scientific reports

Check for updates

OPEN

2D-Cosine power sine coupled map with fractal-Fibonacci fusion for hyperchaotic image encryption

Maram Kumar[1,2] & Deepak Ch[1,2]✉

Image security is vital in sectors such as healthcare, defence, finance, and personal data exchange, where breaches of image integrity can result in severe consequences. To address this challenge, we propose a novel image encryption framework. It combines a Fractal-Fibonacci diffusion process based on the Hilbert curve, recursive scrambling guided by chaotic sequences, and a new chaotic map entitled the Two Dimensional Cosine Power Sine Coupled Map (2D-CPSCM). These components enhance randomness and ensure maximum efficiency, resistance against cryptographic attacks. The proposed two-dimensional chaotic system exhibits positive Lyapunov exponents and superior statistical properties compared to traditional systems, as demonstrated by high sample entropy, permutation entropy, and Kolmogorov entropy, confirming its hyperchaotic behaviour. The encryption system has been evaluated using extensive simulations on benchmark images. The findings demonstrate strong key sensitivity, with an entropy of 7.9994, Number of Pixel Change Rate (NPCR) of 99.6%, Unified Average Changing Intensity (UACI) of 33.47%, and Number of Bit Change Rate (NBCR) of 50%. Additionally, Structural Similarity Index Metric (SSIM) and Visual Information Fidelity (VIF) values of 1 between input and decrypted images guarantee successful decryption, whereas low Peak Signal to Noise Ratio (PSNR), SSIM, and VIF between input and encrypted images reduce information leakage. The superior security, resilience, and robustness of the 2D-CPSCM based approach against statistical, noise, and cropping attacks highlights its potential for safe multimedia transmission and useful cryptographic applications.

Keywords Image encryption, Hyperchaotic system, Fractal-Fibonacci diffusion, Hilbert curve

In recent years, the rapid growth of digital communication has led to extensive sharing of information in the form of digital images. Many of these images contain sensitive data, especially in domains such as healthcare, defence, satellite imaging, and intelligent transportation systems. Protecting such information has become a high priority, as the increased transmission of digital images over communication channels raises the risk of unauthorized access. To address this concern, image encryption has emerged as a crucial solution for safeguarding image data. With the rising demand for secure communication, research in the field of image cryptography has become increasingly important. Recently, researchers have shown keen interest in the field of image cryptography by exploring a wide range of techniques, such as image hiding[1], image steganography[2], wavelet transforms[3,4], DNA and RNA based methods[5–8], image compression approaches[9], neural networks[10], and chaos theory[11–13]. Among the various approaches, chaotic based image encryption[14] has gained significant attention due to the natural characteristics of chaotic maps, such as ergodicity, randomness, and high sensitivity to initial conditions. These properties make chaotic maps ideal for designing and implementing cryptographic algorithms for digital images. Chaotic systems are generally classified into one-dimensional and multi-dimensional categories. One-dimensional chaotic maps are simple to implement and require less computation however, they often suffer from drawbacks such as a limited key space and periodicity. In contrast, multi-dimensional chaotic systems provide a larger key space and exhibit higher randomness, but they are more complex to implement and demand greater computational resources.

Two-dimensional (2D) chaotic maps have emerged as efficient tools for image encryption due to their simplicity, strong ergodicity, and large key spaces. Early models such as the classical 2D Logistic Map[15], 2D-SLMM[16], 2D-LASM[17], and 2D-SIMM[18] improved dynamical complexity while maintaining low cost. Later variants including 2D-LSCM[19], and 2D-LSMCL[20] enhanced randomness and robustness, while cross 2D Hyperchaotic[21] and 2D-CLSS[22] further strengthened ergodicity and resistance to attacks. Recent contributions

[1]School of Electronics Engineering, VIT-AP University, Beside AP Secretariat, Amaravati, Andhra Pradesh 522241, India. [2]Maram Kumar, Deepak Ch contributed equally to this work. ✉email: deepakchenu@gmail.com

such as 2D-SPCM[23], 2D Cosine-Sine[24], 2D-CSIM[25], 2D-TFCDM[26], and 2D-ILM[27] emphasize lightweight computation with high security, while Li et al.[28] introduced the 2D-ECSLM to expand chaotic intervals and strengthen unpredictability. Collectively, these advancements reflect a consistent trend toward richer dynamics, expanded key space, and tighter integration with permutation diffusion frameworks for robust image encryption.

Chaotic map based image encryption has evolved significantly over the past few years, with researchers progressively addressing weaknesses in randomness, key space, and computational cost. Zheng et al.[29] proposed the 2D logistic–sine chaotic map (2D-LSMM) combined with DNA coding, which improved randomness, complexity, and key space compared to traditional 1D maps. However, its parameters were constrained to [0,4], limiting flexibility. Teng et al.[22] overcame this limitation by developing the 2D cross-logistic sine sine chaotic map (2D-CLSS), which offered higher structural complexity and improved chaotic performance. While effective, it still relied heavily on conventional scrambling and diffusion, leaving scope for innovation in adaptive mechanisms. Demla et al.[30] designed a medical image encryption scheme using an improved cosine fractional chaotic map with DNA operations, demonstrating strong robustness through NPCR, UACI, and entropy metrics. The main drawback lies in its higher computational overhead due to DNA encoding. Similarly, Dua et al.[31] combined wavelet transform with Lorenz and logistic maps for key generation, achieving high security, low complexity, and resilience against cropping attacks, though its reliance on standard chaotic maps may restrict novelty. Huang et al.[27] proposed a 2D ICMIC logistic modulation with Latin square permutation, reducing sequence length requirements and improving efficiency, but the method lacked extensive cryptanalytic validation. Gao et al.[32] integrated a 2D discrete hyperchaotic system with parallel compressive sensing, index scrambling, and diffusion under SHA-512-based key generation. While it enhanced efficiency, compressive sensing introduces reconstruction sensitivity that may affect robustness. Yang et al.[33] introduced a double image encryption method using a fractional order chaotic system with 2D compressive sensing, Zigzag confusion, and discrete wavelet transform. The scheme improved robustness and security but incurred higher computational cost due to fractional-order dynamics.

Gao et al.[34] presented a parallel encryption approach using the 2D logistic Rulkov neuron map (2D-LRNM) with cross channel interaction and block wise parallelism, which enhanced efficiency and task load balancing but required large memory resources for parallel processing. Xu et al.[35] developed a 2D cubic–tent map (2D-CTM) with strong chaotic behaviour, employing bit-level scrambling, chaotic flipping, and 3D Hilbert diffusion, thereby enhancing security and reducing pixel correlation. However, the increased complexity might limit real-time deployment. Zheng et al.[36] proposed the 2D iterative Gaussian sine chaotic map (2D-IGSCM) combined with a 3D Hill cipher, addressing weaknesses of the classical Hill cipher and achieving high security and efficiency, though cipher dependency on key scheduling could be a potential vulnerability. Wang et al.[37] designed the 2D log logistic sine chaotic map (2D-LLSCM) with a non-linear log function, achieving an enlarged chaotic range and dynamic complexity. Its joint scrambling diffusion scheme improved resistance against attacks, though its non-linear design may complicate hardware implementation. Li et al.[38] proposed the 2D exponential tangent cosine system (2D-ETCS), exhibiting hyperchaos, and introduced a cross permutation based color encryption method with multiple rounds of permutation, rotation, and masking. This significantly improved security but required multiple iterations, adding to computational load. Li et al.[39] introduced the 2D cross Gaussian hyper chaotic map (2D-CGHM) with dynamic polyhedra permutation and arnold diffusion (DPPAD-IE), enabling encryption of arbitrary-sized images with strong pseudo randomness. Its main limitation lies in the added algorithmic complexity compared to lightweight schemes. Based on the literature survey, to overcome the shortcomings and drawbacks of previous algorithms, we proposed a new image encryption framework. The main contributions of this research article are summarized as follows

- A new two-dimensional chaotic map, termed the 2D-Cosine Power Sine Coupled Map, is proposed. This map exhibits strong randomness and unpredictability, supported by high statistical values such as Lyapunov exponent, permutation entropy, and sample entropy.
- A novel recursive scrambling method is introduced, which leverages chaotic sequences to enhance the randomness and unpredictability of image encryption.
- A new diffusion process is developed by using a Fractal Fibonacci based approach, where the fractal structure is derived from the Hilbert curve. This mechanism effectively modifies the statistical relationship between adjacent pixels in the image.

The remaining sections of this paper describe the proposed chaotic map and its performance evaluation, the fundamental building blocks of the suggested encryption scheme, followed by a detailed analysis of its performance and security.

Proposed chaotic map

Talhaiui et.al proposes an one dimensional iterative chaotic map[40] which delivers maximum lyapunov exponent and randomness as in Eq. (1).

$$x_{n+1} = \cos\left(\frac{\alpha}{x_n^{\beta}}\right) \tag{1}$$

The chaotic map has its limitation wherein, for small values of x_n and large values of the exponent β, the term x_n^{β} approaches zero, resulting in the argument of the cosine function becoming unbounded. This leads to severe numerical instability and chaotic behaviour that is difficult to control, especially in finite precision systems. To increase randomness and chaotic area a one dimensional improved discrete cosine fractional chaotic map (1D-IDCF)[41] is proposed as defined in Eq. (2).

$$x_{n+1} = \mod((\alpha - 3).\cos(\frac{\alpha}{x_n^{\beta}}) * (2^{14}), 1) \tag{2}$$

Though it increases chaotic area and delivers high Lyapunov exponent it has certain limitations are, when $\alpha = 3$ the chaotic system has a value zero , it kills chaos leading to fixed point and lost all sensitivity to initial conditions. If x(n) nearer to zero the trigonometric cosine power can become extremely large which causes undefined behaviour in floating point computation.

To avoid such scenarios we are proposing a two dimensional Cosine Power Sine Coupled Map (CPSCM) Eq. (3) to increase randomness and unpredictability by adding a sinusoidal chaotic function which erases the situation of $\alpha = 3$ and η to fraction of cosine power to eliminate the denominator to zero

$$\begin{aligned} x_{n+1} &= \mod(f(x_n) + (\frac{\alpha}{\alpha+1})(\sin(\pi y_n))), 1) \\ y_{n+1} &= \mod(f(y_n) + (\frac{\alpha}{\alpha+1})(\sin(\pi x_{n+1}))), 1) \end{aligned} \tag{3}$$

where

$$f(x_n) = (\alpha)\cos(\frac{\alpha}{x_n^{\beta} + \eta})$$

The term $\frac{\alpha}{\alpha+1}$ is incorporated as a coupling coefficient to ensure that the additive sinusoidal interaction remains within a bounded range, satisfying $\left|\frac{\alpha}{\alpha+1} \cdot \sin(\pi x)\right| < 1$ for all $x \in [0, 1]$ and $\alpha > 0$, thereby preserving the invariant domain of the map under modular arithmetic and enabling controlled modulation of chaotic intensity with respect to α. To avoid singularities and ensure numerical stability in the non-linear mapping, a small positive constant $\eta > 0$ is added to the denominator in the expression $f(x_n) = \alpha\cos\left(\frac{\alpha}{x_n^{\beta}+\eta}\right)$. This guarantees that the argument of the cosine function remains finite for all $x_n \in (0, 1]$, especially when $x_n \to 0$ and $\beta > 1$, thereby preserving the continuity and boundedness of the chaotic system.

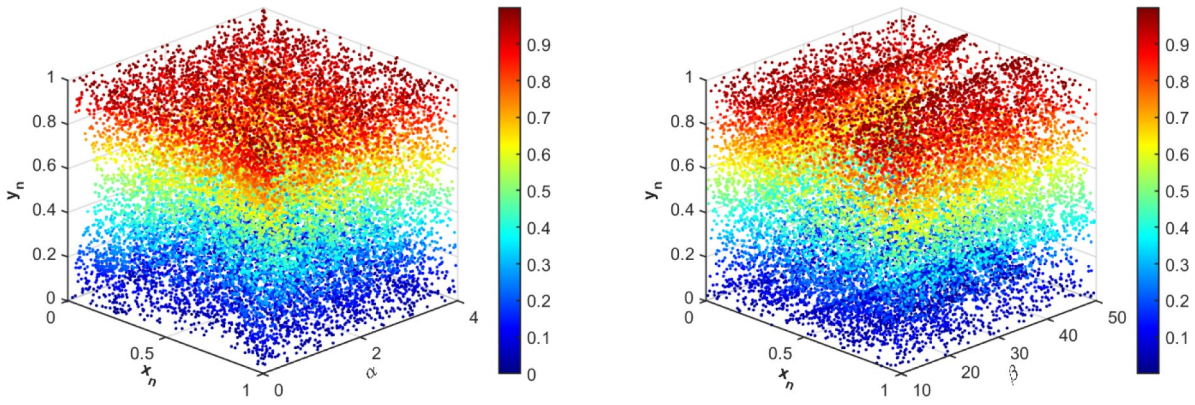
The proposed two dimensional chaotic system parameters are within α, β and $\eta \in [10^{-12}, 10^{-4}]$ to ensure bounded dynamics and maintain numerical stability.

Performance analysis of proposed chaotic map

This section describes about proposed chaotic system and its performance analysis by considering the characteristics of chaotic map like Lyapunov exponent (LE), Bifurcation diagram, Trajectory plots, key sensitivity, Sample Entropy (SE), Permutation Entropy (PE), Correlation Dimension (CD), Kolmogorov entropy (KE), Correlation analysis, 0-1 test , NIST randomness test.

Dynamic behaviour analysis

The dynamical behaviour of the proposed two-dimensional chaotic map was thoroughly examined to characterize its chaotic properties and evaluate its suitability for cryptographic applications. The bifurcation plot, shown in Fig. 1, illustrates how the system responds to variations in the control parameters α and β, revealing a wide chaotic range and rich unpredictable behaviour across the parameter space. Figure 2 presents the comparison of bifurcation diagrams of the proposed chaotic map with other existing chaotic maps presented in Table 1, where it exhibits a wider chaotic region compared to the others. Complementing this, trajectory plots



(a) Chaotic sequence x

(b) Chaotic sequence y

Fig. 1. Bifurcation Plots generated from proposed 2D-CPSCM (**a**) $\alpha \in (0, 4)$, $\beta = 20$ and $\eta = 10^{-8}$ (**b**) $\beta \in (10, 50)$, $\alpha = 2.5$ and $\eta = 10^{-8}$.

