Randomness evaluation of coupled chaotic maps via NIST tests: A comparative study

Hadjer Bourekouche
LIST Laboratory, Department Engineering of Electrical Systems, Faculty of Technology
University M'Hamed Bougara of Boumerdes
35000 Boumerdes, Algeria
h.bourekouche@univ-boumerdes.dz

Samia Belkacem
LIMOSE Laboratory, Department Engineering of Electrical Systems, Faculty of Technology
University M'Hamed Bougara of Boumerdes
35000 Boumerdes, Algeria
s.belkacem@univ-boumerdes.dz

Noureddine Messaoudi
LIST Laboratory, Department Engineering of Electrical Systems, Faculty of Technology
University M'Hamed Bougara of Boumerdes
35000 Boumerdes, Algeria
n.messaoudi@univ-boumerdes.dz

***Abstract*— A vital requirement for any random number generator based on chaos is to ensure that the generated sequence always benefits of a significant level of randomness. It is critical to examine such sequences by means of Lyapunov exponents, bifur-cation diagrams, or other tests in order to accurately select the parameters of the dynamic system. However, the sequence's randomness quality varies depending on the generator's design and must be examined in different ways. Therefore, we argue to use the National Institute of Standards and Technology (NIST) suite tests to evaluate and compare the randomness properties of two coupled systems found in existing literature: the logistic-sine system (LSS) and the logistic-tent system (LTS). The results reveal that the LSS has much superior statistical features in terms of randomness than the LTS in the range [3.1–4]. This conclusion will substantially affect the selection of the perfect chaotic map to create sequences of keys that match the requirements of cryptography applications.**

Keywords—Random number generator, logistic-tent system, logistic-sine system, NIST, randomness.

I. INTRODUCTION

Random number generators (RNGs) that use chaotic systems (CSs) are fascinating because they provide high throughput data without the requirement for statistical post-processing and may be implemented as electrical circuits using very simple hardware [1]. In reality, using weak random values enables an opponent to break the whole system [2], that's why chaotic sequences have received a lot of interest lately because of their appealing characteristics, including great sensitivity to initial conditions [3]. With the help of this feature, it is possible to create a huge number of sequences with unique correlation properties and unique control pa-rameters, such as beginning conditions and bifurcation parameters [4].

The basic structure and ease of use of typical 1D chaotic maps are highlighted [5], however, they struggle with three major problems, including the limited or dis-continuous range of chaotic behaviors, the sensitivity of low-computation-cost analysis utilizing iteration and correlation functions, and the non-uniform data distribution of chaotic output sequences [6]. Therefore, it is necessary to create new chaotic systems with improved chaotic performance.

For instance, a nonlinear mixture of different 1D chaotic maps, notably the Logistic-Sine System (LSS) and the Logistic-Tent System (LTS), is proposed by Zhou et al. [6] to larger the chaotic ranges and strengthen the chaotic behavior com-pared with their seed maps. These qualities grabbed the attention of many re-searchers, who tried to use them in cryptography applications. Therefore, multiple tests are employed to quantify and evaluate its chaotic behavior, as well as the bi-furcation diagram, Lyapunov exponent, phase portrait, Poincare map, and various entropy metrics.

In [7], the 0-1 test and the three state test are used to provide a thorough investigation of the behavior of the LSS and LTS (3ST). While Zhou et al. [6] have proved that the LSS and LTS exhibit a continuous chaotic behavior in the range $r \in (0,4]$, Muthu et al. [7] portray stronger and weaker regions of chaos, with some regions exhibiting quasiperiodic behavior. In this paper, we aim to demonstrate that the map has the most chaotic nature and is nominated to produce high quality randomness; thus, we analyze and compare the randomness properties of the generated sequences by the LSS and the LTS using the NIST test suite SP 800-22.

The rest of the paper is structured as follows: in Section II, the dynamic behavior of the LSS and LTS via the bifurcation diagram, the Lyapunov exponent, the 0–1 test, and the 3ST are briefed. In section III, we use the NIST tests to compare and discuss the randomness quality of the two chaotic sequences generated by the LSS and LTS, followed by the conclusion of the work in section IV.

