



Enhanced chaotic maps for sustainable cryptographic security: A comparative study

Nasr-Eddine Mellah^a , Samir Ladaci^b , Murilo S. Baptista^c ,
Celso Grebogi^d 

^aDepartment of Electronics, DCCP Lab, National Polytechnic School,
El Harrach 16200 Algiers, Algeria
nasr_eddine.mellah@g.enp.edu.dz

^bDepartment of Automatic Control Engineering, National Polytechnic School,
El Harrach 16200 Algiers, Algeria
samir.ladaci@g.enp.edu.dz

^cDepartment of Physics, Institute for Complex Systems and Mathematical Biology,
University of Aberdeen, Aberdeen AB24 3UX, United Kingdom
murilo.baptista@abdn.ac.uk

^dInstitute for Complex Systems and Mathematical Biology,
University of Aberdeen, Aberdeen AB24 3UE, United Kingdom
grebogi@abdn.ac.uk

Received: December 26, 2025 / **Revised:** April 3, 2026 / **Published online:** May 25, 2026

Abstract. We propose a comparative study of chaotification techniques that enhance the complexity of one-dimensional maps for sustainable cryptographic applications. Specifically, we examine the use of modulo operation, remainder operation, and k -deep-zoom (k -DZ) transformation applied to the sine map. Each technique's effectiveness is analyzed using bifurcation diagrams, Lyapunov exponents, and correlation results. Additionally, the statistical performance of the techniques is assessed using the NIST SP 800-22 battery of tests, and the computational efficiency is evaluated in terms of the number of operations. The study aims to identify the best chaotification method for generating robust pseudorandom bit generators (PRBGs) suitable for secure encryption and sustainable cryptography.

Keywords: chaotification, cryptography, Lyapunov exponents, NIST tests, complexity enhancement.

1 Introduction

Data security through encryption based on fractional-order chaotic systems has attracted the interest of a great number of researchers because of their advantageous properties such as long memory, inherent unpredictability, and sensitivity to initial conditions [9, 18, 26]. Nowadays, sustainable cryptography has the objective to balance information security

with the lowest environmental impact in order to guarantee long-term viability [1, 25]. In particular, much recent work has considered their use in improving cryptographic security by developing and using chaos processing algorithms to protect and obscure transmitted information [2–4]. Many among these techniques were dedicated to image encryption [7, 15, 20, 30]. A major research direction is focused on consolidating the complexity of encryption systems through the introduction of chaotic fractional-order systems [6, 11, 31] and guaranteeing improved secure communication [8, 12, 14]. Their control, synchronization, and stability analysis are the subject of extensive investigations [13, 19, 27].

One-dimensional chaotic maps, such as the sine map, offer a simple yet effective platform for developing pseudorandom bit generators (PRBGs). Many recent works have been developed in this area: Soni et al. [28] reviewed the state of the art to illustrate the potential of chaotic maps for cryptography applications and the growing significance of data security in present time. In [17] a novel one-dimensional sine powered chaotic map was designed and applied in a new image encryption scheme. Recently, Htiti et al. [10] proposed a new one-dimensional chaotic map with improved sine map dynamics. Moysis et al. [21, 23] introduced a chaotification method for one-dimensional maps based on remainder operator addition. Talhaoui et al. [29] proposed a new one-dimensional cosine polynomial (1-DCP) chaotic map and its use in image encryption. Beal [5] presented an algorithm for extracting basis functions from the chaotic Lorenz system along with timing and bit-sequence statistics. However, the basic sine map may not provide sufficient complexity for robust encryption, necessitating the development of chaotification techniques to increase unpredictability [16, 22, 24].

This paper presents a comparative analysis of three chaotification techniques: the modulo operation, the remainder operation, and the k -deep-zoom (k -DZ) transformation. The objective is to identify which method best enhances the complexity of the sine map, making it more suitable for cryptographic applications. To assess each technique, we utilize bifurcation diagrams, Lyapunov exponents, and statistical correlation analysis, alongside the NIST SP 800-22 battery of tests. We also compare the computational efficiency of each method to provide a comprehensive evaluation.

