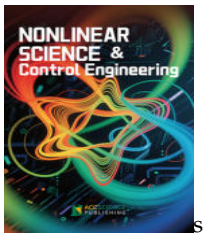
Contents lists available at AccScience Publishing
Nonlinear Science and Control Engineering (NSCE)
Vol. X, No. X (2025)
https://accscience.com/journal/nsce



Hybridization of benchmark functions for a high-performance 1D chaotic map and image encryption application

Uğur Erkan[1*], Abdurrahim Toktas[1], Feyza Toktas[2], Yiting Lin[3,4] and Suo Gao[5]

[1]*Department of Artificial Intelligence and Data Engineering, Faculty of Engineering, Ankara University, Golbasi, Ankara, Türkiye*
[2]*Department of Computer Engineering, Faculty of Engineering, Ankara University, Golbasi, Ankara, Türkiye*
[3]*Guangdong Provincial/Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science, Beijing Normal-Hong Kong Baptist University, Zhuhai, Guangdong, China*
[4]*Department of Computer Science, Faculty of Science, Hong Kong Baptist University, Hong Kong, China*
[5]*School of Information Science and Engineering, Dalian Polytechnic University, Dalian, Liaoning, China*

Article History:
Received: August 24, 2025
Revised: September 12, 2025
Accepted: September 15, 2025
Published online: October 14, 2025

ABSTRACT

Data security has become one of the most critical issues in information technology. Among the approaches developed to ensure secure data transmission and storage, chaotic maps play a central role due to their inherent unpredictability and sensitivity to initial conditions. In particular, 1D chaotic maps have attracted significant attention because of their low computational complexity and ease of implementation in practical systems. In this study, a novel 1D hybrid chaotic map is proposed through the hybridization of two widely used optimization benchmark functions, namely Problem 14 and Problem 20. The construction of the proposed map is based on multiplying and combining the initial and latter segments of these benchmark functions, followed by the incorporation of a control parameter to enhance its dynamic behavior. The newly designed chaotic system was rigorously evaluated through a series of standard security analyses, including statistical randomness tests, Lyapunov exponent, and sensitivity evaluations. Furthermore, the proposed map was integrated into an image encryption framework to validate its cryptographic applicability. A set of 10 natural images obtained from public datasets, along with the Lena color image, was employed to assess the practical performance of the encryption scheme. Extensive experiments covering information entropy, correlation analysis, chi-square and variance tests, the number of pixels change rate, and the unified average changing intensity metrics, as well as robustness evaluations under cropping and noise attacks, confirm that the proposed encryption scheme achieves high security and reliability. Comparative results demonstrate that the method performs competitively with, and in some metrics better than, state-of-the-art techniques.

Keywords: Chaos; Chaotic map; Image encryption; Nonlinear dynamics; One-dimensional map

(cc) BY

***Corresponding author(s)**:
Uğur Erkan (ugurerkan@ankara.edu.tr).

Citation:
Erkan U, Toktas A, Toktas F, Lin Y, and Gao S. Hybridization of benchmark functions for a high-performance 1D chaotic map and image encryption application. *Nonlinear Sci Cont Eng.* doi: 10.36922/NSCE025340010

Copyright: © 2025 The Author(s). This is an Open Access article distributed under the terms of the Creative Commons Attribution License, permitting distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Nowadays, the digital image is a widely used data format across almost every field.[1,2] In recent years, with the improvement of internet speed, the development of digital communication and the widespread use of smartphones, numerous images, and videos are transmitted through the internet.[3] However, transmissions made over unprotected channels increase the risks of unauthorized access, attacks, and threats. It is particularly important to conceal image content in areas where secure communication is critical, such as industrial projects, medical, and military applications. Therefore, techniques for the safe storage and transmission of digital images are receiving increasing attention.[4,5]

One-dimensional (1D) chaotic maps have gained significant interest in recent years due to their applications in secure communications, cryptography, and complex system modeling.[3] These maps are valued for their inherent sensitivity to initial conditions, high pseudo-randomness, and ability to generate complex dynamics from simple mathematical expressions. Evaluating the performance of a chaotic map often involves using benchmark functions that exhibit multimodal behavior and multiple local extrema, providing a rigorous test of nonlinearity, sensitivity, and unpredictability. Designing multi-dimensional chaotic maps is also of significant importance, as such systems exhibit richer dynamical behaviors and are extensively used in various applications, including secure communications, cryptography, image encryption, and complex system modeling. Their enhanced complexity and sensitivity make them valuable tools in fields requiring high unpredictability and robustness.[6–9]

Among the commonly used benchmark functions, Problem 14[10] and Problem 20[11] serve as standard tests for 1D chaotic systems. Problem 14 is a damped oscillatory function defined as the negative exponential of the variable multiplied by the sine of the variable. This function exhibits multiple local extrema and achieves its global minimum near the value of the variable equal to approximately 1.1951, with a function value of about -0.0635. Problem 20 is defined as the negative of the difference between the variable and its sine, multiplied by the exponential of the negative square of the variable. This function is also multimodal, with multiple local peaks and valleys, and its global minimum occurs near the same variable value as Problem 14. These two functions provide complementary dynamic features as follows: Problem 14 contributes damped oscillatory behavior, while Problem 20 offers a multimodal landscape with steep gradients.

In this study, we construct a novel hybrid 1D chaotic map by multiplicatively coupling the characteristic components of Problem 14 and Problem 20. The first components of the functions are combined to form a basic oscillator–transformer structure, while the second components are multiplied to introduce high-frequency, phase-controlled modulation. A control parameter, denoted as a, and a constant set as 2^{12}, are included to adjust phase and frequency. This multiplicative coupling produces strong nonlinear interaction at both amplitude and phase levels. The resulting hybrid map effectively inherits the damped oscillatory features from Problem 14 and the multimodal structure from Problem 20, creating a sum of two exponentially weighted nonlinear terms. The term corresponding to the exponential of the negative variable introduces asymmetric amplitude scaling, enhancing the folding mechanisms of the dynamics, whereas the exponential of the negative square of the variable constrains the behavior around the origin while generating steep gradients and frequent sign changes, reinforcing repeated stretching and folding processes. Additionally, the sine term with the scaled variable and phase modulation allows fine-grained control of oscillations and increases the density of critical points, which broadens the parameter regions where the magnitude of the derivative exceeds one. This ensures positive maximal Lyapunov exponents (LEs) and confirms chaotic behavior. Compared with the original benchmark functions individually, the hybrid map exhibits richer multimodality, stronger sensitivity to initial conditions, and a broader range of chaotic regimes, while remaining analytically tractable and easily tunable through its parameters.

To rigorously evaluate the proposed hybrid map, we conduct performance tests, including maximal LE analysis, bifurcation diagrams, and sensitivity tests with respect to initial conditions and control parameters. Positive LEs verify the presence of strong chaos, while bifurcation analysis identifies wide parameter regions with complex, aperiodic behavior. Sensitivity tests show that even infinitesimal changes in the initial values or control parameters produce drastically different trajectories, confirming the map's unpredictability. These characteristics demonstrate that the hybrid map is highly suitable for applications in secure communications, pseudo-random sequence generation, and other nonlinear systems requiring both high complexity and robustness.

The study of 1D chaotic maps has received significant attention in recent years due to their applications in secure communications, cryptography, and complex system modeling. Chaotic maps are particularly valued for their sensitivity to initial conditions, pseudo-randomness, and ability to generate complex dynamical behaviors from simple mathematical expressions. The performance of these maps is commonly assessed using benchmark functions that exhibit multimodal landscapes and multiple local extrema, providing a rigorous test of their nonlinear characteristics. In this context, Problem 14[7] and Problem 20[8] are widely used 1D multimodal benchmark functions. Problem 14 is characterized by damped oscillatory behavior with multiple local extrema and a global minimum near $x \approx 1.1951$ with $f(x) \approx -0.0635$. Similarly, Problem 20 exhibits multimodal features and a global minimum at a similar location. These benchmark functions provide a foundation for evaluating the complexity, sensitivity, and robustness of newly developed chaotic systems. In this study, we construct a novel hybrid 1D chaotic map by multiplicatively coupling the characteristic components of Problem 14 and Problem 20. The first components form a basic oscillator–transformer structure, while the second components introduce high-frequency, phase-controlled modulation through a control parameter a and a constant $k = 2^{12}$. The resulting hybrid map integrates the damped oscillatory behavior of Problem 14 with the multimodal

structure of Problem 20, producing asymmetric amplitude scaling, repeated stretching–folding mechanisms, and dense critical points.

The inclusion of the $\sin(k\pi x + a)$ term allows fine-scale oscillatory control and phase modulation, enhancing the density of critical points and expanding regions of chaotic behavior. Compared to the original functions individually, the hybrid map exhibits richer multimodality, stronger sensitivity to initial conditions, and broader chaotic regimes, while remaining analytically tractable and easily tunable through the parameters a and k.

The primary contributions of this study can be summarized as follows:

(i) Proposal of a new 1D hybrid chaotic (1DHC) map, systematically derived by multiplicatively coupling the structural components of two established benchmark functions, Problem 14 and Problem 20, thereby combining complementary dynamical characteristics within a unified framework.

(ii) Integration of damped oscillatory features with a multimodal functional landscape, enabling the 1DHC map to exhibit enriched dynamical properties, including enhanced multimodality, stronger sensitivity to initial conditions, and extended regions of chaotic regimes, surpassing the complexity of its constituent functions.

