ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

Performance Analysis of Random NumberGenerators in Cryptographic Algorithms

Anusuya K V[1] and Navindran N[2]

[1] Associate Professor, ECE, PSG College of Technology, Coimbatore, India
[2] PG Scholar, Department of ECE, PSG College of Technology, Coimbatore, India

Abstract— Random Numbers are applied in Cryptography for padding of messages, key generation, and initialization of vectors. The algorithms that lack randomness can cause serious damage to the cryptographic protocols that lead attackers to exploit vulnerabilities. Hence, it is important to design a Pseudo-Random Number Generator (PRNG) for single-time pad key Generation and authentication protocol. Moreover, the random numbers used in cryptographic algorithms should not be predictable and reproductive, and they must resist the attacker from learning the previous or subsequent values. This paper aims to analyze the comparative performance of Random number generators such as Logistic system, Tent system, and Compound Logistic-Tent system concerning the quality parameters such as Histogram, Scattering plot, Avalanche effect, Shannon's information entropy, Time analysis, and Randomness test.

Keywords— Key Generation; Logistic system; performance analysis; Random Number generation; Tent system.

1. INTRODUCTION

Random numbers are widely used in gaming, security applications, numerical analysis, and in the simulation of network protocols. The good quality and high-performance random number generators yield increasing interest from the research community [1]. Pseudorandom sequence with good performance plays an important role in the security of the cryptosystem [2]. The safety of a random number generator is based on the assumption that the future random numbers which are produced by the PRNGs should be unpredictable. In cryptography, the Random number generators are considered to be the only entropy sources in the system [10]. In General, RNGs are classified into two categories namely,

- Pseudo-Random Number Generator (PRNG)
- True Random Number Generator (TRNG)

The PRNG is a generator that uses a mathematical formula to extract random numbers by using some initial value or seed. The random sequence is generated using the software methods [7]. The TRNG is a Generator that uses some unpredictable physical phenomena to extract random numbers. Physical phenomena which are used for the generation of true random numbers are jitter, atmospheric noise, radiation, etc. TRNG resources need some costly hardware and some of them are unrealistic [9].

This paper aims to analyze the performance of PRNG using a chaotic system such as the Logistic system, Tent system, and the new compound Logistic-Tent system. The advantage of the chaotic system includes its high sensitivity for initial conditions, leading to a very difficult prediction of random sequences. Hence, the chaotic systems are more suitable for symmetric and asymmetric cryptographic applications [2].

2. RELATED WORK

In paper [1], the author proposed a new pseudo-random number generator algorithm based on chaotic maps named as Logistic system and tent system. The proposed compound Logistic-Tent system yields wider chaotic behavior and has better chaotic features compared to Logistic and tent systems. The author performed several statistical tests such as histogram, sensitivity, and information entropy analysis. The paper [2] demonstrates the concept of generating random numbers from chaotic jerk system through periodic sampling of the system with analog to digital conversion. The jerk equation shows better dynamic complexity in a compact form that permits its usage as a source of random numbers for encryption algorithms.

In paper [3], the author proposed a true random number generator which is a cascade circuit. From the theoretical research and experiments, it is found that this algorithm is well suited for the hidden transfer of keys. These generators are built in the form of a cascade scheme based on adders and the author discussed the procedure for the hidden transfer of keys. In paper [4], the author designed a cryptographically secured pseudo-random number generator that involves a permutation of the internal state. The author has performed several statistical tests and with the permutation, proved that the statistical quality is increasing.

In paper [5], the author proposed the concept of generating the pseudo-random numbers from the Hash function. Most of the modern random number generators use noisy channels such as disk seek time and CPU temperature. Instead of that, the Hash function can produce pseudo-random numbers that demand limited hardware only.

3. PROPOSED WORK

A chaotic system is a dynamic and nonlinear system that performs random and unpredictable behaviors in time. It is a dynamic system whose random states of disorder and irregularities are governed by underlying patterns and deterministic laws that are very sensitive to initial conditions. For a small change in initial conditions, long-term prediction is impossible, and the system produces the most diverging outcomes.

3.1 Logistic system

The logistic function is based on a differential equation that treats time as a continuous function. The Logistic map uses a nonlinear difference equation that treats time as discrete time steps. It maps the value of the population at any time step to its value at the next time step [1]. Hence, it is called a Logistic map.

$$X_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

Equation (1) defines the dynamics of the system. Here, μ is the system parameter and takes the value from 0 to 4. x_n takes the value between 0 and 1.