This article continues as follows: Section 2 introduces some mathematical foundations for the considered encryption techniques. In Section 3, we present a detailed comparison of three chaotification techniques: modulo operation, remainder operation, and k -deep-zoom (k -DZ) transformation. Section 4 gives the concluding remarks.

2 Methodology

This section presents the mathematical formulations for the proposed chaotification techniques, integrating the sine map as the core model.

2.1 Sine map definition

The sine map, serving as the basis of the chaotic system, is defined as

$$x_i = r \sin(\pi x_{i-1}),$$

where:

- r is the control parameter ranging from 1 to 10,
- x_i represents the state at iteration i , and
- $x_0 = 0.5$ is the initial condition.

2.2 Modulo operation

The modulo operation enhances the sine map's complexity by constraining its output within a fixed range. It is expressed as

$$B_i = \text{mod}(\lfloor 10^k \cdot x_i \rfloor, 256),$$

where:

- k is the zoom factor, set at values 10 and 15 to test different sensitivity levels,
- x_i is the current state of the sine map at iteration i .

2.3 Remainder operation

The remainder operation further enhances the system's complexity by adding multiple scaled values:

$$x_i = H_m(x_{i-1}) = F(x_{i-1}) + \sum_{j=1}^m \text{rem}(a_j \sin(\pi x_{i-1}), N_j),$$

where:

- $F(x_{i-1})$ denotes the original sine map,
- $a_j > 0$ are control parameters scaling the remainder terms,
- $N_j \in \mathbb{R}^+$ maps the remainder results within $(-N_j, N_j)$,
- $m \in \mathbb{N}$ specifies the number of terms.

For simplicity, we use $N = 1$ to constrain the domain. Two specific cases illustrate the technique.

Case 1 (10 remainders, $a_j = 20^j$):

$$x_i = r \sin(\pi x_{i-1}) + \sum_{j=1}^{10} \text{rem}(20^j x_{i-1}, 1).$$

Case 2 (15 remainders, $a_j = 20^j$):

$$x_i = r \sin(\pi x_{i-1}) + \sum_{j=1}^{15} \text{rem}(20^j x_{i-1}, 1).$$

2.4 k -deep-zoom (k -DZ) transformation

The k -DZ transformation intensifies chaotic behavior by zooming on specific decimal places:

$$\phi_k(x) = x \cdot 10^k - \lfloor x \cdot 10^k \rfloor,$$

where $k \in \{10, 15\}$ controls the zoom level. The derivative

$$\frac{d}{dx}\phi_k(x) = 10^k$$

shows how the transformation scales sensitivity.

2.5 Evaluation criteria

The following metrics assess the effectiveness of the chaotification techniques:

1. *Bifurcation diagrams* visualize changes in system behavior with $r \in [1, 10]$ and $x_0 = 0.5$, showing transitions from periodic to chaotic behavior.
2. *Lyapunov exponents (LE)* measure the rate of divergence of nearby trajectories, indicating chaos when $\lambda > 0$. The LE is calculated as

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \ln \left| \frac{xi_i}{dx_{i-1}} \right|.$$

3. *Correlation analysis* evaluates statistical properties to ensure low correlation between successive outputs.
4. *NIST SP 800-22 tests* validate the randomness and unpredictability of generated sequences.
5. *Computational efficiency* analyzes and optimizes the execution time and resource usage of the techniques.

3 Results and discussion

This section presents a detailed comparison of three chaotification techniques: modulo operation, remainder operation, and k -deep-zoom (k -DZ) transformation. The comparison is based on bifurcation diagrams, Lyapunov exponents, correlation analysis, and statistical tests. Additionally, the computational efficiency of each technique is evaluated to determine their suitability for cryptographic systems.

3.1 Bifurcation diagrams

Bifurcation diagrams visually represent a system's dynamics as a key parameter varies. For the sine map, they illustrate how each chaotification technique affects the map's behavior.

Modulo operation. The bifurcation diagram for the modulo operation applied to the sine map (Fig. 1) shows an increase in the number of bifurcations and transitions to chaotic regions. Despite the complex patterns, periodic windows occasionally emerge, indicating temporary nonchaotic behavior.

Remainder operation. The remainder operation produces a dense bifurcation diagram with fewer periodic windows (Fig. 2), indicating sustained chaos. The disruption of periodicity leads to enhanced unpredictability.