(iii) Rigorous verification of the map's dynamic performance through maximal LE analysis, bifurcation investigations, and sensitivity evaluations, which collectively confirm its strong chaoticity, unpredictability, and structural robustness.

(iV) Practical applicability of the 1DHC map, supported by its simple mathematical formulation, low computational overhead, and verified chaotic strength, making it a promising candidate for secure communication systems, pseudo-random sequence generation, and particularly, image encryption frameworks.

To evaluate the dynamic characteristics of the proposed 1DHC map, standard performance tests such as maximal LE analysis, bifurcation diagrams, and sensitivity tests with respect to initial conditions and control parameters are conducted. Positive LEs confirm the presence of strong chaos, while bifurcation analysis reveals wide parameter regions with complex, aperiodic behavior. Sensitivity tests demonstrate that even infinitesimal changes in initial values or control parameters produce significantly divergent trajectories, confirming the map's potential for applications in encryption, pseudo-random sequence generation, and other nonlinear systems requiring high unpredictability. These evaluations establish the proposed 1DHC map as a robust and flexible tool for further investigation in chaos-based applications.

2. Existing studies

Recent advances in image encryption have explored the integration of 1D chaotic maps with novel encryption strategies to enhance security, randomness, and computational efficiency. Several such 1D chaotic maps are summarized in Table 1. Mansouri and Wang[12] introduced a sine-powered chaotic map (1DSP) and a row-by-row/column-by-column encryption scheme (1DSP-IE) that disrupts pixel correlations and propagates small changes throughout the cipher image, achieving high key sensitivity and resistance to differential attacks. The 1DSP, derived from the classical sine map and extended with two control parameters, exhibited strong chaotic behavior characterized by high sensitivity and randomness. The corresponding encryption scheme utilized 1DSP-generated sequences for sequence addition, employing a structured row-by-row and column-by-column strategy to achieve confusion and diffusion. This approach effectively ensured that even minor changes in the plain image are thoroughly propagated throughout the cipher image. Simulation results confirmed the scheme's efficiency in both encryption and decryption, along with competitive computational speed. Moreover, security analysis indicated high key sensitivity and robustness against statistical, noise, and differential attacks, outperforming several existing image encryption schemes. The study underscores the potential of chaos-based systems for enhancing image security and suggests future improvements through the integration of seed maps and advanced algorithms.

Midoun et al.[13] introduced a novel 1D chaotic map, termed 1-DFCS, based on the fraction of cosine over sine. This map exhibited complex chaotic behavior, an infinite chaotic range, and high sensitivity to initial conditions and control parameters. Building upon this, they developed a sensitive dynamic mutual image encryption scheme (SDME) that integrates dynamic diffusion and confusion processes, enabling a unique encryption for each image. A key component of SDME is the proposed plain image sensitivity function, which combines the 1-DFCS, the plain image, and the secret key to enhance unpredictability and resistance to differential attacks. The scheme also incorporates a mutual part encryption technique, where small changes in one data segment influence another, further strengthening security. Experimental evaluations demonstrated that SDME provides high-security performance in a single encryption round while maintaining fast processing speed, outperforming several state-of-the-art image encryption methods. The study highlights the potential of 1-DFCS-based encryption for secure real-time communication and establishes SDME as a robust, sensitive, and efficient chaos-based cryptosystem.

Ponmaheshkumar and Perumal[14] proposed an innovative image encryption framework combining a 1D improved sine chaotic map with an origami-inspired confusion mechanism to enhance security in digital image transmission. The improved sine map exhibited complex dynamical behavior, including high sensitivity to initial conditions and parameters, a large key space, and robust pseudo-randomness, forming the basis for secure encryption. The origami-based approach introduced geometrically controlled pixel permutations inspired by folding operations, significantly improving diffusion and entropy characteristics. Experimental results on benchmark images demonstrated near-ideal performance, with information entropy close to 8, low correlation coefficients in the vertical, horizontal, and diagonal directions, and strong resistance to differential attacks, as evidenced by the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) values. The scheme also maintained computational efficiency and supported accurate decryption. This work emphasizes the potential of integrating chaotic systems with geometric transformations, offering a secure, practical, and novel approach to image encryption applicable to real-time

Table 1. Chaotic systems employed in existing studies.

Ref.	2D chaotic map	Cont. par.
1DSP[12]	$x_{n+1} = (x_n(\alpha+1))^{\sin(\beta\pi+x_n)}$	$\alpha > 0,\ \beta \in [0,1]$
1-DFCS[13]	$x_{n+1} = \dfrac{\cos\left((ax_n+1)^2+1\right)}{\sin\left((ax_n+1)^2+1\right)+2}$	$a > 0$
ISC[14]	$x_{n+1} = \left(\alpha \sin\left(\beta(\arccos(x_n))^{1-\alpha}\right)\right) \bmod 1$	$\beta \in [0,\infty],\ \alpha = 7$
DSC[15]	$x_{n+1} = \Big\lvert\, \lvert\sin(-rx_n + x_n^3 - r\tan(x_n))\rvert - \lvert\cos(-rx_n + x_n^3 - r\tan(x_n))\rvert \,\Big\rvert$	$\gamma \in [0,\infty],\ \alpha \in [1,5]$
1D-ICCM[16]	$x_{n+1} = \dfrac{\omega(1-x_n)}{x_n(x_n^2-1)} \bmod 1$	$\omega \in [0,\infty]$

Abbreviations: Cont. par., control parameter; DSC, delta sine–cosine; ISC, improved sine chaotic map; 1DSP, one-dimensional sine-powered chaotic map; 1D-ICCM, improved one-dimensional composite chaotic map; 1-DFCS, one-dimensional chaotic map based on the fraction of cosine over sine.

communication, surveillance, and medical imaging, while suggesting new research directions in spatially inspired cryptographic designs.

Dua et al.[15] introduced a novel 1D chaotic map, termed the delta sine–cosine (DSC) map, and developed an image encryption scheme that integrates chaotic sequences with DNA encoding to achieve high security and computational efficiency. The DSC map exhibited strong chaotic behavior, as confirmed by bifurcation and LE analyses, and provided a broader chaotic range compared with existing 1D maps. The proposed encryption framework operates in three stages: permutation, diffusion, and confusion. Pixels are first permuted using DSC-generated chaotic sequences, followed by a two-step diffusion process involving XOR operations inspired by chess knight movements and additional masking matrices. In the final confusion stage, the permuted image is encoded into DNA sequences and processed through DNA XOR and addition using additional DSC-based DNA sequences, resulting in a noise-like cipher image. Performance evaluations, including NPCR, UACI, correlation coefficients, histogram analysis, and entropy measures, demonstrated strong resistance to statistical and differential attacks while maintaining high sensitivity to input changes. This work underscores the potential of combining chaotic maps with DNA-based operations for secure image encryption and suggests future enhancements for broader multimedia applications and error resilience.

Huang et al.[16] presented a novel color image encryption algorithm that integrates an improved 1D composite chaotic map (1D-ICCM) with a hierarchical strategy (HS-IEA) to enhance both security and computational efficiency. The 1D-ICCM exhibited strong chaotic characteristics, confirmed through LE analysis, National Institute of Standards and Technology Special Publication (NIST SP) 800-22 tests, and sensitivity evaluations. HS-IEA leverages a multi-level encryption process, beginning with pixel-level integration and secondary diffusion, followed by bidirectional dynamic scrambling of restored color channel matrices and bit-plane decomposition. High-order bit planes are processed using bit-level diffusion, while low-order planes undergo simpler bit-plane rotations, enabling a trade-off between encryption quality and processing speed. Experimental results demonstrated that the proposed method achieved superior security metrics, including NPCR, UACI, and information entropy, while significantly reducing chaotic sequence generation and decryption times compared to previous approaches. The study highlights the advantages of combining optimized chaotic maps with hierarchical and hybrid encryption strategies, providing a robust and efficient framework for secure, real-time color image encryption applications.

In summary, these studies demonstrate that 1D chaotic maps, when combined with dynamic diffusion, geometric transformations, DNA encoding, or hierarchical strategies, offer promising avenues for secure and efficient image encryption, emphasizing trends toward higher complexity, real-time applicability, and robustness against statistical, differential, and noise-based attacks.

3. Proposed chaotic map

This section introduces the proposed 1DHC map and presents its performance tests.