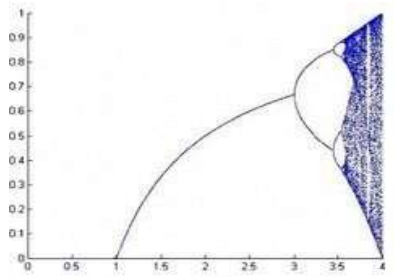

Fig 1: Bifurcation diagram of Logistic system

The bifurcation diagram shown in figure 1 has the values visited or approached asymptotically (fixed points or chaotic attractors) as a function of bifurcation parameter for dynamic systems. Here, stable values are represented with a solid line, and unstable values are represented with a dotted line. The X-axis represents System parameter values, Y-axis represents Lyapunov exponent values.

3.2 Tent System

One of the famous chaotic systems is the tent map. The Bifurcation diagram shown in figure2 looks like a tent [1]. The equation 2and 3 defines the tent system.

$$x_{n+1} = (\mu/2) \times (x_n), \quad \text{if } x_n < 0.5 \quad (2)$$

$$x_{n+1} = \mu/2 \times (1 - x_n), \quad \text{if } x_n \geq 0.5 \quad (3)$$

μ is the system parameter and takes the value from 0 to 4. When the system parameter is between 2 and 4, the tent system arises to a chaotic phenomenon. The disadvantage of the Tent system is the narrow parameter range of chaos. Output values have a pattern of uneven distribution.

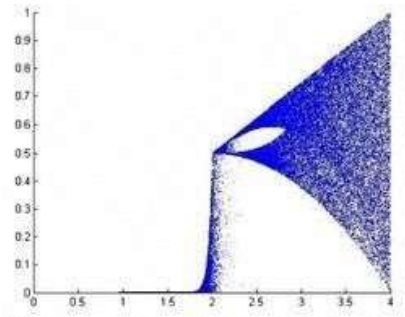

Fig 2: Bifurcation diagram of the Tent system

3.3 Logistic-Tent System

The performance of the chaotic system is improved by the compound Logistic-Tent system [1]. The iterative equation of the Logistic-tent system is given in equations 4 and 5.

$$x_{n+1} = \mu \times x_n \times (1 - x_n) + (4 - \mu) / 2 \times x_n \quad \text{if } x_n < 0.5 \quad (4)$$

$$x_{n+1} = \mu \times x_n \times (1 - x_n) + (4 - \mu) / 2 \times (1 - x_n) \quad \text{if } x_n \geq 0.5 \quad (5)$$

The advantage of the compound Logistic-Tent system is that the chaotic parameter range is wider than the Logistic map and tent map. The output values have a pattern of even distribution.

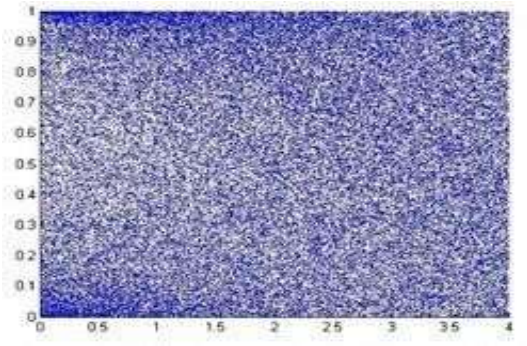

Fig 3: Bifurcation diagram of Logistic-Tent system

4. RESULTS AND ANALYSIS

The PRNG algorithms – Logistic system, Tent system and Combo Logistic – Tent systems are analyzed using the following metrics to obtain their comparative performance.

4.1 Histogram analysis

The histogram represents the numerical distribution characteristics of an integer sequence. The randomness of the sequence is greater for uniform numerical distribution of the sequence [1]. To test the statistical distribution characteristics of sequence Y, the secret key values are set as $x0 = 0.231$, $\mu = 2.371$, $d = 0.001$, $L = 65536$, and $N0 = 500$. The horizontal ordinate represents the possible integer value in sequence Y, and the longitudinal coordinates represent the number of occurrences of each value in the sequence Y. Figures 4,5 and 6 show the uniformity of the numerical distribution in the Y sequence, indicating that the sequence Y is pseudo-random for logistic, tent and Combo systems.