II. ANALYZE OF THE COMPORTEMENT BEHAVIOR OF LSS AND LTS FROM THE LITERATURE

The LSS and LTS are a form of chaotic coupled map that are often employed in image encryption due to the benefits of more advanced dynamical behavior. Numerous tests, such as the bifurcation diagram and the Lyapunov exponents in addition to the 0–1 and 3-ST tests, are used to measure its chaotic behaviors. In this section, we cover the theoretical elements of these tests applied to the LSS and the LTS.

A. *Logistic-sine and the logistic-tent systems*

The logistic-sine system (LSS) and logistic-tent system (LTS) proposed by Zhou et al. [6] whose main structure is illustrated in Fig. 1 are a nonlinear mixing of several 1D chaotic maps: the logistic, tent, and sine maps.

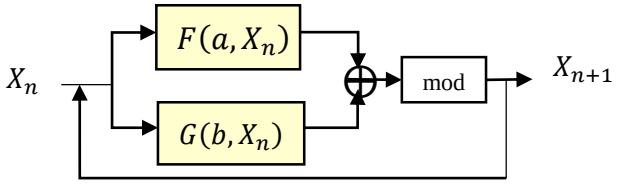


Fig. 1. General structure of 1D combined maps

$$X_{n+1} = \mathcal{F}_{LSS}(r, X_n)$$
$$X_{n+1} = \left[\mathcal{L}(r, X_n) + S\left((4-r), X_n\right)\right] mod 1$$
$$= [rX_n(1-X_n) + (4-r)\sin(\pi X_n)] mod 1 \quad (1)$$
$$r \in (0;\ 4]$$

$$X_{n+1} = G_{LTS}(r, X_n)$$
$$X_{n+1} = \left[\mathcal{L}(r, X_n) + T\left((4-r), X_n\right)\right] mod 1$$
$$= \begin{cases} \left[rX_n(1-X_n) + (4-r)\frac{X_n}{2}\right] \bmod 1 & X_i < 0{,}5 \\ \left[rX_n(1-X_n) + \frac{(4-r)(1-X_n)}{2}\right] \bmod 1 & X_i \geq 0{,}5 \end{cases} \quad (2)$$
$$r \in (0;\ 4]$$

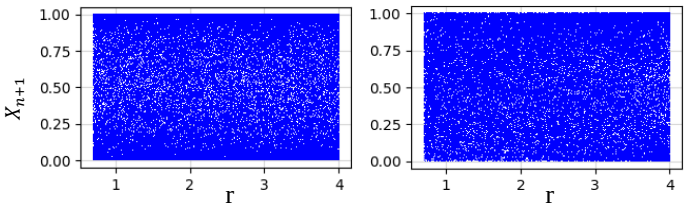
Several tests are available in the literature to emphasize the chaotic behavior of these 1D chaotic systems, including the bifurcation diagram, Lyapunov exponent, 0–1 test, and 3ST.

1) Bifurcation diagram

An essential feature for showing the behavior of chaotic systems is the bifurcation diagram [8] by plotting the output sequences X(n+1) of the chaotic map along with the change of its parameter r [9]. Fig. 2 (a-b) compares the bifurcation diagrams of the LSS and the LTS. From these figures, it is obvious that the chaotic range of the LSS and LTS is inside (0,4], and their bifurcation behavior is evenly dispersed over the full space from 0 to 1. Visually, this finding is not sufficient to compare and determine zones of chaos and regularity; consequently, identifying them using just bifurcation diagrams is difficult. Classification tests are useful allies in dealing with this kind of situation more clearly [10]. In general, the classification by Lyapunov Exponents is the most often used approach in the literature [11].

2) Lyapunov Exponents

When examining the dynamic behavior of chaotic systems, Lyapunov Exponents (LE) as key indicator that examines predictability is used [11]. It is one of the most frequently utilized tests since it is easy to implement when the map f is known explicitly. The Lyapunov Exponent of a discrete time system $X_{n+1} = f(X_n)$ is given by:



(a) (b)

Fig. 2. Bifurcation diagram: (a) logistic-tent system; (b) logistic-sine system

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln|f'(x_i)| \quad (3)$$

Lyapunov Exponents are used to measure chaos. This depends on the sign of Lyapunov exponent λ as follows:

λ > 0, $\{X_n\}$ shows chaotic behavior;

λ < 0, $\{X_n\}$ shows periodic behavior;

λ = 0, a bifurcation occurs.