3.1. Problem 14 benchmark function

Problem 14[10] is a 1D multimodal benchmark function commonly used to assess the performance of optimization algorithms. Defined over a bounded domain, the function exhibits multiple local extrema and attains its global minimum near $x \approx 1.1951$, with a function value of approximately -0.0635. The mathematical formulation of this function is given in Equation (1), and its characteristic landscape is illustrated in Figure 1.

$$f(x) = -e^{-x} \times \sin(2\pi x) \tag{1}$$

3.2. Problem 20 benchmark function

Problem 20[11] is also a 1D multimodal benchmark function frequently employed to evaluate the performance of optimization algorithms. Like Problem 14, it is defined over a bounded domain and exhibits multiple local extrema, with its global minimum occurring near $x \approx 1.1951$, and a function value of approximately -0.0635. The mathematical formulation of this function is provided in Equation (2), and its characteristic landscape is shown in Figure 2.

$$f(x) = -(x - \sin(x)) \times e^{-x^2} \tag{2}$$

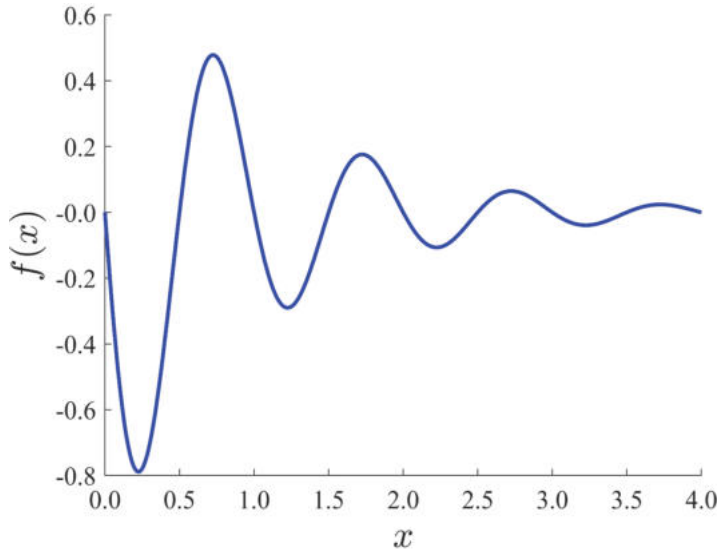


Figure 1. Problem 14 benchmark function illustrating its damped oscillatory structure with multiple local extrema and a global minimum

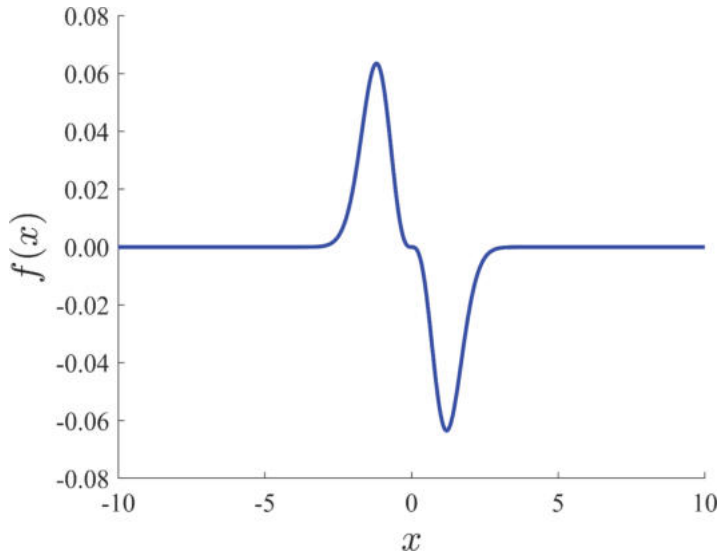


Figure 2. Representation of the one-dimensional Problem 20 benchmark function illustrating its multimodal structure

3.3. Hybridization of benchmark functions

In this study, the characteristic components of Problem 14 and Problem 20 were multiplied to construct a novel 1D chaotic map: the first components were combined to form the basic oscillator–transformer structure, while the second components were multiplied to introduce a high-frequency, phase-controlled modulation (using control parameter a and constant $k = 2^{12}$). This multiplicative coupling induces strong nonlinear interaction at both amplitude and phase levels, enabling the hybrid map to simultaneously inherit the damped oscillatory features of Problem 14 and the multimodal structure of Problem 20. The closed-form representation of the hybrid map is given in Equation (3).

$$f(x_i) = x_{i+1} = -(x_i - \sin(x_i)) \times \left(-e^{-x_i}\right) + \sin(k\pi x_i + a) \times \left(e^{-x_i^2}\right) \tag{3}$$

The hybrid map in Equation (3) combines the damped oscillatory driver of Problem 14 with the multimodal structure of Problem 20 through multiplicative coupling, resulting in the sum of two exponentially weighted nonlinear terms. The component with e^{-x} introduces asymmetric amplitude scaling, which enhances the folding mechanisms of the system, while the e^{-x^2} term confines the dynamics near the origin yet produces steep gradients and frequent sign changes in the derivative, thereby reinforcing repeated stretching–folding mechanisms. The $\sin(k\pi x + a)$ term enables fine-scale oscillatory control via k, and phase modulation via a, increasing the density of critical points and expanding the parameter regions where $\left|f'\right| > 1$, leading to positive maximal LEs. Compared to the original functions individually, the hybrid map exhibits richer multimodality, greater sensitivity to initial conditions, and broader chaotic regimes, while remaining analytically tractable and easily tunable through the parameters (a, k).

To further demonstrate the time efficiency of the proposed 1DHC map, computational experiments were conducted on a system equipped with an AMD Ryzen 9 7945HX processor (2.50 GHz), 48 GB RAM, running Windows 11, and MATLAB 2023b. For a sequence length of

10 million, the mean execution time over 100 independent runs was calculated as 0.8672031 s.

3.3.1. Bifurcation diagram

Figure 3 presents the bifurcation diagram of the proposed 1DHC map for the control parameter $a \in [0, 10]$. The analysis shows that the chaotic behavior of the system is preserved not only within this interval but also for values of $a > 10$, confirming its robustness over a wide parameter domain. Moreover, the map densely fills the state space and generates values distributed within the interval $[-1, 1]$. This property is particularly desirable for applications such as random number generation and chaotic cryptosystems, as it guarantees both uniform distribution and high unpredictability.

3.3.2. Lyapunov exponent

The LE is a fundamental quantitative measure used to characterize the chaotic behavior of a dynamical system, as it captures the sensitivity of system trajectories to infinitesimal perturbations in the initial conditions.[17,18] A positive LE indicates exponential divergence of nearby trajectories, which is an essential hallmark of chaos, whereas negative values correspond to convergence toward stable periodic or fixed-point behavior. Thus, the LE not only serves as a reliable indicator of chaos but also reflects the unpredictability and complexity of the underlying system. For a discrete map $f(x_n)$, the LE is mathematically expressed as:

$$L = \lim_{n\to\infty} \left\{ \frac{1}{n} \sum_{k=0}^{n-1} ln|f^{'}(x_n)| \right\} \tag{4}$$

This expression represents the long-term average rate at which trajectories diverge.

Figure 4 illustrates the variation of the LE with respect to the control parameter for several well-known chaotic maps, in comparison with the proposed system. It is evident that the proposed map consistently achieved substantially higher LE values, reaching an average of 8.4555, which far surpasses those of the other benchmark systems, as shown in Table 2. This clearly demonstrates that the proposed system exhibits stronger chaotic dynamics, enhanced sensitivity to initial conditions, and a broader parameter range over which chaos is sustained. Consequently, the proposed 1DHC map offers superior performance in applications requiring high levels of complexity and unpredictability, such as secure communications, random number generation, and cryptographic systems.

The sensitivity of the proposed chaotic map is further evaluated through a test involving two sequences with nearly identical initial values. One sequence starts with $x_1 = 0.5$, while the other begins with $x_2 = x_1 + 10^{-14}$. The circles in Figure 5 represent the difference between these sequences over time. Notably, the $+$ and $\times$ markers never overlap, indicating that even with an extremely small initial difference, the 1DHC map generates entirely distinct chaotic sequences. This behavior underscores the map's high sensitivity to initial conditions, which is a critical property for robust chaotic systems.

3.3.3. Sample entropy

Sample entropy (SE) is an effective measure of complexity in chaotic systems, where higher SE values indicate more irregular and less predictable dynamics.[19] As shown in Figure 6, the proposed 1DHC map maintains nearly stable SE values across the entire control parameter range, demonstrating robust complexity and low predictability. Although it achieved the second-highest mean SE value of 1.89712 among the compared systems (as shown in Table 2), the stability of its entropy profile underscores the reliability and strength of the proposed 1DHC map in generating complex sequences suitable for secure applications. Notably, its performance is very close to that of the best-performing system.

3.3.4. Correlation dimension

The correlation dimension (CD) is a nonlinear metric that quantifies the fractal structure and dimensional complexity of a chaotic attractor, where higher values suggest richer and more intricate dynamics. As illustrated in Figure 7 and presented in Table 2, the proposed 1DHC map consistently achieved the highest and most stable CD values across the entire control parameter range, with an average of 1.80310. In contrast, benchmark systems exhibit lower and more irregular values, indicating reduced dimensionality and weaker chaotic behavior. These results confirm that the proposed 1DHC map sustains robust high-dimensional chaos and maintains complex dynamics regardless of parameter variations, thereby outperforming existing chaotic maps in terms of structural richness and dynamical reliability.

3.3.5. Kolmogorov entropy

Kolmogorov entropy (KE) is a quantitative measure of a dynamical system's unpredictability and complexity, indicating the rate at which information about the system's state is lost over time. In chaotic systems, higher KE values reflect greater randomness, which is beneficial for applications like image encryption, where unpredictability enhances security robustness.[20] Our evaluation of KE across different control parameter pairs, presented in a comparative graph in Figure 8, shows consistently high values (approximately 2.1–2.3). As shown in Table 2, the highest KE value achieved is 2.18878, while the proposed 1DHC map yielded a KE value of 2.13946, producing the second-best score, very close to the highest. This stability suggests the system is resilient to minor parameter changes, making it suitable for practical implementations.

