International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 48 No. 1 Mar. 2026, pp. 178-193
© 2026 Innovative Space of Scientific Research Journals
http://www.ijias.issr-journals.org/

A New One-Dimensional Polynomial-Sinusoidal Chaotic Map for Image Cryptography

***Ahmat Mahamat Saleh*[1], *Kalsouabé Zoukalne*[2], *Mahamat Charfadine Nimane*[3], *and Amir Moungache*[4]**

[1]Multimedia and Telecommunications department, Institute of Sciences and Techniques of Abeche, Abeche, Chad

[2]Decentralized Digital Campus Unit, Digital University of Chad, N'djamena, Chad

[3]Telecommunications department, Ecole Nationale Supérieure des Technologies de l'Information et de la Communication (ENASTIC), N'Djamena, Chad

[4]Department of Technology, University of N'Djamena, N'Djamena, Chad

ABSTRACT: In this article, we propose a new one-dimensional discrete chaotic map, obtained by combining a polynomial logistic map and a sinusoidal map. Dynamic analysis of the proposed map shows that it has better chaotic properties, good ergodicity over a wide range of parameters, and a relatively large key space. Compared to classical logistic and sinusoidal maps, the proposed map exhibits improved ergodicity, with state variables uniformly distributed in the interval [0,1], confirming the dynamic superiority of the proposed map and its suitability for cryptographic and pseudo-random generation applications. Based on these properties, we propose a new image encryption algorithm using sequences from the new chaotic map. The scheme is based on a permutation phase and two a diffusion phase driven by the chaotic sequences generated by the new discrete map. The performance of the proposed system is evaluated through sensitivity tests to initial conditions and keys, key space analysis, and differential attacks. In addition, security indicators such as information entropy, NPCR, UACI, correlation coefficients, and execution time are calculated to validate the effectiveness and robustness of the encryption algorithm.

KEYWORDS: one-dimensional chaotic map, polynomial–sinusoidal, chaotic system, chaos theory, chaotic map.

1 INTRODUCTION

Since its emergence, chaos theory has established itself as a promising area of re-search in many scientific fields [1–3]. In cryptography, chaotic systems are of particular interest due to their intrinsic properties, such as ergodicity, unpredictability, and high sensitivity to initial conditions and control parameters, which can be used to enhance the security and confidentiality of information protection algorithms [4–6]. Discrete chaotic systems are widely used for multimedia data encryption because they are easily implementable in digital environments [7]. Numerous studies have sought to improve the performance of security algorithms, reduce execution time, and increase resistance to cryptanalysis [8], relying mainly on chaotic maps or fractional order maps to improve confusion and

diffusion mechanisms [9]. In recent decades, the use of chaos in image encryption has become widespread [10–13]. Several effective schemes have been pro-posed, including algorithms based on fractional chaotic systems [14], pixel confusion and diffusion [15], and one-dimensional polynomial chaotic maps of the PWQPCM type in-corporating segmentation, substitution, and combined diffusion [16]. In [17], the authors introduced an image encryption scheme based on a logistic map whose parameters de-pend on the values of the pixels in the plaintext image, allowing image-specific pseudo-random sequences to be generated while maintaining low computational complexity. Similarly, Wen et al. showed that the integration of hybrid chaotic maps significantly improves cryptographic qualities in terms of entropy, NPCR, and UACI [18].

However, despite the many advantages of nonlinear dynamical systems, discrete logistic recurrence maps have certain disadvantages, such as restricted chaotic regions, the presence of periodic windows, and low sensitivity to parameters and initial conditions, which can render them ineffective for cryptographic applications [19-20].In order to overcome these constraints, several new discrete chaotic maps with improved performance have been developed. For example, Yicong Zhou et al. [21] proposed a one-dimensional discrete chaotic system obtained by the parallel combination of two maps, offering good distribution uniformity and high sensitivity to initial conditions, without periodic windows on the interval [0,4]. Xie et al. [22] introduced an improved variant of the logistic map that resolves several classic limitations, although the chaotic range remains limited. Similarly, Zhongyun Hua et al. [23] proposed chaotic maps based on the cosine transform (Cosine-Transform-Based Chaotic Systems, CTBCS), characterized by complex dynamics and the absence of periodic windows. Zhang et al. [24] recently presented an encryption scheme based on new chaotic maps and a compression technique offering good performance and computational efficiency.

Motivated by research aimed at improving the dynamic qualities of logistic maps, we introduce in this article a new one-dimensional discrete chaotic map, called the polynomial–sinusoidal map. The polynomial-sinusoidal map combines a polynomial logistic map and a sinusoidal term, controlled by several independent parameters, allowing the chaotic range to be widened and unwanted periodic windows to be eliminated. It is then used to design a high-performance and secure image encryption system. Section 2 describes the classic chaotic map. Section 3 presents the mathematical definition of the polynomial-sinusoidal map and the analysis of its chaotic properties. Section 4 describes the proposed image encryption system. Finally, the last section concludes the article.

2 Preliminary

2.1 Polynomial Logistic Map

The polynomial logistic map is a nonlinear dynamic system developed from the fundamental characteristics of the classical logistic map [25]. Mathematically, it is defined by the following expression:

$$x\_(n+1) = r/4\; x\_n\; (1-\tfrac{1}{2}x_n-\beta x_n^2) \qquad (1)$$

where r ∈ [0, 13] and β ∈ [0.5, 1] are the control parameters, while x_n ∈ [0, 1] represents the value of the chaotic sequence at iteration n. Fig. 1a and 1b show the bifurcation diagram and the Lyapunov exponent of the polynomial logistic map, respectively. As shown in this figure, the map exhibits chaotic behaviour interspersed with periodic windows in the interval r ∈ [10.5, 12.5]. This chaotic zone remains relatively narrow and limited. Furthermore, the system depends on only two control parameters, which reduces the overall dynamic complexity of the model. These drawbacks are an obstacle to its use in cryptography, where a wide chaotic parameter range and high complexity are required to guarantee a satisfactory level of security.