The Lyapunov Exponent of the LSS and LTS is tested in [6]as shown in Fig. 3. Visually, it is obvious that the LSS and LTS have more complex chaotic qualities as evidenced by their Lyapunov Exponents which are greater than 0 over the whole parameter setting range r, and they consistently behave chaotically in the range r ∈ (0,4] [7].

3) The 0-1 Test

A relatively new method for testing for chaos in deterministic discrete and continuous systems is the 0-1 test [10]. It is used to determine if there is chaos in digital sequences when a mathematical model is not available. Since the test directly applies to time series data and phase space reconstruction is not required, it has been shown to be more favorable than the Lyapunov exponent [7].

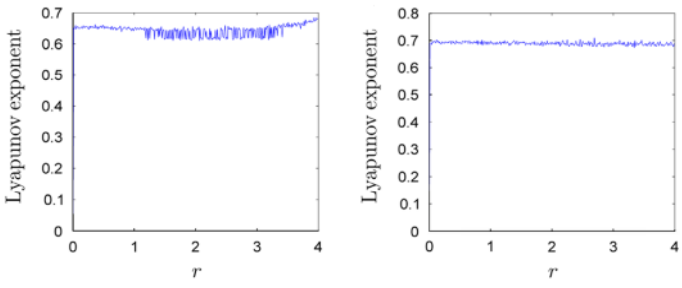
A single real number K and a two-dimensional graph with translation variables p and q make up the test's result. Information about the chaotic sequence may be revealed by the value of K [10]:

$K \approx 0$, Chaotic.

$K \approx 1$, Regular (non-chaotic).

The 0-1 test was experimented by Muthu et al. [7] on the LSS and the LTS with parameters N=5000 and $X_0 = 0.01$.

The K values obtained for the r values are shown in Fig. 4, which demonstrates a slope towards 1 for all values of r in the range [3.1, 4] for the LSS and LTS, demonstrating that these



(a) (b)

Fig. 3. Lyapunov Exponent diagram: (a) logistic-tent system; (b) logistic-sine system [6]

maps do not have a consistently chaotic character over the given range. Furthermore, Muthu et al. [7] demonstrate that the LSS possesses the strongest chaotic nature in most areas of r.

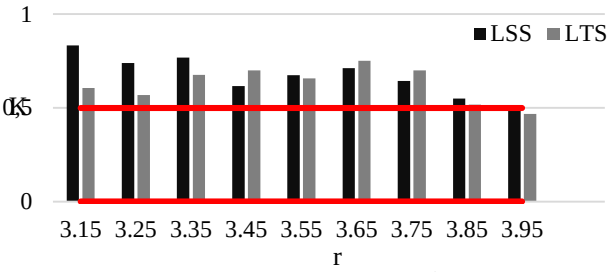


Fig. 4. 0-1 Test results: K values obtained for the r values

TABLE I. Results of behavior comparison of the LSS and LTS using 3ST proved by [7]

r	LSS	LTS
[3,1-3,19]	Chaotic	Quasi-periodic
[3,2-3,29]	Chaotic	Quasi-periodic
[3,3-3,39]	Chaotic	Chaotic
[3,4-3,49]	Quasi-periodic	Chaotic
[3,5-3,59]	Quasi-periodic	Chaotic
[3,6-3,69]	Chaotic	Chaotic
[3,7-3,79]	Quasi-periodic	Chaotic
[3,8-3,89]	Quasi-periodic	Quasi-periodic
[3,9-3,99]	Quasi-periodic	Quasi-periodic

4) 3ST

The 3ST is based on data series pattern analysis. The approach determines whether the dynamics are chaotic or regular by looking at the properties of periodic and quasi-periodic signals. The 3ST looks at how a data series' distribution of system states changes over time [12]. It is aimed at discriminating between the three major dynamics represented by the LE chaotic (> 0), quasi-periodic (<0), and periodic (= 0) dynamics [13].