The incorporation of modular operations in chaotic map design often introduces additional computational overhead and may reduce numerical efficiency. This drawback arises because modulo operations involve costly division-based calculations and disrupt numerical continuity, which can slow down execution and affect precision. According to the rank mean values presented in Table 2, both the ISC and the proposed 1DHC map occupy the top overall rank. Moreover, in cases where the proposed 1DHC map ranks second, its performance remains very close to that of the ISC[14] demonstrating competitive efficiency. An additional distinction lies in the structural design of the two maps: while the ISC[14] incorporates a modulo function,

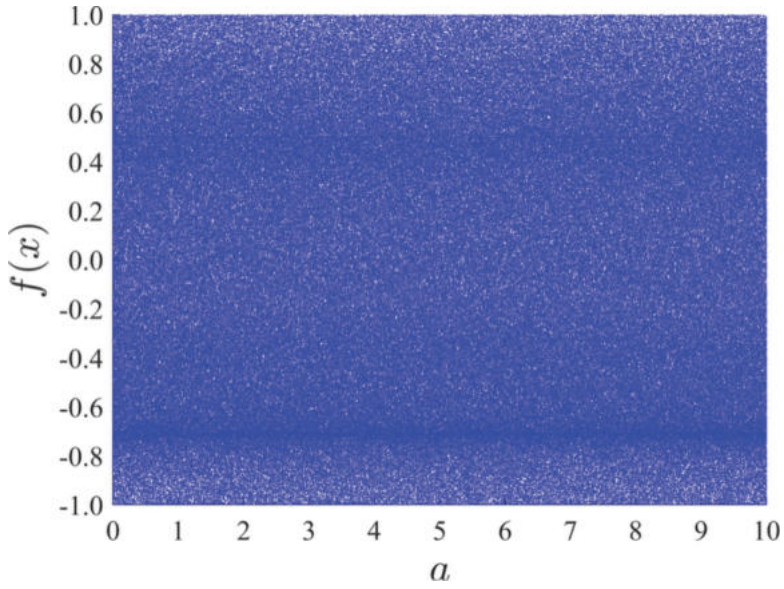


Figure 3. Bifurcation diagram for $a \in [0, 10]$, showing dense filling of the interval $[-1, 1]$

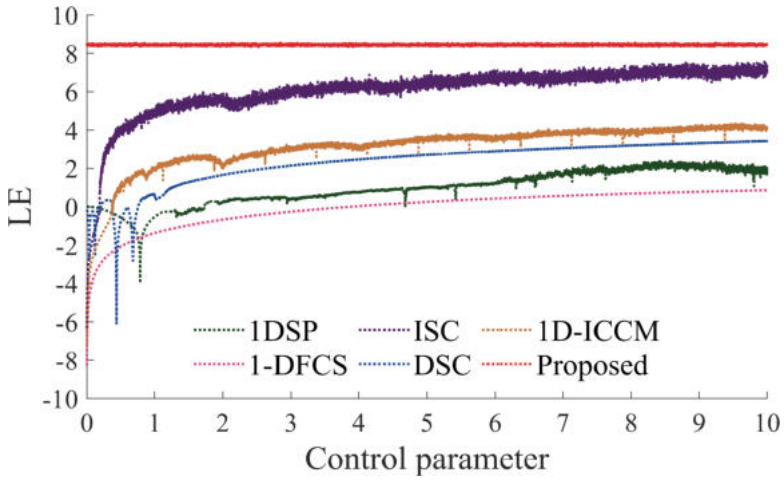


Figure 4. Lyapunov exponent (LE) comparison of the proposed map with existing chaotic systems, showing its superior chaotic strength Abbreviations: DSC, delta sine–cosine; ISC, improved sine chaotic map; 1DSP, one-dimensional sine-powered chaotic map; 1D-ICCM, improved one-dimensional composite chaotic map; 1-DFCS, one-dimensional chaotic map based on the fraction of cosine over sine.

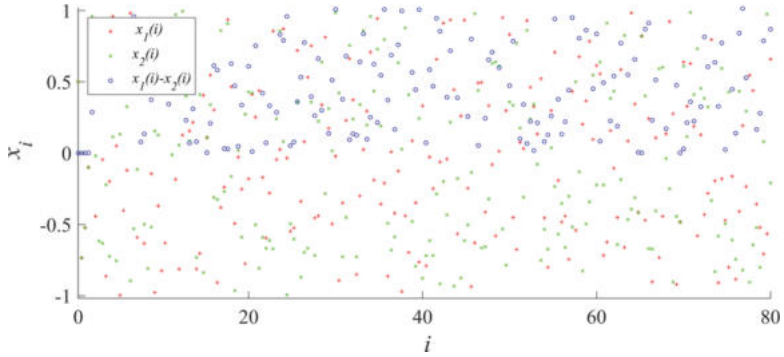


Figure 5. Two distinct sequences generated by the proposed one-dimensional hybrid chaotic map over 200 iterations, starting with $x_1 = 0.5$ and $x_2 = x_1 + 10^{-14}$. Circles show the difference between sequences, highlighting the map's high sensitivity to initial conditions.

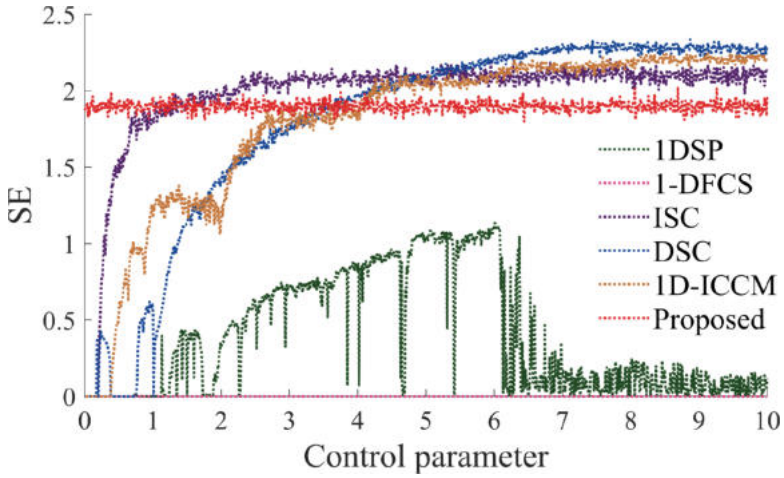


Figure 6. Sample entropy (SE) comparison of the proposed map and existing chaotic systems, showing stable entropy behavior and the second-highest mean sample entropy value
Abbreviations: 1-DFCS, one-dimensional chaotic map based on the fraction of cosine over sine; 1DSP, one-dimensional sine-powered chaotic map; 1D-ICCM: improved one-dimensional composite chaotic map; DSC, delta sine–cosine; ISC, improved sine chaotic map.

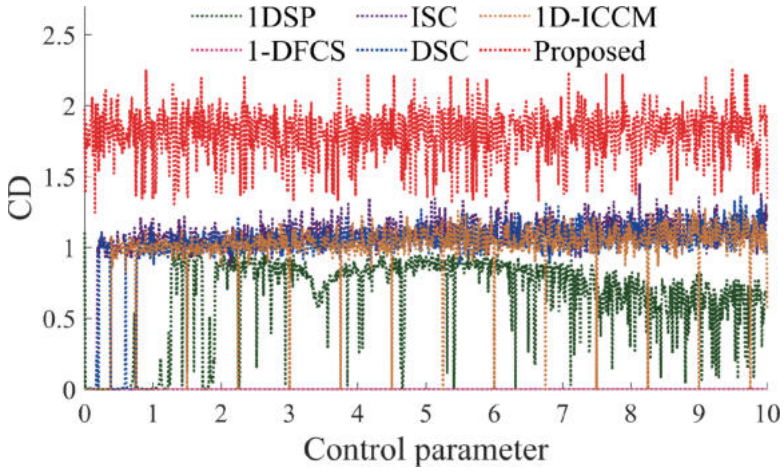


Figure 7. Correlation dimension (CD) comparison of the proposed one-dimensional hybrid chaotic map and existing chaotic systems, showing the highest and most stable values across the parameter range
Abbreviations: 1-DFCS, one-dimensional chaotic map based on the fraction of cosine over sine; 1D-ICCM, improved one-dimensional composite chaotic map; 1DSP, one-dimensional sine-powered chaotic map; DSC, delta sine–cosine; ISC, improved sine chaotic map.

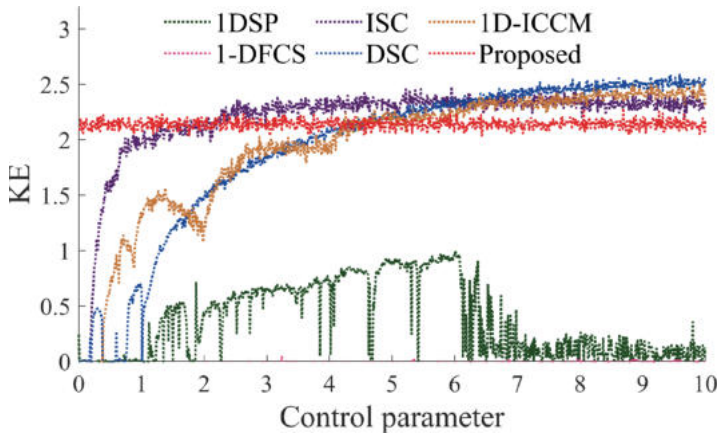


Figure 8. Comparison of Kolmogorov entropy (KE) values for the proposed one-dimensional hybrid chaotic map against benchmark chaotic maps, showcasing its competitive performance for encryption-oriented applications
Abbreviations: 1-DFCS, one-dimensional chaotic map based on the fraction of cosine over sine; 1D-ICCM, improved one-dimensional composite chaotic map; 1DSP, one-dimensional sine-powered chaotic map; DSC, delta sine–cosine; ISC, Improved sine chaotic map.