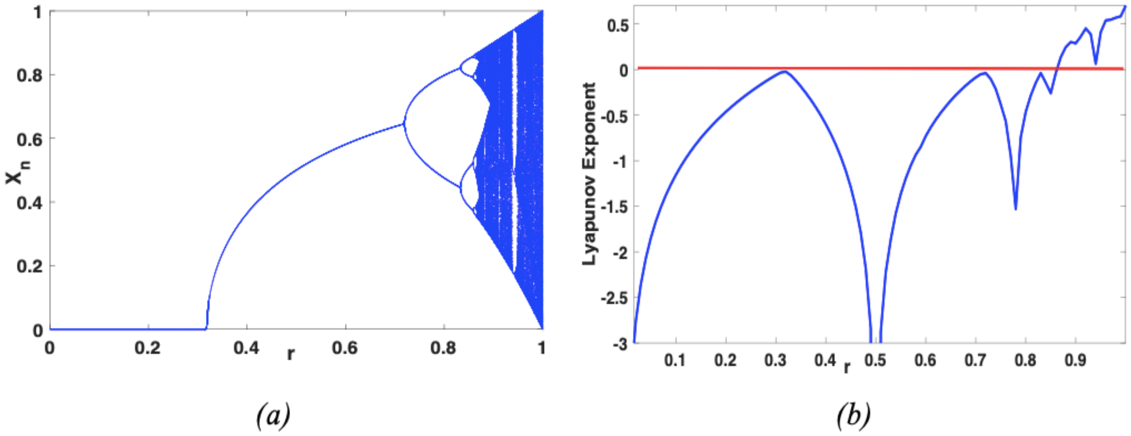


Fig. 1. Bifurcation diagram (a) and Lyapunov exponent (b) of polynomial logistic map

2.2 SINE MAP

The sine map is a non-linear, one-dimensional iterative map defined by the recurrence relation (2) [26]. It is presented as a representative example of the complexity of chaotic dynamical systems.

$$x_{n+1} = \lambda x_n \sin(\pi x_n) \tag{2}$$

In this equation, λ ∈ [0,1] is a control parameter, while xn ∈ [0,1] represents the state variable of iteration n. The different dynamic behaviors of the sine map are illustrated by the bifurcation diagram and the Lyapunov exponent plotted in Fig. 2a and b, respectively. As indicated, the sinusoidal map exhibits similar behaviors and comparable limits to those of the classical logistic map.

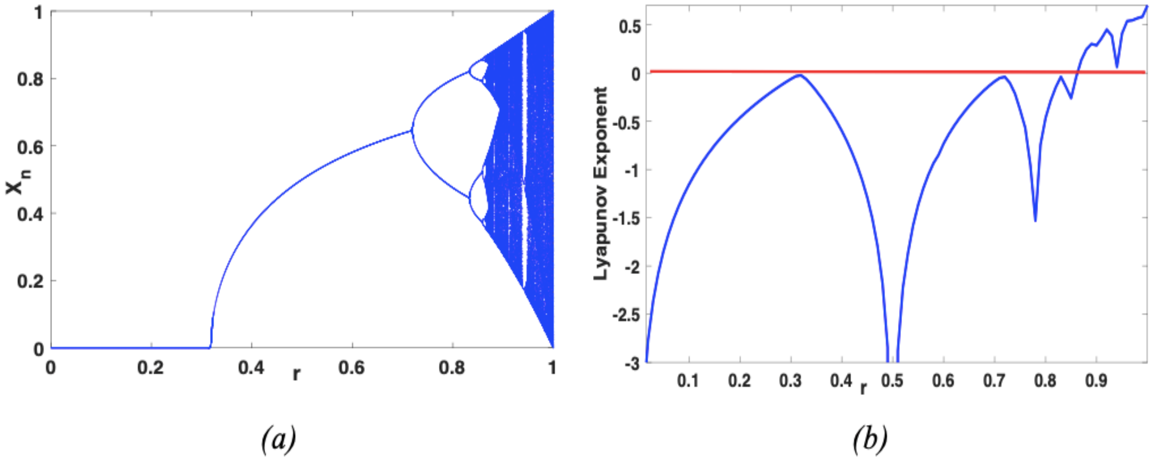


Fig. 2. Bifurcation diagram (a) and Lyapunov exponent (b) of sine map

3 NEW CHAOTIC 1D MAP

In this section, a new one-dimensional (1D) chaotic map, referred to as the polynomial–sinusoidal map, is proposed. This map is obtained by combining the polynomial logistic map and the sinusoidal map presented in the previous section. The proposed map involves a larger number of control parameters compared to the two reference maps, which enhances its dynamic complexity. The resulting nonlinear dynamical system is defined by the equation given in relation (3).

$$x\_(n+1) = (r/4\,x\_n\,(1-\tfrac{1}{2}x_n-\beta x_n^2)+\lambda x_n\sin(\pi x_n))\ \mathrm{mod1} \tag{3}$$

where r∈ [0, +∞ [, β∈ [0.5,1] and λ∈ [0, +∞ [are the control parameters, x_n denotes the initial condition, and mod 1 represents the modulo operator that ensures the output of the proposed map remains within the interval [0,1]. The proposed map exhibits chaotic behaviour over a wide range of the parameters λ and β. To further characterize and analyze these nonlinear dynamics, the map is investigated using the principal techniques commonly employed for chaos characterization in dynamical systems.

3.1 COBWEB DIAGRAM ANALYSIS

Cobweb diagrams are graphical methods for analysing the iterative behaviour of one-dimensional discrete dynamical systems [27]. They allow the visualization of the iterative trajectories of a nonlinear mapping starting from a given initial condition.

Fig. 3a and 3b show the cobweb diagrams of the proposed map and the polynomial logistic map, respectively. It can be observed that the proposed discrete map generates a set of non-repeating and highly irregular iterative trajectories, which demonstrates its chaotic nature. Moreover, the trajectories of the proposed map fill the entire rectangular output space, unlike those of the polynomial logistic map. This result indicates that the proposed map exhibits stronger chaotic behaviour than the conventional polynomial logistic map.

