SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V13I7P102

Volume 13 Issue 7, 8-15, July 2026

Original Article

Comparing Chaotic Maps as Pseudorandom Generators for Stream Cipher Encryption

Vivaan Mansukhani

Sanskriti School, Chanakyapuri, New Delhi, India.

Corresponding Author : vivaan.mansukh@gmail.com

Received: 18 May 2026 Revised: 24 June 2026 Accepted: 12 July 2026 Published: 30 July 2026

Abstract *- Chaos theory offers a compelling foundation for cryptographic pseudorandom number generation owing to the extreme sensitivity of chaotic dynamical systems to initial conditions. This paper presents a comparative study of five well-known chaotic maps—Logistic, Tent, Sine, Piecewise Linear Chaotic Map (PWLCM), and Hénon—as keystream generators for a basic XOR stream cipher. Each map is evaluated under identical conditions using five statistical metrics: keystream bit balance, 8-bit Shannon entropy, adjacent-byte Pearson correlation, compression ratio, and avalanche bit error rate (BER). Results show substantial variation in cryptographic suitability. The tent map produces keystreams closest to ideal randomness across all metrics, exhibiting near-perfect bit balance, the highest entropy (7.95 bits/byte), near-zero byte correlation, and incompressible ciphertext. The logistic map shows strong bit bias; PWLCM displays high adjacent-byte correlation; and the Hénon map produces compressible ciphertext with the lowest entropy, suggesting finite-precision periodicity. All five maps demonstrate strong key sensitivity (BER ≈ 0.50). These findings confirm that mathematical chaos alone does not guarantee cryptographic randomness, and that map selection, parameterisation, and output-extraction method are critical design choices for chaos-based stream ciphers.*

Keywords *- Avalanche Effect, Chaotic Maps, Pseudorandom Number Generation, Shannon Entropy, Stream Cipher.*

1. Introduction

The security of digital information relies a great deal on the ability to create a ciphertext that is indistinguishable from random noise [1, 2]. This is accomplished in traditional encryption algorithms like AES with complicated confusion and diffusion techniques, producing a ciphertext with almost maximum entropy without discernible patterns [1, 2]. Over the past few years, chaos theory has been investigated as another foundation for encryption. Chaotic dynamical systems are deterministic, but also display certain cryptographic properties such as pseudo-random and extremely sensitive to initial conditions [3]. A variety of chaos-based ciphers have been proposed since Matthews' early research involving a logistic map [3] in the 1980s, many of which attempt to take advantage of this butterfly effect to create effectively random output from the encrypted text by the introduction of noise.

Chaos-based cryptography is inspired by Shannon's ideas on confusion/diffusion, and it is expected that those that involve the smallest change in plaintext or key should lead to the most drastic and diffused change in the ciphertext [3]. The chaotic maps also have the property of having diverging trajectories that start very close to each other but grow more and more distant over time, which makes them well-suited to a similar kind of use in developing a cipher. Maps with one dimension, like logistic, tent and sine maps and two dimensions like the Hénon map are known to provide cryptographic pseudorandomness sources [4]. They are simple and fast, and can be used to generate keystreams in resource-constrained or real-time applications [4].

There is a lacuna in this literature. The comparisons that have been performed generally vary in plaintext, sequence length and metric, if used at all, and most recent contributions introduce new or modified chaotic systems, so it is hard to compare different systems unless the same ones are used [4]. Since the guidelines of Alvarez and Li [15] were called for, there has been no agreed practice in evaluating chaos-based cryptosystems, and a practitioner who wants to choose a map for a light-weight cipher has little like-for-like evidence to use in making this choice. The present study provides such evidence, consisting of five standard maps, one pipeline, one plaintext and five common metrics.

This paper examines five chaotic maps (Logistic, Tent, Sine, PWLCM, and Hénon) combined with a very easy-to-implement XOR stream cipher and tested under the same conditions. Performance is measured as balanced bit frequency, high entropy, low correlation, incompressibility and high sensitivity to keys. It was expected that maps with

near-ideal statistical properties would be generated from maps with higher dimensionality, such as the Hénon map. The purpose was to do this testing and elucidate the practical factors related to the cryptographic suitability.

2. Literature Survey

Most chaotic maps are not suitable for use in cryptographically secure Pseudorandom Number Generators (PRNGs) [5]. Song and Ding [5] evaluated the extent of pseudorandomness and efficiency in the use of hardware resources for the logistic map (1D) and the Hénon map (2D). They determined that the Hénon sequence was pseudorandom and that the logistic map was efficient in terms of hardware resources. In general, random chaotic sequences are not a good enough cryptographically secure PRNG if not carefully processed or enhanced [4].