Table 2. Comparative results between the proposed 1DHC map and those reported in existing literature.

Ref.	Test				Rank				Rank mean
	LE	SE	CD	KE					
1DSP[12]	0.96702	0.39329	0.64890	0.36908	5	5	5	5	5.00
1-DFCS[13]	−0.07022	0.00001	0.00129	−0.00042	6	6	6	6	6.00
ISC[14]	6.04296	1.98039[a]	1.07639	2.18878[a]	2	1	2	1	1.50
DSC[15]	2.33021	1.79344	1.00180	1.91833	4	4	3	4	3.75
1D-ICCM[16]	3.11380	1.80096	0.99099	1.93841	3	3	4	3	3.25
Proposed 1DHC	8.45553[a]	1.89712	1.80310[a]	2.13946	1	2	1	2	1.50

Abbreviations: 1D-ICCM, one-dimensional composite chaotic map; 1-DFCS, one-dimensional chaotic map based on the fraction of cosine over sine; 1DHC, one-dimensional hybrid chaotic map; 1DSP, one-dimensional sine-powered chaotic map; CD, correlation dimension; DSC, delta sine–cosine; ISC, improved sine chaotic map; KE, Kolmogorov entropy; LE, Lyapunov exponent; SE, sample entropy.
[a] Represents the highest value in each column.

the proposed 1DHC map achieved comparable, and in some cases superior performance without relying on any modulo operation. This characteristic underscores the superiority of the proposed 1DHC map, as it enables simpler implementation while maintaining robust chaotic behavior. In contrast, maps constructed without modular dependence typically yield faster execution and retain stronger dynamical performance, making them more suitable for high-efficiency applications.

3.3.6. National Institute of Standards and Technology test

To evaluate the statistical randomness of the proposed 1DHC map, the NIST SP 800-22 test suite was applied. This standardized framework is widely used for assessing the randomness of data, particularly in cryptography, secure communications, and nonlinear system analysis.[21] The *x*-sequences generated by the map were subjected to the full set of tests. As presented in Table 3, all three sequences achieved *p*-values above the threshold of 0.01 and passed with proportions exceeding 98%, indicating strong statistical randomness. These results demonstrate the capability of the proposed 1DHC map to generate high-quality pseudo-random sequences, reinforcing its applicability in systems that require robust chaotic behavior.

The NIST SP 800-22 test suite plays a critical role in evaluating the statistical quality of pseudo-random number generators, particularly in domains requiring high security and unpredictability. In this evaluation, the proposed 1DHC chaotic map was tested using the complete set of NIST SP 800-22 tests. The *x*-sequences were generated using the control parameters $a = 5$, $b = 2^{12}$, and an initial value of $x_0 = 0.5$. As shown in Table 3, all three sequences passed the tests with *p*-values above the 0.01 threshold and proportions exceeding 98%, indicating strong statistical randomness. These results demonstrate the proposed 1DHC map's capability to generate high-quality pseudo-random sequences, reinforcing its suitability for systems that require robust chaotic behavior.

4. Image encryption implementation

To evaluate the applicability of the proposed 1DHC map in chaos-based applications, it was integrated into an image encryption framework.[5] Here, the goal is to demonstrate the encryption capability of the 1DHC map using a simple image encryption algorithm. In the algorithm presented in Gao et al.[5] study, a two-dimensional (2D) chaotic map was employed, generating eight values for permutation and diffusion, derived from the initial conditions x, y, and the control parameters a, b. In contrast, the proposed chaotic map is 1D and involves only a single control parameter; therefore, only four values (two initial conditions and two control parameters) are sufficient for the two encryption stages. As a result, a slight modification was required in the parameter calculator module. The updated algorithm incorporating this revision is provided in Algorithm 1. Furthermore, to ensure that the initial values of X remain within the interval $[-1, 1]$, the transformation $2 \times \begin{bmatrix} g_1 & g_3 \end{bmatrix} - 1$ was applied (Line 10).

In the permutation and diffusion processes, only the sequence generation stage was modified. The sequence generator (SG) was reformulated to accept a single initial condition and one control parameter, expressed as $SG\,(k, x_1,\ a)$. Rather than using 2D sequence generation, the proposed 1DHC map was employed for sequence production. The redefined SG is presented in Algorithm 2.

5. Practical application of the encryption scheme to color images

In this section, the effectiveness of the proposed 1DHC map is evaluated through its integration into an image encryption algorithm. To this end, a set of 10 natural images collected from publicly available sources[22] was used as test data to ensure diversity in image content and complexity. In addition, the widely used Lena 512×512 color image was included for comparison, as it is a standard benchmark in the image encryption literature. By incorporating both natural and benchmark images, the robustness and adaptability of the encryption scheme can be more comprehensively assessed. The original plaintext images and their corresponding encrypted versions, generated by the proposed scheme, are presented in Figure 9. These 10 natural images were also utilized in the subsequent analyses to provide consistent and reliable evaluation results.

5.1. Histogram

Histogram analysis is a fundamental technique for evaluating the statistical properties of encrypted images, as an ideal encryption scheme should produce ciphertext histograms that are uniformly distributed and significantly different from those of the corresponding plaintext images. Such uniformity ensures that pixel intensity values are evenly spread across the full dynamic range, thereby minimizing the risk of statistical attacks.

Table 3. Results of the National Institute of Standards and Technology Special Publication 800-22 randomness tests for the control parameters $a = 5$, $b = 2^{12}$, and initial value $x_0 = 0.5$

Test	x-sequence p-value	Pro. (%)
Frequency	0.162606	100
Block frequency	0.392456	100
Cumulative sums	0.834308	100
Runs	0.311542	100
Longest runs of ones	0.637119	100
Rank	0.242986	100
FFT	0.637119	100
No overlapping templates	0.997147	100
Overlapping templates	0.941144	98
Universal	0.991468	98
Approximate entropy	0.311542	98
Random excursions	0.437274	100
Random excursions variant	0.637119	100
Serial	0.585209	100
Linear complexity	0.689019	100

Abbreviations: FFT, Fast Fourier transform; Pro., proportion.

Algorithm 1. Pseudocode of parameter calculator (PC)

Input : $B[b_{1p}]_{1\times 512}$
Output : X, U
$PC(B)$
for $i = 1$ to 32
  $C_i = (B^{(16(i-1)+1):16i})_{10}$
$T = mod\,(\text{sum}(C), 256)$
for $i = 1$ to 4
  $D = B^{128(i-1)+1:128i}$
  for $j = 1$ to 16
    $E = D^{4(j-1)+1:4j}$
    $F = \text{mod}(floor(T) + (E)_{10}, 10)$
    $g_i = g_i + \frac{F}{10^j}$
$X = 2 \times [g_1 \quad g_3] - 1$
$U = 10 \times [g_2 \quad g_4]$

Algorithm 2. Pseudocode of sequence generator (SG)

Input : l, s_1, a
Output : X, Y, Z
$SG\,(k, s_1,\ a)$
$k = 2^{12}$
for $i = 2$ to $4l$
$s_{i+1} = -(s_i - \sin(s_i)) \times \left(-e^{-s_i}\right) + sin(k\pi s_i + a) \times (e^{-s_i^2})$
Obtain $X = [s_{ij}]_{1\times l},\ Y = [s_{ij}]_{l+1\times 2l}, Z = [s_{ij}]_{2l+1\times 4l}$

Figure 10A illustrates the histograms of the plaintext images presented in Figure 9, where the distributions are distinctive and highly non-uniform, revealing both visual and statistical redundancies. In contrast, Figure 10B displays the histograms of the corresponding encrypted images, which exhibit a flat and nearly uniform distribution across all color channels. This transformation conceals the statistical features of the plaintext data, effectively eliminating exploitable patterns. The results confirm that the encryption scheme successfully disrupts pixel intensity correlations and achieves strong resistance against histogram-based statistical attacks.

The statistical randomness and uniformity of the encrypted image histograms were quantitatively assessed using the chi-square (χ^2) test and variance analysis. In secure encryption systems, χ^2 values below the critical threshold of 293.25 (α = 0.05, df = 255), along with low variance values, indicate effective tonal distribution and reduced predictability. As depicted in Figure 11, the encryption scheme achieved average χ^2 values of 261.21 (Red), 256.76 (Green), and 260.59 (Blue), yielding an overall RGB mean of 259.52. Although 4 out of 30 channel measurements slightly exceed the threshold, the average values for all color channels remain well below 293.25, thereby passing the statistical test. In parallel, the variance values are significantly reduced from the very high levels observed in the plain images—1.444×10^9 (Red), 1.466×10^9 (Green), and 1.404×10^9 (Blue)—to much lower levels in the encrypted images: 2493.09, 2444.67, and 2482.33, respectively. This sharp decline underscores the encryption scheme's capacity to eliminate intensity concentration and achieve near-uniform histograms across all color channels. Collectively, these results validate the robustness of the encryption scheme in producing secure and statistically balanced cipher images.