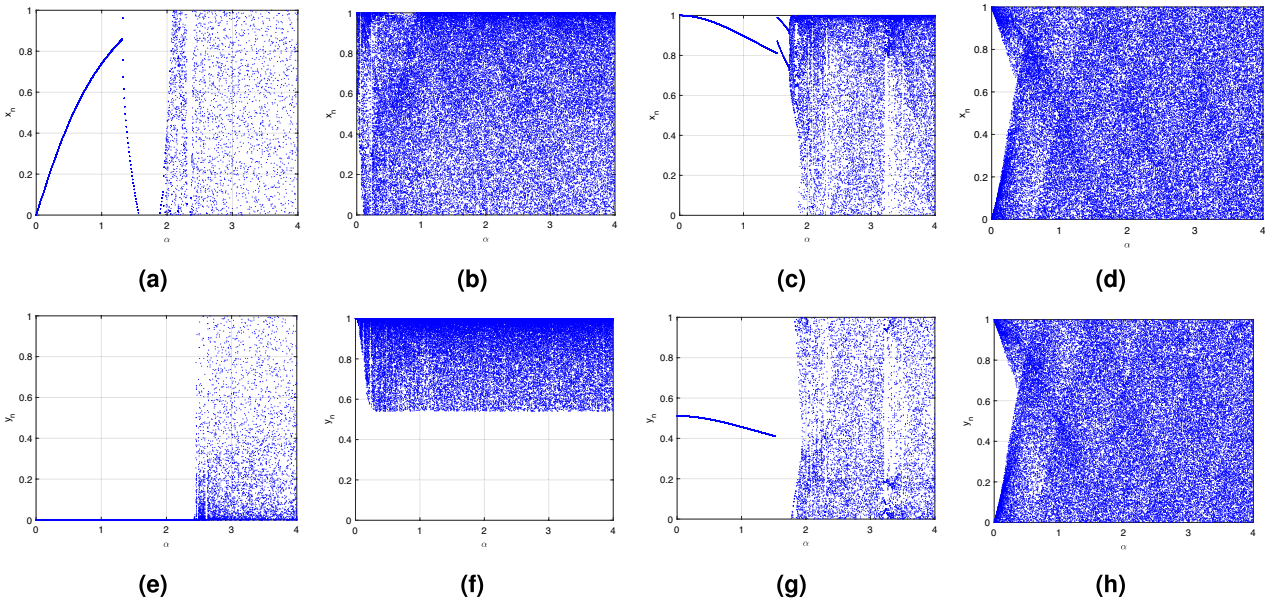


Fig. 2. Bifurcation diagrams of different two dimensional chaotic maps considering α as control parameter. Row 1: Chaotic sequence x and Row 2: Chaotic sequence y of 2D-TFCDM, 2D-CSM, 2D-CSIM and Proposed 2D-CPSCM, (Left to Right side).

Chaotic map	Mathematical equation	Parameters
2D-ILM[27]	$\begin{cases} x_{n+1} = \mod\left(x_n + \alpha\, y_n(y_n - 1),\ 1\right), \\ y_{n+1} = \sin\left(10/\sin(x_n + y_n)\right) \end{cases}$	$\alpha \in (0, 5]$
2D-TFCDM[26]	$\begin{cases} x_{n+1} = \alpha\cos(x_n - y_n), \\ y_{n+1} = \sin(y_n)\,(x_n^2) \end{cases}$	$\alpha \geq 2.5$
2D-CTM[35]	$\begin{cases} x_{i+1} = \begin{cases} (ay_i(1-x_i^2)^2 + 2\pi(10 - y_i^2)x_i) \bmod 1, & x_i \in (0, 0.5) \\ ay_i(1-x_i^2)^2 + 2\pi(10 - y_i^2)(1 - x_i) \bmod 1, & x_i \in [0.5, 1) \end{cases} \\ y_{i+1} = \begin{cases} (ax_{i+1}(1-y_i^2)^2 + 2\pi(10 - x_{i+1}^2)y_i \bmod 1, & y_i \in (0, 0.5) \\ (ax_{i+1}(1-y_i^2)^2 + 2\pi(10 - x_{i+1}^2)(1 - y_i)) \bmod 1, & y_i \in [0.5, 1) \end{cases} \end{cases}$	$a \in (0, +\infty)$
2D-CSM[24]	$\begin{cases} x_{i+1} = \left\lvert \cos\left(\sin(4\pi x_i^2(r+1)^2) + \sin(\pi r x_i y_i) + \sin(\pi r y_i^2)\right) \right\rvert, \\ y_{i+1} = \cos\left(\sin(4\pi y_i^2(r+1)^2))\sin(2\pi r x_{i+1} y_i)\right) \end{cases}$	$r \in [0.5, 10]$
2D-CSIM[25]	$\begin{cases} x_{i+1} = \cos(\beta y_i), \\ y_{i+1} = x_i - \sin(y_i) \end{cases}$	$\beta \in [10, 100]$
2D-CPSCM	$\begin{cases} x_{n+1} = \mod\left(f(x_n) + \dfrac{\alpha}{\alpha+1}\sin(\pi y_n),\ 1\right), \\ y_{n+1} = \mod\left(f(y_n) + \dfrac{\alpha}{\alpha+1}\sin(\pi x_{n+1}),\ 1\right), \\ f(x_n) = \alpha\cos\left(\dfrac{\alpha}{x_n^{\beta} + \eta}\right) \end{cases}$	$\alpha > 0,\ \beta > 1,\ \eta \in [10^{-12}, 10^{-4}]$

Table 1. Mathematical comparison of different chaotic maps.

Fig. 3 were used to visualize the evolution of the systems state sequences under fixed parameters. In the chaotic regime, the trajectories do not converge to periodic cycles but instead explore the entire phase space, forming an aperiodic attractor and highlighting the inherent randomness of the system. A key characteristic of chaos, the sensitivity to initial conditions, was analysed by generating sequences with slightly perturbed initial values, $(x_0, y_0) = (0.6, 0.6)$ and $(x_0, y_0) = (0.6 + 10^{-15}, 0.6 + 10^{-15})$, with $\alpha = 2.5$ and $\beta = 20$ over 50 iterations. As depicted in Fig. 4, even such a minimal variation leads to rapid divergence of trajectories, demonstrating high sensitivity, unpredictability, and strong chaotic characteristics.

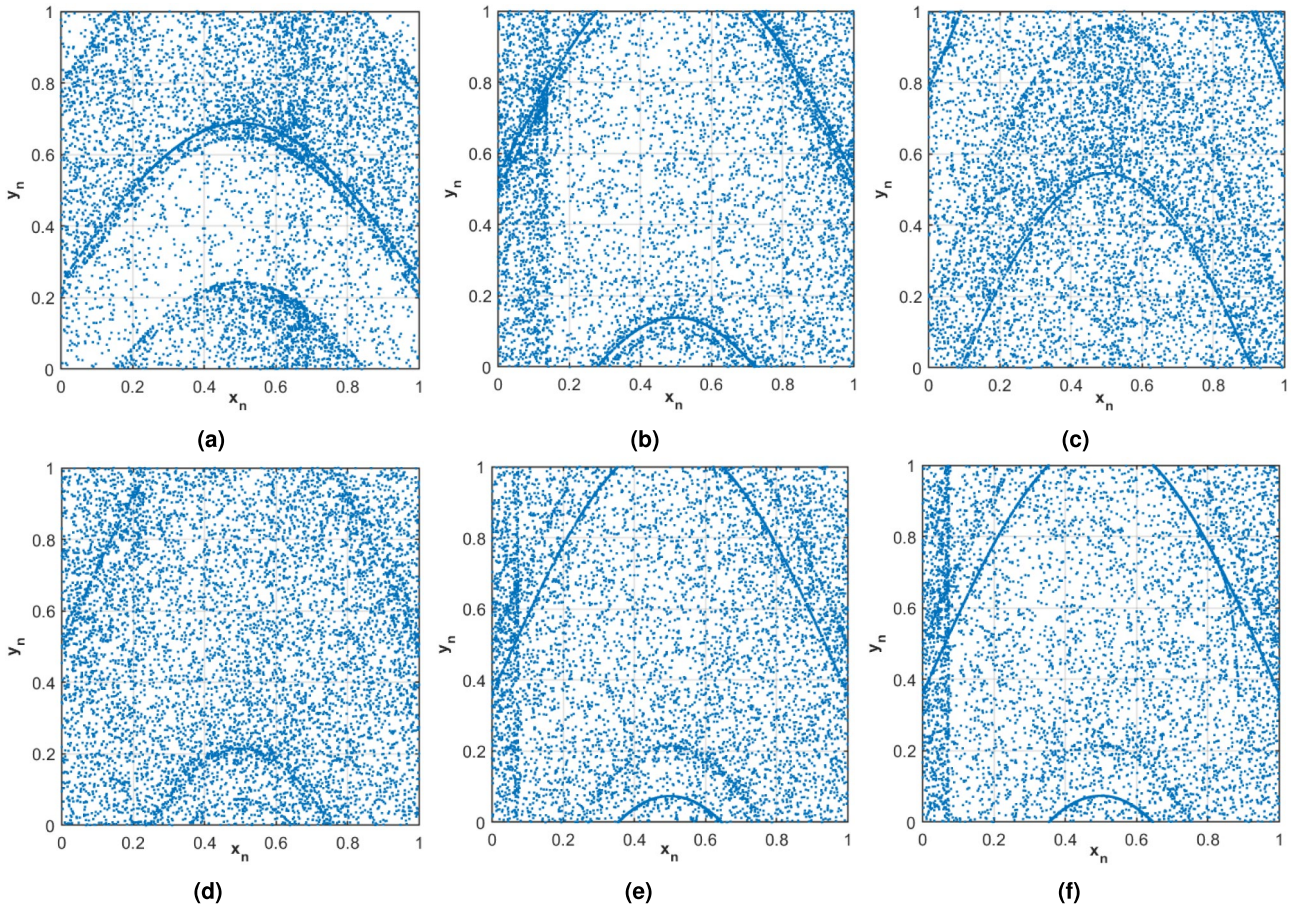
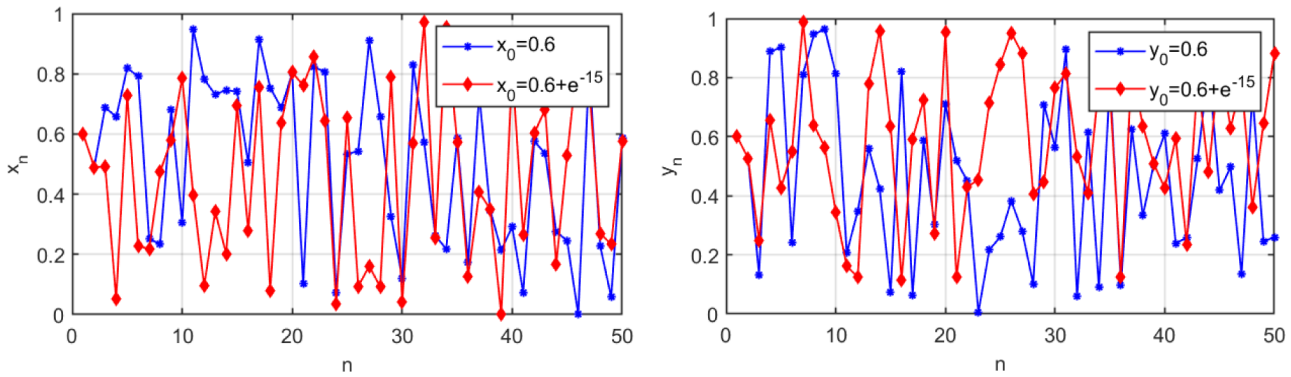


Fig. 3. Phase Attractor Plots: (**a**–**c**) for $\alpha = 0.8, 1.5, 3.2$ with $\beta = 20$; (**d**–**f**) for $\beta = 10, 20, 30$ with $\alpha = 2.5$.



(a) Chaotic sequence x **(b)** Chaotic sequence y

Fig. 4. Initial sensitivity analysis.

To quantitatively measure this divergence, the Lyapunov exponents (LEs) of the system were computed. LEs quantify how fast two initially close trajectories diverge, and a positive LE indicates chaos. For an n-dimensional system, the i-th Lyapunov exponent is calculated as Eq. (4)

$$LE_i = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \ln \left|\lambda_i(J_k)\right| \tag{4}$$

where $\lambda_i(J_k)$ is Jacobian matrix J_k eigenvalues at iteration k. The Jacobian matrix of the system is defined in Eq. (5)

$$J_n = \begin{bmatrix} \frac{\partial \phi_1}{\partial x_n} & \frac{\partial \phi_1}{\partial y_n} \\ \frac{\partial \phi_2}{\partial x_n} & \frac{\partial \phi_2}{\partial y_n} \end{bmatrix} \tag{5}$$

and the eigenvalues satisfy the characteristic equation in Eq. (6)

$$\det(\lambda I - J_k) = 0 \tag{6}$$

For hyperchaotic systems, having more than two positive Lyapunov exponents further confirms strong chaotic behaviour.

Lyapunov exponent numerical calculation
The partial derivative calculations of the proposed 2D-CPSCM are

$$\frac{\partial \phi_1}{\partial x_n} = \frac{\partial}{\partial x_n}\left[\mathrm{mod}\left(f(x_n) + \frac{\alpha}{\alpha+1}\sin(\pi y_n), 1\right)\right] = \frac{\partial f(x_n)}{\partial x_n}. \tag{7}$$

$$\frac{\partial \phi_1}{\partial y_n} = \frac{\partial}{\partial y_n}\left[\mathrm{mod}\left(f(x_n) + \frac{\alpha}{\alpha+1}\sin(\pi y_n), 1\right)\right] = \frac{\alpha}{\alpha+1}\pi\cos(\pi y_n). \tag{8}$$

$$\frac{\partial \phi_2}{\partial x_n} = \frac{\partial}{\partial x_n}\left[\mathrm{mod}\left(f(y_n) + \frac{\alpha}{\alpha+1}\sin(\pi x_{n+1}), 1\right)\right] = \frac{\alpha}{\alpha+1}\pi\cos(\pi x_{n+1})\frac{\partial x_{n+1}}{\partial x_n}. \tag{9}$$

$$\frac{\partial \phi_2}{\partial y_n} = \frac{\partial}{\partial y_n}\left[\mathrm{mod}\left(f(y_n) + \frac{\alpha}{\alpha+1}\sin(\pi x_{n+1}), 1\right)\right] = \frac{\partial f(y_n)}{\partial y_n} + \frac{\alpha}{\alpha+1}\pi\cos(\pi x_{n+1})\frac{\partial x_{n+1}}{\partial y_n}. \tag{10}$$

considering

$$f(x_n) = \alpha\cos\left(\frac{\alpha}{x_n^\beta + \eta}\right),$$

$$\frac{\partial f(x_n)}{\partial x_n} = \alpha\frac{\partial}{\partial x_n}\left[\cos\left(\frac{\alpha}{x_n^\beta + \eta}\right)\right] = \frac{\alpha^2\beta x_n^{\beta-1}}{(x_n^\beta + \eta)^2}\sin\left(\frac{\alpha}{x_n^\beta + \eta}\right). \tag{11}$$

Similarly,

$$\frac{\partial f(y_n)}{\partial y_n} = \frac{\alpha^2\beta y_n^{\beta-1}}{(y_n^\beta + \eta)^2}\sin\left(\frac{\alpha}{y_n^\beta + \eta}\right). \tag{12}$$

Hence the Jacobian is simplified to

$$J_n = \begin{bmatrix} \frac{\alpha^2\beta x_n^{\beta-1}}{(x_n^\beta+\eta)^2}\sin\left(\frac{\alpha}{x_n^\beta+\eta}\right) & \frac{\alpha}{\alpha+1}\pi\cos(\pi y_n) \\ \frac{\alpha}{\alpha+1}\pi\cos(\pi x_{n+1})\frac{\partial x_{n+1}}{\partial x_n} & \frac{\alpha^2\beta y_n^{\beta-1}}{(y_n^\beta+\eta)^2}\sin\left(\frac{\alpha}{y_n^\beta+\eta}\right) + \frac{\alpha}{\alpha+1}\pi\cos(\pi x_{n+1})\frac{\partial x_{n+1}}{\partial y_n} \end{bmatrix}. \tag{13}$$

Evaluating at the representative point $(x_n, y_n) = (0.131, 0.124)$ with parameters $\alpha = 3$, $\beta = 2$, and $\eta = 0.0001$:

$$x_n^\beta + \eta = 0.131^2 + 0.0001 \approx 0.017261, \quad \frac{\alpha}{x_n^\beta + \eta} = \frac{3}{0.017261} \approx 173.8022.$$

Thus,

$$J \approx \begin{bmatrix} 854.434 & 2.356133 \\ 1.872 & 850.621 \end{bmatrix}. \tag{14}$$

To find the the eigenvalues , the characteristic equation

$$\det(\lambda I - J) = 0.$$

$$\begin{vmatrix} 854.434 - \lambda & 2.356133 \\ 1.872 & 850.621 - \lambda \end{vmatrix} = 0. \tag{15}$$

the characteristic equation now as

$$\lambda^2 - 1705.055\,\lambda + 727518.39 = 0. \tag{16}$$

The corresponding eigenvalues are $\lambda_1 \approx 879.28,\ \lambda_2 \approx 825.77$..

