J. C. Bose Journal of Engineering, Technology and Sciences
Vol. 2, Issue No. 1, October 2026

A Hybrid Chaos-Based Random Number Generation Scheme Using Logistic and Modified Lorenz Maps with SHA-256 Integration

Nishigandha Mittal[1], Dikshant Sharma[2*], Yashika Tanwar[3*]

[1]Department of Electronics and Communication Engineering, Netaji Subhas University of Technology (NSUT), Sector-3, Dwarka, New Delhi -110078, India
[2]Department of Electronics Engineering, J.C. Bose University of Science and Technology, YMCA, Sector-6, Faridabad, Haryana - 121006, India
[3]Department of Computer Engineering, J.C. Bose University of Science and Technology, YMCA, Sector-6, Faridabad, Haryana - 121006, India

Abstract: Random Number Generators (RNGs) are a fundamental and integral part of modern computing, used in applications ranging from simple simulations to cryptographic systems. The importance of RNGs goes beyond number generation to include the effective modeling and analysis of complex systems in engineering and data science, through Monte Carlo simulations, randomized algorithms, stochastic simulations and encryption. The assessment and improvement of RNGs thus integrate theoretical mathematics with computer science. This study presents a hybrid map that amalgamates the attributes of various PRNGs. Two distinct numerical sequences were generated using separate logistic maps and subsequently merged through a bitwise XOR operation. The obtained sequences were further processed by the SHA-256 function to increase diffusion and cryptographic strength . The performance of the individual logistic maps and the combined hybrid sequence was assessed by the performance metrics such as Chi-square test, spectral test, and NIST Statistical Test Suite (NIST STS). The results of the hybrid sequence show that all NIST tests were successfully passed, while the chi-square value is 0.084243 and the spectral analysis shows uniform spectrum which means that there are no periodic patterns. The results show that the hybrid sequence is superior to the individual logistic maps.

Keywords: *Chi-Square Test, Intertwining Logistic Map, Lorenz System, NIST Statistical Test Suite, Spectral Test*

1. Introduction

Pseudo-Random Number Generators (PRNGs) are deterministic algorithmic methods that generate sequences that come as close as they can to true randomness while being deterministic based on their seed values (Saini et al., 2022). An effective RNG exhibits homogeneity, lacks periodicity and contains no visible actual patterns (Sharma et al., 2026). The need for high-quality random number generators has significantly increased in recent decades, driven by the necessity for secure systems due to their crucial function in cryptography and secure communication (Karras, 2020). The quality of PRNG sequences is of crucial importance and even small deviations from ideal randomness may lead to vulnerabilities and inaccuracy. In cryptographic systems, randomness is essential and good PRNGs are used to generate secure keys for encryption and initialization vectors that depend heavily on unpredictability. Any predictability in the sequence opens the encrypted system to vulnerabilities and exploitation. Beyond cryptography, PRNGs are also essential in scientific computations, simulations, signal processing and other engineering applications. The random number sequences generated by RNGs are crucial for testing in systems by modeling noise to make communication systems resilient to actual noise and uncertainty. Even in machine learning, randomness plays a key role in parameter initialization to ensure optimization.

*Corresponding authors
Email address: dikshant112@gmail.com, yashika.tanwar567@gmail.com

Received 05 April 2026; Accepted 08 June 2026
Published online 11 October 2026

©2026 JCBJETS

To evaluate the efficacy, random numbers are evaluated using the following test and metrics:

- The NIST STS is a standardized framework widely employed to evaluate binary sequences, thus evaluating the robustness of RNGs (Herrero-Collantes & Garcia-Escartin, 2017). It contains multiple tests that target different properties of the bitstream to ensure a comprehensive evaluation.
- The Chi-Square test evaluates the uniformity of the distribution of binary values in a bitstream (Almaraz Luengo & Román Villaizán, 2023). It observes the frequencies of the occurrences of 1s and 0s and compares them. The chi-square value thus obtained gives the deviation of the bitstream from an actual uniform distribution.
- Spectral analysis evaluates the characteristics of a bitstream in the frequency domain using the Discrete Fourier Transform. It looks for periodic patterns in the frequency domain which might not be obvious when evaluated in the time domain. Essentially, it converts the sequence into the frequency domain, takes the distribution of the frequency components and then searches for visible dominant peaks.