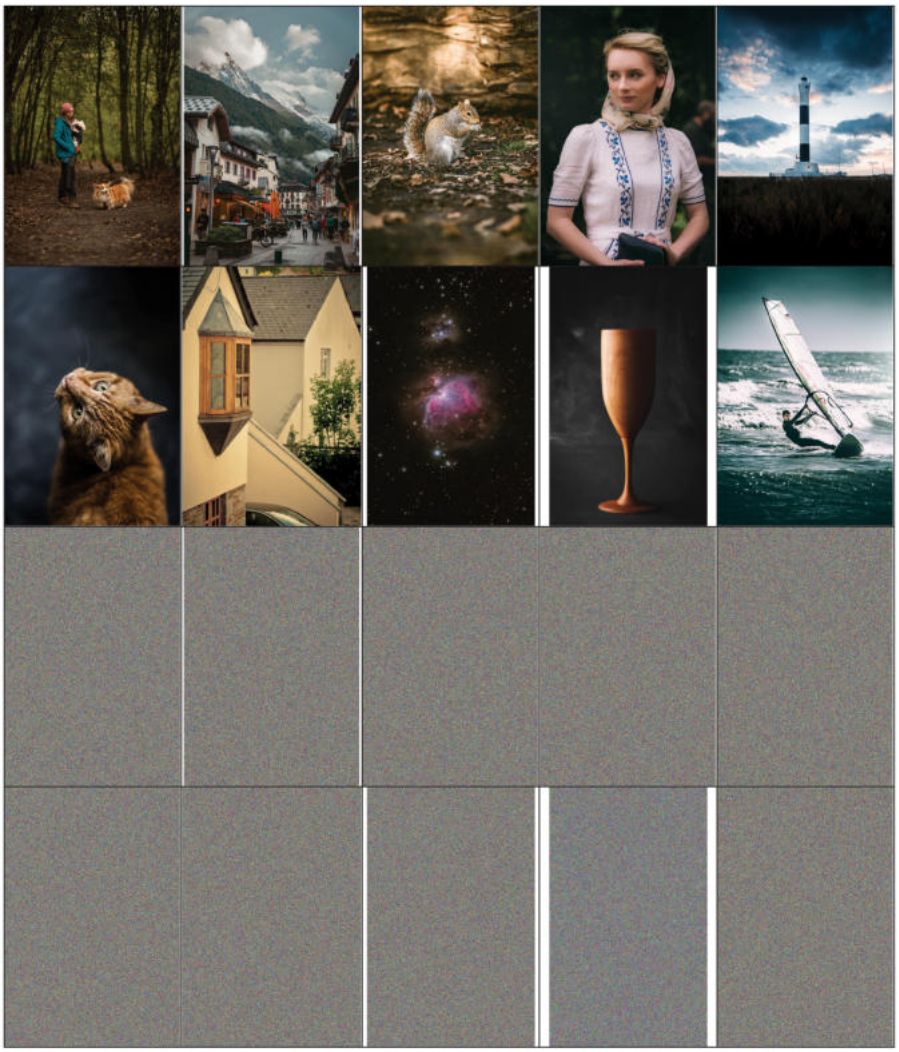


Figure 9. The first and second rows present the natural color plaintext images, while the third and fourth rows display the corresponding encrypted images produced by the encryption scheme

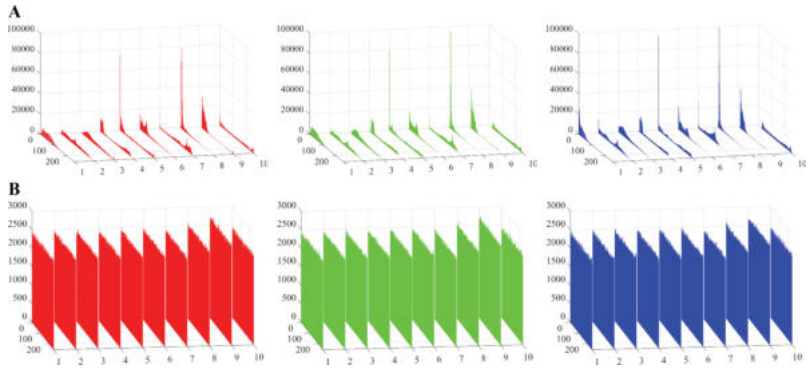


Figure 10. Visual comparison of images and their histograms: (A) histograms of plaintext images; (B) corresponding histograms of ciphertext images

5.2. Information entropy

Information entropy (IE) is a fundamental metric for evaluating the randomness and unpredictability of pixel distributions in encrypted images. For an ideal 8-bit image, the maximum entropy value of 8 represents perfect uncertainty and the absence of exploitable statistical patterns. In this context, higher entropy values indicate stronger resistance against statistical and entropy-based cryptanalytic attacks. As illustrated in Figure 12, the encryption scheme achieved entropy values remarkably close to the theoretical optimum across 10 test images and all color channels. Specifically, the red channel increases from an average of 6.97681 (plain) to 7.99969 (encrypted), the green channel increases from 6.88782 to 7.99970, and the blue channel improves from 6.63862 to 7.99969. These substantial enhancements demonstrate the encryption scheme's effectiveness in eliminating redundancies and

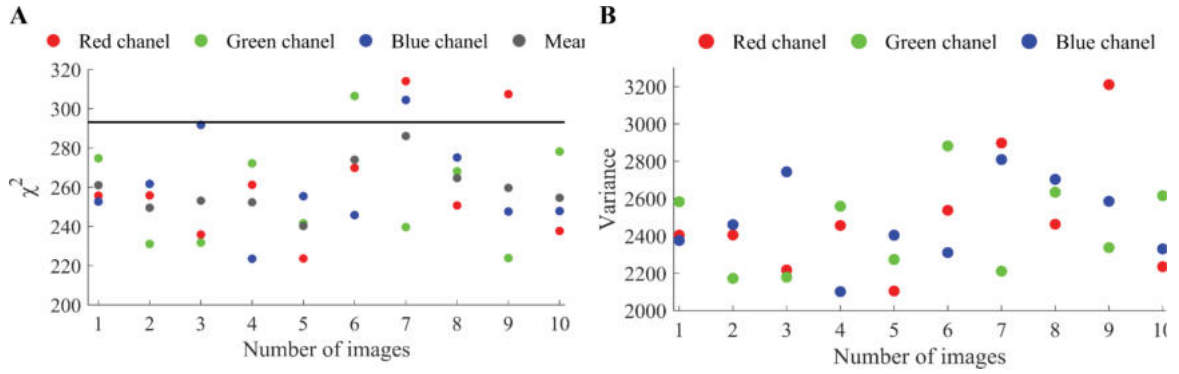


Figure 11. Chi-square (χ^2) and variance scores for RGB images in Figure 10: (A) χ^2 scores – red channel mean: 261.21; green channel mean: 256.76; blue channel mean: 260.59; overall RGB mean: 259.52. (B) Variance scores – red channel mean: 2493.09; green channel mean: 2444.67; blue channel mean: 2482.33.

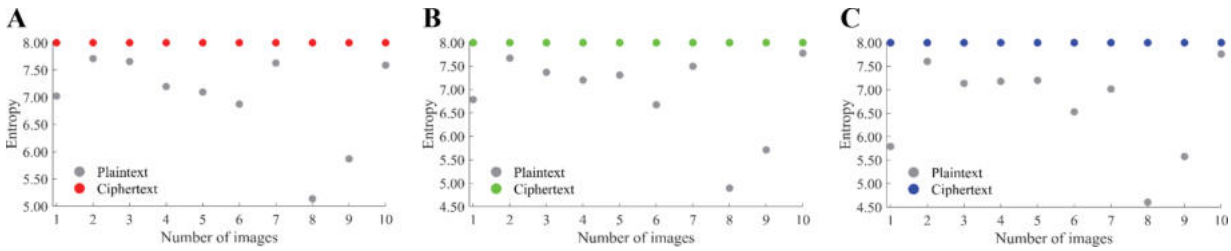


Figure 12. Information entropy for RGB images in Figure 9: (A) red channel – mean for plain images: 6.9768, mean for cipher images: 7.9996; (B) Green channel – mean for plain images: 6.8878, mean for cipher images: 7.9997; (C) blue channel – mean for plain images: 6.6386, mean for cipher images: 7.9996

producing highly unpredictable cipher images, thereby reinforcing its overall cryptographic strength.

5.3. Correlation

Correlation coefficient analysis evaluates the statistical dependence between adjacent pixels, which is typically high in natural images due to smooth intensity transitions.[23] Figure 13A–C, D–F, and G–I shows scatter plots for the red, green, and blue channels, illustrating the effect of the encryption scheme. While plaintext images exhibit strong linear clustering, the encrypted images display uniformly dispersed points with no visible patterns. This marked reduction in correlation confirms that the encryption scheme effectively disrupts spatial redundancy and enhances resistance against statistical attacks.

5.4. Cropping attack

Cropping operations, depicted in Figure 14, were used to evaluate the recovery capability of the encryption scheme. A 512×512 color image was employed in the experiments, where cropped cipher images with ratios of 1/16, 1/4, 1/2, and a center 1/16 were tested. The peak signal-to-noise ratio (PSNR) values of the corresponding decrypted results are 20.62, 14.61, 11.61, and 20.68, respectively. Although higher cropping ratios increased blurriness, the recovered images remained visually distinguishable. These findings confirm that the encryption scheme can tolerate significant data loss, providing acceptable reconstruction even when up to half of the ciphertext is removed.