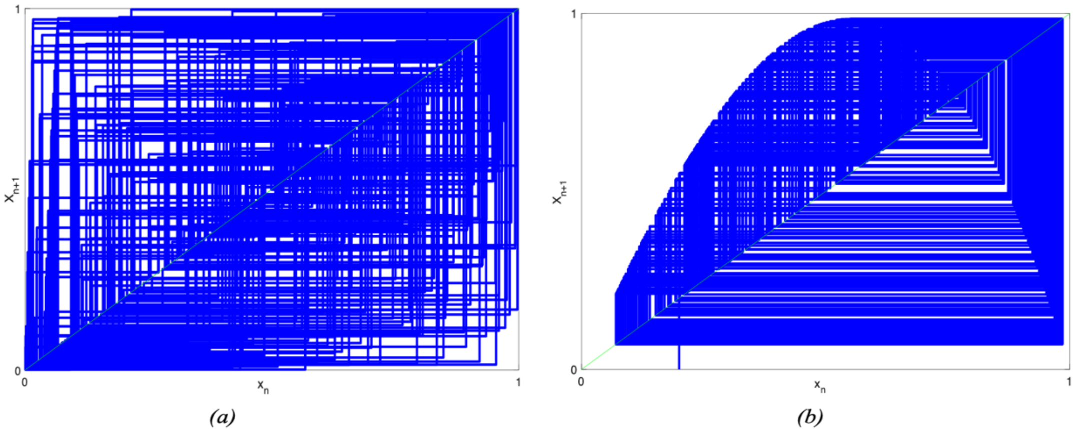
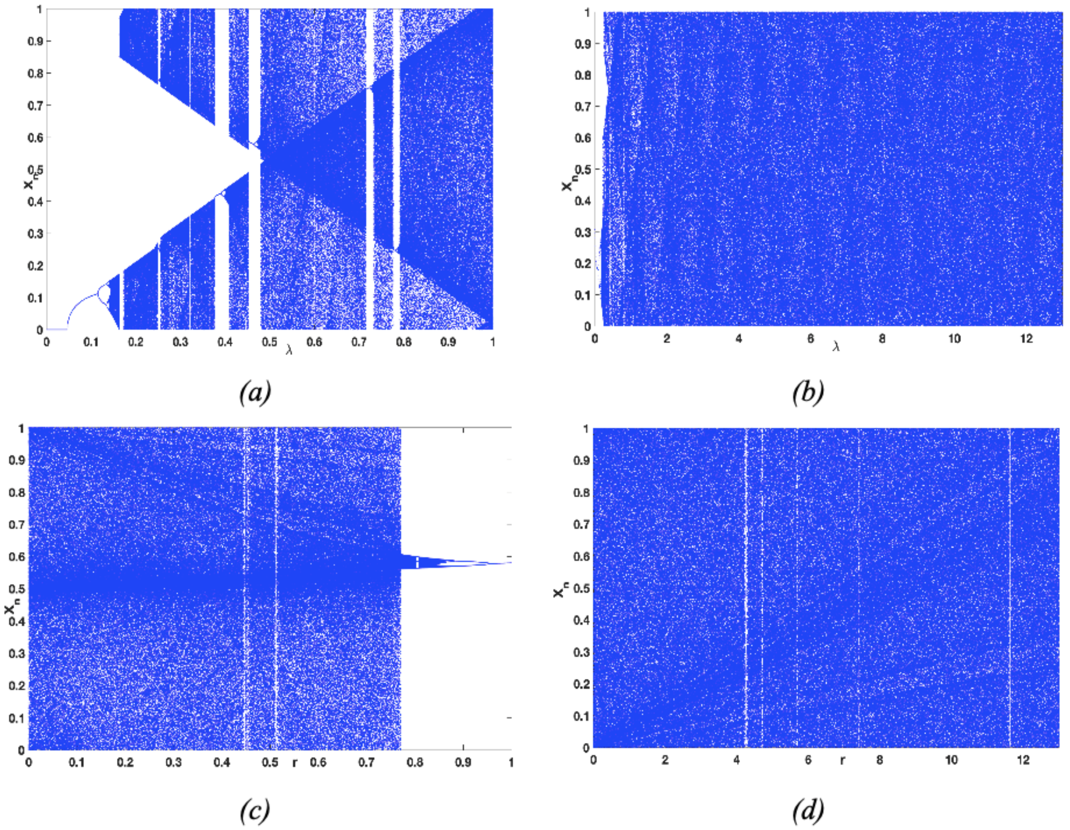


Fig. 3. Cobweb diagrams of the proposed map (a) and the polynomial logistic map (b)

3.2 Bifurcation Analysis

Figure 4 shows the bifurcation diagram of the new map as a function of the control parameters r and λ. For r=0.5 (Fig. 4 (a)), the proposed system exhibits periodic behaviour for low values of λ. As λ increases, a sequence of successive bifurcations appears, indicating a transition toward more complex dynamical regimes, characterized by the emergence of chaos interspersed with periodic windows. In contrast, for λ=0.5 (Fig.4 (c)), the system displays chaotic behaviour for low values of r, and then evolves toward a periodic regime, eventually converging to a steady state when r exceeds the interval [0.8,1]. When the control parameters increase significantly (Fig. 4 (b) and 4 (d)), the discrete map enters a chaotic regime over the entire parameter space considered. This regime is characterized by non-periodic trajectories and a dense occupation of the interval [0,1], with only a few isolated periodic windows. Furthermore, compared with the bifurcation diagrams of the polynomial logistic map (Fig. 1 (a)) and the sinusoidal map (Fig. 2 (a)), the bifurcation structure of the proposed map shows an enlarged chaotic region, a noticeable reduction in periodic windows, and a high degree of uniformity in the distribution of state variables. These results confirm a significant improvement in dynamic complexity, enhanced ergodicity, and robust pseudo-random behaviour, highlighting the suitability of the proposed system for pseudo-random sequence generation and encryption applications.