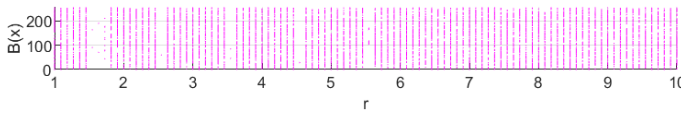


Figure 1. Bifurcation diagram for $B(x)$ with respect to r .

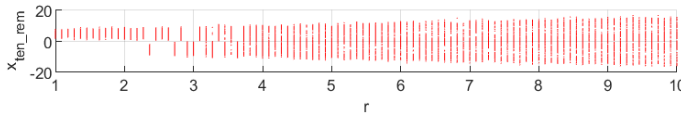


Figure 2. Bifurcation diagram (10 remainders) for x_{ten_rem} with respect to r .

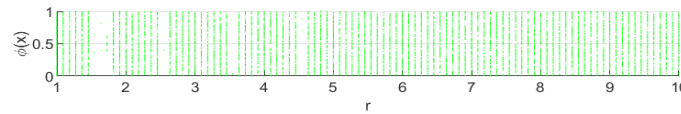


Figure 3. Bifurcation diagram for $\phi(x)$ with respect to r .

k-deep-zoom transformation. The *k*-DZ transformation results in a gradual increase in complexity (Fig. 3). Higher values of *k* enhance the map’s sensitivity to initial conditions, though they require careful tuning to avoid degeneracies.

3.2 Lyapunov exponents (LE)

Lyapunov exponents provide a numerical measure of chaos, where higher values indicate stronger chaotic behavior—an essential quality for cryptographic applications.

Modulo operation. LE analysis shows a moderate increase, suggesting enhanced chaos (Fig. 4). However, the plateau observed indicates that increasing *k* beyond a point does not significantly enhance chaotic behavior.

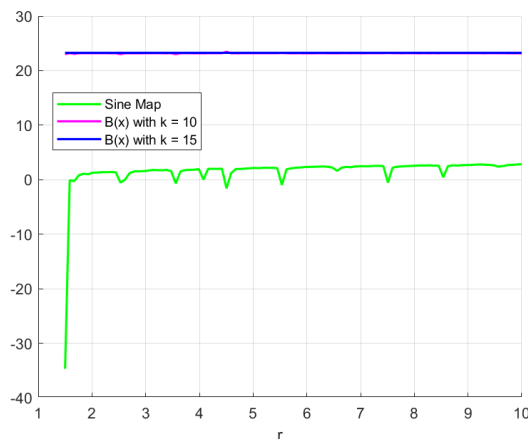


Figure 4. Lyapunov exponents of $B(x)$ for $k = 10$ and $k = 15$ with respect to r .

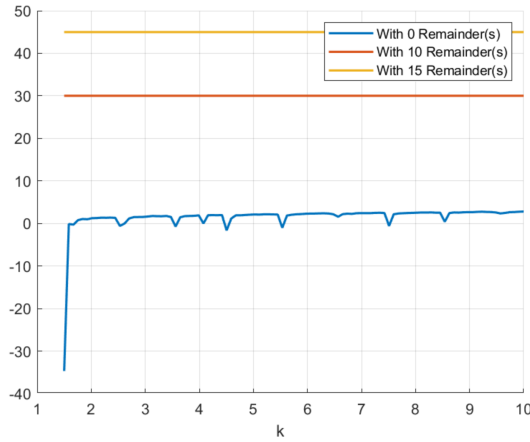


Figure 5. Lyapunov exponents of the remainder operation for 10 and 15 remainders with respect to r .

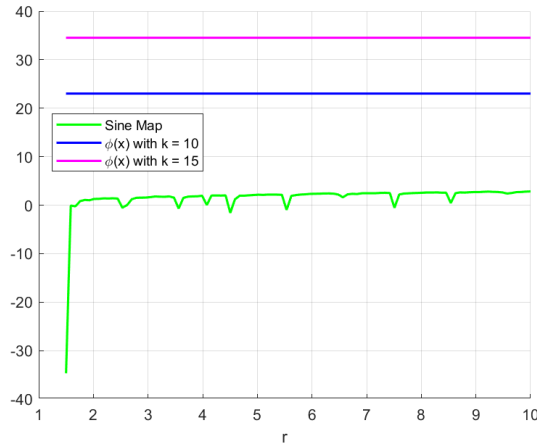


Figure 6. Lyapunov exponents of the k -DZ transformation $\phi(x)$ for $k = 10$ and $k = 15$ with respect to r .