There are many proposed methods to overcome shortcomings of individual maps, such as perturbing chaotic iterates, increasing map dimension or using multiple maps [4]. Murillo-Escobar et al. have suggested a 2D Hénon-Sine hyperchaotic map to enhance the complexity and presented a microcontroller implementation [14]. Al-Hyari et al. [7] combined Hénon and logistic maps to implement image encryption, and Sharma and Chawla [6] proposed an XOR-based hybrid 2D-Hénon map for the same. Al-Daraiseh et al. presented a state-based modified tent map that satisfies the NIST SP 800-22 test suite, and it is cryptographic grade in terms of randomness [8]. Yin et al. used PWLCM for bit-level colour image encryption [9], Chen et al. applied PWLCM to the standard map [10], and Hasheminejad and Rostami suggested a multiphase scheme of PWLCM [11] for bit-level colour image encryption. Umar et al. showed that modified skew tent maps lead to a high degree of statistical randomness [12].

Since chaos-based generators are most commonly suggested to be used on constrained platforms, they need to be evaluated for implementation cost. On a Virtex-7 FPGA, Garcia-Bosque et al. utilized 510 look-up tables and 120 registers to implement a bitwise chaotic generator. They demonstrated that modifying the chaotic parameters during operation, to ensure that the chaotic orbit does not become a short period, increased the NIST pass rate from 0.252 to 0.989 [16]. In [17], Dridi et al. showed that a stream cipher implemented using three weakly coupled chaotic maps, apart from the ills of the maps, has the advantage that the coupling puts limits on the amount of information that the side-channel adversary can gather.

This is a statement that is commonly not featured in comparative studies of this sort. Luo et al. took a chaotic cryptosystem in the field of microcontrollers. They passed NIST SP 800-22 suite successfully, along with frequency and avalanche test, and managed to recover the key by correlation power analysis [18]. Acikkapi et al. examined this common belief and found that this is true. However, with some caveats: while a chaos-based construction was more resistant than AES to the attacks, both constructions were recoverable when about 30 plaintexts were present [19]. The authors believe that side channel attacks, in particular of chaos-based ciphers, are not widely known and therefore have a small literature.

Many recent publications present new chaotic systems, and most of them lack the possibility to compare the classical maps with each other with a set of common statistical criteria [4], such as those given by Dinu and Frunzete. This study is an attempt to meet this need.

What is offered here is not so much a proposal for a further map, but methodological. It differs from the previous work in three respects. The first is that the same 3.44 KB plaintext is fed into all five maps and the same four-stream interleaving and thresholding rule is used, so that any variations in output are due to the map and not to the rest of the system. Secondly, the results were different from expected: the 2D Hénon map has the lowest entropy of the two, 7.5347 bits/byte, but the only compressible encrypted text, 0.9742. However, the Hénon sequence is more pseudo-random than the other one, according to Song and Ding [5]. Here, this disagreement is thought to stem from the extraction method and finite precision behaviour, rather than from the dynamics. Thirdly, a map can have one criterion but not the other, as PWLCM has the best bit balance, 0.4987, with the adjacent-byte correlation being by far the worst, 0.3754.

3. Problem Definition

The main research question is: What is the best approximation of ideal cryptographic randomness among the following five maps: Logistic, Tent, Sine, PWLCM, Hénon, when subjected to the same experiment? This study is guided by three sub-questions:

- Do all 5 maps generate statistically balanced keystreams and/or statistically entropy-maximising keystreams, or are there noticeable characteristics of the keystream which are structurally flawed (bit bias, compressibility, etc.)?
- How does key sensitivity (avalanche effect) differ among the five maps, and does dimensionality relate to greater sensitivity?
- Can the observed differences in the performance be attributed to mathematical aspects of each map (invariant density, finite precision behaviour, Lyapunov exponent) or to incidental parameterisation?

4. Materials and Methods

This study provides comparisons of five chaotic maps as pseudorandom keystream generators to the basic XOR stream cipher. The process involves four steps: creating

chaotic sequences, transforming these sequences to binary keystreams, encrypting a 3.44 KB plaintext file following a procedure of XOR, and comparing the ciphertext with five statistical tests.