The local Lyapunov exponents (LE) for the proposed chaotic map is given by

$$LE_i = \ln|\lambda_i|, \quad i = 1, 2. \tag{17}$$

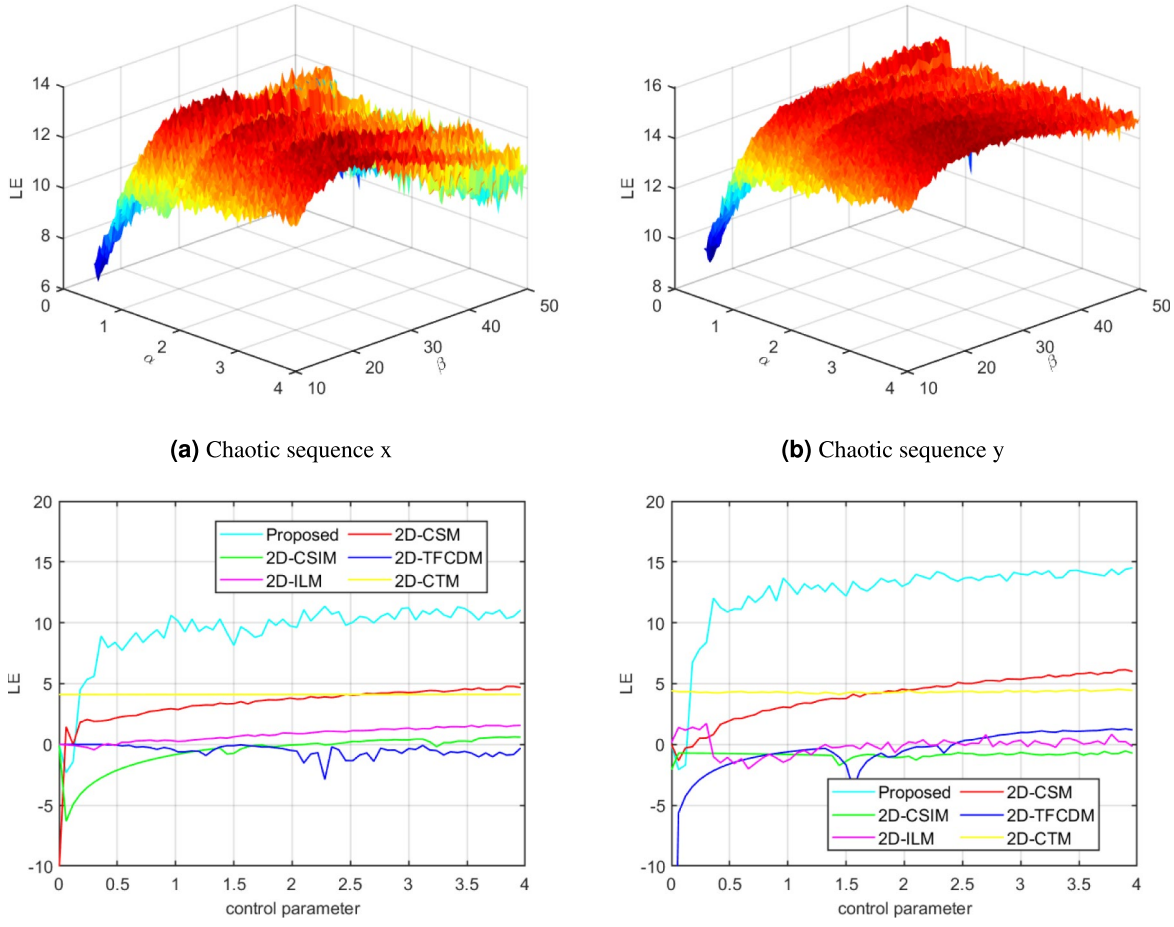
Thus, $LE_1 = \ln(879.28) = 6.779,\ LE_2 = \ln(825.77) = 6.716$.

As both LE_1 and LE_2 are positive, at $(x_n, y_n) = (0.131, 0.124)$ confirms the hyper chaotic nature of the proposed chaotic map.

The calculated LEs of the proposed map Fig. 5a, b are positive, which confirms the high divergence and unpredictability observed in the phase trajectories and initial sensitivity analysis. Together, these analyses confirm that the proposed chaotic map exhibits robust, aperiodic, and highly unpredictable behaviour, making it suitable for secure cryptographic applications where both randomness and sensitivity are critical. Furthermore, Fig. 5c, d present a comparative analysis between the proposed chaotic map and several existing two-dimensional maps, namely the 2D Cosine–Sine Map (CSM) [24], 2D-CSIM [25], 2D-TFCDM [26], 2D-ILM [27], and 2D-CTM [35]. The evaluation is carried out for both x and y sequences under variations in the control parameters of each chaotic system while maintaining the same initial conditions $(x_0, y_0) = (0.131, 0.124)$. The results clearly indicate that the proposed two-dimensional chaotic map achieves higher Lyapunov exponent values compared to the other benchmark maps, thereby confirming its superior chaotic behaviour.

Fixed point stability analysis

For a dynamical system a fixed point[42] is a point where the next state output is equal to the current output i,e $x_{n+1} = x_n$. If a point x^* is said to be equilibrium point of a chaotic map then $x^* = f(x^*)$. For the proposed two dimensional chaotic map assume $S(x^*, y^*)$ be fixed point then it satisfies $x_{n+1} = x*$ and $y_{n+1} = y*$, from Eq.3



(a) Chaotic sequence x

(b) Chaotic sequence y

(c) Comparison of LE for chaotic sequence x

(d) Comparision of LE for chaotic sequence y

Fig. 5. LE analysis.

$$\begin{aligned} x_{n+1} &= \phi_1(x_n, y_n) = f(x_n) + \frac{\alpha}{\alpha+1}\sin(\pi y_n), \\ y_{n+1} &= \phi_2(x_n, y_n) = f(y_n) + \frac{\alpha}{\alpha+1}\sin\left(\pi x_{n+1}\right), \end{aligned} \tag{18}$$

where

$$f(x_n) = \alpha\cos\left(\frac{\alpha}{(x_n)^\beta + \eta}\right), \qquad \alpha, \beta, \eta > 0.$$

A fixed point (x^*, y^*) satisfies the nonlinear system

$$\begin{cases} x^* = \phi_1(x^*, y^*) = f(x^*) + \frac{\alpha}{\alpha+1}\sin(\pi y^*), \\ y^* = \phi_2(x^*, y^*) = f(y^*) + \frac{\alpha}{\alpha+1}\sin(\pi x^*). \end{cases} \tag{19}$$

The stability analysis of each fixed point like S(X,Y) of the proposed chaotic system is determined by by deriving Jacobian matrix Eq. (20)

$$J_n = \begin{bmatrix} \dfrac{\alpha^2\beta x_n^{\beta-1}}{(x_n^\beta+\eta)^2}\sin\left(\dfrac{\alpha}{x_n^\beta+\eta}\right) & \dfrac{\alpha}{\alpha+1}\pi\cos(\pi y_n) \\ \dfrac{\alpha}{\alpha+1}\pi\cos(\pi x_{n+1})\dfrac{\partial x_{n+1}}{\partial x_n} & \dfrac{\alpha^2\beta y_n^{\beta-1}}{(y_n^\beta+\eta)^2}\sin\left(\dfrac{\alpha}{y_n^\beta+\eta}\right) + \dfrac{\alpha}{\alpha+1}\pi\cos(\pi x_{n+1})\dfrac{\partial x_{n+1}}{\partial y_n} \end{bmatrix}. \tag{20}$$

The corresponding characteristic polynomial of J is

$$\lambda^2 - (\mathrm{Trace}(J))\lambda + \det(J) = 0, \tag{21}$$

The corresponding eigenvalues are determined by finding the roots for equation

$$\lambda_{1,2} = \frac{\mathrm{Trace}(J) \pm \sqrt{(\mathrm{Trace}\,J)^2 - 4\det(J)}}{2}, \tag{22}$$

where $\mathrm{Trace}(J) = J_{11} + J_{22}$ and $\det(J) = J_{11}J_{22} - J_{12}J_{21}$.

The stability classification the proposed map of infinite fixed points is depends on the magnitude of eigenvalues λ_1 and λ_2 of Eq. (22) as

1. If both eigenvalues are$|\lambda_1| < 1$ and $|\lambda_2| < 1$ then S(X,Y) is stable fixed point ,
2. The eigenvalues$|\lambda_1| > 1$ or $|\lambda_2| > 1$, then S(X,Y) unstable fixed point ,
3. If $|\lambda_1| < 1$ and $\lambda_2 = -1$ (or vice versa) then the fixed point S(X,Y) is called as period-doubling bifurcation point (PBP),
4. If $|\lambda_{1,2}| = 1$ with $\mathrm{Re}(\lambda_{1,2}) < 1$ then the fixed point S(X,Y) is Neimark–Sacker bifurcation point (NBP).

To analyse the fixed point behaviour of the proposed chaotic map in the x-y phase plane, the system parameters are set as $(\alpha, \beta, \eta) = (1.5, 40, 10^{-8})$ and $(2.5, 20, 10^{-8})$. The corresponding phase attractors are shown in the Fig. 6, where red filled circles denote unstable fixed points with eigenvalues $|\lambda| > 1$, and dense tiny coloured dots represent chaotic trajectories around them. To determine the attractor type, trajectories are generated with slight perturbation in the unstable fixed points, all converging to the same chaotic region without specific initial conditions. The existence of multiple unstable fixed points with bounded chaotic trajectories confirms that the system exhibits self excited chaotic attractors, as the trajectories originate directly from the neighbourhood of the unstable fixed points.

Complexity and randomness measures

The complexity and randomness of the proposed two-dimensional chaotic map were evaluated using Sample Entropy (SE), Permutation Entropy (PE), and Kolmogorov Entropy (KE) to assess the unpredictability and information richness of the generated sequences. Sample Entropy measures the irregularity and intricacy of time series sequences by counting the number of identical patterns within a acceptable threshold. For a time series $\{y_1, y_2, \ldots, y_n\}$, the SE is defined as Eq. (23)

$$\text{Sample Entropy}(r, d, n) = -\log\frac{E}{F} \tag{23}$$

where E and F are the counts of vector pairs satisfying the inequalities $G[Y_{r+1}(i), Y_{r+1}(j)] < d$ and $G[Y_r(i), Y_r(j)] < d$, respectively, with $G[\cdot]$ representing the Chebyshev distance between vectors $Y_r(i) = \{y_i, y_{i+1}, \ldots, y_{i+r-1}\}$. For the proposed system, the embedding dimension $r = 2$ and threshold $d = 0.2 \times \mathrm{STD}$, where STD is the standard deviation of the series. Figure 7 demonstrates that the SE values of the proposed map for x and y sequences are significantly higher than those of benchmark chaotic maps, indicating strong aperiodicity and pseudo-randomness.

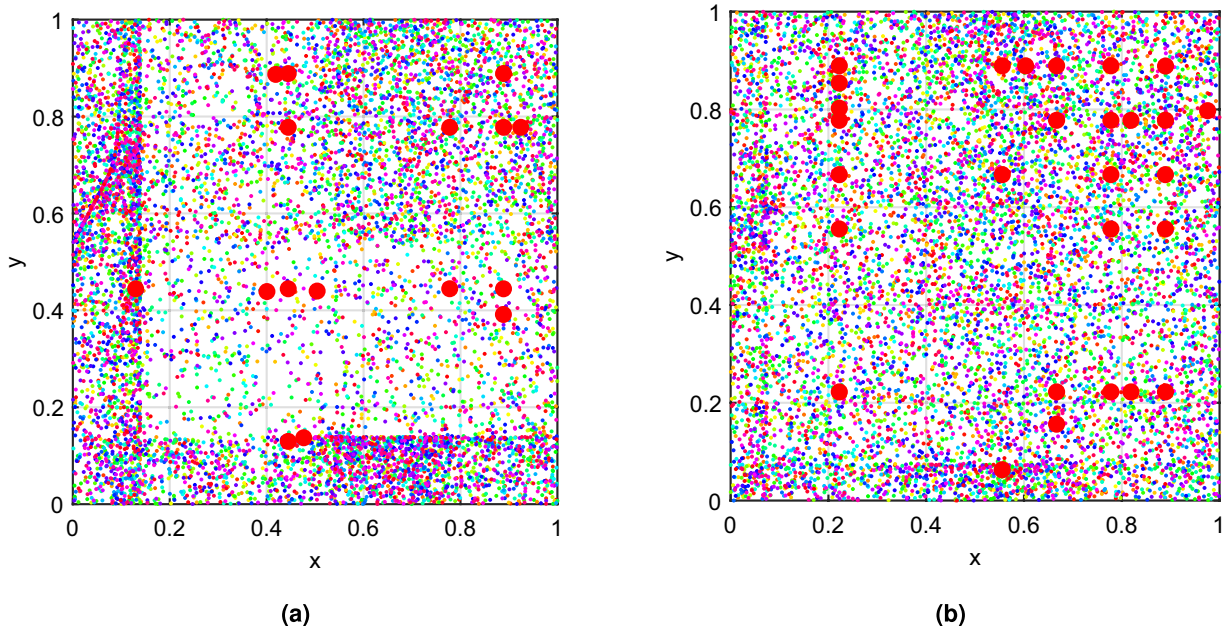
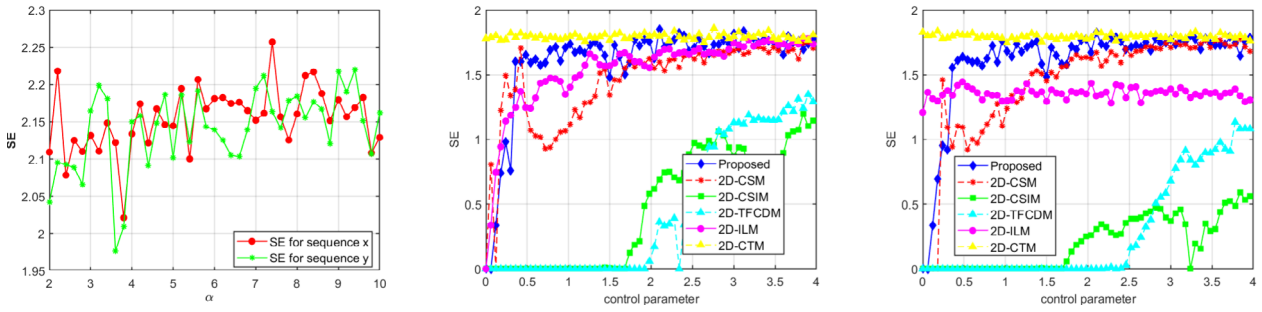


Fig. 6. Phase portraits for fixed system parameters: (**a**) $(\alpha, \beta, \eta) = (1.5, 40, 10^{-8})$, (**b**) $(\alpha, \beta, \eta) = (2.5, 20, 10^{-8})$, where red filled circles represent unstable fixed points, and dense tiny coloured dots indicate chaotic trajectories around them.