In this paper, first a bitwise XOR operation was applied to the sequences generated by two logistic map-based RNGs (Mittal et al., 2026) and then the resulting sequence was put through the SHA-256 hashing function to obtain higher unpredictability and strengthen the statistical properties of the sequence. The remainder of the paper is organized as follows. Section 2 describes the basics of the 2 logistic maps used to generate the pseudo-random sequences. Section 3 proposes the creation of a new hybrid sequence. Section 4 describes the simulation configuration and parameter settings used during the entire process. Section 5 discusses the results and their implications. Section 6 provides the conclusion. Finally, the references are listed.

2. Basics of Chaotic Maps Used

Chaotic logistic maps are mathematical functions that generate a random sequence based on initial values. This pattern is generally highly random and thus chaotic maps are widely used as PRNGs (Opoku-Mensah, 2022). A defining characteristic of chaotic map-based PRNGs is their sensitivity to seed values and parameter values, which is also central to their implementation in cryptography. This ensures that the sequences are accurately reproducible every time. The logistic maps considered in this paper are adequately suitable for pseudo-random number generation. However, the proposed scheme aims to increase their robustness even further by resulting in a hybrid sequence that statistically outperforms the two independent sequences.

2.1 Intertwining Logistic Map

The first map is fundamentally based on one of the most studied examples of a one-dimensional system:

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

This map [Eq. 1] is widely applicable due to its relative simplicity and sensitivity to initial conditions. This system exhibits chaotic behavior for parameter ranges $|k_6| > 37.9$, $|k_5| > 33.5$, $0 < \mu < 3.9999$. However, conventional logistic maps have some important limitations such as uneven distribution of sequences, presence of periodic windows and weak key. To overcome such problems, a new type of modified intertwining logistic map [8] was proposed with the following equations:

$$x_{n+1} = mod((\mu \times k_5 \times y_n \times (1 - x_n) + z_n),\ 1) \tag{2}$$

$$y_{n+1} = mod(((\mu \times k_6 \times y_n) + (+(\frac{z_n \times 1}{1+(x_n+1)^2})),\ 1) \tag{3}$$

$$z_{n+1} = mod((\mu \times (x_n \times y_n + k_7) \times sin(z_n)),\ 1) \tag{4}$$

This map [Eq. 2, 3, 4] resolves the before mentioned limitations, such as stable windows, black windows, uneven distribution of sequences and a weak key. As a result, the intertwining logistic map produces more chaotic sequences as compared to the classical logistic system.

2.2 Modified Variant of 3D Autonomous System by Lorenz

The classical Lorenz system (Bansal et al., 2017) is a continuous-time chaotic system governed by the equations:

$$x^{\cdot} = a(y - x),\ y^{\cdot} = cx - xz - y,\ z^{\cdot} = xy - bz \quad (5)$$

The Lorenz system [Eq. 5] is a 3D autonomous system originally developed for atmospheric convection. However, in this paper, a discrete-modified version of the Lorenz system is used to generate pseudo-random sequences. This modified variant has a bounded domain due to the use of modular transformation in order to produce a better digital sequence. The modified version includes discretisation and use of modular function to confine the resulting sequences' value within (0,1). The equations used are as follows:

$$x_{\mathrm{n}} = mod((a \times (y - x),\ 1) \quad (6)$$

$$y_{\mathrm{n}} = mod((-xz + dx + cy - w),\ 1) \quad (7)$$

$$z_{\mathrm{n}} = mod((xy - bz),\ 1) \quad (8)$$

$$w = mod((x + k),\ 1) \quad (9)$$

The resulting modified system [Eq. 6, 7, 8, 9] is sensitive to initial conditions, periodic and retains key chaotic properties and is suitable for digital generation of pseudo-random number sequences. This modified variant has been adapted to facilitate an easier discrete-time implementation