4.1. The use of Parameters and Chaotic Maps

The parameters were chosen in the well-known chaotic regimes, and the initial values were fixed constants acting as the key for encryption in these maps. Each map drives four parallel streams that are interleaved bitwise, and the values quoted below are those of the first stream. The logistic map is shown as Equation 1:

$$x_{n+1} = r x_n(1 - x_n), \quad r = 3.90 \tag{1}$$

The slope of the tent map is piecewise linear and has parameter μ = 1.999, see equation 2 below.

$$x_{n+1} = \mu \cdot \min(x_n, 1 - x_n) \tag{2}$$

The sine map has the form given in Equation 3, with μ = 0.99:

$$x_{n+1} = \mu \cdot \sin(\pi x_n) \tag{3}$$

PWLCM is implemented in its two-segment form, $x_{n+1} = x_n/p$ for $x_n < p$ and $(1 - x_n)/(1 - p)$ otherwise, with $p = 0.25$. The two-dimensional Hénon map is given by Equation 4:

$$x_{n+1} = 1 - a x_n^2 + y_n, \quad y_{n+1} = b x_n \tag{4}$$

with $a = 1.4$ and $b = 0.3$. Its x output is squashed by tanh and rescaled to (0, 1) before thresholding.

4.2. Keystream Generation

Continuous values were thresholded to be converted to bits: If $x_n < 0.5$, then the output bit is 0, and if $x_n > 0.5$, then the output bit is 1. The first 1,000 transient values of the Hénon orbit were ignored prior to the extraction of the keystream. Sufficient bits were generated to encrypt a 3.44-KB plaintext file.

4.3. XOR Encryption

Each bit of the ciphertext is the XOR of the plaintext corresponding bit and a key bit: $c_i = m_i \oplus k_i$. This simple cipher makes any weakness in the keystream immediately visible to the observer in measurable statistics in the ciphertext. All five maps were successfully decrypted and verified to produce the same plaintext with 100% accuracy for each map.

4.4. Evaluation Metrics

Five metrics were used: bit balance (ones ratio – should be 0.50); byte Shannon entropy (8 bits/byte – ideal); adjacent-byte Pearson correlation (r should be near 0.00); compression ratio (should be ≥ 1.00); and avalanche BER proxy (should be near 0.50) with a one-bit-flipped key versus the correct key ciphertext. All experiments were carried out in Python and performed in double precision (FP-64) floating point format.

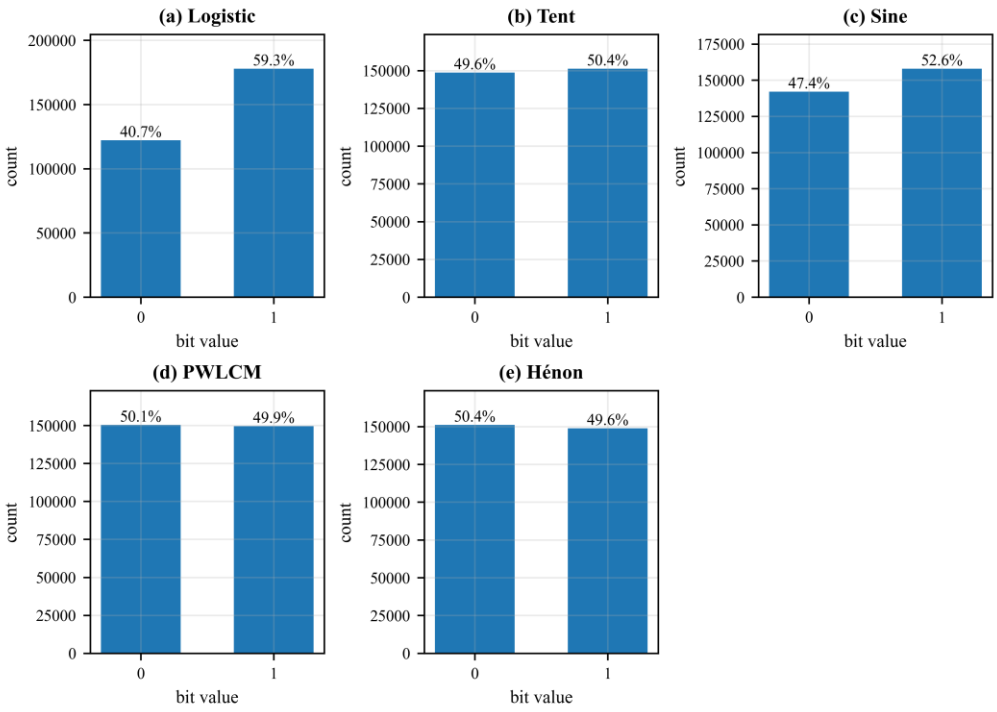

Fig. 1 All five chaotic maps are shown in terms of the ratio of the number of bits that are ones in the figure produced by the keystream, that is, the bit balance, plotted as shown in figure 1: (a) Logistic, (b) Tent, (c) Sine, (d) PWLCM, and (e) Hénon. The optimum ratio is 0.50.

5. Results and Discussion

5.1. Keystream Bit Balance

The one ratio is displayed for each map in Figure 1. The logistic map created an extremely biased keystream (59.3% ones), meaning that non-uniform sampling of the state space was obtained.