(a)

(b)

(c)

(d)

Fig. 4. Bifurcation diagrams of the proposed map as functions of the control parameters r and λ for the cases: (a) r=0.5, (b) r=5, (c) λ=0.5, and (d) λ=5

3.3 Analysis Of The Lyapunov Exponent

The Lyapunov exponent is a very important tool in chaos analysis. A positive value of the Lyapunov exponent indicates a large divergence of neighbouring trajectories and thus reflects a strong dependence on initial conditions [28]. The evolution of the Lyapunov exponent of the new map as a function of the control parameters λ and r is shown in Fig. 5. The results presented show that the new nonlinear map has strong chaotic dynamics over the entire range of control parameters, as indicated by the largely positive Lyapunov exponents. In contrast, for low parameter values, the Lyapunov exponent is negative or close to zero, which corresponds to the presence of periodic states, as noted in the bifurcation diagram. The presence of a few very small periodic windows provides information on the quality and dynamic complexity of the proposed chaotic map on the one hand, and on the high sensitivity to initial conditions and parameters on the other.

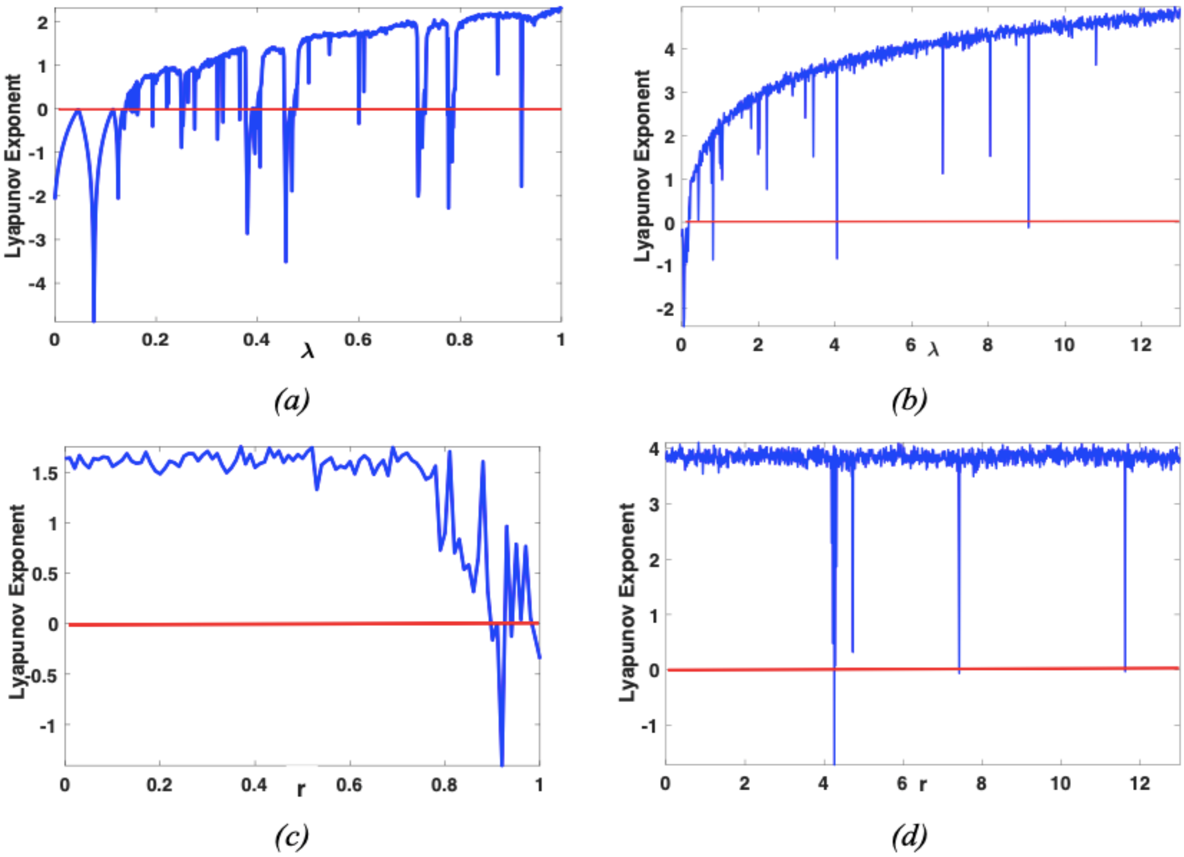
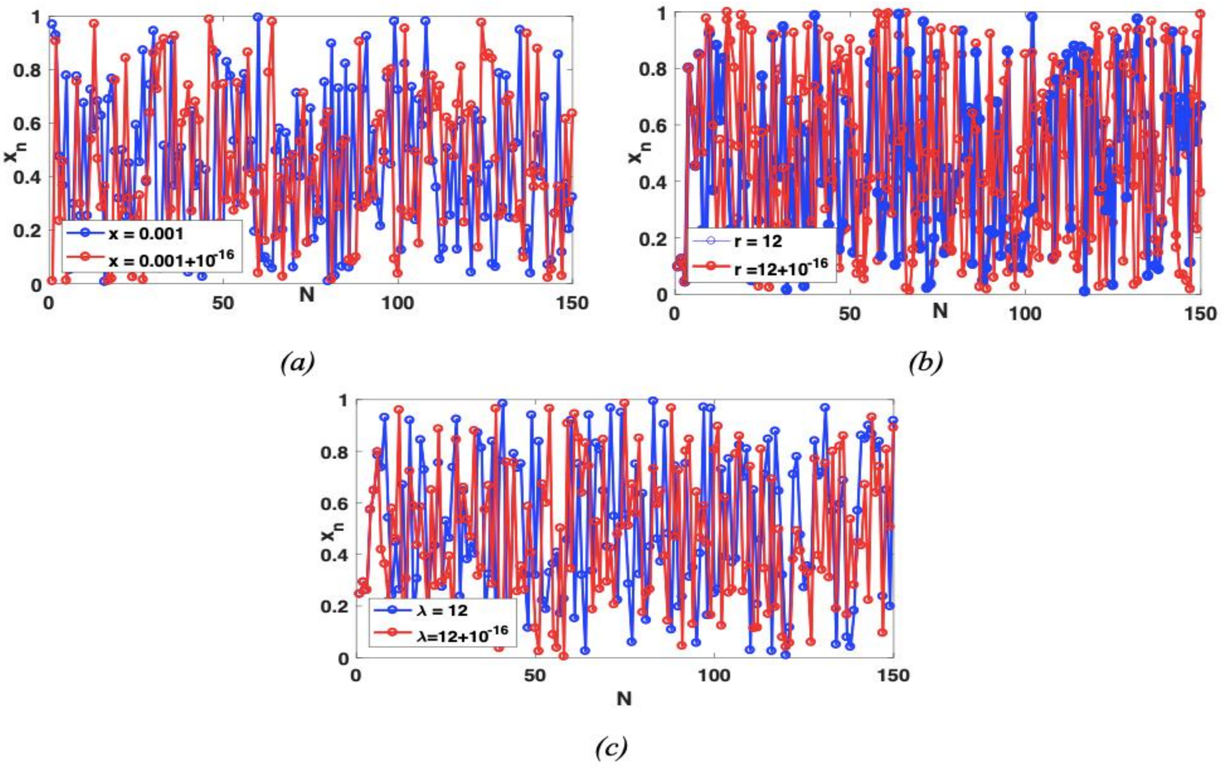