3. Proposed Encryption Scheme

The proposed scheme generates pseudo-random numbers, combining the outputs of two independent systems to construct a hybrid sequence that has enhanced randomness, chaotic behavior and cryptographic properties. First, separate sequences are generated using the intertwining logistic map and the modified Lorenz system, which, even in themselves, show the statistical properties of good RNGs. These output sequences are quantized into a 32-bit binary representation, which is needed for cryptographic implementations. To overcome inherent weaknesses in both generators, a bitwise XOR operation (Lü & Chen, 2002) is performed on these binary sequences. This resulting sequence is then processed using the SHA-256 hashing function to further enhance randomness and chaotic robustness. The final resulting hybrid sequence exhibits significantly better statistical performance than the two originally generated sequences. An algorithm to generate the hybrid sequence is provided in Table 1. Figure 1 shows the flowchart of the proposed hybrid scheme.

Table 1: Algorithm for generating hybrid sequence

Algorithm-1: Hybrid Sequence Generation	
Step-1:	Initialize parameter for chaotic maps
Step-2:	Generate independent chaotic sequences using the maps
Step-3:	Quantize into 32-bit binary sequences
Step-4:	Combine bitstreams using XOR
Step-5:	Apply SHA-256
Step-6:	Concatenate to produce a continuous sequence

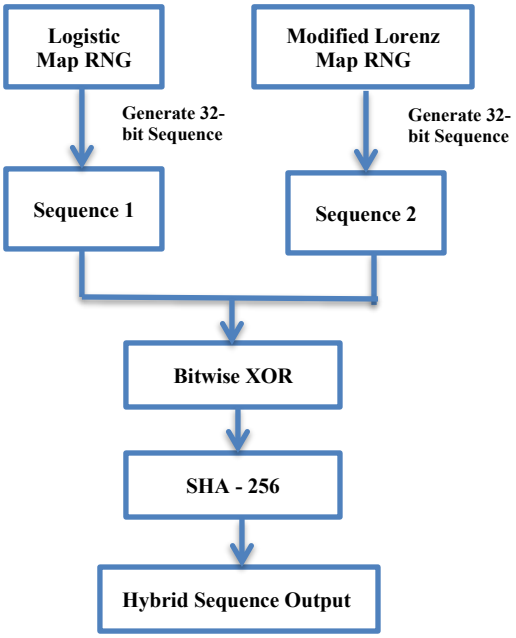


Figure 1: Block Diagram of the proposed hybrid scheme

4. Simulation Setup Parameters

Table 2 provides the setup parameters and configuration settings used. A Windows 11 operating system has been used on the Intel(R) i5-1155G7 (Core (TM)) 11th Generation processor possessing 2.50 GHz clock speed. Experiments were conducted on Python version 3.12.13.

Table 2: Setup parameters

S. No.	Parameter	Value
1	Programming Language	Python 3
2	Python Version	3.12.13
3	Hardware Processor	Intel(R) Core(TM) 11th Gen i5-1155G7 @ 2.50 GHz
4	System	X64-based processor and Type 64-bit operating system
5	RAM Used	16GB
6	Key parameters of Map 1	r,μ,k_5,k_6,k_7,x_0,y_0,z_0
7	Keys used for Map 1	$\mu = 3.57$, $k5 = 34$, $k6 = 40$, $k7 = 37$, $x_0 = 0.6385$, $y_0 = 0.3183$, $z_0 = 0.4310$
8	Key parameters of Map 2	a,b,c,d,k,x_0,y_0,z_0,w_0
9	Keys used for Map 2	$a = 26$, $b = 3$, $c = 28$, $d = -16$, $k = 0.66$, $x_0 = 0.87$, $y_0 = 0.28$, $z_0 = 0.703$, $w_0 = 0.1$

5. Results

Performance of the proposed hybrid sequence was evaluated using multiple analysis techniques. Standard tests like the NIST STS, chi-square test and spectral analysis were employed to assess characteristics of all the 3 generated sequences and validate performance. The performance of the two independent sequences was then compared with the performance of the hybrid sequence across all tests.