The tent map (0.5042), PWLCM (0.4987), and Hénon map (0.4961) were near-ideal, while the sine map showed a mild bias (0.5264). The results here demonstrate that if the invariant density is not flat over [0, 1], then simple thresholding reveals structural non-uniformity in maps.

5.2. Ciphertext Entropy

The block entropy is normalised over block sizes m = 1 to 8, for which it is plotted as a function of m, as depicted in Figure 2. These are the highest 8-bit byte entropies obtained from the tent map (7.9468 bits/byte) and sine map (7.9448 bits/byte). The value of the logistic map (7.8793) and the PWLCM (7.9080) were lower, and the Hénon map showed the lowest entropy (7.5347), which means there was a lot of structural redundancy in the ciphertext. The curve of the tent map is very close to 1.00 at all block sizes; the Hénon map shows the steepest decline, consistent with its higher-order pattern structure.

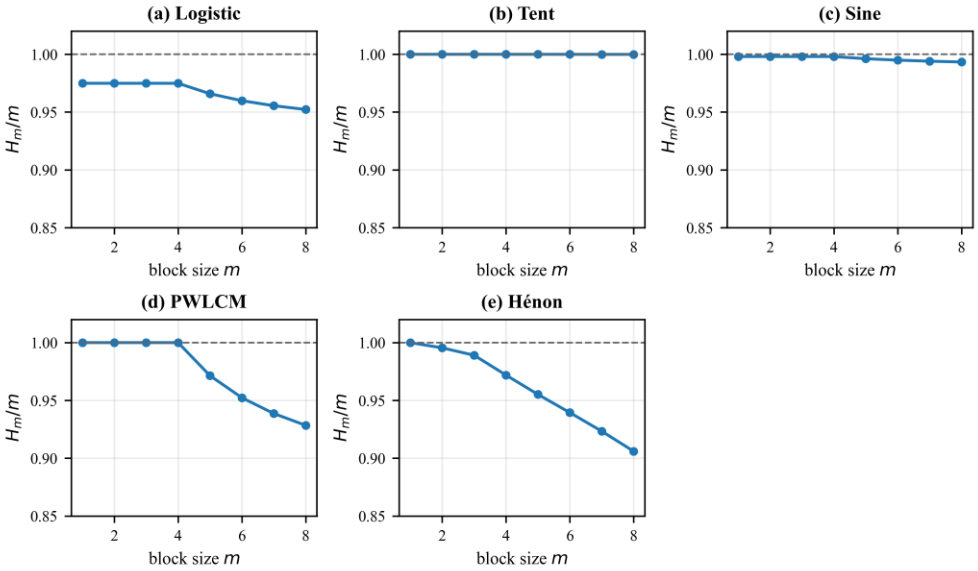

Fig. 2 Normalized block entropy H_m/m, m = 1 - 8: (a) Logistic, (b) Tent, (c) Sine, (d) PWLCM, (e) Hénon. This should be 1.00 at all block sizes

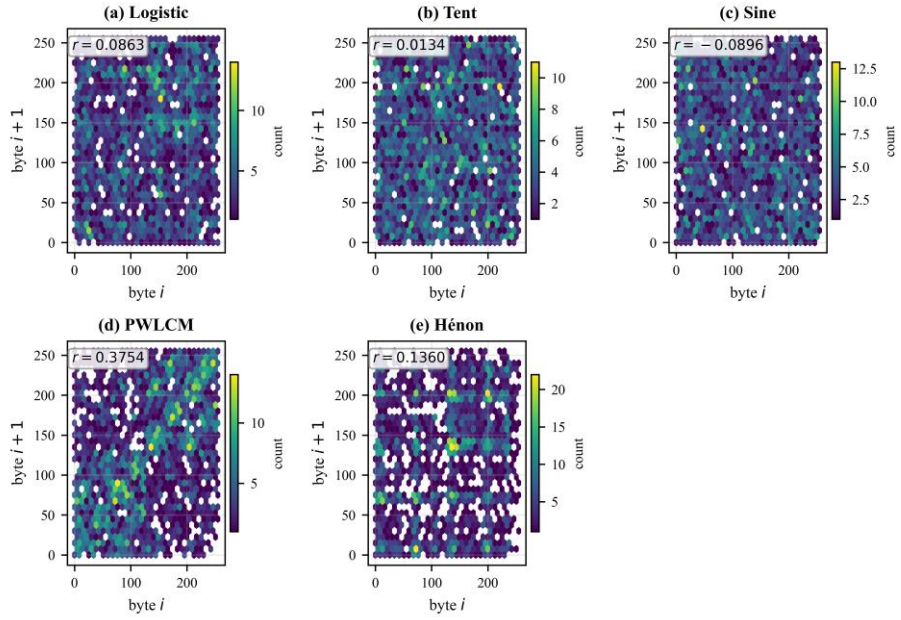

Fig. 3 Neighbouring-byte density plots of the ciphertext for each map: (a) Logistic, (b) Tent, (c) Sine, (d) PWLCM and (e) Hénon. Nearly no correlation means that the cloud has a uniform appearance; dependency means that the cloud has a banded appearance.