Muthu et al. [7] performed 3ST on the LSS and LTS in the range r [3.1, 4]. Surprisingly, it clearly differentiates three types of behavior at various r values, periodic, quasi-periodic, and chaotic nature as categories in Table 1, which clearly demonstrate that LTS has a wider chaotic region than other maps. Further, it is demonstrated in [7] that the chaotic behavior of these maps is not uniformly distributed, and certain parts are found to be quasi-periodic in the LSS and LTS. This conclusion refutes what is asserted in [6] that LSS and LTS are chaotic throughout.

III. Experimental Study

In order to further study and compare the random properties of the chaotic sequence formed by the LSS and LTS, the National Institute of Standards and Technology (NIST) is used in this section to identify the areas of randomness and lack of randomness of these two sequences.

A. NIST test of chaotic sequence

In this test, we have expanded our study about the correspondence between the NIST statistical tests for pseudo-random number generators and certain chaotic metrics, including Lyapunov exponents, bifurcation diagrams, the 0-1 Test, and 3ST as a viable technique to verify findings in [6] and [7] .

First, the LSS and LTS systems are utilized to construct the chaotic series X (n+1) with control parameters r in the range (0,4] and X 0= 0.1 using the iterative procedures specified in (1) and (2). The bit length of each sequence n was set to 1000 bits. Then the statistical tests are done using NIST SP 800-22. The 15 sub-tests that make up the NIST test may all be used to assess the randomness of the sequences. By analyzing the sequence's uniformity, the test results largely show the benefits and draw-backs of the pseudo-random sequence [8], in which the probability value (P-value) reflects the regularity of the sequence. The p-value of each subtest is compared to a tester-determined significance threshold (which, for cryptography and in the case of NIST test suite version SP800-22, is commonly set to = 0.01[14]). If the P-value is greater than α, the sequence is random; otherwise, the sequence is not random. The NIST tests may be divided up into four basic categories of testing. These tests include the frequency test from 1–4, repetitive pattern tests from 5–6, pattern matching tests from 7–12, and random walk tests from 13–15 [15].

Since we can't determine which maps exhibit superior randomness simply by doing one test for just one value of r, we have to repeat the test according to r's transitions from 3,15 to 3,95, and then we have calculated the likelihood that a random sequence fails one or more tests for each testing process. Fig. 5 depicts the histogram plot of the uniformity test p-values at three values of r: 3.15, 3.65, and 3.95 for the two maps LSS and LTS. Table 2 shows the results of 15 failed tests at NIST for all r values mentioned.

SS findings exhibit excellent randomness, where all P-values are much over the significance threshold in most r values, expected Binary Matrix Rank Test, Overlap-ping Template Matching Test, and Maurer's Universal Statistical Test. It should be noted that some of these tests are not always appropriate. These tests are run only if the sequence meets certain criteria (for example, passing the frequency test, having more than 500 [16] cycles, and having a sufficient bit-length). However, LSS remains regarded as random even if it fails 3 to 4 tests, according to [16], where data may still be deemed random at the significance level α = 0.01 if they fail fewer than 7 NIST statistical tests.

LTS fails multiple tests when r is in the quasi-periodic range [3.1-3.29] and in the chaotic range [3.4-3.59]. That might be explained by the fact that the randomness of the sequences does not rely only on the chaotic state of the underlying system but also on the post-processing and the generator's design. It is obvious that the randomization qualities of these maps in such a range have exposed major security needs, which make its usage inappropriate for image encryption and demand a solid selection of the chaotic system parameters when employing them.