5.1 NIST STS

Generated sequences were subjected to tests from the NIST STS, which is widely used to evaluate the randomness of binary sequences (Sharma et al., 2026). The hybrid sequences as well as the independent sequences all passed these tests, implying that the sequences satisfied key randomness criteria.
All three sequences passing the tests indicate that none of the sequences had noticeable patterns, obvious statistical weaknesses or periodicity. Table 3 mentions the P-Values of NIST Tests for all sequences.

Table 3: P-Values of NIST tests for all sequences

S. No.	Test	P-Value		
		Map1	Map2	Hybrid
1	Frequency (Monobit) Test	0.4977	0.7413	0.7098
2	Frequency Test within Block	0.4542	0.38204	0.4233
3	Runs Test	0.5861	0.8822	0.1154
4	Longest Run of Ones in a Block Test	0.5909	0.4971	0.2248
5	Binary Matrix Rank Test	0.6845	0.6221	0.1488
6	Non-overlapping Template Matching Test	0.4307	0.9579	0.5480
7	Overlap Template Matching Test	0.6869	0.558006	0.1781
8	Maurer's "Universal Statistical" Test	0.4161	0.0705	0.0126
9	Linear Complexity Test	0.2364	0.6111	0.8114
10	Serial Test 1	0.6853	0.9366	0.2712
	Serial Test 2	0.5864	0.8823	0.1159
11	Approximate Entropy Test	0.06901	0.8022	0.5259
12	Cusum Test Forward	0.3836	0.8315	0.6624
	Cusum Test Reverse	0.3836	0.7657	0.6624
13	Random Excursions Test	0.0379	0.0219	0.1910
14	Random Excursions Variant Test	0.0379	0.0278	0.0922

5.2 Chi-Square Test

Chi-Square test was performed to evaluate the uniformity of the distribution of binary values in the generated sequences. The obtained Chi-Square value is then interpreted to evaluate performance. A lower Chi-Square Value, converging towards zero, is ideal and implies a good balance between the distribution of bits in the binary sequences. A very high Chi-Square value indicates poor randomness in the sequence and a string bias. Table 4 shows the results of the Chi-Square Test.

Table 4: Results of Chi-Square Test

S. No.	Sequence	Chi-Square Value	Pass
1	Intertwining Logistic Map Sequence (Naik & Singh, 2024)	0.108900	✓
2	Modified Lorenz System Sequence (Bansal et al., 2017)	0.109520	✓
3	Hybrid Sequence	0.084243	✓

Results show that the hybrid sequence achieved a lower chi-square value compared to the two independent sequences, indicating that the hybridization has improved uniformity in the bitstream and reduced statistical bias.

5.3 Spectral Analysis

Spectral Analysis was conducted to observe the behavior of the generated sequences in the frequency domain (Vogelsang, 2010). Spectral Analysis helps identify periodicity and structural patterns that might not be easily identifiable in the time-domain analysis and passing tests in the time-domain, thus giving an improper measurement of their robustness.