5.5. Noise attack

During image transmission, ciphertext images may be corrupted by impulse noise, such as salt-and-pepper noise (SPN). To evaluate robustness, SPN with densities of 0.001, 0.05, 0.01, and 0.1 was applied to the encrypted image. The decrypted results achieved PSNR values of 39.25, 31.82, 28.71, and 18.65, respectively. As illustrated in Figure 15, the encryption scheme effectively mitigates noise effects at low and moderate densities, ensuring that the recovered images remain visually recognizable even under severe noise conditions.

5.6. Comparison with State-of-the-Art methods using an encryption scheme

To assess the effectiveness of the proposed encryption scheme, experiments were conducted on the Lena color image (512×512), and the results were compared with several state-of-the-art approaches reported in the literature,[24–30] as summarized in Table 4. In terms of entropy, all methods yielded values very close to the ideal benchmark of 8, while the proposed scheme maintains stable and consistent scores across all color channels. Regarding correlation, the proposed scheme achieved notably low values, making it competitive with the best results in the literature. For differential attack resistance, the obtained NPCR of 99.6089 and UACI of 33.4657% confirm strong robustness, aligning well with top-performing methods. Furthermore, statistical tests such as variance (1011.29) and χ^2 (251.83) demonstrated the reliability of the proposed method, showing comparable or improved performance relative to recent schemes. These findings indicate that the proposed encryption scheme not only aligns with the most advanced techniques in the literature but also outperforms recent methods in several evaluation metrics, demonstrating its competitiveness and robustness for practical secure communication applications.

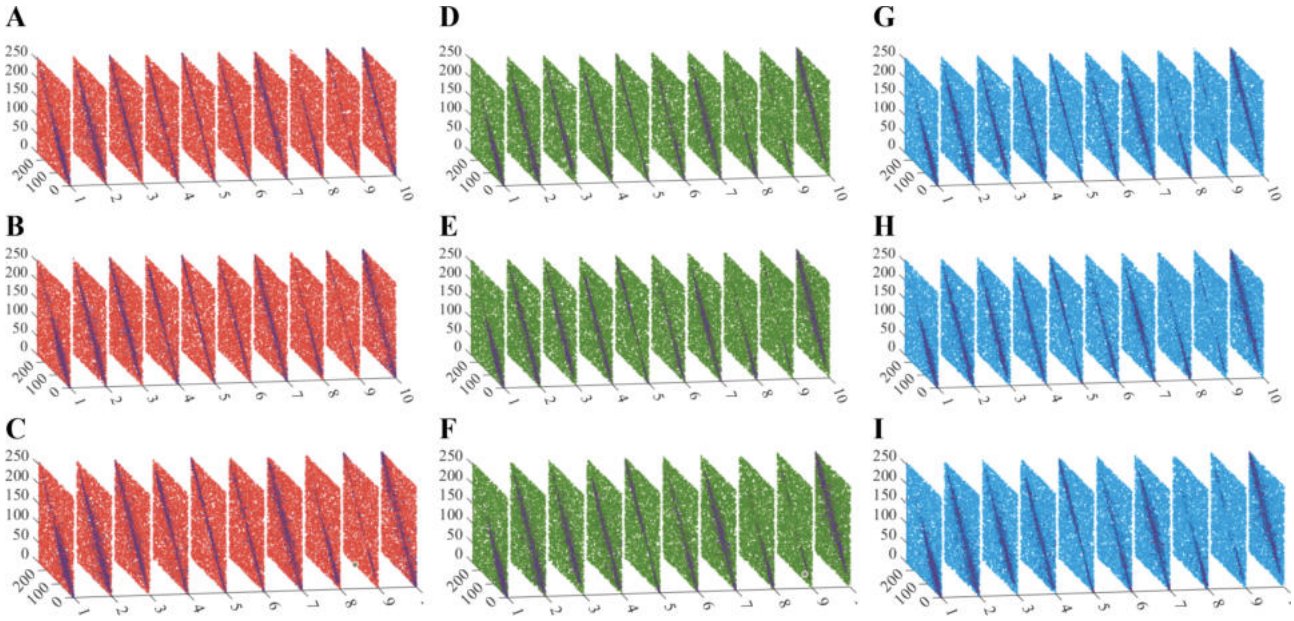


Figure 13. Pixel correlation scatter plots before and after encryption of the images in Figure 10: red channel – (A) horizontal, (B) vertical, (C) diagonal; green channel – (D) horizontal, (E) vertical, (F) diagonal; Blue channel – (G) horizontal, (H) vertical, (I) diagonal

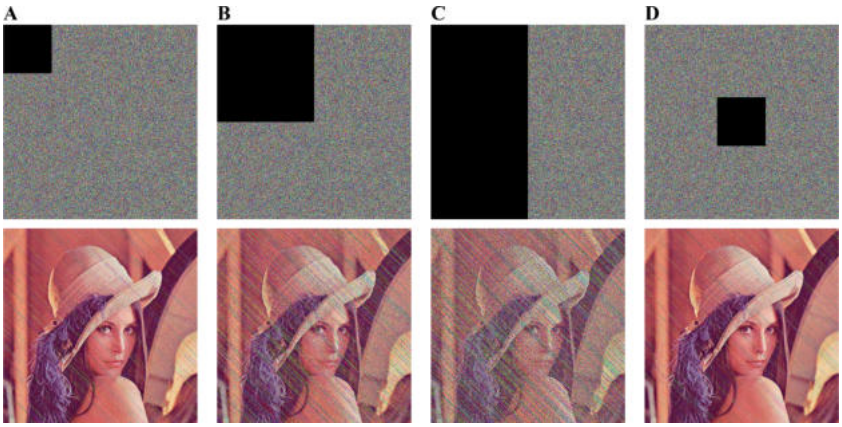


Figure 14. Ciphered and deciphered images cropped with: (A) 1/16 (peak signal-to-noise ratio [PSNR]: 20.62), (B) 1/4 (PSNR: 14.61), (C) 1/2 (PSNR: 11.61), (D) center 1/16 (PSNR: 20.68).

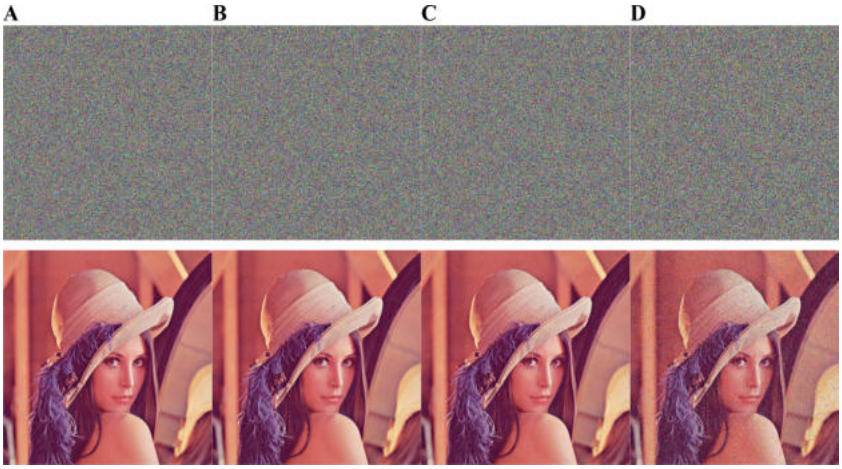


Figure 15. Ciphered and deciphered images with salt-and-pepper noise densities: (A) 0.001 (peak signal-to-noise ratio [PSNR]: 39.25), (B) 0.05 (PSNR: 31.82), (C) 0.01 (PSNR: 28.71), (D) 0.1 (PSNR: 18.65)

Table 4. Comparison of evaluation metrics between the proposed encryption scheme and the Secure Online Transaction Algorithm methods

Metrics	Channel	24	25	26	27	28	29	30	Proposed
Entropy	R	7.9994	7.9994	7.9994	7.9993	7.9992	7.9992	7.9993	7.9993
	G	7.9993	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993
	B	7.9994	7.9993	7.9992	7.9992	7.9993	7.9992	7.9994	7.9993
Correlation	R	0.0007	0.0009	0.0036	0.0008	0.0018	0.0050	0.0022	0.00056
	G	0.0022	0.0014	0.0004	0.0004	0.0021	0.0062	0.0029	0.00068
	B	0.0062	0.0007	0.0018	0.0001	0.0033	0.0048	0.0023	0.00044
Differential attack	NPCR	99.6096	99.6148	99.5997	99.6005	99.6063	–	–	99.6089
	UACI	33.4625	33.4312	33.4521	33.4670	33.5023	–	–	33.4657
Statical test	Variance	–	–	–	–	1049.161	–	–	1011.29
	χ^2 test	–	–	240.1849	–	–		249.87	251.83

Note: Numbers 24-30 indicate the references.
Abbreviations: B, blue; G, green; NPCR, number of pixels change rate; R, red; UACI, unified average changing intensity.

6. Conclusion

In this study, a novel 1DHC map was introduced, derived from the hybridization of two benchmark functions, Problem 14 and Problem 20. The proposed map demonstrated strong chaotic dynamics, achieving scores of 8.45553, 1.89712, 1.80310, and 2.13946 for LE, SE, CD, and KE, respectively. Compared to other maps, it ranked first, second, first, and second for these metrics, with an overall average rank of 1.5, making it the top-performing map among those evaluated. Furthermore, the map successfully passed all 15 tests of the NIST SP 800-22 statistical suite, confirming its robustness and suitability for cryptographic applications.