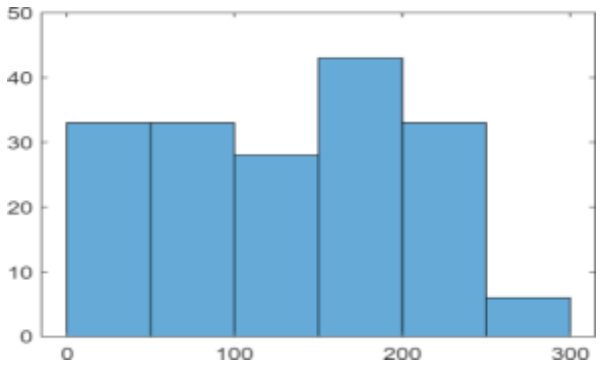

Fig 4: Histogram of Logistic system

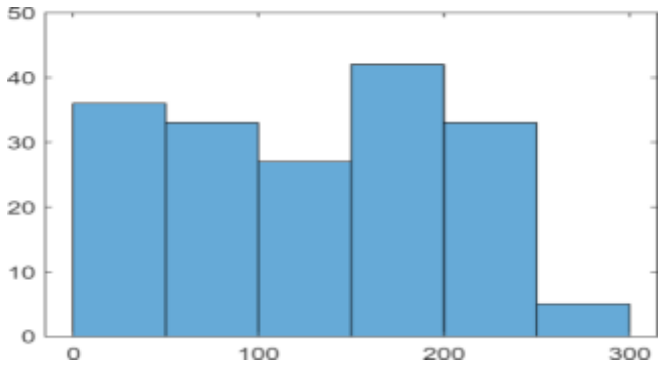

Fig 5: Histogram of Tent System

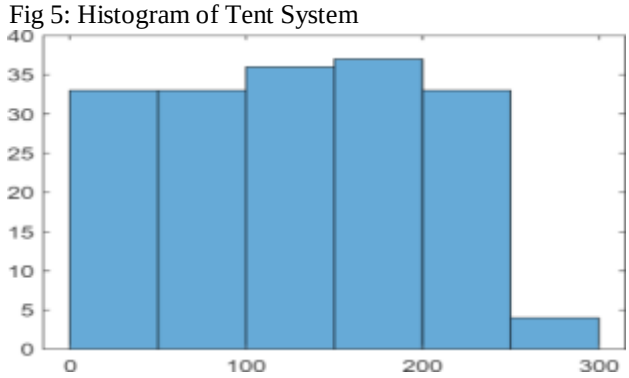

Fig 6: Histogram of Logistic-Tent system

4.2 Scatter Plot

A scatter plot or scatter graph uses Cartesian coordinates to display values for two variables for a set of data. One additional variable can be displayed if the points are coded [8]. The data are represented as a collection ofpoints, each having the value of one variable determining the position on the X-axis and the value of the other variable determining the position on the Y-axis.

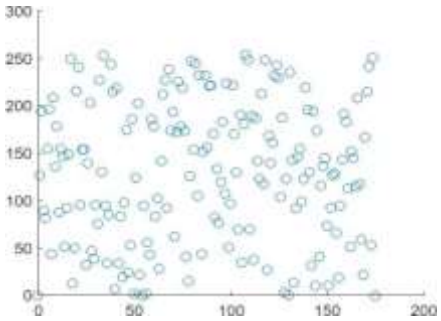

Fig 7: Scatter plot of Logistic system

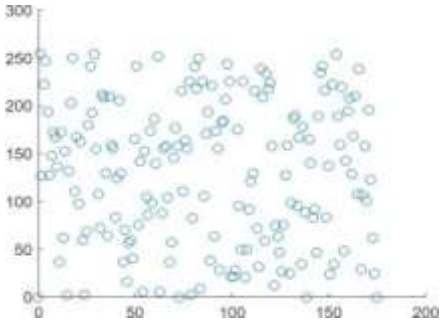

Fig 8: Scatter plot of the Tent system

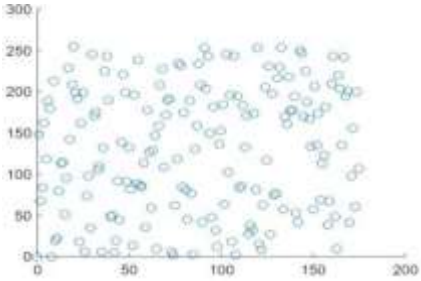

Fig 9: Scatter plot of Logistic-tent system

From Figures 7, 8 and 9, it is very clear that the random values generatedare taking the values from 0-255. Since each random number isof type of 8 bit unsigned integer (uint8).

4.3 Information Entropy

Information entropy can measure the uncertainty of any information source [1]. Here, the entropy represents the uncertainty of the generated sequence. To determine the information entropy of array Y, X0 value is set to 0.5 and the entropy values of the sequences which are generated from Logistic, tent, and the compound logistic tent are given in table1.

Table1. Entropy Analysis

Algorithm	Entropy Value
Logistic system	5.9213
Tent system	6.3811
Logistic – tent system	7.8562

The Logistic-Tent system alone yields a better entropy value which is close to 8, compared to the other two algorithms which show the uncertainty in generated random sequence.

4.4 Time Analysis

In real-time implementation, the amount of time required to generate the sequence of the random number is very important. The time taken by three algorithms to generate the same count of the random number is given in Table 2.