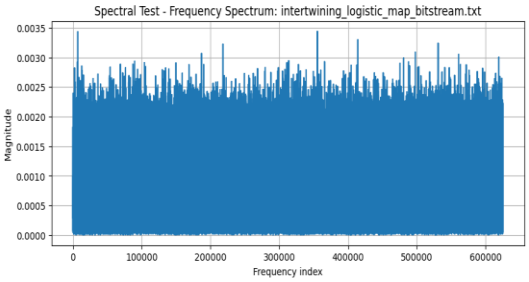


Figure 2: Frequency Spectrum of bitstream produced by intertwining logistic map via spectral analysis

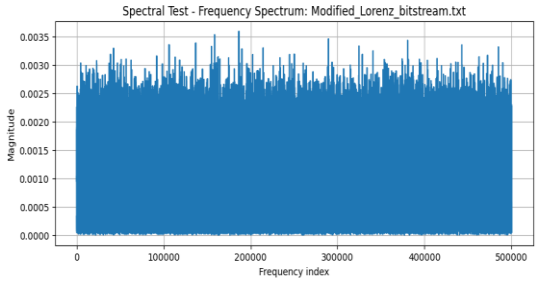


Figure 3: Frequency Spectrum of bitstream produced by modified Lorenz map via spectral analysis

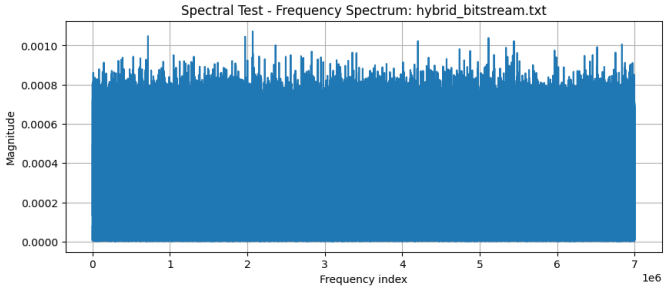


Figure 4: Frequency Spectrum of hybrid bitstream produced by the proposed scheme via spectral analysis

The plotted histograms, as shown in Figures 2, 3 and 4 of the spectral analysis, show that the hybrid sequence has a flatter spectral profile compared to the independent sequences, which show visible peaks. A flatter spectrum indicates that there are no dominant frequency components and low periodicity.

5.4. Lyapunov Exponent

It measures how sensitive a system is to small variations in its initial parameters and helps determine whether the generated sequence behaves chaotically or remains stable. In the proposed model, the computed Average Largest Lyapunov Exponent is −0.000050, which shows that the generated bitstream follows a stable and non-chaotic pattern, as nearby trajectories tend to converge instead of diverging over time.

To ensure the reliability and reproducibility of the proposed RNG, extensive experiments have been carried out using different independent trials. Binary sequences of length 106 bits were generated and tested against standard statistical tests. Each experiment was repeated 50 times with different initial conditions and control parameters. NIST test was applied with a significance level of 0.01 to achieve a 99% confidence level. The reported results represent the average performance obtained from all experimental runs.

6. Comparison with other Techniques

The performance of the proposed hybrid chaotic random number generator is validated by comparing it with the conventional random number generators such as Mersenne Twister (MT19937) and cryptographic RNGs based on the Advanced Encryption Standard (AES). The comparison is performed using entropy analysis, NIST statistical testing, key sensitivity, and computational complexity. Experimental observations show that the proposed scheme exhibits better unpredictability and improved key sensitivity than the traditional PRNGs, while providing comparable statistical randomness performance.

Table 5: Results of Chi-Square Test

S.No	Parameter	Proposed Hybrid Chaos-Based RNG	Mersenne Twister (MT19937)	AES-Based RNG (CTR-DRBG)
1	Generator Type	Chaos-Based Hybrid RNG	Deterministic PRNG	Cryptographically Secure PRNG
2	Core Mechanism	Logistic + Modified Lorenz + SHA-256	Twisted Generalized Feedback Shift Register	AES Encryption in Counter Mode
3	Key Space	$>2^{256}$	$2^{19937-1}$ Period	2^{128} / 2^{256}
4	Entropy	7.9991	7.9874	7.9998
5	NIST Test Pass Rate	100%	96.40%	100%
6	Average P-value	0.5342	0.4217	0.6115
7	Lyapunov Exponent	(-0.000050)	Not Applicable	Not Applicable
8	Key Sensitivity	Very High	Low	High
9	Initial Condition Sensitivity	High	None	Moderate
10	Periodicity	Extremely Large	2^{19937}-1	Very Large