Remainder operation. This technique yields the highest LE values (Fig. 5), signifying consistent chaotic behavior across a wide range of parameters, making it suitable for robust pseudorandom bit generation.

k-deep-zoom transformation. The k -DZ transformation shows a similar trend to the modulo operation (Fig. 6), with higher k values leading to increased LE values. Although not as pronounced as the remainder operation, it remains a viable option.

3.3 Correlation analysis

Correlation analysis evaluates the effectiveness of chaotification in disrupting predictability in output sequences, critical for generating pseudorandom bit sequences.

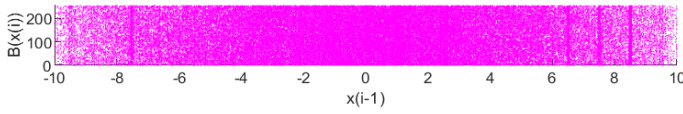


Figure 7. Phase diagram for $B(x(i))$ vs. $x(i - 1)$.

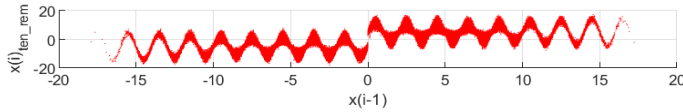


Figure 8. Phase diagram for 10 remainders $x(i)_{\text{ten_rem}}$ vs. $x(i - 1)$.

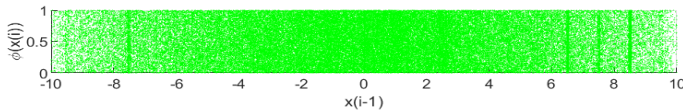


Figure 9. Phase diagram for $\phi(x)$ vs. $x(i - 1)$.

Modulo operation. Correlation analysis reveals moderate unpredictability (Fig. 7), though periodic windows suggest potential vulnerabilities.

Remainder operation. This technique minimizes correlation, leading to highly unpredictable sequences (Fig. 8), enhancing cryptographic security.

k-deep-zoom transformation. The k -DZ transformation provides unpredictability comparable to the modulo operation (Fig. 9), especially at higher k values.

3.4 Summary

All three chaotification techniques improve the sine map’s unpredictability, with the remainder operation demonstrating the most robust performance. While the k -DZ transformation remains competitive with the modulo operation, its simplicity and efficiency make it a viable alternative. Each technique offers distinct advantages that make it suitable for various cryptographic applications based on specific requirements and constraints.

3.5 NIST SP 800-22 tests

Table 1. NIST SP 800-22 results (significance level = 0.01). Bold indicates failure (p – value < 0.01).

Test	Modulo	k -deep-zoom	With eemainder
Frequency	Pass	Pass	Pass
BlockFrequency	Fail (0.009)	Pass	Pass
CumulativeSums	Pass	Pass	Pass
Runs	Pass	Pass	Pass
LongestRun	Pass	Pass	Pass
Rank	Pass	Fail (0.003)	Pass
FFT	Pass	Pass	Pass

Continued on next page

Table 1 (continued from previous page)

Test	Modulo	k -deep-zoom	With remainder
NonOverlappingTemplate	Pass	Pass	Pass
OverlappingTemplate	Pass	Pass	Pass
Universal	Pass	Pass	Pass
ApproximateEntropy	Pass	Pass	Pass
RandomExcursions	Pass	Pass	Pass
RandomExcursionsVariant	Pass	Pass	Pass
Serial	Pass	Pass	Pass
LinearComplexity	Pass	Pass	Pass

3.6 Computational efficiency

Lastly, we evaluate the computational efficiency of each technique, as this factor is crucial for real-time applications.

3.6.1 Modulo operation

This operation exhibits relatively low computational cost, making it suitable for environments with limited resources. The simplicity of the modulo operation allows for rapid calculations, crucial for applications that require quick response times:

$$\text{Total Time} = 3 \text{ units (constant for any } k\text{)}.$$

Efficiency. Highly efficient, suitable for low-resource environments.