5.3. Adjacent-Byte Correlation

Figure 3 shows neighbouring-byte density plots. This tent map resulted in close to zero correlation ($r = 0.0134$) and a fairly uniform cloud. The logistic map was small (0.0863), but not zero; the Hénon map was higher (0.1360). The most interesting one was PWLCM ($r = 0.3754$); the density plot revealed a strong linear banding, and consecutive bytes are not independent. The sin map exhibited a small negative correlation (−0.0896), comparable in magnitude to that of the logistic map.

Table 1. For each of the chaotic maps, statistical evaluation is performed, and the resulting data is displayed.

Map	Ones Ratio	Entropy (bits/byte)	*Adj. Corr. r*	Compress. Ratio	BER
Logistic	0.5930	7.8793	0.0863	1.0031	0.5018
Tent	0.5042	7.9468	0.0134	1.0031	0.5033
Sine	0.5264	7.9448	−0.0896	1.0031	0.5029
PWLCM	0.4987	7.9080	0.3754	1.0031	0.5091
Hénon	0.4961	7.5347	0.1360	0.9742	0.5008

5.4. Compression Ratio

The compression ratios are given in Table 1. Four maps (Logistic, Tent, Sine, and PWLCM) made an incompressible ciphertext (ratio 1.0031). This Hénon map, which has an entropy score of 7.5347, was compressed to 0.9742, thus representing detectable redundancy in its output.

5.5. Key Sensitivity (Avalanche Effect)

Figure 4 shows BER vs key perturbation magnitude for all 5 maps. The values of BER for all maps are in the vicinity of 0.50 (Logistic 0.5018, Tent 0.5033, Sine 0.5029, PWLCM 0.5091, and Hénon 0.5008); they indicate very strong key sensitivity in all maps.

With either of these maps, a ciphertext is very different for a single-bit change in the key. The key major differences between maps, then, are on the statistical side of things and not on the avalanche side of things.

