simple Chaotic Flow with a Plane of Equilibria. " *International Journal of Bifurcation and Chaos*", vol. 26, no. 6, p. 1650098, 2016.

[8] X. Zhu 1 and Wei-Shih Du. "A New Family of Chaotic Systems with Different Closed Curve Equilibrium*". Mathematics,* vol. 7, no. 1, p. 94, 2019.

[9] M. A. Murillo-Escobar, *et-al.* "A novel pseudorandom number generator based on pseudo randomly enhanced logistic map". *Nonlinear Dyn*, vol. 87, no. 1, pp. 407-425, 2017.

[10] Li, Chunhu and Luo, Guangchun and Qin, Ke and Li, C. "An image encryption scheme based on chaotic tent map". *Nonlinear Dyn.* vol. 87, no. 1, pp. 127-133, 2017.

[11] López, A. B. Orue., et al. "Trident, A new pseudo random number generator based on coupled chaotic maps". *3rd Int. Workshop on Computational Intelligence in Security for Information Systems (CISIS'10), Leon (Spain)*, pp. 183-190, 2010.

[12] Volodymyr, Lynnyk, N. Sakamoto, and S. Colikovisky. "Pseudo random number generator based on generalized Lorenz chaotic system". *IFAC-Papers OnLine*, vol. 48, no. 18, pp. 257-261, 2015.

[13] M. A. Therib, *et-al*., "Smart Digital Bi-Directional Visitors Counter Based on IoT", J. Phys.: *Conf. Ser*., vol. 1530, no. 1, p. 012018, 2020.

[14] E. Yavuz, et al., "A chaos-based image encryption algorithm with simple logical functions". *Comput. Electr. Eng.* vol. 54, pp. 471-483, 2016.

[15] Machkour, M., Saaidi, A. & Benmaati, M. L. "A Novel Image Encryption Algorithm Based on the Two-Dimensional Logistic Map and the Latin Square Image Cipher". *3D Res*., vol. 6, no. 4, p. 36, 2015.

[16] H. Xu, X. Tong, and X. Meng, "An efficient chaos pseudo-random number generator applied to video encryption". *Opt. - Int. J. Light Electron Opt.,* vol. 127, no. 20, pp. 9305-9319, 2016.

[17] N. K. Pareek, V. Patidar. and K. K. Sud, "A Random Bit Generator Using Chaotic Maps". *International Journal of Network Security*, vol. 10, no. 1, pp. 32-38, 2010.

[18] M. Krim, A. Ali-Pacha, and N. Hadj-Said," New Binary Code Combined with New Chaotic Map and Gold Code to Ameliorate the Quality of the Transmission", *Indonesian Journal of Electrical Engineering and Computer Science* vol. 5, no. 1, pp. 166-180, 2017.

[19] M. J. Mohsin, H. A. Marzog, and M. A. Therib, "Enhancement throughput and increase security of image transmitted over wireless network using (DNC)" *IOP Conf. Series: Materials Science and Engineering,* vol. 928, no. 2, p. 022078, 2020.

[20] N. A. N. Hashim, et-al., "Memristor based ring oscillators true random number generator with different window functions for applications in cryptography", *Indonesian Journal of Electrical Engineering and Computer Science* vol. 14, no. 1, pp. 201-209, 2019.

[21] A. M. Radhi," Risk assessment optimization for decision support using intelligent model based on fuzzy inference renewable rules*", Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 2, pp. 1028-1035, 2020.

[22] M. Francois, T. Grosges, D. Barchiesi, and R. Erra, "A New Pseudo-Random Number Generator Based on Two Chaotic Maps". *Informatica*, vol. 24, no. 2, pp. 181-197, 2013.

[23] A. A Sabri and M. J Mohsin " A New Algorithm for a Steganography System", *Engineering and Technology*, vol. 33, no. 8, pp. 1955-1970, 2015.

[24] X. Y. Wang and X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration". *Nonlinear Dyn*. vol. 70, no. 2, pp. 1589-1592, 2012.

[25] M. M. A. Zahra, *et-al,* " Artificial intelligent smart home automation with secured camera management-based GSM, cloud computing and Arduino". *Periodicals of Engineering and Natural Science*, vol. 8, no. 4, pp. 2160-2168, 2020.

[26] Y. Wang, et al., "A pseudorandom number generator based on piecewise logistic map", *Nonlinear Dyn*. vol. 83, no. 4, pp. 2373-2391, 2016.

[27] M. A. Therib, *et-al*, “Medical remotely caring with COVID-19 virus infected people using optimized wireless arm tracing system”, *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 6, pp. 2886-2893, 2020.

[28] M. García-Martínez and E. Campos-Cantón, “Pseudo-random bit generator based on multi-modal maps, *Nonlinear Dyn*, vol. 82, no. 4, pp. 2119-2131, 2015. https://doi.org/10.1007/s11071-015-2303-y.

[29] M. K. Rafsanjani and H. Fatamidokht, "A Survey on Algorithms Based on Bee Swarms for Ad Hoc Networks", *Walailak J. Sci & tech Information Technology*, vol. 12, no. 1, pp. 21-26, 2015.

[30] M. A. Therib, *et-al*, “Design a Suitable Optimized Low Pass FIR Filter for Ultrasonic Signal”, *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 928, no. 2, p. 022149, 2020.

[31] A. Rukhin. et.al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications". *Special Publication 800-22 Revision 1a. Lawrence E Bassham III,* 2001.

BIOGRAPHIES OF AUTHORS

Heyam A. Marzog, Assistant Lecturer at Engineering Technical College/Al-Njaf-Al-Furat Al-Awsat Technical University, Iraq. She was born was born in 1978 in Iraq. She obtained her Bachelor's degree in communication Engineering from technical college of Najaf Al-Furat al-Awsat University in 2002, and the MSc degree in Electrical Engineering (communication system) in 2012 from the University of Tenaga National in Malaysia. Her fields of interest include the security and saving energy of Wireless Communication Networks and their application to Energy Management Systems, Control and Optimization. Also, her current field of interest internet of things.

Marwa Jalil Mohsin, Bachelor’s degree in communication technical engineering, Al- Furat alawset University/Najaf technical college/communication technical engineering department 2003-2006. Master’s degree in communication engineering, University of technology /electrical engineering department Baghdad 2012-2015. PhD student in communication and electronic engineering, university of Babylon/electrical engineering department. She is un instructor in Najaf technical college from 2007 till now. The research field in image processing, digital communication, wireless communication and digital signal processing.

Mohammed Azher Therib, Assistant Lecturer at Engineering Technical College/Al-Njaf-Al-Furat Al-Awsat Technical University, Iraq. He was born in 1988 in Iraq. He obtained his bachelor's B.Sc. degree in Electrical Engineering from Babylon University, Iraq in 2009-2010. Then, he obtained his Master M.Sc. degree in Electrical Engineering/Electronic and Communications from Electrical Engineering Department in Babylon University at 2013-2014. His fields of interest include Electronic, Power Electronics, Coding, Security, IoT, Control, Optimization and Wireless Communications.