(a) α versus SE **(b)** Comparison of SE for Chaotic sequence x **(c)** Comparison of SE for Chaotic sequence y

Fig. 7. SE analysis.

Permutation Entropy (PE) further quantifies the unpredictability of the system by evaluating the probability distribution of ordinal patterns in the sequences. The normalized PE is computed as Eq. (24)

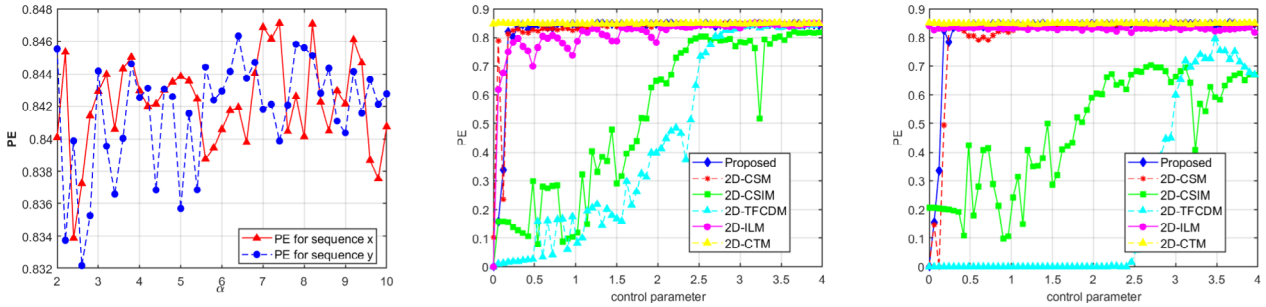
$$PE_{\text{norm}} = \frac{PE}{\log(n!)}, \quad PE = -\sum_{i=1}^{n!} p(x_i)\log(p(x_i)) \tag{24}$$

where $p(x_i)$ denotes the probability of each ordinal pattern. The proposed map achieves an average PE of 0.852, near to the theoretical maximum of 1, which is higher and more stable than other contemporary two-dimensional chaotic systems Fig. 8. This indicates enhanced randomness and unpredictability, reinforcing its suitability for secure encryption.

Kolmogorov Entropy (KE) complements SE and PE by quantifying the rate of information generation within the system. Mathematically, KE is expressed as Eq. (25)

$$KE = -\lim_{n\to\infty}\lim_{\varepsilon\to 0}\lim_{\tau\to 0}\frac{1}{n\tau}\sum_{i_0,i_1,\ldots,i_n} p(i_1,\ldots,i_n)\ln\left[p(i_1,\ldots,i_n)\right] \tag{25}$$

where the n-dimensional phase space is partitioned into boxes $(i_0, i_1, \ldots, i_n)$ of size ε, τ is the temporal delay, and $p(i_1, \ldots, i_n)$ is the joint probability of the trajectory occupying the corresponding boxes. A positive KE reflects high unpredictability, and Fig. 9 illustrates KE variations with α and β. The proposed chaotic map achieves



(a) α versus PE **(b)** Comparison of PE for Chaotic sequence x **(c)** Comparison of PE for Chaotic sequence y

Fig. 8. PE analysis.

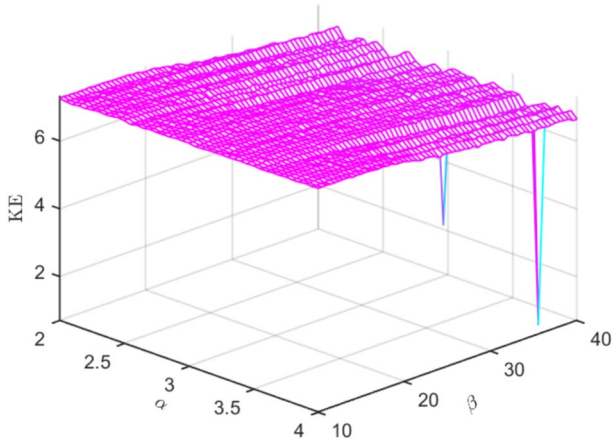


Fig. 9. KE analysis for α and β.

an average KE of 7.3159, confirming both high unpredictability and stable chaotic behaviour. Collectively, SE, PE, and KE analyses demonstrate that the proposed system generates complex, highly unpredictable sequences suitable for robust cryptographic applications.

Correlation and statistical analysis

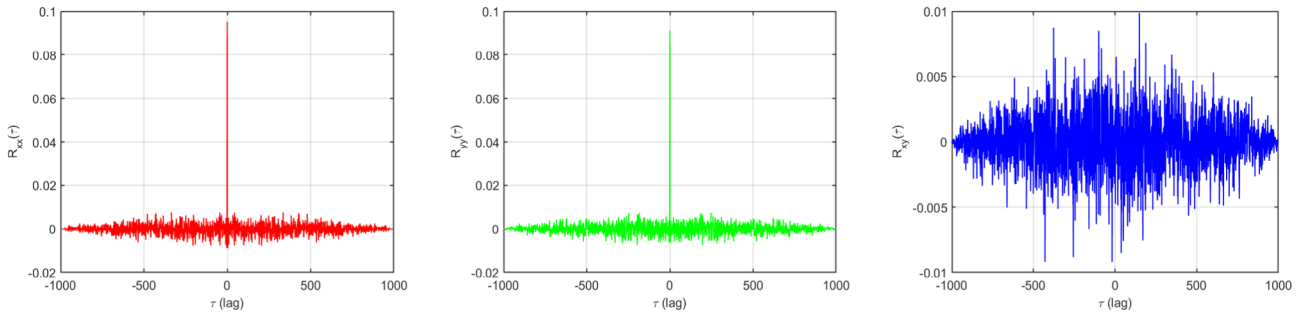
To further evaluate the statistical properties and complexity of the proposed two-dimensional chaotic map, autocorrelation, cross-correlation, and correlation dimension analyses were performed. Autocorrelation quantifies the similarity of a time series with itself at different lags, while cross-correlation measures the similarity between two distinct sequences as a function of displacement τ. Mathematically, these are defined as Eq. (26)

$$\begin{aligned} r_{xy}(\tau) &= \frac{1}{N-\tau}\sum_{t=1}^{N-\tau}\left(x(t)-\mu_x\right)\left(y(t+\tau)-\mu_y\right), \\ r_{xx}(\tau) &= \frac{1}{N-\tau}\sum_{t=1}^{N-\tau}\left(x(t)-\mu_x\right)\left(x(t+\tau)-\mu_x\right) \end{aligned} \tag{26}$$

where r_{xx} and r_{xy} denote the autocorrelation and cross-correlation, respectively, N is the number of points in each series, and μ_x and μ_y are the mean values of $x(t)$ and $y(t)$. Figure 10a and b illustrate the autocorrelation of the x and y sequences, showing a prominent spike at lag 0 and near-zero values at other lags, confirming the absence of significant self-similarity and the generation of aperiodic sequences. The cross-correlation between the two sequences, depicted in Fig. 10c, exhibits a near-zero zigzag pattern, indicating that x and y are highly uncorrelated and statistically independent.

The correlation dimension (CD) provides a quantitative measure of the attractor's fractal complexity in the phase space. It is calculated through the integral of correlation $C_e(r)$ as Eq. (27)

$$CD = \lim_{r\to 0}\lim_{M\to\infty}\frac{C_e(r)}{\log(r)} \tag{27}$$



(a) Chaotic sequence x **(b)** Chaotic sequence y **(c)** Cross Correlation

Fig. 10. Correlation analysis.

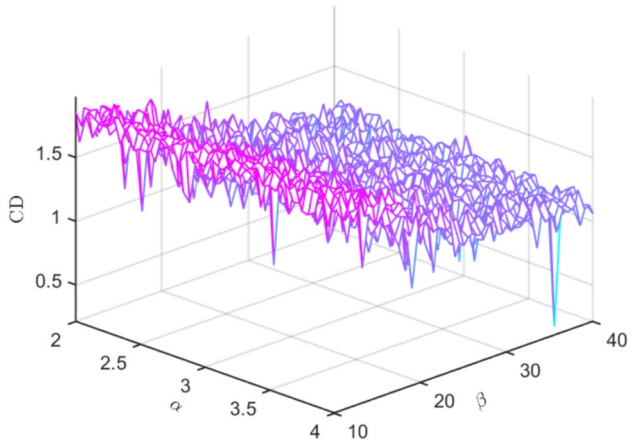


Fig. 11. CD analysis for α and β.

Higher CD values correspond to more complex and irregular behavior, indicating that the time series spans a higher-dimensional phase space. The three-dimensional visualization of CD, shown in Fig. 11, confirms that the proposed chaotic map exhibits rich and diverse dynamics. Collectively, autocorrelation, cross-correlation, and correlation dimension analyses validate that the sequences generated by the proposed system are statistically independent, aperiodic, and highly complex, reinforcing their suitability for cryptographic applications.

Chaos validation and randomness testing

To further validate the chaotic nature and cryptographic suitability of the proposed two-dimensional map, both the 0-1 test and NIST statistical test suite were employed. The 0-1 test provides a sensitive measure of chaos directly from time series data, without requiring phase space reconstruction. For a sequence $u(n)$, the auxiliary variables $p(n)$ and $q(n)$ are defined as Eq. (28)

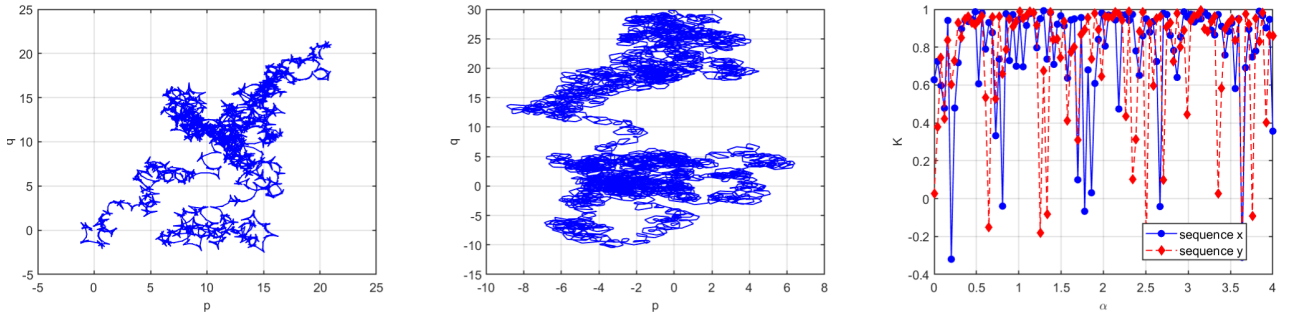
$$\begin{aligned} p(n+1) &= p(n) + u(n)\cos c(n), \\ q(n+1) &= q(n) + u(n)\sin c(n) \end{aligned} \tag{28}$$

where c is a constant in the interval $(0, 2\pi)$. This leads to Eq. (29)

$$\begin{aligned} p_c(n) &= \sum_{j=1}^{n} u(j)\cos(jc), \\ q_c(n) &= \sum_{j=1}^{n} u(j)\sin(jc) \quad n = 1, 2, \ldots, N \end{aligned} \tag{29}$$

and the mean square displacement is calculated as Eq. (30)

$$M(n) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} \left[\big(p(j+n) - p(j)\big)^2 + \big(q(j+n) - q(j)\big)^2 \right] \tag{30}$$



(a) Chaotic sequence x **(b)** Chaotic sequence y **(c)** Asymptotic Growth Rate (K) Analysis

Fig. 12. 0-1 test analysis.

Test name	Sequence x		sequence y	
	p-value	Result	*p*-value	Result
Single bit test	0.4021 ± 0.279	✓	0.4033 ± 0.292	✓
Frequency test within a block	0.4964 ± 0.222	✓	0.5123 ± 0.324	✓
Nun test	0.5417 ± 0.267	✓	0.4934 ± 0.239	✓
The longest run test	0.4693 ± 0.269	✓	0.4784 ± 0.183	✓
Binary matrix rank test	0.5256 ± 0.273	✓	0.4791 ± 0.265	✓
Discrete Fourier test	0.3745 ± 0.190	✓	0.5345 ± 0.268	✓
Non-overlapping template matching test	0.6513 ± 0.284	✓	0.4156 ± 0.302	✓
Overlap template test	0.463 ± 0.364	✓	0.3597 ± 0.245	✓
MaurerGeneral statistical test	0.5827 ± 0.312	✓	0.4974 ± 0.305	✓
Linear complexity tests	0.5191 ± 0.244	✓	0.4288 ± 0.326	✓
Sequence test	0.2398 ± 0.177	✓	0.4285 ± 0.284	✓
Approximate entropy test	0.4032 ± 0.257	✓	0.3296 ± 0.198	✓
Accumulation and test	0.5156 ± 0.286	✓	0.3902 ± 0.334	✓
random travel test	0.1864 ± 0.093	✓	0.1635 ± 0.125	✓
Random variation testing	0.2198 ± 0.144	✓	0.1344 ± 0.084	✓

Table 2. NIST test results average $\pm$ standard deviation for 10 independent runs. (✓) indicates sequence passed the test

The asymptotic growth rate is Eq. (31)

$$K = \lim_{n\to\infty} \frac{\log M(n)}{\log n} \tag{31}$$

indicates chaos when K approaches 1, and regular dynamics when K is close to 0. For the proposed map, with $\alpha = 2.5, \beta = 20$, and initial values $(x_0, y_0) = (0.131, 0.124)$, the 0-1 test results Fig. 12 show (p, q) trajectories resembling Brownian motion, and the K values for x and y sequences are 0.9077 and 0.9081, respectively, confirming hyperchaotic behaviour.

In addition, the NIST statistical test suite was employed to rigorously evaluate the randomness and unpredictability of the generated sequences. This suite consists of 15 subtests examining different aspects of statistical randomness, with outcomes expressed as p-values. Sequences are considered random if the p-values exceed 0.01. As summarized in Table 2, all p-values for the proposed chaotic map sequences surpass this threshold, confirming strong randomness, unpredictability, and suitability for cryptographic applications. Collectively, the 0-1 test and NIST results validate that the proposed map exhibits robust chaotic dynamics and produces highly unpredictable sequences.

Furthermore, the comparative analysis of the proposed chaotic map with other systems, in terms of statistical measures reported in Table 3, indicates that the proposed two-dimensional chaotic map delivers superior values for LE, Asymptotic growth rates (K_1, K_2), CD and KE, while achieving approximately equal performance for the remaining metrics. These results confirm the effectiveness and competitiveness of the proposed chaotic system.