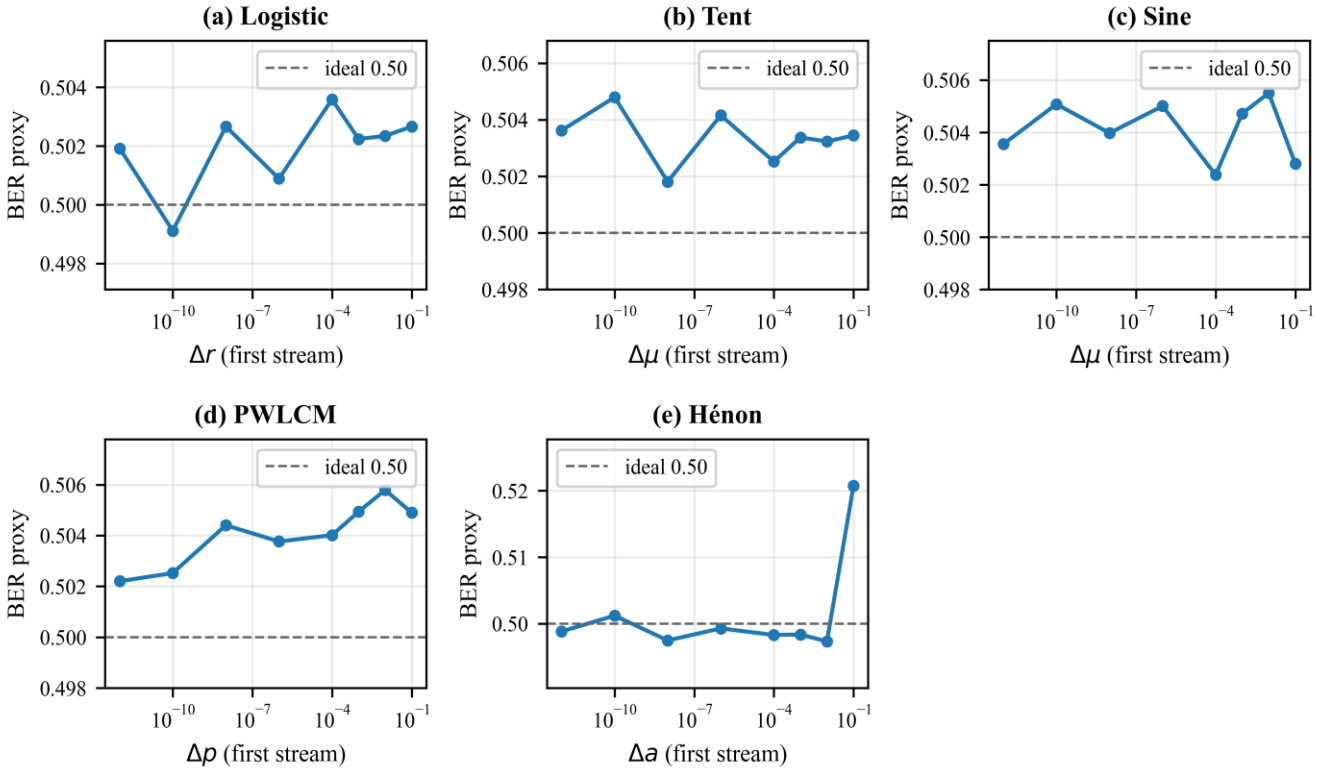

Fig. 4 Shows the avalanche bit error rate (BER) (y-axis) as a function of the key perturbation magnitude (x-axis) on a log scale for each map considered: (a) Logistic map, (b) Tent map, (c) Sine map, (d) PWLCM, and (e) Hénon map. The ideal BER is 0.50.

5.6. Discussion

The tent map was the most regular of the maps for producing random text. It has the characteristic of uniform invariant density on [0, 1], naturally resulting in very close bit balance, low byte correlation and high entropy. This is in line with previous research, which has shown that suitably parameterised tent-map PRNGs can serve as cryptographic-quality systems [8].

This bias towards 1 bits was a detriment to the logistic map because of the non-uniform invariant density near $r = 4$, where bits tend to be concentrated at the extremes. The Hénon map, although being a two-dimensional map, did not do well in the entropy and compressibility; probably due to finite-precision effects which produce short lengths of internal cycles, reducing the randomness of the output. In order to add dimensionality to improve the cryptographic capability, the extraction process must make complete use of the entropy provided.

For bits balance and entropy, PWLCM was quite good, with very high adjacent-byte correlation. However, this is due to the piecewise linear nature, causing the creation of short deterministic patterns. The sine map was actually pretty close to the tent map; a small tweak of the parameters may make it match the tent map. Again, in all 5 maps, avalanche properties were good, and the statistical quality of the keystream was not a more general characteristic of chaotic systems than key sensitivity.

These findings have a number of caveats. All these measures are statistical, but statistical testing is not enough for security: Preishuber et al. demonstrated that there exist encryption schemes that were designed to be insecure, but passed the widely used test batteries [20]. This study does not provide any attempt at cryptanalysis, not even a known-plaintext, chosen-plaintext or key-recovery attack. The XOR construction used here is trivially broken if a keystream is reused. The sample is also small. The statistics for the ciphertexts were taken over 3,524 bytes, of which the expected entropy of a truly random source is 7.9478 bits/byte; the tent map's 7.9468 sits at that ceiling, so any differences between the best maps should not be taken too literally.

The standard error for the Pearson coefficient on this sample is 0.0168, so that the −0.0896 for the sine map and the +0.0863 for the logistic map are equally likely true, and each is at 5.3 and 5.1 standard deviations from the true value of 0. The avalanche figure shown here is the mean of the bits recovered, and if the key is incorrect, it is not a BER between two ciphertexts. Last, but not at all least, the key space was not quantified; a total of eight double precision quantities nominally participate, but neighbouring values of these parameters lead to correlated orbits, which decrease the actual key space. There are existing studies of finite precision dynamical degradation of digital chaotic maps [21].

6. Conclusion

In this research work, a basic XOR stream cipher has been used, and five chaotic maps have been compared as Pseudorandom (PR) keystream generators for the XOR stream cipher. The tent map consistently produced the most cryptographically suitable results, having very close to perfect bit balance, maximum entropy, extremely low byte correlation, incompressible ciphertext and excellent key sensitivity. But a logistic map is not suitable due to the high bit bias. PWLCM has problematic adjacent-byte correlation and good entropy. Secondly, the Hénon map was not as good as the simpler 1D maps, most likely because of the degradation of the trajectories due to the finite precision.

An important result is the lack of a direct link between mathematical chaos and randomness in cryptography. The output has to be carefully extracted, the invariant density must be uniform, and the parameters must be appropriately set. The implications for the designers of lightweight chaos-based stream ciphers are that a test for any candidate map should be done in a rigorous statistical way before implementation.