Fig. 5. Lyapunov exponent of the proposed map as a function of the control parameters r and λ in the cases: (a) r=0.5, (b) r=5, (c) λ=0.5, and (d) λ=5

3.4 Analysis Of Sensitivity To Initial Conditions And Parameters

Sensitivity to initial conditions and control parameters is one of the fundamental properties of chaotic behaviour [29]. To analyze this property, time series of the proposed map are plotted by introducing a small perturbation of 10^{-16} to the initial conditions and control parameters, as shown in Fig. 6. As can be observed, infinitesimal variations of the order of 10^{-16} lead to a rapid divergence of the generated sequences, which clearly confirms the strong sensitivity of the system to both initial conditions and parameters. In addition, the high sensitivity of the control parameter λ contributes to enlarging the overall key space. These characteristics endow the pro-posed system with high robustness and strong resistance to cryptanalysis, making it particularly suitable for secure encryption applications.



(a)

(b)

(c)

Fig. 6. (a) Sensitivity analysis with respect to initial conditions; (b) sensitivity of the proposed map to the parameter r; and (c) sensitivity of the proposed map to the parameter λ

3.5 Approximate Entropy Analysis

Approximate entropy measures the complexity and randomness of a time series. It is equal to zero for a periodic series and strictly positive for a chaotic series, increasing with the degree of unpredictability of the sequence [30]. Fig. 7 shows that the proposed map exhibits high and stable approximate entropy values over a wide range of control parameters, indicating strong complexity and enhanced randomness of the generated sequences. In contrast, the polynomial logistic map exhibits significant decreases in approximate entropy, revealing the presence of periodic regimes. These results confirm the superiority of the proposed map for cryptographic applications.

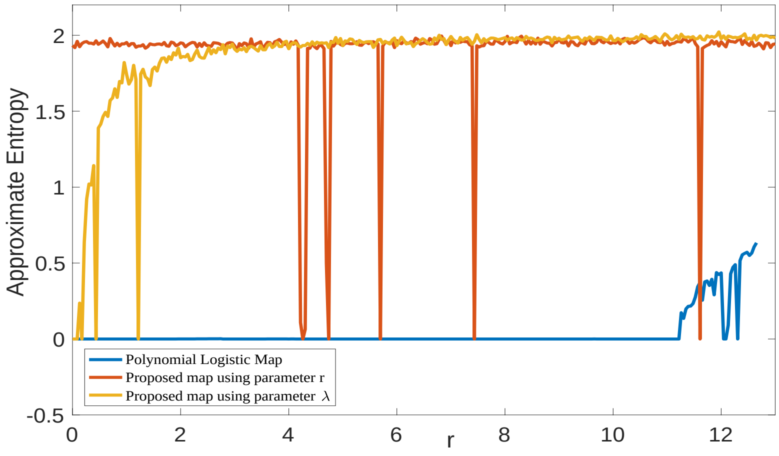


Fig. 7. Approximate Entropy Analysis

4 Application To Image Cryptography

4.1 Encryption Scheme

In this section, we propose a new image encryption algorithm based on the use of a new chaotic map, a permutation, and two diffusion processes. The synoptic diagram of the proposed image encryption algorithm is shown in Fig.8. In the permutation phase, the original image is decomposed to obtain column vectors. Next, the chaotic sequences S1 generated by the new map are used to determine the permutation indices of the pixels. Finally, to eliminate correlations between adjacent pixels, recurrent operations are performed to mix the positions of the pixels in the original image.

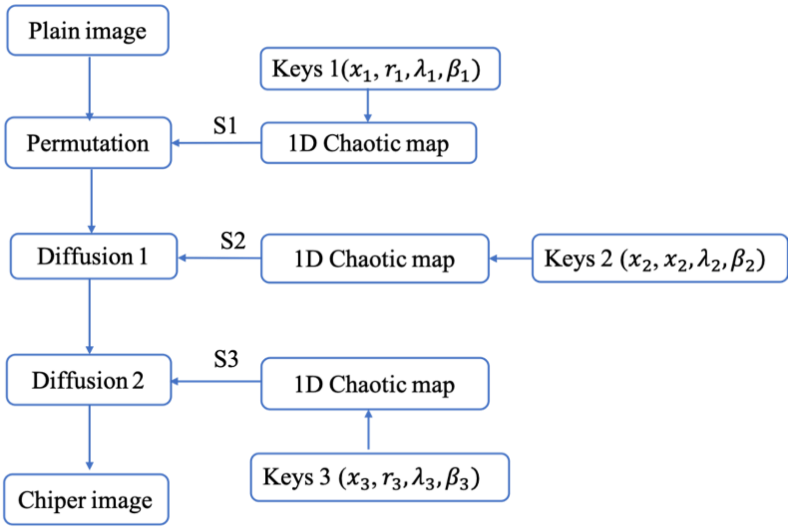

Plain image
Keys 1$(x_1, r_1, \lambda_1, \beta_1)$
S1
Permutation
1D Chaotic map
S2
Diffusion 1
1D Chaotic map
Keys 2 $(x_2, x_2, \lambda_2, \beta_2)$
S3
Diffusion 2
1D Chaotic map
Keys 3 $(x_3, r_3, \lambda_3, \beta_3)$
Chiper image