Chaotic map	LE_1	LE_2	SE_1	SE_2	PE_1	PE_2	r_{xx}	r_{yy}	r_{xy}	K_1	K_2	CD	KE
Proposed	**11.715**	**14.674**	1.850	1.830	0.850	0.852	**−0.0070**	−0.0086	−0.0084	**0.907**	**0.908**	**1.855**	**7.315**
[24]	4.778	6.148	1.742	1.777	0.851	0.851	−0.0446	−0.0232	−0.0344	0.677	0.653	1.734	7.101
[25]	0.658	0.059	1.197	0.592	0.820	0.705	−0.1426	−0.7804	−0.3764	0.560	0.528	0.029	2.197
[26]	0.609	1.340	1.379	1.111	0.849	0.797	−0.6394	−0.1499	−0.2449	0.801	0.268	0.761	3.365
[27]	1.618	1.907	1.792	1.446	0.841	0.850	−0.0080	−0.1731	−0.0225	0.894	0.857	1.736	7.002
[35]	4.122	4.541	1.868	1.842	0.852	0.853	−0.0097	−0.0064	−0.0072	0.892	0.897	1.736	7.312

Table 3. Statistical analysis of chaotic maps. Significant values are in bold

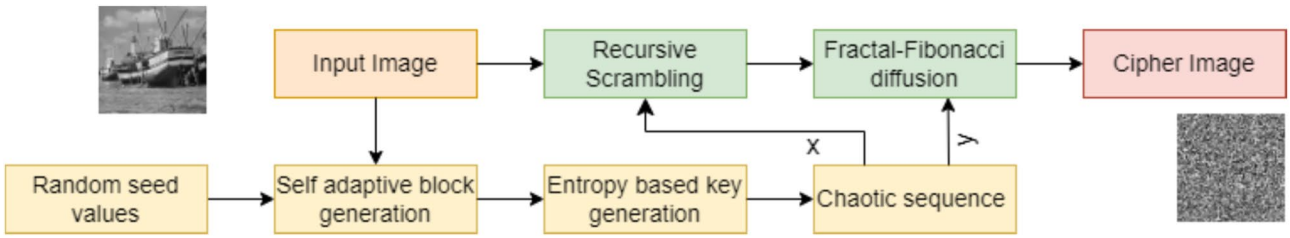


Fig. 13. Image encryption algorithm flow chart.

Proposed encryption scheme

This section presents the proposed encryption algorithm, outlining its fundamental building blocks and their integration in transforming an input image into a highly randomized encrypted image. The overall process is illustrated in the flowchart shown in Fig. 13.

Self adaptive prime modulo based Hashing algorithm

The proposed self-adaptive prime-modulo block hashing method partitions an image into dynamically assigned hash blocks and iteratively refines their distribution using a feedback-driven mechanism. Given an input image I of size $m \times n$, it is first converted to grayscale, flattened into a one-dimensional sequence, and the number of hash blocks is defined as $B = \min(m, n)$. To ensure uniform and collision-resistant mapping, the smallest prime $q \geq mn$ is selected as the modular space. This process starts with two secret seeds r_{ini} and s_{ini} are converted into integer keys r and s as Eq. (32)

$$\begin{aligned} r &= \mod\left(\lfloor r_{\text{ini}} \times 10^{10} \rfloor, q-1\right) + 1, \\ s &= \mod\left(\lfloor s_{\text{ini}} \times 10^{10} \rfloor, q\right) \end{aligned} \tag{32}$$

which control the initial pixel-to-block allocation through the hash function defined by Eq. (33)

$$h(i) = \mod\left(\mod\left(r \cdot i + s,\ q\right),\ B\right) + 1 \tag{33}$$

where i is the pixel index in the flattened sequence. Each pixel is assigned to a block $h(i)$, and after all pixels are distributed, block statistics such as the total sum $S_{\text{total}} = \sum_{b=1}^{B} \sum_{x \in \mathscr{B}_b} x$ and cumulative standard deviation $\sigma_{\text{total}} = \sum_{b=1}^{B} \sigma(\mathscr{B}_b)$ are computed. These statistics are fed back to update the hash keys across rounds using Eq. (34)

$$\begin{aligned} r &\leftarrow \left(r + \lfloor S_{\text{total}} \rfloor\right) \bmod (q-1) + 1, \\ s &\leftarrow \left(s + \lfloor \sigma_{\text{total}} \rfloor\right) \bmod q \end{aligned} \tag{34}$$

which introduces adaptivity and ensures that even minor variations in the image propagate across multiple iterations. After a predefined number of rounds, this feedback mechanism yields a highly irregular and content dependent block structure that enhances confusion and diffusion properties, making it well suited for cryptographic applications such as chaotic initialization, DNA based diffusion, or permutation driven image encryption. The step wise implementation of this procedure is summarized in Algorithm 1.

Require: Image $I \in \mathbb{Z}^{m\times n}$, seeds $r_{\text{ini}}, s_{\text{ini}} \in (0,1)$, rounds R
Ensure: Hash blocks $\{\mathscr{B}_1, \ldots, \mathscr{B}_B\}$
$B \leftarrow \min(m,n)$
$q \leftarrow$ smallest prime $\geq mn$
$r \leftarrow \mod(\lfloor r_{\text{ini}} \times 10^{10} \rfloor, q-1)+1$
$s \leftarrow \mod(\lfloor s_{\text{ini}} \times 10^{10} \rfloor, q)$
for round $\leftarrow 1$ to R **do**
  Initialize empty blocks: $\mathscr{B}_1, \ldots, \mathscr{B}_B \leftarrow \emptyset$
  for $i \leftarrow 0$ to $mn-1$ **do** ▷ Assign each pixel to a block
    $row \leftarrow \lfloor i/n \rfloor + 1$
    $col \leftarrow (i \bmod n)+1$
    $h \leftarrow \mod(\mod(r \times i + s, q), B)+1$
    Append pixel to block: $\mathscr{B}_h \leftarrow \mathscr{B}_h \cup \{I(row,col)\}$
  end for
  Compute :

$$S_{\text{total}} = \sum_{b=1}^{B} \sum_{x\in\mathscr{B}_b} x, \quad \sigma_{\text{total}} = \sum_{b=1}^{B} \sigma(\mathscr{B}_b)$$

  Update keys:

$$r \leftarrow \mod(r + \lfloor S_{\text{total}} \rfloor, q-1)+1, \quad s \leftarrow \mod(s + \lfloor \sigma_{\text{total}} \rfloor, q)$$

end for
return $\{\mathscr{B}_1, \ldots, \mathscr{B}_B\}$

Algorithm 1. Self-adaptive block hashing

Entropy based key generation

This section describes the generation of control parameters for the proposed chaotic system based on the blocks generated from self adaptive prime modulo based hashing algorithm. In this step each block entropy is calculated and concatenated into a one dimensional vector to apply to SHA-256 hash algorithm, and convert this 256 bit hash value into 512 bit binary number and group onto 64 groups and calculate the control parameters.

The generation of image-dependent chaotic keys is performed in five sequential steps as described below.

Step 1: The input image is initially partitioned into B non-overlapping pixel blocks using self adaptive block hashing algorithm 1 and the Shannon entropy of each block is computed as Eq. (35)

$$\{\mathscr{B}_1, \mathscr{B}_2, \ldots, \mathscr{B}_B\},$$
$$H_b = -\sum_i p_i^{(b)} \log_2 p_i^{(b)}, \quad b = 1,2,\ldots,B. \tag{35}$$

where $p_i^{(b)}$ is i-th intensity in block $\mathscr{B}_b$ probability. The resulting entropy vector is Eq. (36)

$$E = [H_1, H_2, \ldots, H_B] \tag{36}$$

Step 2: The entropy vector E is fed to SHA-256 algorithm producing a 256-bit digest. The digest is represented as a 512-bit binary sequence, which is further divided into 64 consecutive 8-bit segments as Eq. (37)

$$\begin{cases} h = \text{SHA-256}(E), \\ H_{\text{bin}} = \text{Binary}(h), \quad H_{\text{bin}} \in \{0,1\}^{512}, \\ K_i = H_{\text{bin}}[\,8(i-1)+1 : 8i\,], \quad i = 1,2,\ldots,64. \end{cases} \tag{37}$$

Step 3: Each 8-bit group K_i is converted into its decimal representation using Eq. (38)

$$K[i] = \text{bin2dec}(K_i) \quad i = 1,2,\ldots,64. \tag{38}$$

Step 4: To mix entropy across different positions, four aggregate integers are obtained using XOR folding as Eq. (39)

$$d_i = \bigoplus_{j=0}^{15} K[i+4j] \quad i = 1, 2, 3, 4. \tag{39}$$

where $\oplus$ denotes bitwise XOR.

Step 5: Finally, the XOR-folded integers are mapped to the initial conditions and control parameters of the chaotic system as Eq. (40)

$$\begin{cases} x_0 = 0.1 + \dfrac{0.8}{255} \times d_1, \\ y_0 = 0.1 + \dfrac{0.8}{255} \times d_2, \\ \alpha = 1.0 + \dfrac{8.0}{255} \times d_3, \\ \beta = d_4 \bmod 20. \end{cases} \tag{40}$$

The tuple $(x_0, y_0, \alpha, \beta)$ serves as the final chaotic key, which generates the chaotic sequences of length $m \times n$, and is modified according to Eqs. (41) and (42) for the usage of subsequent encryption stages. Here consider $\eta = 10^{-8}$ as constant for generation of chaotic sequences.

$$x(i) = \bmod\left(\left\lfloor x(i) \times 10^5 \right\rfloor, 6\right) + 1 \tag{41}$$

$$y(i) = \left\lfloor \bmod\left(y(i) \times 10^8, 256\right) \right\rfloor \tag{42}$$

where $\lfloor . \rfloor$ indicates floor operation.

Recursive chaotic based block scrambling

Traditional image scrambling methods such as row column shuffling, zigzag scanning, Arnold cat maps, and global chaotic permutations offer basic obfuscation but suffer from limited key space, predictable structures under chosen plaintext attacks, weak entropy diffusion, and low resistance to local statistical analysis. To overcome these shortcomings, we propose a Recursive Chaotic Scrambling scheme that leverages fractal inspired quadtree decomposition and chaotic key driven geometric transformations for multi-scale disruption of spatial dependencies.

Given an input image block $\mathrm{I} \in \mathbb{Z}^{N \times N}$, the algorithm recursively partitions it into four sub blocks $\{\mathrm{Q}_1, \mathrm{Q}_2, \mathrm{Q}_3, \mathrm{Q}_4\}$ at each recursion level ℓ, where a chaotic key vector x from Eq. (41) assigns a transformation index $k = \mathrm{x}[4(\ell-1)+i],\ i \in \{1,2,3,4\}$. Each partitioned sub block then undergoes a reversible operation horizontal/vertical flip, $90^\circ/180^\circ$ rotation, or transposition while $k = 1$ leaves the block unchanged. After local transformation, the blocks are recursively processed up to a maximum depth L and recombined to form the scrambled output O. This whole process is explained in Algorithm 2.

This hierarchical strategy breaks coarse structures in early levels and fine pixel correlations in deeper levels, yielding multilevel permutation with high sensitivity to initial keys. The combined use of flips, rotations, and transpositions enhances permutation entropy, enlarges the key space, and provides high resistance to statistical and differential attacks, while remaining lightweight and fully reversible for seamless integration with subsequent diffusion stages in secure image encryption.

Fractal Fibonacci fusion diffusion

The proposed Fractal Fibonacci Fusion Diffusion scheme enhances image encryption by combining fractal-space traversal with Fibonacci inspired recursive diffusion. First, the input scrambled image $O \in \mathbb{Z}^{M \times N}$ is linearized into a one-dimensional sequence P using a Hilbert space filling curve of order $\log_2 N$ as shown in Fig. 14, which preserves local neighbourhood relations while introducing a fractal mapping that disperses spatial correlations.

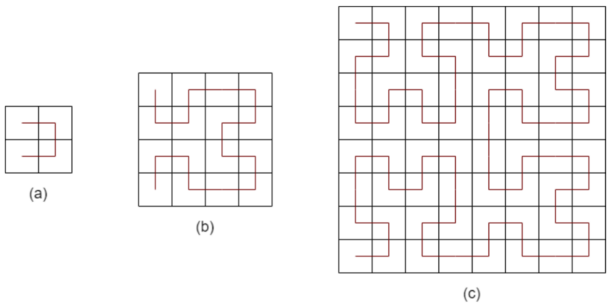


Fig. 14. Hilbert curve (**a**) order 1, (**b**) order 2, and (**c**) order 3.

Require: Image $\mathbf{I} \in \mathbb{Z}^{N \times N}$, chaotic key sequence $\mathbf{x}$, recursion depth $\ell \leq L$
Ensure: Scrambled block $\mathbf{O}$

if $\ell > L$ **then**
  return $\mathbf{I}$
end if
Partition $\mathbf{I}$ into quadrants:

$$\mathbf{I} \rightarrow \{\mathbf{Q}_1, \mathbf{Q}_2, \mathbf{Q}_3, \mathbf{Q}_4\}$$

for $i = 1$ to 4 **do**
  $k \leftarrow \mathbf{x}[4(\ell - 1) + i]$
  Apply chaos-controlled transformation

$$\mathbf{Q}_i \leftarrow T_k(\mathbf{Q}_i),$$

where

$$T_k \in \{\mathbb{I}, \text{Flip}_h, \text{Flip}_v, \text{Rot}_{90}, \text{Rot}_{180}, \text{Transpose}\}$$

  Recursively scramble:

$$\mathbf{Q}_i \leftarrow \texttt{RecursiveScramble}(\mathbf{Q}_i, \mathbf{x}, \ell + 1, L)$$

end for
Recombine quadrants:

$$\mathbf{O} = \begin{bmatrix} \mathbf{Q}_1 & \mathbf{Q}_2 \\ \mathbf{Q}_3 & \mathbf{Q}_4 \end{bmatrix}$$

return $\mathbf{O}$

Algorithm 2. Recursive chaotic scrambling

Unlike raster scans and zig-zag scans, the Hilbert traversal ensures that 2D neighbours remain close in 1D, enabling local perturbations to propagate globally during diffusion. The chaotic sequence y from Eq. (42) generated from the key dependent system. The diffusion follows the Fibonacci inspired recursion, where the first two pixels are updated as Eq. (43)

$$\begin{aligned} D(1) &= (P(1) + y(1)) \bmod 256, \\ D(2) &= (P(2) + D(1) + y(2)) \bmod 256 \end{aligned} \tag{43}$$

and each subsequent pixel for $i \geq 3$ is computed as Eq. (44)

$$D(i) = \big(P(i) + D(i-1) + D(i-2) + y(i)\big) \bmod 256 \tag{44}$$

This recursive fusion ensures that every pixel depends on its two predecessors and the chaotic input, amplifying sensitivity to both plaintext and keys. Finally, the diffused 1D sequence is remapped to 2D using the inverse Hilbert curve, yielding the final diffused image C_{cipher} as described in Algorithm 3. By jointly leveraging fractal space filling traversal, Fibonacci style dependency, and chaotic modulation, this lightweight diffusion achieves high entropy, strong nonlinearity, and robust resistance against statistical and differential attacks.