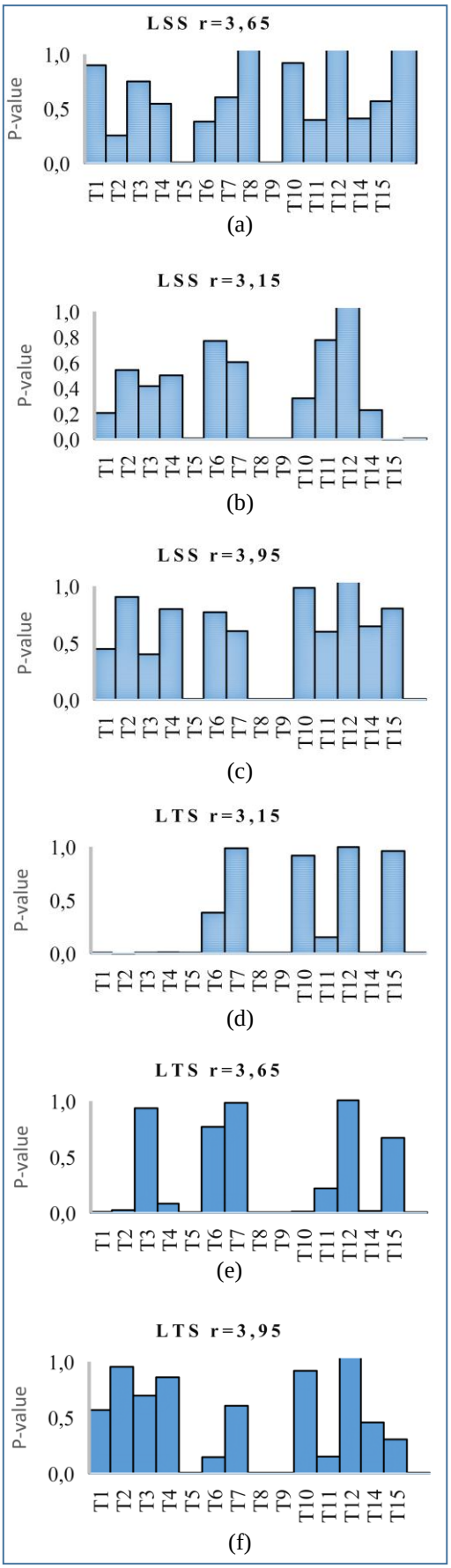


Fig. 5.The P-value of 15 statistical tests, the x axis lists the name of the statistical test in NIST test suit: T1- Frequency, T2- Frequency within a Block,T3- Runs,T4- Longest run of ones, T5- Rank,T6- Spectral,T7- Non-overlapping, T8- Overlapping, T9- Maurer's Universal, T10- Linear complexity, T11- Serial, T12- Approximate Entropy, T13- Cumulative sums, T14- Random Excursions, T15- Random Excursions Variant

TABLE II. Failed tests relatively to 15 tests for r listed values, we have use NR: Not random, R: Random

	r	3,15	3,25	3,35	3,45	3,55	3,65	3,75	3,85	3,95
LSS	Failures	4	3	3	3	3	3	3	3	3
	Conclusion	R	R	R	R	R	R	R	R	R
LTS	Failures	8	7	3	8	7	4	6	3	3
	Conclusion	NR	NR	R	NR	NR	R	R	R	R

Finally, the results reveal a strong relationship between the NIST tests and the chaotic metrics described in Part II. The seeds for which the maps are chaotic, are the seeds that determine a low number of failed NIST tests, which demonstrates the notion that a required criterion for a successful pseudo random number generator is that the development of the underlying system is chaotic. Thus, according to [7], the LSS that processed the strongest chaotic behavior in the range [0-4] is the one with the fewest failed NIST tests and the ability to generate a highly random chaotic sequence.

IV. Conlusion

Coupling chaotic maps is a common way to develop more sophisticated dynamic behavior. This paper gives a comparative examination of two coupled systems, namely the logistic-sine system (LSS) and the logistic-tent system (LTS), considering their randomization qualities to verify which performs the best. Since several test batteries are available to debate which system is best utilized as a random number generator, we pick the NIST test suite, which is regarded as the most appropriate one. We have demonstrated through NIST tests that the LSS presents better properties of randomness than the LTS, while the LTS is discontinuity random in the range of [3.1–3.95], the LSS is random throughout; thus, this will strongly influence the selection of the perfect chaotic map to generate sequences of keys used later for many applications, such as image encryption. We also discovered experimentally that using Lyapunov exponents, bifurcation diagrams, the 0-1 test, 3ST, and NIST tests is required to select the dynamic system characteristics required to develop chaos-based random generators. However, merely making a proper selection of the chaotic system characteristics is not enough; the unpredictability or lack of randomness of such a sequence relies on many aspects, including post-processing and the generator's design, and must be assessed in other ways.

Acknowledgment

The authors would like to thank the anonymous reviewers for their constructive comments on the earlier version of the paper.

References

[1] K. Demir and S. Ergün, "A comparative analysis on chaos-based random number generation methods," *Eur. Phys. J. Plus*, vol. 137, no. 5, Art. no. 5, May 2022, doi: 10.1140/epjp/s13360-022-02793-6.