Fig. 8. Schéma synoptique de l'algorithme de cryptage d'image proposé

The diffusion is carried out in two phases. In the first phase, the chaotic sequences S2 generated with Keys 2 are used to encrypt the pixels. Pixel encryption is achieved by performing an XOR operation between the result of the permutation phase and the sequences S2. In the second phase, another diffusion is performed using the chaotic sequences S3. This consists of reinforcing the first diffusion by applying a new XOR operation between the pixels encrypted in the first diffusion and the elements of S3. Cascading the diffusion operations significantly reinforces the robustness of the algorithm in both directions. Details of the process are given in the pseudo-code below.

Algorithm Encryption algorithm

```
Input: Original image, I x1, $\beta_1$, $r_1$,$\lambda_1$, $x_2$,$\beta_2$ ,$r_2$,$\lambda_2$, $x_3$, $\beta_3$, $r_3$, $\lambda_3$
Output: Encrypted image C
for $i = 1 : M \times N$ do
        $S1(i) = mod(\frac{r_1}{4}\left(x_1(i-1)\left(1-\frac{1}{2}x_1(i-1)-\beta_1 x_1(i-1)^2\right) + \lambda_1 x_1(i-1)\sin\left(\pi x_1(i-1)\right), 1\right)$
end for
img1 ← reshape(I, 1, M × N)
for $i = M \times N$ down to 2 do
        J ← mod(floor(S1(i)·i), i) + 1
        temp ← img1(i)
        img1(i) ← img1(j)
```

```
            img1(j) ← temp
    end for
    for i = 1 : M × N do
            $S2(i) = mod(\frac{r_2}{4}\left(x_2(i-1)\left(1-\frac{1}{2}x_2(i-1)-\beta_2 x_2(i-1)^2\right) + \lambda_2 x_2(i-1)\sin\left(\pi x_2(i-1)\right), 1\right)$
    end for
        img2(1) ← img1(1) ⊕ floor(S2(1) × 256)
        for i = 2 : M × N do
            img2(i) ← img1(i) ⊕ img2(i−1) ⊕ floor(S2(i) × 256)
    end for
        for i = 1 : M × N do
            $S3(i) = mod(\frac{r_3}{4}\left(x_3(i-1)\left(1-\frac{1}{2}x_3(i-1)-\beta_3 x_3(i-1)^2\right) + \lambda_3 x_3(i-1)\sin\left(\pi x_3(i-1)\right), 1\right)$
    end for
        for i = M × N − 1 downto 1 do
            img3(i) ← img2(i) ⊕ img2(i+1) ⊕ floor(S3(i) × 256)
    end for
        C ← reshape(img3, M, N)
```

Le décryptage de l'image est l'opération inverse du cryptage. La figure 2.7 présente les principales phases du processus de décryptage.

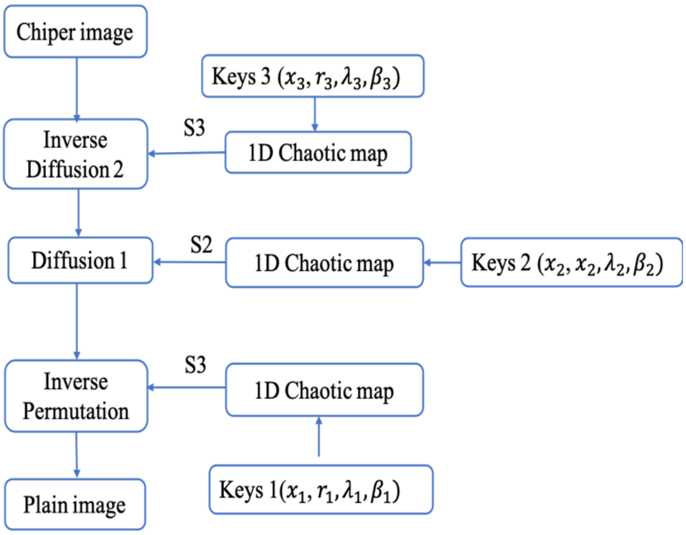


Fig. 9. Schéma synoptique du processus de décryptage d'image

4.2 Experimental Results And Performance Evaluation

The results presented in this subsection were obtained using simulations performed in MATLAB R2016b, installed on a MacBook Air (13-inch, 2017) equipped with a 2.2 GHz dual-core Intel Core i7 processor and 8 GB of 1600 MHz DDR3 RAM. The cryptosystem was tested on two images of size 256×256, namely Lena and Cameraman. Figure 10 illustrates the results of the image encryption and decryption processes. The encrypted images are visually very different from the original images, while the decryption process accurately restores the original images.