3.6.2 Remainder operation

While slightly more complex than the modulo operation, the remainder operation remains computationally efficient. The addition of terms introduces minimal overhead, allowing for real-time processing without significant delays:

$$\text{Total Time} = 3m + 2 \text{ units (dependent on } m\text{)}.$$

Efficiency. Efficient for real-time applications, but computational load increases linearly with the number of terms m .

3.6.3 k -deep-zoom (k -DZ) transformation

This technique presents a trade-off between computational complexity and enhanced chaotic behavior. The k -DZ transformation may require more processing power, especially at higher values of k , potentially limiting its use in environments with stringent computational constraints:

$$\text{Total Time} = 3 \text{ units (constant for any } k\text{)}.$$

Efficiency. Slightly less efficient than the modulo operation but still manageable for most real-time applications. For higher values of k , the processing cost might increase due to precision requirements.

Table 2. Modulo operation computational steps.

Step #	Operation	Formula	Time (units)
1	Multiply x_i by 10^k	$10^k \cdot x_i$	1
2	Floor operation	$\lfloor 10^k \cdot x_i \rfloor$	1
3	Modulo operation	$\text{mod}(\lfloor 10^k \cdot x_i \rfloor, 256)$	1

Table 3. Remainder operation computational steps.

Step #	Operation	Formula	Time (units)
1	Sinusoidal calculation	$\sin(\pi x_{i-1})$	1
2	Multiply by a_j	$a_j \sin(\pi x_{i-1})$	1
3	Remainder operation	$\text{rem}(a_j \sin(\pi x_{i-1}), N_j)$	1
4	Summation over m terms	$\sum_{j=1}^m [\dots]$	$m \times 3$
5	Add to $F(x_{i-1})$	$F(x_{i-1}) + [\dots]$	1

Table 4. k -deep-zoom transformation computational steps.

Step #	Operation	Formula	Time (units)
1	Multiply x by 10^k	$x \cdot 10^k$	1
2	Floor operation	$\lfloor x \cdot 10^k \rfloor$	1
3	Subtract floor from product	$x \cdot 10^k - \lfloor x \cdot 10^k \rfloor$	1

4 Conclusion

This study compared three chaotification techniques for sustainable cryptography—modulo operation, remainder operation, and k -deep-zoom transformation—applied to the sine map. Each method demonstrated unique strengths in enhancing the map’s complexity, as evident from bifurcation diagrams, Lyapunov exponents, and statistical tests. The remainder operation showed significant improvement in generating pseudorandom sequences with higher Lyapunov exponents, while the k -DZ transformation offered a straightforward method to increase complexity with minimal computational cost. Future work will focus on optimizing these techniques and testing them in more complex encryption protocols towards an improved sustainable cryptographic security.

Author contributions. All authors (N.-E.M., S.L., M.S.B., and C.G.) have contributed as follows: formal analysis, N.-E.M., S.L., M.S.B., and C.G.; methodology, N.-E.M. and S.L.; software, N.-E.M.; writing – original draft, N.-E.M. and S.L.; writing – review & editing, S.L. All authors have read and approved the published version of the manuscript.

Conflicts of interest. The authors declare no conflicts of interest.

References

1. Abhishek, R. Sehrawat, Sustainable image-based encryption using cryptography and steganography with autoencoder, in M.A. Alam, F. Siddiqui, S. Zafar, I. Hussain (Eds.), *Proceedings of 4th International Conference on ICT for Digital, Smart, and Sustainable Development*.