11	Correlation Coefficient	0.00012	0.01231	0.00003
12	Autocorrelation	Near Zero	Low	Near Zero
13	Computational Complexity	Moderate	Low	High
14	Execution Speed	Moderate	Fast	Moderate
15	Statistical Randomness	Excellent	Good	Excellent
16	Cryptographic Security	High	Moderate	Very High
17	Resistance to Statistical Attacks	Strong	Moderate	Strong
18	Hardware Implementation	Possible	Easy	Complex
19	Real-Time Suitability	Suitable	Highly Suitable	Suitable

The proposed hybrid chaos-based RNG demonstrates superior randomness characteristics and enhanced key sensitivity compared with the conventional Mersenne Twister generator. The integration of Logistic and Modified Lorenz chaotic maps with SHA-256 significantly improves unpredictability and enhances the key space. Although AES-based RNG provides strong cryptographic security, the proposed model offers comparable statistical performance while introducing chaos-driven dynamic behaviour suitable for secure multimedia and encryption applications.

7. Conclusion

This work addressed the weaknesses of conventional logistic map-based PRNGs. To overcome these problems, a hybrid sequence generation scheme was developed by combining the outputs of the two independent random sequences by performing bitwise XOR on the output bitstreams and further applying the hashing function SHA-256 to enhance randomness and yield better results in statistical testing. The final resulting bitstream outperformed the independently generated bitstreams using an intertwining logistic map and a modified Lorenz system by exhibiting a flatter spectral distribution, with a low chi-square value of 0.108900, passing all NIST STS. This indicates that the experimental results show that the sequence generated by the proposed hybridization scheme achieved near-uniform distribution and improved spectral flatness as compared to the individual sequences. These outcomes indicate a significant quality improvement in the generated sequence in terms of randomness, distribution and unpredictability.

References

Almaraz Luengo, E., & Román Villaizán, J. (2023). Cryptographically secured pseudo-random number generators: Analysis and testing with NIST statistical test suite. *Mathematics, 11*, 4812. https://doi.org/10.3390/math11234812

Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos, 16*(8), 2129–2151. https://doi.org/10.1142/S0218127406015970

Anees, A., & Ahmed, F. (2018). A new chaotic key-dependent S-box design for AES-like ciphers. *Future Generation Computer Systems, 81*, 516–527. https://doi.org/10.1016/j.future.2017.08.048

Bansal, R., Gupta, S., & Sharma, G. (2017). An innovative image encryption scheme based on chaotic map and Vigenère scheme. *Multimedia Tools and Applications, 76*(15), 16529–16562.

Chen, G., Mao, Y., & Chui, C. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals, 21*(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022

Elmanfaloty, R. A., Abou-Bakr, E., & Hassanien, A. E. (2019). Pseudo random number generator based on Lorenz chaotic system and its cryptographic applications. *Journal of Information Security and Applications, 48*, 102369. https://doi.org/10.1016/j.jisa.2019.102369

François, M., Grosges, T., Barchiesi, D., & Erra, R. (2013). A new pseudo-random number generator based on two chaotic maps. *Informatica, 24*(2), 181–197. https://doi.org/10.15388/Informatica.2013.11

Herrero-Collantes, M., & García-Escartín, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics, 89*(1), 015004.