Require: Grayscale image $O \in \mathbb{Z}^{M\times N}$, chaotic sequence $y \in \mathbb{R}^N$
Ensure: Cipher image C_{cipher}
Convert O to double precision
$P \leftarrow \text{HilbertCurveTraversal}(O)$ ▷ Hilbert-ordered pixel sequence
$D \leftarrow \text{zeros}(1, N)$
$D(1) \leftarrow (P(1) + y(1)) \bmod 256$
$D(2) \leftarrow (P(2) + D(1) + y(2)) \bmod 256$
for $i = 3$ to N **do**
    $D(i) \leftarrow (P(i) + D(i-1) + D(i-2) + y(i)) \bmod 256$
end for
$C_{\text{cipher}} \leftarrow \text{InverseHilbertMapping}(D)$
return C_{cipher}

Algorithm 3. Fractal Fibonacci fusion diffusion

Simulation and security analysis

This section presents the simulation results and security analysis of the proposed encryption algorithm, implemented using MATLAB 2023a. For evaluation, we considered ten different grayscale images from diverse categories, including Chemical Plant, Golden Gate, Couple, Boat, Baboon, Pentagon, and Male from the SIPI database[43], Brain Tumour[44], Chest CT Scan[45], and Berry from the RSSCN7 dataset[46]. These images collectively represent a wide range of content, including natural, medical, aerial, and remote sensing images.

Visual evaluation

Visual evaluation illustrates the input, encrypted, and reconstructed images. An effective encryption scheme should produce an encrypted image with no recognizable information and a decrypted image closely resembling the original. Figure 15 shows the histogram analysis: the input image exhibits distinct peaks representing data distribution, the encrypted image histogram is flat and uniform, resembling noise, and the decrypted image histogram closely matches the original. These results confirm the proposed scheme's effectiveness in obscuring visual information while preserving recoverability.

Entropy-based analysis

Entropy-based analysis evaluates image randomness via Global Information Entropy (GIE) and Local Information Entropy (LIE). GIE measures overall image entropy, while LIE computes the average GIE of randomly selected non-overlapping blocks. GIE is calculated as Eq. (45)

$$\text{GIE} = -\sum_{i=0}^{L-1} p(x_i)\log(p(x_i)) \tag{45}$$

where L is the maximum intensity level and $p(x_i)$ the probability of intensity x_i. LIE is given by Eq. (46)

$$\text{LIE} = \frac{1}{k}\sum_{i=1}^{k} \text{GIE}(B_i, T_B) \tag{46}$$

with k randomly selected blocks B_i, each containing T_B pixels. For our analysis, $k = 30$ and $T_B = 1936$. At a 5% significance level, an image passes if LIE lies within $(7.9019,\ 7.9030)$. As summarized in Table 4, the input image exhibits lower GIE than the encrypted image, and its LIE falls outside the interval, whereas encrypted images meet the LIE criterion. This confirms that the proposed encryption ensures strong global and local randomness.

Pixel level statistical analysis

This section evaluates the proposed encryption scheme visually and statistically using histogram variance analysis and the Chi-square test. Histogram analysis shows pixel distribution, the original image exhibits peaks revealing information, while the encrypted image is uniform, preventing data leakage. The Chi-square statistic is computed as Eq. (47)

$$\chi^2 = \sum_{i=0}^{255} \frac{(o(i) - e(i))^2}{e(i)} \tag{47}$$

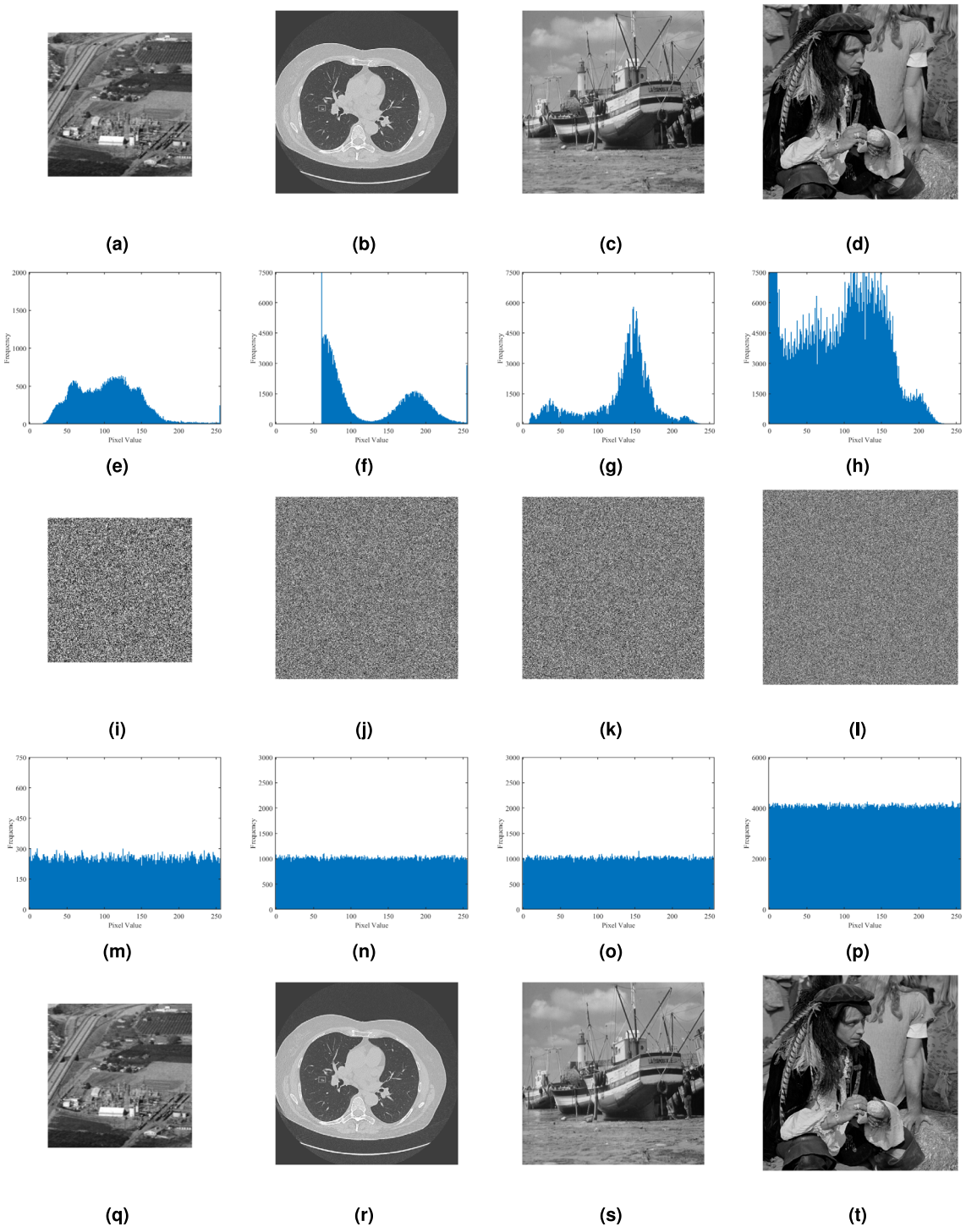


Fig. 15. Histogram analysis of images chemical plant, chest CT scan, boat and male: Row 1→ Original Images; Row 2 → Original Image Histograms; Row3 → encrypted images; Row 4 → Encrypted image histograms; Row 5 →Decrypted Images.

Image name	Size	GIE		LIE	
		O	E	O	E
Chemical plant	256×256	7.3424	7.9972±0.0002	6.7985	7.9029±0.0018
Brain tumour	256×256	6.0437	7.9972±0.0003	5.8458	7.9029±0.0022
Berry	256×256	7.5220	7.9972±0.0001	6.0668	7.9024±0.0021
Golden gate	512×512	5.8848	7.9993±0.0001	4.6133	7.9020±0.0006
Couple	512×512	7.2010	7.9992±0.0001	6.0094	7.9022±0.0005
Boat	512×512	7.1913	7.9992±0.0001	6.1026	7.9027±0.0011
Baboon	512×512	7.3583	7.9994±0.0001	6.6610	7.9025±0.0006
Chest CT scan	512×512	6.1347	7.9993±0.0001	5.4756	7.9030±0.0009
Pentagon	1024×1024	6.7326	7.9998±0.0001	6.0869	7.9023±0.0006
Male	1024×1024	7.5237	7.9998±0.0001	5.9708	7.9027±0.0002

Table 4. Entropy analysis of different images with$\text{average} \pm \text{standard deviation}$ for 10 independent runs. O, Original image; E, Encrypted image

Image name	Histogram variance		Chi_square test			
	O	E	O	Result	E	Result
Chemical plant	50326.45	251.55	50326.45	Failed	251.55	Passed
Brain tumour	1513599.55	280.12	1513600	Failed	280.12	Passed
Berry	36014.30	250.09	36014.3	Failed	250.09	Passed
Golden gate	6025667.85	989.19	1506417	Failed	247.29	Passed
Couple	1195460.98	1115.03	298865.2	Failed	278.75	Passed
Boat	1535878.75	1189.60	383969.7	Failed	289.40	Passed
Baboon	749426.29	897.21	187356.6	Failed	224.30	Passed
Chest CT scan	14627115.66	941.83	3656779	Failed	235.45	Passed
Pentagon	31893181.01	4608.02	1993324	Failed	288.00	Passed
Male	11349450.88	3929.33	709340.7	Failed	245.58	Passed

Table 5. Histogram and distribution analysis.

Here $o(i)$ is observed and $e(i)$is expected frequency of pixel intensity i. The variance of histogram is calculated by Eq. (48)

$$\text{Var}(F) = \frac{1}{(256)^2}\sum_{i=1}^{256}\sum_{j=1}^{256}(f_i - f_j)^2 \tag{48}$$

Here f_i and f_j are the histogram frequencies at gray levels *i* and *j*. Table 5 reports variance and Chi-square results for original and encrypted images. The encrypted images show significantly lower variance and χ^2 values, satisfying $\chi^2 < 293.2478$, indicating a uniform pixel distribution. These results confirm strong randomness in the encrypted images, enhancing the security of the proposed scheme.

Statistical analysis

The proposed encryption algorithm is further evaluated using statistical metrics, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Visual Information Fidelity (VIF), which quantify distortion during encryption and reconstruction quality during decryption. These are defined as in Eq. (49)

$$\begin{aligned}
\text{PSNR} &= 10\log_{10}\frac{L^2}{\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(r_{i,j}-d_{i,j})^2},\\
\text{SSIM}(r,d) &= \frac{(2\mu_r\mu_d + C_1)(2\sigma_{rd} + C_2)}{(\mu_r^2 + \mu_d^2 + C_1)(\sigma_r^2 + \sigma_d^2 + C_2)},\\
\text{VIF} &= \frac{\sum\limits_{i\in\text{subbands}} I\left(\vec{C}_{N,i};\vec{d}_{N,i} \mid s_{N,i}\right)}{\sum\limits_{i\in\text{subbands}} I\left(\vec{C}_{N,i};\vec{r}_{N,i} \mid s_{N,i}\right)}.
\end{aligned} \tag{49}$$

Image name	PSNR		MSE		SSIM		VIF	
	O-E	O-D	O-E	O-D	O-E	O-D	O-E	O-D
Chemical plant	9.1841	∞	7846.38	0	0.00983	1	0.002	1
Brain tumour	7.0654	∞	12780.31	0	0.00821	1	0.0018	1
Berry	8.4997	∞	9185.68	0	0.01004	1	0.0015	1
Golden gate	10.3685	∞	5973.54	0	0.01036	1	0.00079	1
Couple	9.6271	∞	7085.56	0	0.01113	1	0.0013	1
Boat	9.2898	∞	7657.79	0	0.01112	1	0.0013	1
Baboon	9.5308	∞	7244.32	0	0.01017	1	0.0028	1
Chest CT scan	8.5379	∞	9105.26	0	0.00837	1	0.0022	1
Pentagon	10.1379	∞	6299.30	0	0.01039	1	0.0013	1
Male	7.9976	∞	10311.43	0	0.00812	1	0.0011	1

Table 6. Image quality analysis. O-E Original image-encrypted image; O-D, Original image-decrypted image

Table 6 presents the results. PSNR, SSIM, and VIF values are very low between the original and encrypted images, confirming strong security, and very high between the original and decrypted images (PSNR $\to \infty$, SSIM and VIF ≈ 1), indicating near perfect reconstruction. This demonstrates that the proposed scheme ensures both confidentiality and faithful image recovery.

Correlation between adjacent pixels analysis

Original images exhibit high correlation between adjacent pixels in horizontal, vertical, and diagonal directions, making them vulnerable to statistical attacks. Reducing this correlation is essential for security. The correlation coefficient (CC) between adjacent pixels u_i and v_i is computed using Eq. (50)

$$CC(u,v) = \frac{\sum_{i=1}^{l}(u_i - \bar{u})(v_i - \bar{v})}{\sqrt{\sum_{i=1}^{l}(u_i - \bar{u})^2 (v_i - \bar{v})^2}} \tag{50}$$

where $\bar{u}$ and $\bar{v}$ are the mean values. Figure 16 shows that original image pixels cluster closely, indicating strong correlation, whereas encrypted image pixels are widely scattered in all three directions. Table 7 confirms that correlation coefficients for encrypted images are near zero, demonstrating minimal adjacent-pixel dependency and enhanced security.

Differential attack analysis

Differential Attack analysis is well known attack test to measure the vulnerability of crypto system. In this analysis two images with slightly differentiate in the features are subjected to undergo encryption process to get two cipher images known as E_1 and E_2. The ability to withstand differential attack of the proposed crypto algorithm is measured by calculating how many number of pixels are differed between two cipher images E_1 and E_2. This difference of pixels are quantified by two statistical metrics known as Number of Pixel Change Rate(NPCR) and Unified Average Changing Intensity(UACI) are calculated using Eqs. (51) and (52) respectively

$$\mathrm{NPCR}(E_1, E_2) = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \xi_{i,j} \times 100\% \tag{51}$$

$$\mathrm{UACI}(E_1, E_2) = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\% \tag{52}$$

$$\xi_{i,j} = \begin{cases} 1, & \text{if } E_1(i,j) \neq E_2(i,j) \\ 0, & \text{if } E_1(i,j) = E_2(i,j) \end{cases}$$

Table 8 presents the statistical results of differential attack analysis by measuring NPCR and UACI. From the table, it is evident that the average values of NPCR exceed 99.6% and UACI exceed 33.4%, which indicates that the proposed algorithm exhibits strong randomness and a high resistance to differential attacks.

Additionally, we compared the statistical values of the Baboon image derived using the proposed encryption algorithm with those from previous algorithms. The results, summarized in Table 9, demonstrate that the proposed algorithm achieves superior performance.