- ICIDSSD 2024. Innovations in Sustainable Technologies and Computing*, Springer, Singapore, 2024, p. 205–214, https://doi.org/10.1007/978-981-97-7831-7_14.
2. M. Abodawood, A.T. Khalil, H.M. Amer, M.M. Ata, Enhancing image encryption using chaotic maps: A multi-map approach for robust security and performance optimization, *Cluster Comput.*, **27**:14611–14635, 2024, <https://doi.org/10.1007/s10586-024-04672-4>.
 3. M. Alawida, Enhancing logistic chaotic map for improved cryptographic security in random number generation, *J. Inf. Secur. Appl.*, **80**:103685, 2024, <https://doi.org/10.1016/j.jisa.2023.103685>.
 4. M. Alawida, A. Samsudin, J.S. Teh, W.H. Alshoura, Digital cosine chaotic map for cryptographic applications, *IEEE Access*, **7**:150609–150622, 2019, <https://doi.org/10.1109/ACCESS.2019.2947561>.
 5. A.N. Beal, Extracting communication, ranging and test waveforms with regularized timing from the chaotic Lorenz system, *Signals*, **4**(3):507–523, 2023, <https://doi.org/10.3390/signals4030027>.
 6. L. Chao, Asynchronous error-correcting secure communication scheme based on fractional-order shifting chaotic system, *Int. J. Mod. Phys. C*, **26**(6):1550065, 2015, <https://doi.org/10.1142/S0129183115500655>.
 7. R. Chapaneri, T. Sarode, S. Chapaneri, Digital image encryption using improved chaotic map lattice, in *2013 Annual IEEE India Conference (INDICON), Mumbai, India, 13–15 December 2013*, IEEE, Piscataway, NJ, 2013, pp. 1–6, <https://doi.org/10.1109/INDCON.2013.6726031>.
 8. Y.-S. Deng, K.-Y. Qin, W. Xiang, Performance analysis of fractional order DCSK secure communication system, in *2009 International Conference on Communications, Circuits and Systems, Milpitas, CA, 23–25 July 2009*, IEEE, Piscataway, NJ, 2009, pp. 850–852, <https://doi.org/10.1109/ICCCAS.2009.5250388>.
 9. M.M. Hadji, S. Ladaci, A novel secure communication scheme design using a fractional-order adaptive observer-based synchronization, *J. Control Autom. Electr. Syst.*, **36**(4):267–282, 2025, <https://doi.org/10.1007/s40313-025-01147-8>.
 10. M. Htiti, I. Akharraz, A. Ahaitouf, A novel one-dimensional chaotic map with improved sine map dynamics, *Int. J. Electr. Comput. Eng.*, **15**(2):2128–2137, 2025, <https://doi.org/10.11591/ijece.v15i2.pp2128-2137>.
 11. S. Iqbal, J. Wang, A novel fractional-order 3-D chaotic system and its application to secure communication based on chaos synchronization, *Phys. Scr.*, **100**(2):025243, 2025, <https://doi.org/10.1088/1402-4896/ad9cfe>.
 12. A. Khan, L.S. Jahanzaib, P. Trikha, Secure communication: Using parallel synchronization technique on novel fractional order chaotic system, *IFAC-PapersOnLine*, **53**(1):307–312, 2020, <https://doi.org/10.1016/j.ifacol.2020.06.052>.
 13. K. Khettab, S. Ladaci, Y. Bensafia, Fuzzy adaptive control of fractional order chaotic systems with unknown control gain sign using a fractional order Nussbaum gain, *IEEE/CAA J. Autom. Sin.*, **6**(3):816–823, 2019, <https://doi.org/10.1109/JAS.2016.7510169>.
 14. M.K. Kirubakaran, P.S. Reddy, A. Mamatha, J. Vellingiri, Enhanced VANET communication: Fractional order water flow optimization and secure communication via spatial Bayesian neural network, *Int. J. Commun. Syst.*, **38**(12):e70147, 2025, <https://doi.org/10.1002/dac.70147>.