[2] A. Doğanaksoy, F. Sulak, M. Uğuz, O. Şeker, and Z. Akcengiz, "New Statistical Randomness Tests Based on Length of Runs,"

Mathematical Problems in Engineering, vol. 2015, p. e626408, Apr. 2015, doi: 10.1155/2015/626408.

[3] "Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-line Conference 2020, Vol. 2 [1st ed.] 9783030519704, 9783030519711," *dokumen.pub*. https://dokumen.pub/artificial-intelligence-and-bioinspired-computational-methods-proceedings-of-the-9th-computer-science-on-line-conference-2020-vol-2-1st-ed-9783030519704-9783030519711.html (accessed Jan. 22, 2023).

[4] H. A. A. Mansour, "Analysis, Study and Optimization of Chaotic Bifurcation Parameters Based on Logistic/Tent Chaotic Maps," in *Artificial Intelligence and Bioinspired Computational Methods*, Cham, 2020, pp. 642–652. doi: 10.1007/978-3-030-51971-1_52.

[5] H. Li, C. Yu, and X. Wang, "A novel 1D chaotic system for image encryption, authentication and compression in cloud," *Multimed Tools Appl*, vol. 80, no. 6, pp. 8721–8758, Mar. 2021, doi: 10.1007/s11042-020-10117-y.

[6] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, Apr. 2014, doi: 10.1016/j.sigpro.2013.10.034.

[7] Joan. S. Muthu, A. J. Paul, and P. Murali, "An Efficient Analyses of the Behavior of One Dimensional Chaotic Maps using 0–1 Test and Three State Test," in *2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, Dec. 2020, pp. 125–130. doi: 10.1109/RAICS51191.2020.9332470.

[8] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Sci Rep*, vol. 10, no. 1, Art. no. 1, Jun. 2020, doi: 10.1038/s41598-020-66486-9.

[9] N. JITEURTRAGOOL, "Developments of CMOS based Chaotic Oscillator Circuits and Its Application," PhD Thesis, 高知工科大学, 2018. Accessed: Jan. 25, 2023. [Online]. Available: https://ci.nii.ac.jp/naid/500001366092

[10] M. Melosik and W. Marszalek, "On the 0/1 test for chaos in continuous systems," *Bulletin of the Polish Academy of Sciences Technical Sciences*, vol. 64, Sep. 2016, doi: 10.1515/bpasts-2016-0058.

[11] M. Tosin, M. V. Issa, D. Matos, A. D. Nascimento, and A. C. Jr, "Employing 0-1 test for chaos to characterize the chaotic dynamics of a generalized Gauss iterated map," presented at the XIV Conferência Brasileira de Dinâmica, Controle e Aplicações (DINCON 2019), Nov. 2019. Accessed: Jan. 21, 2023. [Online]. Available: https://hal.science/hal-02388470

[12] J. S. A. Eyebe Fouda, J. Y. Effa, M. Kom, and M. Ali, "The three-state test for chaos detection in discrete maps," *Applied Soft Computing*, vol. 13, no. 12, pp. 4731–4737, Dec. 2013, doi: 10.1016/j.asoc.2013.07.020.

[13] J. S. A. Eyebe Fouda and W. Koepf, "Efficient detection of the quasi-periodic route to chaos in discrete maps by the three-state test," *Nonlinear Dyn*, vol. 78, no. 2, pp. 1477–1487, Oct. 2014, doi: 10.1007/s11071-014-1529-4.

[14] R. Stępień and J. Walczak, "Statistical analysis of the LFSR generators in the NIST STS test suite," *Computer Applications in Electrical Engineering*, vol. Vol. 11, 2013, Accessed: Jan. 22, 2023. [Online]. Available: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-6b8818c1-d909-4960-8c08-647e878b1531

[15] M. Kaas-Mason, G. Prpić, S. Suriyasuphapong, and N. Bailey, "Comparison of Pseudo, Chaotic and Quantum Random Number Generators and their use in Cyber Security".

[16] M. Sýs, Z. Riha, V. Matyas, K. Marton, and A. Suciu, "On the interpretation of results from the NIST statistical test suite," vol. 18, pp. 18–32, Jan. 2015.