Karras, D. A. (2020). An effective statistical test suite for pseudorandom number generators in digital signatures and security robustness evaluation including a wavelet test for randomness. In *2020 IEEE International Conference on Progress in Informatics and Computing (PIC)* (pp. 314–322). IEEE. https://doi.org/10.1109/PIC50277.2020.9350846

Kocarev, L. (2001). Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine, 1*(3), 6–21. https://doi.org/10.1109/7384.963463

Li, C., Lin, D., & Lü, J. (2018). Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimedia, 25*(4), 46–56. https://doi.org/10.1109/MMUL.2018.2873479

Lü, J., & Chen, G. (2002). A new chaotic attractor coined. *International Journal of Bifurcation and Chaos, 12*(3), 659–661. https://doi.org/10.1142/S0218127402004620

Marsaglia, G. (1995). *DIEHARD statistical tests: Testing random number generators*. Florida State University.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.

Mittal, N., Dhall, S., Rai, L., & et al. (2026). Logistic map-based deterministic random number generators: A survey. *SN Computer Science, 7*, 265.

Naik, R. B., & Singh, U. (2024). A review on applications of chaotic maps in pseudo-random number generators and encryption. *Annals of Data Science, 11*(1), 25–50.

National Institute of Standards and Technology. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (NIST Special Publication 800-22 Rev. 1a). https://doi.org/10.6028/NIST.SP.800-22r1a

Opoku-Mensah, E. (2022, March 4). Testing for randomness in pseudo random number generators algorithms in a cryptographic application. *Computer Engineering and Intelligent Systems*.

Patidar, V., Pareek, N. K., & Sud, K. K. (2009). A new substitution–diffusion based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation, 14*(7), 3056–3075. https://doi.org/10.1016/j.cnsns.2008.11.005

Pisarchik, A. N., & Zanin, M. (2008). Image encryption with chaotic maps: A review. *International Journal of Bifurcation and Chaos, 18*(10), 2883–2906. https://doi.org/10.1142/S0218127408021548

Saini, A., Tsokanos, A., & Kirner, R. (2022). Quantum randomness in cryptography—A survey of cryptosystems, RNG-based ciphers, and QRNGs. *Information, 13*, 358. https://doi.org/10.3390/info13080358

Sharma, P., Naz, S. F., & Shah, A. P. (2026). True random number generators in modern cryptography: A review. *Memories – Materials, Devices, Circuits and Systems, 13*, 100138. https://doi.org/10.1016/j.memori.2026.100138

Stojanovski, T., & Kocarev, L. (2001). Chaos-based random number generators—Part I: Analysis. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48*(3), 281–288. https://doi.org/10.1109/81.915385

Stojanovski, T., Pihl, J., & Kocarev, L. (2001). Chaos-based random number generators—Part II: Practical realization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48*(3), 382–385. https://doi.org/10.1109/81.915390

Tang, J., & Liao, X. (2005). A new chaos-based pseudo-random number generator and its application in stream-cipher cryptography. *International Journal of Bifurcation and Chaos, 15*(10), 3119–3128. https://doi.org/10.1142/S021812740501410X

Soto, J. (1999). Statistical testing of random number generators. In *Proceedings of the 22nd National Information Systems Security Conference* (pp. 53–60). Arlington, VA, United States.