15. I.J.Y. Lim, A. Mandangan, Chaotic encryption scheme for colour image using 3D Lorenz chaotic map and 3D Chen system, *Int. J. Comput. Think. Data Sci.*, **1**(1):10–24, 2024, <https://doi.org/10.37934/ctds.1.1.1024a>.
16. J. Machicao, O.M. Bruno, M.S. Baptista, Zooming into chaos as a pathway for the creation of a fast, light and reliable cryptosystem, *Nonlinear Dyn.*, **104**(1):753–764, 2021, <https://doi.org/10.1007/s11071-021-06280-y>.
17. A. Mansouri, X. Wang, A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme, *Inf. Sci.*, **520**:46–62, 2020, <https://doi.org/10.1016/j.ins.2020.02.008>.
18. N.-E. Mellah, S. Ladaci, Feedback state space stabilization of fractional-order chaotic Lorenz-84 atmosphere model, in *Proceedings of the 4th International Conference on Advanced Engineering in Process Intelligence (ICAEPI2023), 28-30 November, 2023, Skikda, Algeria, 2023*, pp. 1–6.
19. N.-E. Mellah, S. Ladaci, PSO-based fractional-order PID control for stabilizing the chaotic Lorenz-84 atmosphere model, *Alger. J. Signals Syst.*, **10**(3):128–134, 2025, <https://doi.org/10.51485/ajss.v10i3.278>.
20. D.E. Mfungo, X. Fu, Y. Xian, X. Wang, A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information, *Appl. Sci.*, **13**(12):7113, 2023, <https://doi.org/10.3390/app13127113>.
21. L. Moysis, I. Kafetzis, M.S. Baptista, C. Volos, Chaotification of one-dimensional maps based on remainder operator addition, *Mathematics*, **10**(15):2801, 2022, <https://doi.org/10.3390/math10152801>.
22. L. Moysis, M. Lawnik, I.P. Antoniadis, I. Kafetzis, M.S. Baptista, C. Volos, Chaotification of 1D maps by multiple remainder operator additions—application to B-spline curve encryption, *Symmetry*, **15**(3):726, 2023, <https://doi.org/10.3390/sym15030726>.
23. L. Moysis, M. Lawnik, C. Volos, M.S. Baptista, G.F. Fragulis, S.K. Goudos, Validating a chaos based PRBG under different chaotic maps, in *2024 Panhellenic Conference on Electronics & Telecommunications (PACET), Thessaloniki, Greece, 28–29 March 2024, IEEE, Piscataway, NJ, 2024*, pp. 1–4, <https://doi.org/10.1109/PACET60398.2024.10497085>.
24. R.B. Naik, U. Singh, A review on applications of chaotic maps in pseudo-random number generators and encryption, *Ann. Data Sci.*, **11**:25–50, 2024, <https://doi.org/10.1007/s40745-021-00364-7>.
25. A. Ozpinar, S.I. Serengil, Towards sustainable cryptography: A comprehensive assessment of compute efficiency and scope 1–3 emissions for partially homomorphic encryption in the cloud, *Preprints*, **2025**:2025021845, 2025, <https://doi.org/10.20944/preprints202502.1845.v1>.
26. K. Rabah, S. Ladaci, A fractional adaptive sliding mode control configuration for synchronizing disturbed fractional order chaotic systems, *Circuits Syst. Signal Process.*, **39**(3):1244–1264, 2020, <https://doi.org/10.1007/s00034-019-01205-y>.
27. K. Rabah, S. Ladaci, M. Lashab, Bifurcation-based fractional order $PI^\lambda D^\mu$ controller design approach for nonlinear chaotic systems, *Front. Inf. Technol. Electron. Eng.*, **19**(2):180–191, 2018, <https://doi.org/10.1631/FITEE.1601543>.

28. R. Soni, M.K. Thukral, N. Kanwar, A relative investigation of one-dimensional chaotic maps intended for light-weight cryptography in smart grid, *e-Prime Adv. Electr. Eng. Electron. Energy*, **7**(100421), 2024, <https://doi.org/10.1016/j.prime.2024.100421>.
29. M.Z. Talhaoui, X. Wang, M.A. Midoun, A new one-dimensional cosine polynomial chaotic map and its use in image encryption, *Visual Comput.*, **37**(3):541–551, 2021, <https://doi.org/10.1007/s00371-020-01822-8>.
30. A. Varshney, P. Routh, G. Sujatha, Comparison of image encryption techniques using chaotic maps and conventional cryptographic techniques, in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, Vellore, India, IEEE, Piscataway, NJ, 2024, pp. 1–7, <https://doi.org/10.1109/ic-ETITE58242.2024.10493645>.
31. Z. Yu, S. Ling, P.X. Liu, H. Wang, Compounding and synchronization of fractional order chaotic systems with prescribed performance for secure communication, *IEEE Trans. Circuits Syst. I, Regul. Pap.*, **71**(3):1335–1345, 2024, <https://doi.org/10.1109/TCSI.2023.3334036>.