Robustness analysis

To evaluate robustness against transmission errors and attacks[41], noise and data loss were simulated on encrypted images. Noise of varying types and densities was added, and portions of encrypted images were

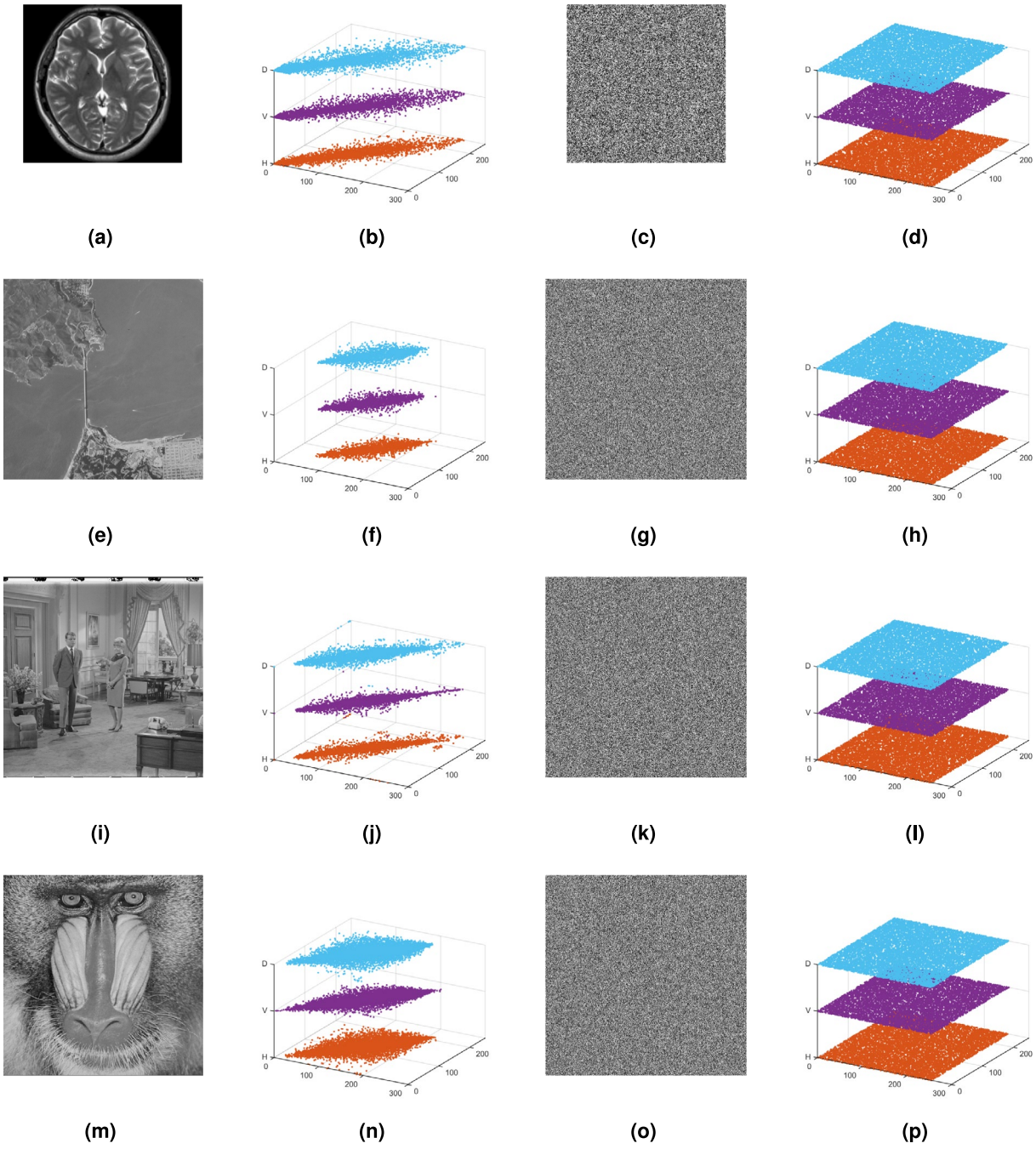


Fig. 16. Correlation analysis: original image → Correlation → Encrypted image → Correlation; (**a**–**d**) Brain Tumour, (**e**–**h**) Golden gate, (**i**–**l**) Couple, (**m**–**p**) Baboon.

cropped, followed by decryption. Figure 17 shows that decrypted images remain recognizable despite noise, with PSNR values in Table 10 decreasing as noise density increases, reflecting reduced resemblance. Similarly, Fig. 18 illustrates that even with cropped portions, decrypted images preserve recognizable content, with PSNR values reported in Table 11. These outcomes confirm the proposed encryption approach resilience against noise and partial data loss.

Key sensitivity and space analysis

Key sensitivity was evaluated using the Berry test image, where encryption and decryption were performed with both the original key and slightly modified keys. As shown in Fig. 19, successful decryption occurs only with the exact key, while even minimal key variations produce unrecognizable outputs, confirming strong key sensitivity. Quantitatively, robustness is measured using the Number of Bit Change Rate (NBCR), defined as Eq. (53)

Direction	Horizontal		Vertical		Diagonal	
Image name	O	E	O	E	O	E
Chemical plant	0.893392	−0.02918	0.941474	-0.02022	0.844118	−0.02783
Brain tumour	0.97356	−0.0085	0.965833	0.010724	0.946471	0.002175
Berry	0.973273	−0.00144	0.969109	0.008763	0.945351	0.009802
Golden gate	0.868076	0.00012	0.879707	0.016889	0.796526	−0.00295
Couple	0.867837	−0.0108	0.910936	-0.03158	0.840118	−0.01942
Boat	0.969824	−0.04259	0.92851	-0.03253	0.913883	−0.02788
Baboon	0.75742	−0.00931	0.865849	0.001046	0.725459	0.009721
Chest CT scan	0.901953	0.0064	0.913544	0.004491	0.882115	−0.00597
Pentagon	0.865628	−0.00073	0.873862	0.007706	0.788741	0.020433
Male	0.979974	−0.00968	0.973724	-0.03051	0.964991	−0.01646

Table 7. Correlation coefficient analysis.

	Diffrential attack analysis			
Image name	NPCR (%)	Result	UACI (%)	Result
Chemical plant	99.6163 ± 0.0262	Passed	33.4553 ± 0.0606	Passed
Brain tumour	99.6218 ± 0.0159	Passed	33.4928 ± 0.0294	Passed
Berry	99.6063 ± 0.0183	Passed	33.5243 ± 0.0794	Passed
Golden gate	99.6089 ± 0.0117	Passed	33.4744 ± 0.0649	Passed
Couple	99.6048 ± 0.0161	Passed	33.4726 ± 0.0664	Passed
Boat	99.6189 ± 0.0073	Passed	33.4664 ± 0.0468	Passed
Baboon	99.6032 ± 0.0165	Passed	33.4469 ± 0.0450	Passed
Chest CT scan	99.6006 ± 0.0128	Passed	33.4480 ± 0.0512	Passed
Pentagon	99.6089 ± 0.0027	Passed	33.4430 ± 0.0159	Passed
Male	99.6086 ± 0.0067	Passed	33.4671 ± 0.0281	Passed

Table 8. Differential attack analysis wth average $\pm$ standard deviation for 10 independent runs.

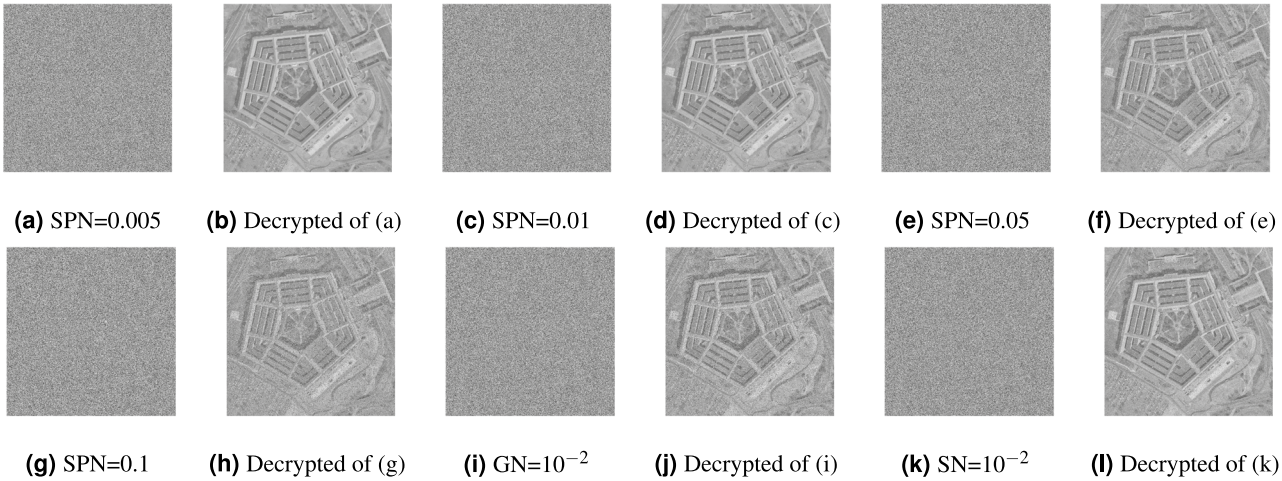
Algorithm	GIE	Correlation coefficient			NPCR (%)	UACI (%)
		H	V	D		
[47]	7.9994	−0.0009	0.0005	0.0004	99.6092	33.4636
[36]	7.9994	−0.0018	−0.0021	−0.0002	99.7884	33.4768
[48]	7.9987	−0.0075	−0.0071	0.0041	99.5800	33.1800
[49]	7.9993	−0.0491	−0.0313	−0.0059	99.6200	33.4700
[50]	7.9965	0.0002	0.002	0.0006	99.6122	33.4615
[51]	7.9966	0.0009	0.0006	−0.0036	99.6012	33.4637
Proposed	**7.9994**	−0.00931	0.00105	0.00972	99.6093	**33.4700**

Table 9. Comparison analysis. H, Horizonta; V, Vertica; D, Diagonal Significant values are in bold

$$NBCR(b_1, b_2) = \frac{Ham(b_1, b_2)}{length} \tag{53}$$

where *Ham(.)* denotes the Hamming distance between two matrices b_1 and b_2, and $length$ represents the total number of bits. Figure 20 illustrates the total number of bit changes between two encrypted images E_1 and E_2, as well as two decrypted images D_1 and D_2, obtained using keys key_1 and key_2, respectively. For each round, the NBCR is approximately 50%, indicating that the proposed encryption algorithm is robust against small key variations, which in turn ensures high randomness in the resulting images.

In addition, the key space analysis and its comparison are summarized in Table 12. Considering the seven parameters random initial seeds(r_{ini}, s_{ini}), α, β, η, and the initial values(x_0, y_0) of the chaotic map represented in double-precision floating-point format with approximately 10^{-15} resolution, the total key space is approximately 2^{348}. This value is significantly greater than 2^{100}, making it suitable for cryptographic applications.



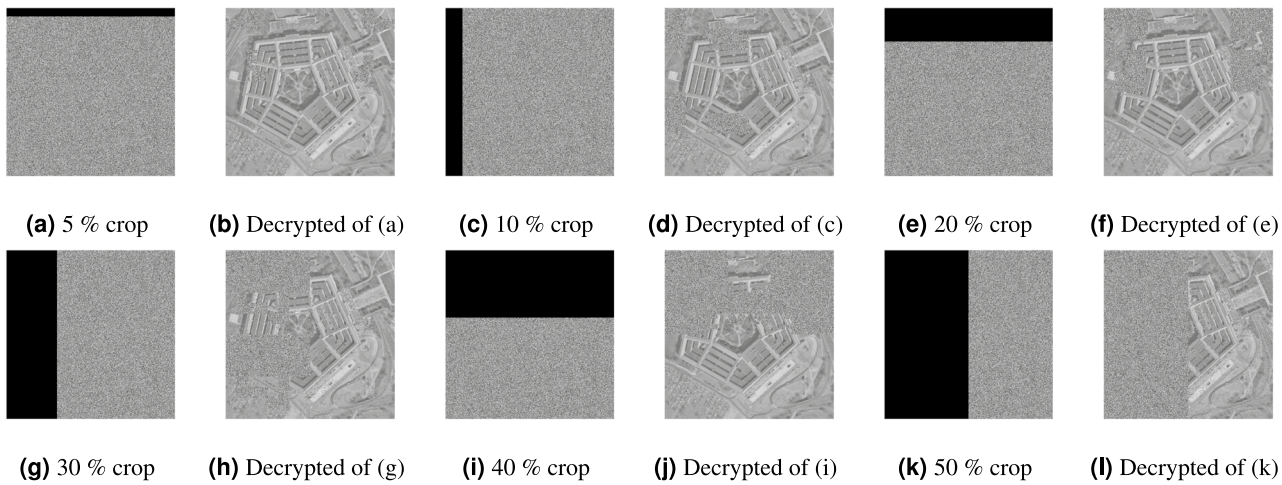
(a) SPN=0.005 **(b)** Decrypted of (a) **(c)** SPN=0.01 **(d)** Decrypted of (c) **(e)** SPN=0.05 **(f)** Decrypted of (e)

(g) SPN=0.1 **(h)** Decrypted of (g) **(i)** GN=10^{-2} **(j)** Decrypted of (i) **(k)** SN=10^{-2} **(l)** Decrypted of (k)

Fig. 17. Noise attack analysis for pentagon image. SPN: Salt and Pepper Noise, GN: Gaussian Noise, SN: Speckle Noise.

Noise type	Density	PSNR	SSIM
SPN	0.005	28.4578	0.8685
	0.01	25.4268	0.7588
	0.05	18.5374	0.3408
	0.1	15.7777	0.1870
SN	0.005	23.3019	0.4855
	0.01	20.3011	0.3482
	0.05	13.5922	0.0995
	0.1	11.6475	0.0454
GN	0.005	18.2998	0.2645
	0.01	15.2945	0.1544
	0.05	10.7930	0.0254
	0.1	10.2637	0.0135

Table 10. Noise attack analysis.



(a) 5 % crop **(b)** Decrypted of (a) **(c)** 10 % crop **(d)** Decrypted of (c) **(e)** 20 % crop **(f)** Decrypted of (e)

(g) 30 % crop **(h)** Decrypted of (g) **(i)** 40 % crop **(j)** Decrypted of (i) **(k)** 50 % crop **(l)** Decrypted of (k)

Fig. 18. Crop analysis for pentagon image with % of crop to encrypted image and its corresponding decrypted image.

Crop (%)	PSNR (dB)	SSIM
5	22.9027	0.9375
10	19.1402	0.7857
20	17.0069	0.7811
30	14.8564	0.5369
40	14.0571	0.5812
50	12.8711	0.3361

Table 11. Crop analysis.

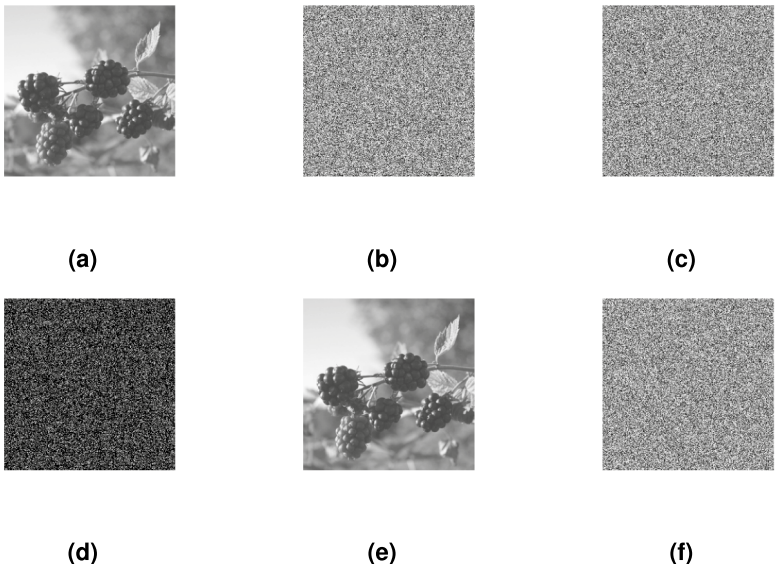


Fig. 19. Key sensitivity analysis. (**a**) Original image, (**b**) Encrypted image with key_1, (**c**) Encrypted image with key_2, (**d**) Difference between (**a**) and (**b**), (**e**) Decrypted image with key_1, (f) Decrypted image with key_2.