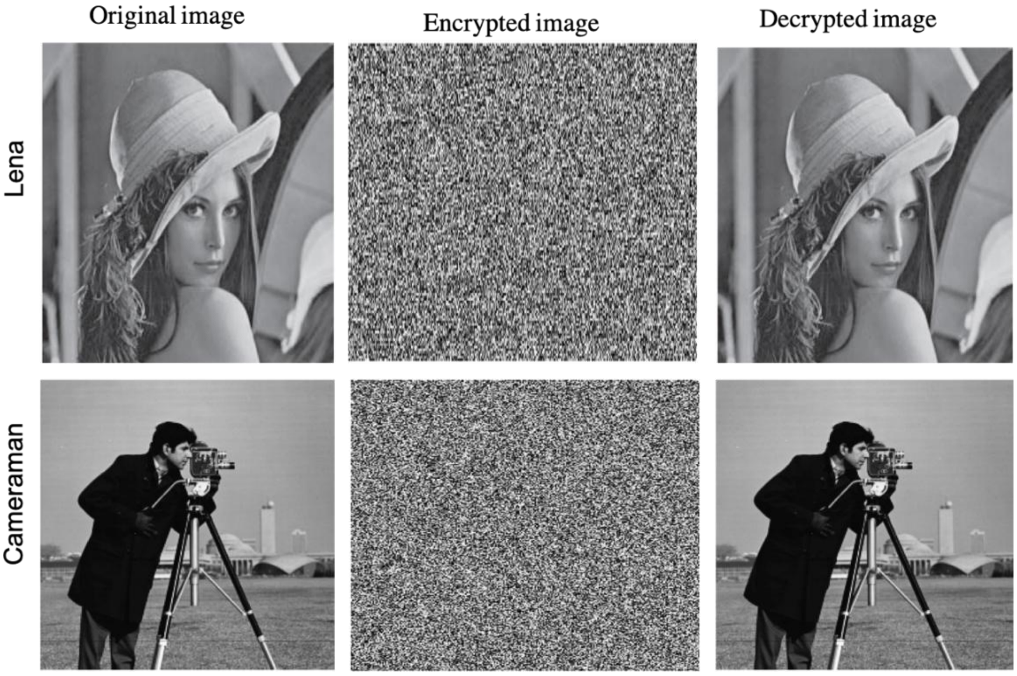


Fig. 10. Results of encryption and decryption processes

4.2.1 Histogram Evaluation

The histogram of an image illustrates the spectral distribution of its intensity levels. To ensure the confidentiality of information, the histogram of the encrypted image must exhibit a uniform distribution, which masks repetitions present in the unencrypted image and improves the system's resistance to statistical attacks [31]. Fig. 11 shows the histograms of the original and encrypted images. In both cases, it is clear that the grey-level distribution of the encrypted images is homogeneous, whereas that of the original images is non-uniform. The histogram analysis therefore leads to the conclusion that the proposed algorithm is effective against statistical attacks.

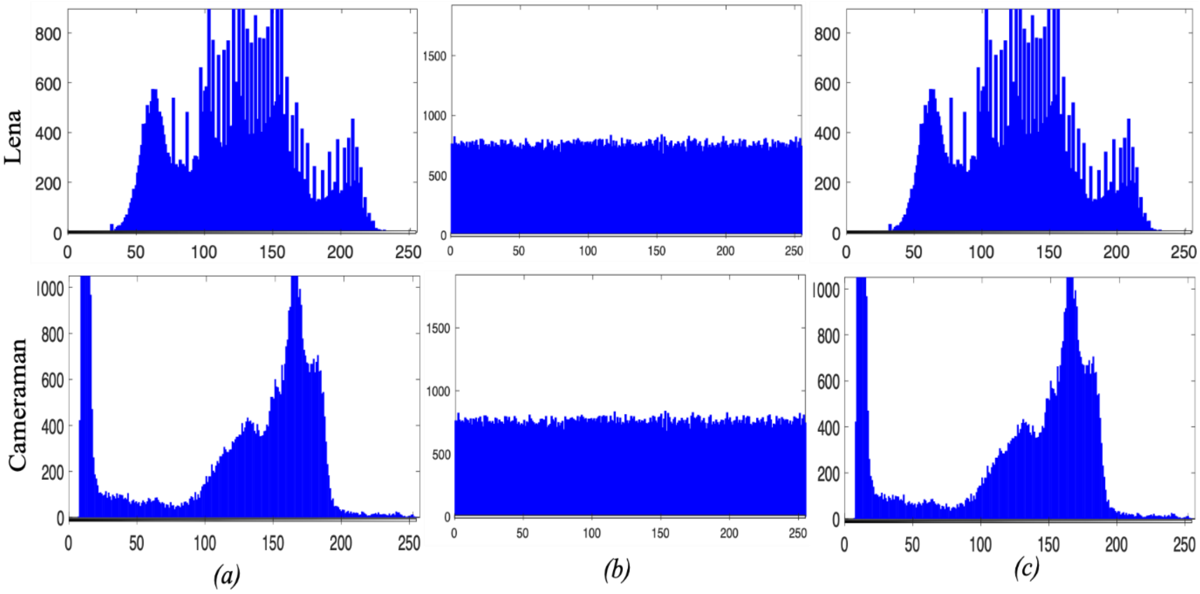
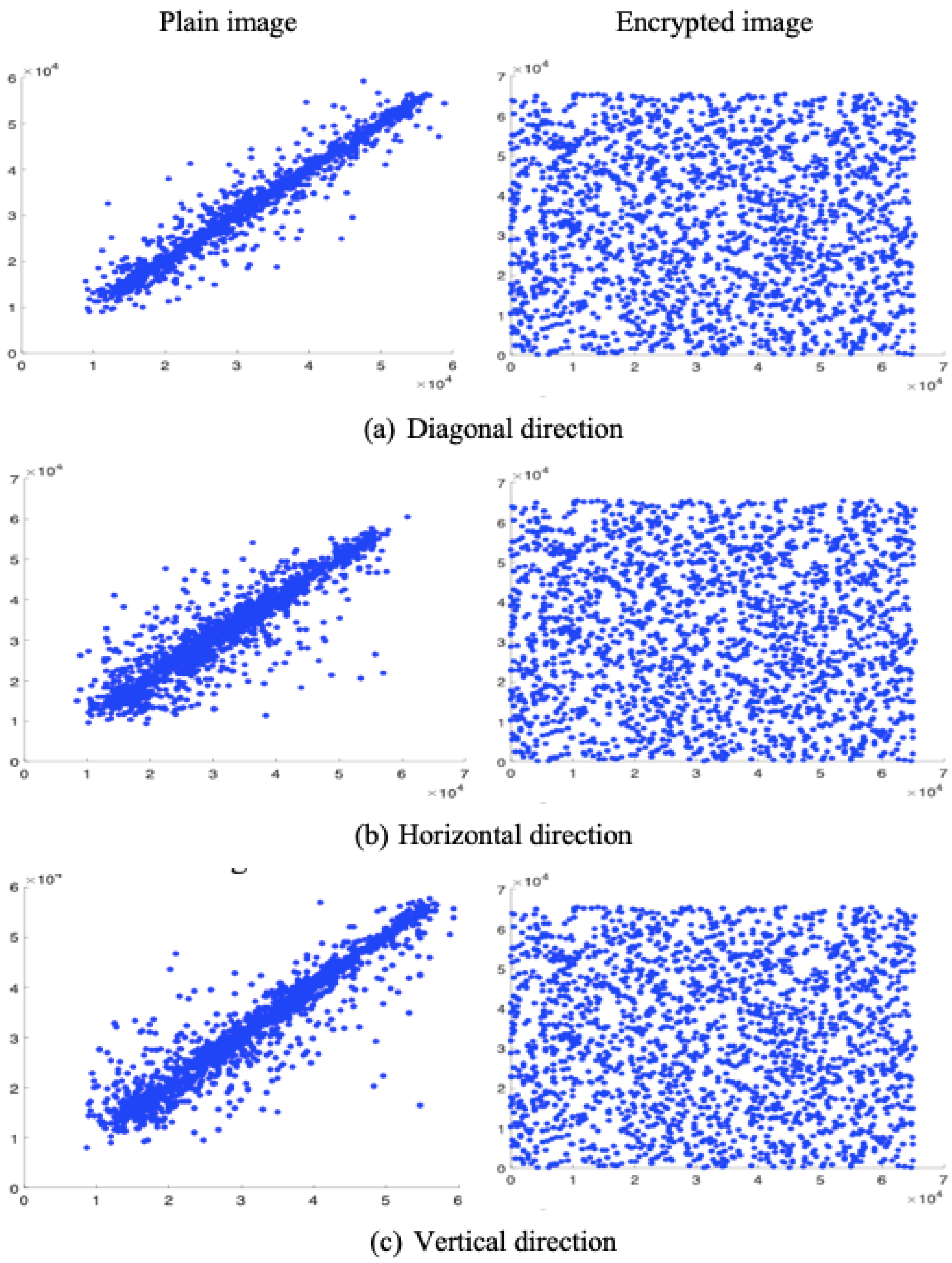