7. Future Scope

Several lines of extension of this work are possible. First, it can be extended to hyper chaotic systems like 4D Lorenz or 3D Chen systems, and it can be verified whether or not there is a possibility to make the dimensionality of the chaos further up, so that the quality of the keystream will increase further. Secondly, there is a formally defined test of randomness in the NIST SP 800-22 testing criteria for randomness that can be applied to each map, to see if it is random [13]. Third, other methods than thresholding for extracting the output information (bit interleaving, delayed feedback perturbation and mixing using multiple maps) can be examined.

Fourth, the precision of the Hénon map is lost and needs careful study, which can be done either with greater precision numbers or by perturbation methods to obtain its theoretical properties. Fifth, a more complete parameter sweep of the entire range of chaos could be done, yielding design information. Finally, the study of FPGA would determine if the efficiency of simpler maps like the tent map and PWLCM can be obtained in a resource-constrained system (like an embedded system). Such a study would take into account the cost of the maps used—namely, the tent map has two multiplications and a comparison operation per output bit. In contrast, the sine map will use a transcendental function that is realised either by a lookup table or a CORDIC stage on hardware that does not incorporate a floating-point unit [16],[17]. Side-channel resistance is not taken into account in the statistics and is also a problem during deployment [18, 19]. Portability is another practical factor. The logistic, tent, PWLCM and Hénon maps use only

IEEE-754 multiplication, addition, subtraction and division, so they will reproduce bit-identically on any platform that conforms to IEEE-754. The one ratio of the sine map, however, does change; it shifts by about 0.001 on the re-running of the present benchmark on two different operating systems, which is sufficient to distinguish their trajectories. This is disqualifying for a stream cipher, for example, because if the sender and receiver platforms were different, then they would generate different keystreams, and decryption would not work.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgments

The author thanks the faculty of Sanskriti School, Chanakyapuri, New Delhi, and his research mentors for their guidance throughout the design and analysis of this study.

Appendix 1

Figure 5 reports the keystream autocorrelation function for each map. An ideal PRNG shows negligible autocorrelation at all non-zero lags.

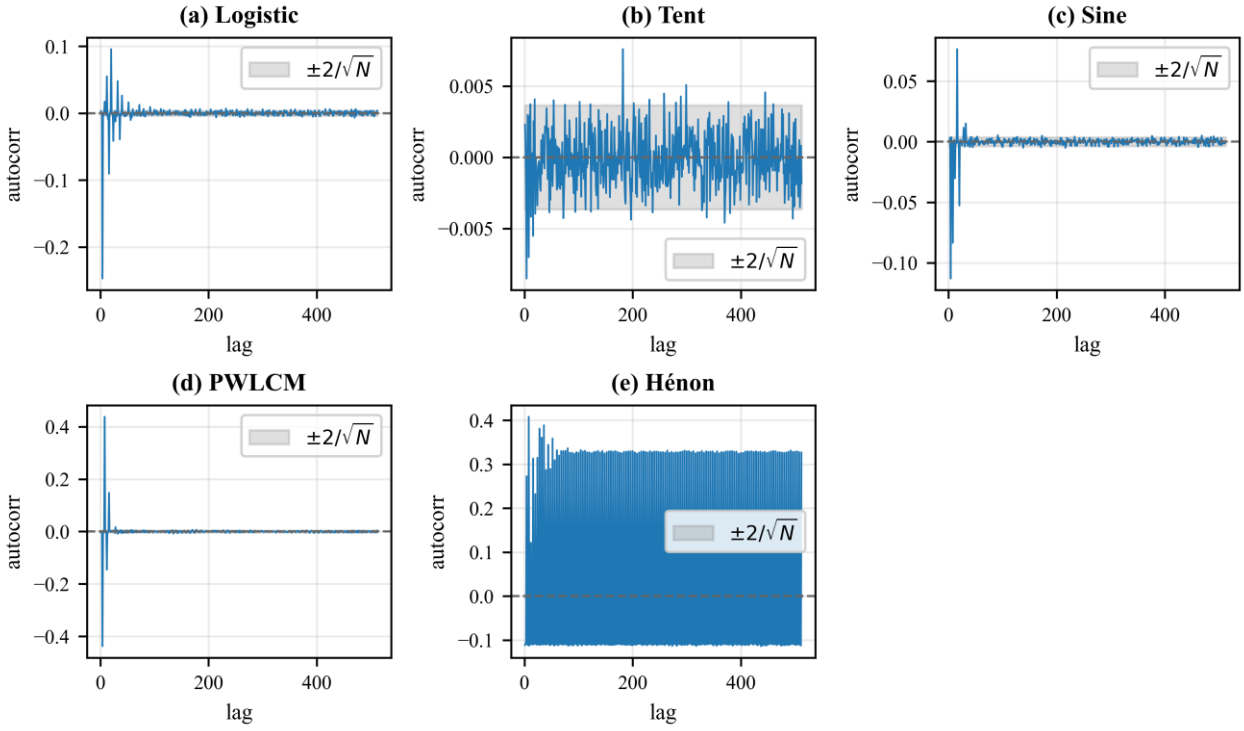

Fig. 5 Autocorrelation of keystreams for each map: ***(a) Logistic, (b) Tent, (c) Sine, (d) PWLCM, and (e) Hénon.***