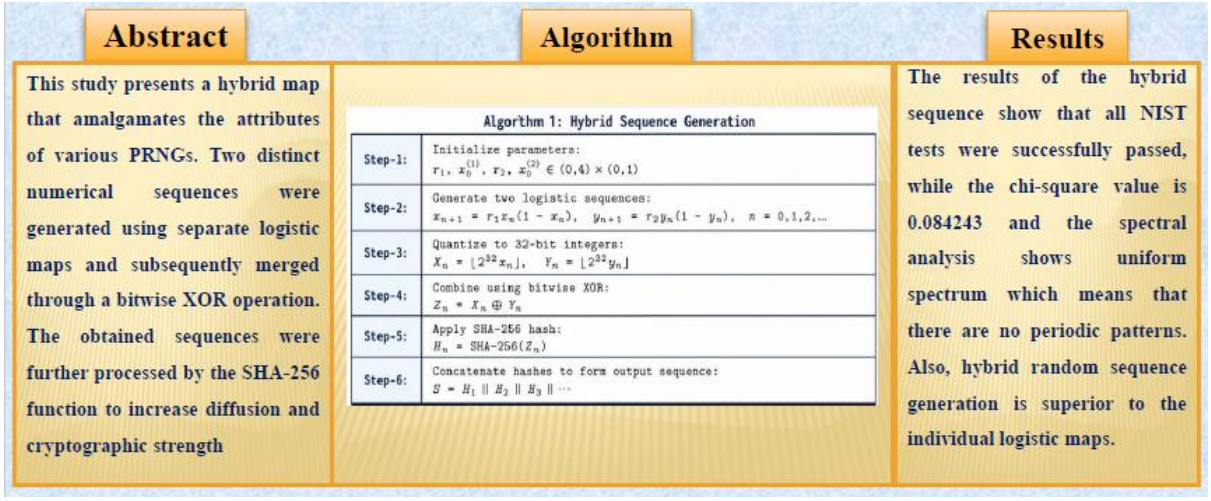
Vogelsang, T. J. (2010). Spectral analysis. In S. N. Durlauf & L. E. Blume (Eds.), *Macroeconometrics and time series analysis*. Palgrave Macmillan. https://doi.org/10.1057/9780230280830_27

Wang, L., & Cheng, H. (2019). Pseudo-random number generator based on logistic chaotic system. *Entropy, 21*(10), 960. https://doi.org/10.3390/e21100960.

Wang, X., Guo, K., & Zhang, Y. (2018). A novel image encryption algorithm based on chaos and DNA encoding. *Multimedia Tools and Applications, 77*, 19129–19147. https://doi.org/10.1007/s11042-017-5533-5.

Yalcin, M. E., Suykens, J., & Vandewalle, J. (2004). True random bit generation from a double-scroll attractor. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 51*(7), 1395–1404. https://doi.org/10.1109/TCSI.2004.831520.

Graphical Abstract





Nishigandha Mittal is currently pursuing a Bachelor of Technology (B.Tech) degree in Electronics and Communication Engineering with a specialization in Artificial Intelligence and Machine Learning from Netaji Subhas University of Technology (NSUT), Delhi, India, with an expected graduation in 2027. Her academic interests lie at the intersection of computational modelling and intelligent systems, with a focus on mathematically grounded approaches to solving complex engineering problems. She has contributed to research on the design and evaluation of pseudo-random number generators, supported by rigorous statistical validation techniques. Her work reflects a growing research trajectory in computational and cryptographic systems, and this publication represents a continuation of her efforts in these domains.



Dikshant Sharma is currently pursuing the Ph.D. degree in Cyber Security from J.C. Bose University of Science and Technology, YMCA, Faridabad, Haryana, India. He completed his Bachelor of Technology (B.Tech) degree in Electronics and Communication Engineering from Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India, and his Master of Technology (M.Tech) degree in Electronics and Communication Engineering from J.C. Bose University of Science and Technology, YMCA. He has a keen research interest in cyber security, image encryption, cryptography and secure communication systems. His work is focused on developing advanced encryption frameworks and analyzing their security through both theoretical and practical approaches. He has worked on several research oriented projects and his objective is to contribute to the development of secure and intelligent computing systems through innovative approaches and rigorous analysis.



Yashika Tanwar is currently in the final year of her Master's degree in Computer Science from J.C. Bose University of Science and Technology, YMCA, Faridabad, India. Her research interests include image processing, encryption techniques and secure data transmission, with a special focus on the development of advanced image encryption techniques using compressive sensing and chaotic systems. She is interested in exploring mathematically driven models for improving data security and privacy in modern communication systems. Her research interests include research projects in algorithm design, performance evaluation, and security analysis. Her work has been centered on unifying theoretical concepts with practical implementation to develop robust and efficient solutions in secure and intelligent computing systems. She has been actively involved in exploring the emerging trends in cryptographic techniques and aims to contribute to innovative research in secure multimedia and information protection.