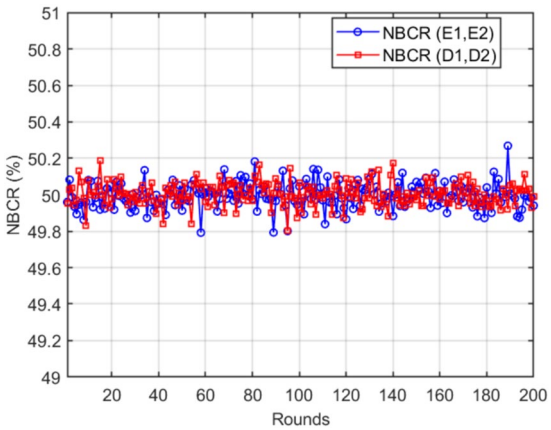


Fig. 20. NBCR analysis.

Algorithm	Proposed	47	36	49	52
Key space	2^{348}	2^{319}	2^{215}	2^{319}	2^{967}

Table 12. Key space analysis.

Algorithm	Encryption time (seconds)		Decryption time (seconds)		Complexity
	256×256	512×512	256×256	512×512	
[35]	1.66	6.51	1.64	6.47	*O*(64*MN*)
[7]	1.828	7.576	–	–	*O*(*NlogN*)
[37]	0.170	0.692	0.697	0.697	–
[47]	–	0.410	–	–	*O*(7*MN*)
[27]	–	0.202	–	–	$O(3M + \frac{17}{16}M \times M)$
[22]	0.459	1.769	0.837	0.837	*O*(*MN*)
[8]	–	1.513	–	1.790	–
Proposed	1.245	6.045	1.325	6.241	*O*(*MNlogM*)

Table 13. Time complexity analysis comparison of different size images.

Time complexity analysis

The proposed algorithm consists of four linear components block hashing, entropy-based key generation, chaotic sequence generation, and Fibonacci diffusion each with complexity $O(MN)$. In addition, recursive scrambling and Hilbert traversal introduce two quasi-linear terms, each $O(MN \log M)$, due to hierarchical recursion and fractal path computation. Thus, the overall complexity is $4O(MN) + 2O(MN \log M) \approx O(MN \log M)$, where the logarithmic factor dominates. This quasi-linear cost is only slightly higher than purely linear schemes, but it significantly improves security by enhancing permutation strength and diffusion robustness, making the trade-off both efficient and defensible. Further, Table 13 presents encryption and decryption times (seconds) for different image sizes, (256×256) and (512×512). It also presents time complexity and compares it with existing algorithms. Our proposed algorithm took 1.2455 s (encryption) and 1.3255 s (decryption) for (256×256) images and 6.045 s (encryption) and 6.241 s (decryption) for (512×512) images. This time complexity for encryption is slightly higher when compared to existing algorithms due to recursive scrambling but within acceptable bounds considering the stronger diffusion.

Conclusion

This study introduced a novel image encryption framework that integrates chaotic-based recursive scrambling with a Fractal–Fibonacci diffusion mechanism derived from the Hilbert curve. At its core lies a new two-dimensional chaotic system, the 2D-CPSCM, which exhibits positive LEs, confirming its hyperchaotic nature. The proposed system outperforms existing chaotic maps in statistical measures, including SE, PE and KE. Comprehensive experiments on multiple benchmark images demonstrate the robustness of the scheme, achieving strong performance in entropy, CC, NPCR, UACI, and NBCR metrics. In addition, its resistance to noise and cropping attacks further validates the resilience of the approach. Although the algorithm introduces higher computational complexity, this trade-off is justified by the enhanced security, improved randomness, and strong resistance to cryptographic attacks, making the proposed approach is suitable for secure multimedia communication. noise and cropping attack tests further validate the resilience of the scheme. Although the complexity of the algorithm increases, this trade-off is justified by the enhanced security and improved randomness in the encrypted images.

Data availability

The corresponding author can provide the data validating the study's conclusions upon reasonable request.

Received: 24 September 2025; Accepted: 19 December 2025
Published online: 09 January 2026

References

1. Guan, Z. et al. Deepmih: Deep invertible network for multiple image hiding. *IEEE Trans. Pattern Anal. Mach. Intell.* **45**, 372–390 (2022).
2. Li, Q., Ma, B., Wang, X., Wang, C. & Gao, S. Image steganography in color conversion. *IEEE Trans. Circuits Syst. II Express Briefs* **71**, 106–110 (2023).
3. Hazzazi, M. M. et al. Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and dwt diffusion: A robust data encryption approach. *Sci. Rep.* **14**, 12277 (2024).
4. Anand, A. & Singh, A. K. Hybrid nature-inspired optimization and encryption-based watermarking for e-healthcare. *IEEE Trans. Computat. Soc. Syst.* **10**, 2033–2040 (2022).
5. Feng, S., Zhao, M., Liu, Z. & Li, Y. A novel image encryption algorithm based on new one-dimensional chaos and DNA coding. *Multimed. Tools Appl.* **83**, 84275–84297 (2024).
6. Allawi, S. T. & Alshibani, D. R. Color image encryption using LFSR, DNA, and 3d chaotic maps. *Int. J. Electric. Comput. Eng. Syst.* **13**, 885–893 (2022).
7. Zhou, S., Wei, Y., Zhang, Y., Iu, H.H.-C. & Zhang, H. Image encryption algorithm based on the dynamic RNA computing and a new chaotic map. *Integration* **101**, 102336 (2025).
8. Belete, B. A., Gelmecha, D. J. & Singh, R. S. Secure image transmission in wireless sensor networks using DNA coding and memcapacitor-based hyperchaotic system for encryption and decryption. *Iran J. Comput. Sci.* https://doi.org/10.1007/s42044-025-00328-7 (2025).

9. Yang, Y., Cheng, M., Ding, Y. & Zhang, W. A visually meaningful image encryption scheme based on lossless compression Spiht coding. *IEEE Trans. Serv. Comput.* **16**, 2387–2401 (2023).
10. Lai, Q., Yang, L., Hu, G., Guan, Z.-H. & Iu, H.H.-C. Constructing multiscroll memristive neural network with local activity memristor and application in image encryption. *IEEE Trans. Cybernet.* **54**, 4039–4048 (2024).
11. Feng, W. et al. Exploiting newly designed fractional-order 3d Lorenz chaotic system and 2d discrete polynomial hyper-chaotic map for high-performance multi-image encryption. *Fract. Fract.* **7**, 887 (2023).
12. Wang, Y., Chen, L., Yu, K. & Fu, T. A secure Spatio-temporal chaotic pseudorandom generator for image encryption. *IEEE Trans. Circuits Syst. Video Technol.* **34**, 8509–8521 (2024).
13. Huang, L. & Gao, H. Multi-image encryption algorithm based on novel spatiotemporal chaotic system and fractal geometry. *IEEE Trans. Circuits Syst. I Regul. Pap.* **71**, 3726–3739 (2024).
14. Belete, B. A., Gelmecha, D. J. & Singh, R. S. Image encryption algorithm based on a memcapacitor-based hyperchaotic system and DNA coding. *Secur. Privacy* **7**, e432. https://doi.org/10.1002/spy2.432 (2024).
15. Wu, Y., Yang, G., Jin, H. & Noonan, J. P. Image encryption using the two-dimensional logistic chaotic map. *J. Electron. Imaging* **21**, 013014–013014 (2012).
16. Hua, Z., Zhou, Y., Pun, C.-M. & Chen, C. P. 2d sine logistic modulation map for image encryption. *Inf. Sci.* **297**, 80–94 (2015).
17. Hua, Z. & Zhou, Y. Image encryption using 2d logistic-adjusted-sine map. *Inf. Sci.* **339**, 237–253 (2016).
18. Liu, W., Sun, K. & Zhu, C. A fast image encryption algorithm based on chaotic map. *Opt. Lasers Eng.* **84**, 26–36 (2016).
19. Hua, Z., Jin, F., Xu, B. & Huang, H. 2d logistic-sine-coupling map for image encryption. *Signal Process.* **149**, 148–161 (2018).
20. Zhu, H., Zhao, Y. & Song, Y. 2d logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **7**, 14081–14098 (2019).
21. Teng, L., Wang, X., Yang, F. & Xian, Y. Color image encryption based on cross 2d hyperchaotic map using combined cycle shift scrambling and selecting diffusion. *Nonlinear Dyn.* **105**, 1859–1876 (2021).
22. Teng, L., Wang, X. & Xian, Y. Image encryption algorithm based on a 2d-CLSS hyperchaotic map using simultaneous permutation and diffusion. *Inf. Sci.* **605**, 71–85 (2022).
23. Tang, J. et al. Novel asymmetrical color image encryption using 2d sine-power coupling map. *Nonlinear Dyn.* **112**, 11547–11569 (2024).
24. Dhingra, D. & Dua, M. Medical video encryption using novel 2d cosine-sine map and dynamic DNA coding. *Med. Biol. Eng. Comput.* **62**, 237–255 (2024).
25. Tang, J., Zhang, Z. & Huang, T. Two-dimensional cosine-sine interleaved chaotic system for secure communication. *IEEE Trans. Circuits Syst. II Express Briefs* **71**, 2479–2483 (2023).
26. Patel, S., Thanikaiselvan, V. & Rearajan, A. Secured quantum image communication using new two dimensional chaotic map based encryption methods. *Int. J. Theor. Phys.* **63**, 49 (2024).
27. Huang, X., Tang, J. & Zhang, Z. Efficient and secure image encryption algorithm using 2d LIM map and latin square matrix. *Nonlinear Dyn.* **112**, 22463–22483 (2024).
28. Li, L. A self-reversible image encryption algorithm utilizing a novel chaotic map. *Nonlinear Dyn.* **113**, 7351–7383 (2025).
29. Zheng, J. & Liu, L. Novel image encryption by combining dynamic DNA sequence encryption and the improved 2d logistic sine map. *IET Image Proc.* **14**, 2310–2320 (2020).
30. Demla, K. & Anand, A. Miewc: Medical image encryption using wavelet transform and multiple chaotic maps. *Secur. Privacy* **7**, e369 (2024).
31. Dua, S., Kumar, A., Dua, M. & Dhingra, D. Icfcm-mie: Improved cosine fractional chaotic map based medical image encryption. *Multimed. Tools Appl.* **83**, 52035–52060 (2024).
32. Gao, Y., Liu, J. & Chen, S. Image encryption algorithms based on two-dimensional discrete hyperchaotic systems and parallel compressive sensing. *Multimed. Tools Appl.* **83**, 57139–57161 (2024).
33. Yang, Y.-G. et al. A new visually meaningful double-image encryption algorithm combining 2d compressive sensing with fractional-order chaotic system. *Multimed. Tools Appl.* **83**, 3621–3655 (2024).
34. Gao, S. et al. A parallel color image encryption algorithm based on a 2d logistic-Rulkov neuron map. *IEEE Internet of Things Journal* (2025).
35. Xu, X.-L., Song, X.-G., Liu, S.-H., Zhou, N.-R. & Wang, M.-M. New 2d hyperchaotic cubic-tent map and improved 3d Hilbert diffusion for image encryption. *Appl. Intell.* **55**, 590 (2025).
36. Zheng, Y., Huang, Q., Cai, S., Xiong, X. & Huang, L. Image encryption based on novel hill cipher variant and 2d-IGSCM hyper-chaotic map. *Nonlinear Dyn.* **113**, 2811–2829 (2025).
37. Wang, M.-M., Song, X.-G., Liu, S.-H., Zhao, X.-Q. & Zhou, N.-R. A novel 2d log-logistic-sine chaotic map for image encryption. *Nonlinear Dyn.* **113**, 2867–2896 (2025).
38. Li, Z., Zhang, S., Tan, W. & Wu, X. Enhanced secure color image encryption using a novel hyperchaotic 2d-etcs model and cross-permutation. *Nonlinear Dyn.* **113**, 18833–18855 (2025).
39. Li, Q. et al. Dppad-ie: Dynamic polyhedra permutating and arnold diffusing medical image encryption using 2d cross gaussian hyperchaotic map. *IEEE Transactions on Consumer Electronics* (2025).
40. Talhaoui, M. Z., Wang, X. & Talhaoui, A. A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. *Vis. Comput.* **37**, 1757–1768 (2021).
41. Kumar, M. & Ch, D. Enhancing image security through a fusion of chaotic map and multi-level scrambling techniques. *SIViP* **19**, 235 (2025).
42. Bao, H. et al. Grid homogeneous coexisting hyperchaos and hardware encryption for 2-d HNN-like map. *IEEE Trans. Circuits Syst. I Regul. Pap.* **71**, 4145–4155. https://doi.org/10.1109/TCSI.2024.3423805 (2024).
43. University of Southern California, Signal and Image Processing Institute. Usc-sipi image database. http://sipi.usc.edu/database/ (1977). Accessed: 25 August 2025.
44. Dubail, T. Brain tumors 256×256. Dataset on Kaggle (2023). Accessed: 25 August 2025.
45. Hany, M. Chest ct-scan images dataset. Dataset on Kaggle (2023). Accessed: 25 August 2025.
46. Zou, T., Ni, J., Gao, Y. & Chen, Z. Rsscn7: A remote sensing image dataset for scene classification. http://www.lmars.whu.edu.cn/xia/AID/AID.html (2015). Accessed: 25 August 2025.
47. Bayari, P. V. B., Sangwan, Y., Bhatnagar, G. & Chattopadhyay, C. A novel chaotic map and its application to secure transmission of multimodal images. *IEEE Transactions on Computational Social Systems* (2025).
48. Kumar, S. & Sharma, D. A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artif. Intell. Rev.* **57**, 87 (2024).
49. Bao, H. et al. *Grid homogeneous coexisting hyperchaos and hardware encryption for 2-d hnn-like map* (Regular Papers, IEEE Transactions on Circuits and Systems I, 2024).
50. Liu, X., Sun, K. & Wang, H. A novel image encryption scheme based on 2d silm and improved permutation-confusion-diffusion operations. *Multimed. Tools Appl.* **82**, 23179–23205 (2023).
51. Zhang, H., Hu, H. & Ding, W. Image encryption algorithm based on Hilbert sorting vector and new spatiotemporal chaotic system. *Opt. Laser Technol.* **167**, 109655 (2023).
52. Lone, M. A. & Qureshi, S. Encryption scheme for RGB images using chaos and affine hill cipher technique. *Nonlinear Dyn.* **111**, 5919–5939 (2023).

Author contributions

Maram Kumar: Conceptualization, Simulated the experiments, Performed the analysis, Wrote the original draft; Deepak Ch: Conceptualization, Methodology, Supervision, validation, review and editing.

Funding

Open access funding provided by Vellore Institute of Technology- AP University. Not applicable.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to D.C.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.