References

[1] Why is Ciphertext from Low Entropy Plaintext Not Compressible?," Cryptography. [Online]. Available: https://crypto.stackexchange.com/questions/2921/why-is-ciphertext-from-low-entropy-plaintext-not-compressible

[2] Lawlor, Information Theory, Entropy, and Key Strength, CS 463 Lecture Notes, 2013. [Online]. Available: https://www.cs.uaf.edu/2013/spring/cs463/lecture/01_25_entropy.html

[3] Avalanche Effect, Wikipedia, The Free Encyclopedia. [Online]. Available: https://en.wikipedia.org/wiki/Avalanche_effect

[4] Alexandru Dinu, and Madalin Frunzete, "Image Encryption using Chaotic Maps: Development, Application, and Analysis," *Mathematics*, vol. 13, no. 16, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Bingbing Song, and Qun Ding, "Comparisons of Typical Discrete Logistic Map and Henon Map," *Intelligent Data analysis and its Applications, Volume I: Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications*, Shenzhen, China, vol. 297, pp. 267-275, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[6] Madhu Sharma, and Priyanka Chawla, "An Image Encryption Algorithm using a XOR Enhanced 2D-Henon Map," *Cluster Computing*, vol. 28, no. 6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Abeer Al-Hyari et al., "Chaotic Hénon-Logistic Map Integration: A Powerful Approach for Safeguarding Digital Images," *Journal of Cybersecurity and Privacy*, vol. 5, no. 1, pp. 1-30, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ahmad Al-Daraiseh et al., "Cryptographic Grade Chaotic Random Number Generator based on Tent-Map," *Journal of Sensor and Actuator Networks*, vol. 12, no. 5, pp. 1-26, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Longxiang Yin, Yongzhen Li, and Zhexu Jin, "A Bit-Level Color Image Encryption Algorithm based on PWLCM Chaotic Maps," *Proceedings of SPIE 13516, Fourth International Conference on Network Communication and Information Security*, Hangzhou, China, vol. 13516, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yucheng Chen, Chunming Tang, and Zongxiang Yi, "A Novel Image Encryption Scheme based on PWLCM and Standard Map," *Complexity*, vol. 2020, no. 1, pp. 1-23, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] A. Hasheminejad, and M.J. Rostami, "A Novel Bit Level Multiphase Algorithm for Image Encryption based on PWLCM Chaotic Map," *Optik*, vol. 184, pp. 205-213, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Talha Umar, Mohammad Nadeem, and Faisal Anwer, "A New Modified Skew Tent Map and its Application in Pseudo-Random Number Generator," *Computer Standards & Interfaces*, vol. 89, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Monobit Test, Computer Security Resource Center, National Institute of Standards and Technology. [Online]. Available: https://csrc.nist.gov/glossary/term/monobit_test

[14] Daniel Murillo-Escobar et al., "Pseudorandom Number Generator based on Novel 2D Hénon-Sine Hyperchaotic Map with Microcontroller Implementation," *Nonlinear Dynamics*, vol. 111, no. 7, pp. 6773-6789, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Gonzalo Alvarez, and Shujun Li, "Some Basic Cryptographic Requirements for Chaos-based Cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[16] Miguel Garcia-Bosque et al., "Chaos-based Bitwise Dynamical Pseudorandom Number Generator on FPGA," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 1, pp. 291-293, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Fethi Dridi et al., "The Design and FPGA-based Implementation of a Stream Cipher based on a Secure Chaotic Generator," *Applied Sciences*, vol. 11, no. 2, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Yuling Luo et al., "Cryptanalysis of Chaos-based Cryptosystem from the Hardware Perspective," *International Journal of Bifurcation and Chaos*, vol. 28, no. 9, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mehmet Sahin Acikkapi, Fatih Ozkaynak, and Ahmet Bedri Ozer, "Side-Channel Analysis of Chaos-based Substitution Box Structures," *IEEE Access*, vol. 7, pp. 79030-79043, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mario Preishuber et al., "Depreciating Motivation and Empirical Security Analysis of Chaos-based Image and Video Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137-2150, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[21] Shujun Li, Guanrong Chen, and Xuanqin Mou, "On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119-3151, 2005. [CrossRef] [Google Scholar] [Publisher Link]