To further validate its practical utility, the chaotic map was integrated into an image encryption framework and extensively tested. Information entropy values of the encrypted images approached the theoretical optimum across all color channels (7.9996–7.9997), while correlation coefficients between adjacent pixels dropped to nearly zero, demonstrating the scheme's effectiveness in eliminating spatial redundancies. The scheme exhibited strong resistance to differential attacks, with NPCR and UACI scores of 99.6089% and 33.4657%, respectively, matching or exceeding state-of-the-art methods. Statistical evaluations further confirm strong histogram uniformity, with χ^2 and variance values (251.83 and 1011.29) well within secure thresholds. Reliability tests showed that the scheme tolerates cropping attack (PSNR: 20.62, 14.61, 11.61, 20.68 for various ratios) and noise attack (PSNR: 39.25, 31.82, 28.71, 18.65 at varying densities), ensuring reliable recovery even under significant distortions.

Overall, the findings demonstrate that the proposed 1DHC map not only exhibits superior theoretical properties but also delivers a practical and efficient solution for secure image encryption. Its strong performance across statistical, cryptographic, and stability metrics underscores its potential as a versatile tool for modern security applications, including random number generation and secure multimedia communication.

Acknowledgments

None.

Funding

None.

Conflict of interest

Abdurrahim Toktas and Suo Gao are the Editorial Board Members of this journal but were not involved in any way, directly or indirectly, in the editorial or peer-review process conducted for this paper. The other authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Author contributions

Conceptualization: Uğur Erkan, Abdurrahim Toktas
Investigation: Uğur Erkan, Feyza Toktas, Yiting Lin
Methodology: Uğur Erkan, Abdurrahim Toktas, Feyza Toktas, Suo Gao
Writing–original draft: All authors
Writing–review & editing: Feyza Toktas, Yiting Lin, Suo Gao

Availability of data

Data sharing is not applicable to this article, as no new data were generated or analyzed during the study.

AI Tools Statement

During the preparation and review of this manuscript, the authors used ChatGPT to assist with language refinement, editing, and text formulation. All scientific content, interpretations, and conclusions are solely the responsibility of the authors

References

1. Lin Y, Xie Z, Chen T, Cheng X, Wen H. Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics. *Expert Syst Appl.* 2024;257:124891. http://dx.doi.org/10.1016/j.eswa.2024.124891
2. Lai Q, Yang L, Chen G. Two-dimensional discrete memristive oscillatory hyperchaotic maps with diverse dynamics. *IEEE Trans Ind Electron.* 2025;72:969-979. http://dx.doi.org/10.1109/TIE.2024.3417974
3. Wang M, Teng L, Zhou W, Yan X, Xia Z, Zhou S. A new 2D cross hyperchaotic sine-modulation-logistic map and its application in bit-level image encryption. *Expert Syst Appl.* 2025;261:125328. http://dx.doi.org/10.1016/j.eswa.2024.125328
4. Gao S, Wu R, Wang X, et al. A 3D model encryption scheme based on a cascaded chaotic system. *Signal Process.* 2023;202:108745. http://dx.doi.org/10.1016/j.sigpro.2022.108745

5. Gao S, Iu HH-C, Erkan U, et al. A 3D memristive cubic map with dual discrete memristors: design, implementation, and application in image encryption. *IEEE Trans Circuits Syst Video Technol.* 2025;1. http://dx.doi.org/10.1109/TCSVT.2025.3545868
6. Toktas A, Erkan U, Ustun D, Lai Q. Multiobjective design of 2D hyperchaotic system using leader pareto grey wolf optimizer. *IEEE Trans Syst Man Cybern Syst.* 2024;54:5237-5247. http://dx.doi.org/10.1109/TSMC.2024.3401412
7. Lai Q, Liu Y. A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map. *Expert Syst Appl.* 2023;223:119923. http://dx.doi.org/10.1016/j.eswa.2023.119923
8. Demirtaş M, Altunkaya S. A novel chirp-based 2D hyperchaotic map for enhanced image encryption. *Phys Scr.* 2025;100:15204. http://dx.doi.org/10.1088/1402-4896/ad9428
9. Liu D, Yu G, Zhao Y, Ding Q. A novel scheme for constructing grid multi-scroll chaotic systems applied to image encryption. *Nonlinear Dyn.* 2025;113:21925-21949. http://dx.doi.org/10.1007/s11071-025-11251-8
10. Infinity77. Problem 14. Published 2023. Accessed September 30, 2025. https://infinity77.net/global_optimization/test_functions_1d.html
11. Infinity77. Problem 20. Published 2023. Accessed September 30, 2025. https://infinity77.net/global_optimization/test_functions_1d.html
12. Mansouri A, Wang X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. *Inf Sci (NY).* 2020;520:46-62. http://dx.doi.org/10.1016/j.ins.2020.02.008
13. Midoun MA, Wang X, Talhaoui MZ. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. *Opt Laser Eng.* 2021;139:106485. http://dx.doi.org/10.1016/j.optlaseng.2020.106485
14. Ponmaheshkumar A, Perumal R. Origami-based image encryption scheme using improved sine map. *Nonlinear Dyn.* Published online 2025. http://dx.doi.org/10.1007/s11071-025-11605-2
15. Dua M, Kumar R, Dua S, Chakravarty N. A novel one-dimensional chaotic map, novel diffusion and DNA encoding-based image encryption scheme. *Int J Dyn Control.* 2025;13:166. http://dx.doi.org/10.1007/s40435-025-01653-2
16. Huang Y, Zhang Q, Zhao Y. A novel color image encryption algorithm based on infinite collapse map and hierarchical strategy. *Digit Signal Process.* 2025;167:105428. http://dx.doi.org/10.1016/j.dsp.2025.105428
17. Gao S, Zhang Z, Iu HH-C, et al. A parallel color image encryption algorithm based on a 2D logistic-rulkov neuron map. *IEEE Internet Things J.* 2025;1. http://dx.doi.org/10.1109/JIOT.2025.3540097
18. Lai Q, Hua H. Secure medical image encryption scheme for healthcare IoT using novel hyperchaotic map and DNA cubes. *Expert Syst Appl.* 2025;264:125854. http://dx.doi.org/10.1016/j.eswa.2024.125854
19. Liu X, Zheng S, Yang J. Color image encryption scheme based on a novel 2D-CLCM chaotic system and RNA encoding. *Math Comput Simul.* 2026;239:340-360. http://dx.doi.org/10.1016/j.matcom.2025.06.009
20. Erkan U, Toktas A, Lai Q. 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Syst Appl.* 2023;213:119076. http://dx.doi.org/10.1016/j.eswa.2022.119076
21. Feng W, Yang J, Zhao X, et al. A novel multi-channel image encryption algorithm leveraging pixel reorganization and hyperchaotic maps. *Mathematics.* 2024;12:3917. http://dx.doi.org/10.3390/math12243917
22. Andrews A. No title. Unsplash. https://unsplash.com/@alex$_{a}ndrews$. Accessed September 30, 2025.
23. Lai Q, Liu Y. A family of image encryption schemes based on hyperchaotic system and cellular automata neighborhood. *Sci China Technol Sci.* 2025;68:1320401. http://dx.doi.org/10.1007/s11431-024-2678-7
24. Yan S, Jiang D, Cui Y, et al. A fractional-order hyperchaotic system that is period in integer-order case and its application in a novel high-quality color image encryption algorithm. *Chaos Solitons Fractals.* 2024;182:114793. http://dx.doi.org/10.1016/j.chaos.2024.114793
25. Huang Y, Huang H, Huang Y, et al. Asymptotic shape synchronization in three-dimensional chaotic systems and its application in color image encryption. *Chaos Solitons Fractals.* 2024;184:114945. http://dx.doi.org/10.1016/j.chaos.2024.114945
26. Tang S, Xu X, Jiang Z, Meng D, Sun K. An image encryption scheme without additional key transmission based on an N-dimensional closed-loop coupled triangular wave model. *Chaos Solitons Fractals.* 2024;185:115039. http://dx.doi.org/10.1016/j.chaos.2024.115039
27. Ding D, Zhu H, Zhang H, Yang Z, Xie D. An n-dimensional polynomial modulo chaotic map with controllable range of Lyapunov exponents and its application in color image encryption. *Chaos Solitons Fractals.* 2024;185:115168. http://dx.doi.org/10.1016/j.chaos.2024.115168
28. Shen H, Shan X, Tian Z. Color image encryption scheme combining a 2D hyperchaotic Sin–Henon system and the division algorithm. *J Inf Secur Appl.* 2024;85:103858. http://dx.doi.org/10.1016/j.jisa.2024.103858
29. Hassan A, Zhou L. A novel 6D four-wing memristive hyperchaotic system: generalized fixed-time synchronization and its application in secure image encryption. *Chaos Solitons Fractals.* 2025;192:115986. http://dx.doi.org/10.1016/j.chaos.2024.115986
30. Obaid MJ, Neamah AA, Shukur AA, Pham V-T, Grassi G. A reliable color image encryption scheme based on a novel dual-wing hyperchaotic map. *Expert Syst Appl.* 2025;289:128237. http://dx.doi.org/10.1016/j.eswa.2025.128237