Table2. Time Analysis

Algorithm	**Time (ms)**
Logistic system	1.247
Tent system	1.514
Logistic – tent system	1.897

4.5 Avalanche effect

The Avalanche effect is one of the desirable properties in cryptography, where the output changes significantly for the slight change in input. A good cryptographic algorithm should satisfy the avalanche effect at greater than 50%. The effect ensures the difficulty for an intruder to predict information through statistical analysis. The results for each algorithm are shown in table 3.

Table 3. Avalanche Effect Analysis

Algorithm	Avalancheeffect (%)
Logistic system	42.23
Tent system	56.98
Logistic – tent system	71.34

The Logistic-Tent and the Tent system yields the more than 50% Avalanche effect value

4.6 Randomness test

A randomness test in data evaluation is a test used to analyze the distribution of data set to determine its description as random (Patternless) or not. If a P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A P-value of zero indicates that the sequence appears to be completely non-random [6] and the results are shown in table 4.

Algorithm	**P-value**
Logistic system	0.5965
Tent system	0.5345
Logistic – tent system	0.8203

Table 4. Randomness Test Analysis

4.7 Inference

The Logistic system, Tent system, Logistic-Tent system are simulated and their performance is analyzed for parameters such as Histogram analysis, Scatter plot, Information entropy, Time analysis, Avalanche effect, and Randomness test. From the obtained results, the Logistic – Tent system yields better performance. The entropy value of the Logistic-Tent system is 7.8562 and is close to 8. It is considered to be more random. However, the Logistic and tent systems have their entropy valuesas 5.9213, 6.1831 respectively.

The avalanche effect of the Logistic tent is also greater than 50%, The P-value for the Logistic-Tent system is close to 1. But, the disadvantage of the Logistic-Tent system is that the time taken to generate the sequence is slightly greater than the Logistic andTent system.

5. CONCLUSION

The Performance analysis of the Logistic system, Tent system, and the compound Logistic tent system is performed using MATLAB 2020b. The obtained results are presented in the form of plots and tables for comparison. Based on the obtained results the Logistic - Tent system yields better performance for entropy, Avalanche effect, Randomness test, and Histogram plot. As the randomness of the sequence is greater compared to other systems, it is well suited for real-time implementation. The security of the protocol is ensured for the Logistic-Tent system used as a source of Random number sequence. It is very difficult for an intruder to predict the previous or subsequent values in the Random number sequence. This work can be further analyzed under real-time applications.

REFERENCES

[1] Congxu Zhu, Shuai Li, Qin Lu, "Pseudo-random Number Sequence Generator Based on Chaotic Logistic-Tent System", 2nd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), (pp. 547-551). IEEE,2019.

[2] R. Chase Harrison, R. Chase Harrison, Ariel N. Ramsey, "A True Random Number Generator based on a Chaotic Jerk System" IEEE, 2019.

[3] Rustam Latypov, Evgeni Stolov, "True Random Generators and Hidden Transfer of Keys", International Russian Automation Conference (RusAutoCon), IEEE, 2019.

[4] Benjamin Williams, Robert E. Hiromoto, Albert Carlson, "A Design For Cryptographically Secure Pseudo-Random Number Generator", 10th International Conference on Intelligent Data Acquisition And Advanced Computing System: Technology And Application (IDAACS), (pp. 864-869). IEEE,2019.

[5] Kamana Sai Charan, Harsha Vardhan Nakkina, B. R. Chandavarkar, "Generation of Symmetric Key Using Randomness of Hash Function", 11th International Conference On Computing Communication and Networking Technologies (ICCNT), IEEE, 2020.

[6] Mandakini Kadam, Saroja V. Siddamal, Shripadraj Annigeri, "Design and Implementation of chaotic nondeterministic random seed-based Hybrid True Random Number Generator", International Symposium on VLSI Design and Test (VDAT), IEEE,2020.

[7] M. Aljohani, I. Ahmad, M. Basheri, M. Alassafi, " Performance Analysis of Cryptographic Pseudorandom Number Generators", (vol. 7, pp. 39794 – 39805) IEEE,2019

[8] Thomas, A. A, Paul V. "Nested Multiplicative Random Number Generator an Efficient Tool for Increasing Security in Social Networking", International Conference on Computer, Communication, and Signal Processing (ICCCSP), IEEE, 2020.

[9] Gergely, A. M., & Crainicu, B. "A succinct survey on (Pseudo)-random number generators from a cryptographic perspective". International Symposium on Digital Forensic and Security (ISDFS).IEEE, 2017.

[10] Chugunkov, I. V., Gulyaev, V. A., Baranova, E. A., & Chugunkov, V.
"Method for Improving the Statistical Properties of Pseudo-random Number Generators". IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), IEEE, 2019.