Fig. 11. Histogram analysis of clear and encrypted images

4.2.2 Correlation Evaluation

In a plain image, adjacent grey levels exhibit strong correlations in the horizontal, vertical, and diagonal directions. To ensure good resistance to statistical attacks, an effective cryptosystem must significantly reduce these correlations in the encrypted image. To this end, the correlations between adjacent pixels in the plaintext and ciphertext Lena images are analyzed in all three directions, and the results are presented in Fig.12. As can be observed, the distributions of adjacent grey levels in the plaintext image are highly concentrated, reflecting a high degree of correlation. In contrast, the corresponding distributions in the encrypted image are widely dispersed, indicating that the encryption process effectively eliminates pixel correlations and produces a low-correlation encrypted image.



Plain image

Encrypted image

(a) Diagonal direction

(b) Horizontal direction

(c) Vertical direction

Fig. 12. Correlation graphs for the clear image and for encrypted image

In addition to the information provided by the correlation graphs, correlation coefficients were calculated for each direction and compared with existing works in the literature. Table 1 presents the obtained results. As can be observed, the correlation coefficients of the original images are very high, whereas those of the encrypted images are very low. It can also be noted that the correlation coefficients of the encrypted images are close to zero in all three directions and for both images considered. Furthermore, for all the analyzed directions, the obtained values are very close to those reported in the works of [32–34]. These results indicate that the proposed encryption system exhibits good resistance against autocorrelation attacks.

Table 1. Correlation coefficients of original and encrypted images

Images	**Direction**	**Original**	**Encrypted**			
			Proposed scheme	[33]	[34]	[35]
Lena	Horizontal	0.9093	0.0080	0.019732	0.0069	0.0074
	Vertical	0.9617	0.0026	0.002467	0.0479	0.0096
	Diagonal	0.8853	0.00034	0.004438	0.0075	0.0193

4.2.3 Evaluation Of Differential Attacks

The ability of the proposed image encryption algorithm to resist differential attacks is evaluated using the NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) metrics. The simulation results, compared with those reported in the literature, are presented in Table 2. As can be observed, the obtained NPCR and UACI values are close to their ideal values. Moreover, these results are very similar to those reported in existing works. This observation demonstrates that the proposed algorithm exhibits high resistance to differential attacks.

Table 2. NPCR and UACI for the image simulation comparing our scheme with other literature methods

	Propose scheme		**[35]**		**[36]**		**[37]**	
File	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.62	33.51	99.60	33.51	-	-	99.6052	33.4561
Cameraman	99.64	33.52	99.61	33.56	99.6196	33.4153	-	-
Baboon	99.61	33.52	99.59	33.53	99.6089	33.4071	99.6125	33.4655

4.2.4 Entropy Evaluation

Since entropy is an important criterion in the evaluation of a cryptosystem, we analyzed this indicator to determine the degree of disorder in the distribution of pixel values in the image. The entropy values of the original and encrypted images are shown in the Table 3. It can be seen that the entropy values of the encrypted images are close to 8, which means that the bites are uniformly distributed.

Table 3. Entropy values for encrypted and original images

Images	**Original**	**Encrypted**			
		Proposed scheme	[37]	[38]	[39]
Lena	7.7792	7.9962	-	7.999359	7.997052
Cameraman	7.0097	7.9971	7.9993	-	7.99672
Baboon	7.3596	7.9960	7.9993	7.999380	7.99742

4.2.5 Key Sensitivity Evaluation

Key sensitivity is the fundamental property of a chaotic cryptosystem. A slight modification of the original keys should give different results during encryption and/or decryption. Fig. 13 shows the sensitivity test for encryption and decryption. The results show that the use of modified keys in the encryption phase produces a visibly different image. At the decryption stage, the use of a modified key does not reconstitute the original image. The encryption algorithm presented is highly key-sensitive.

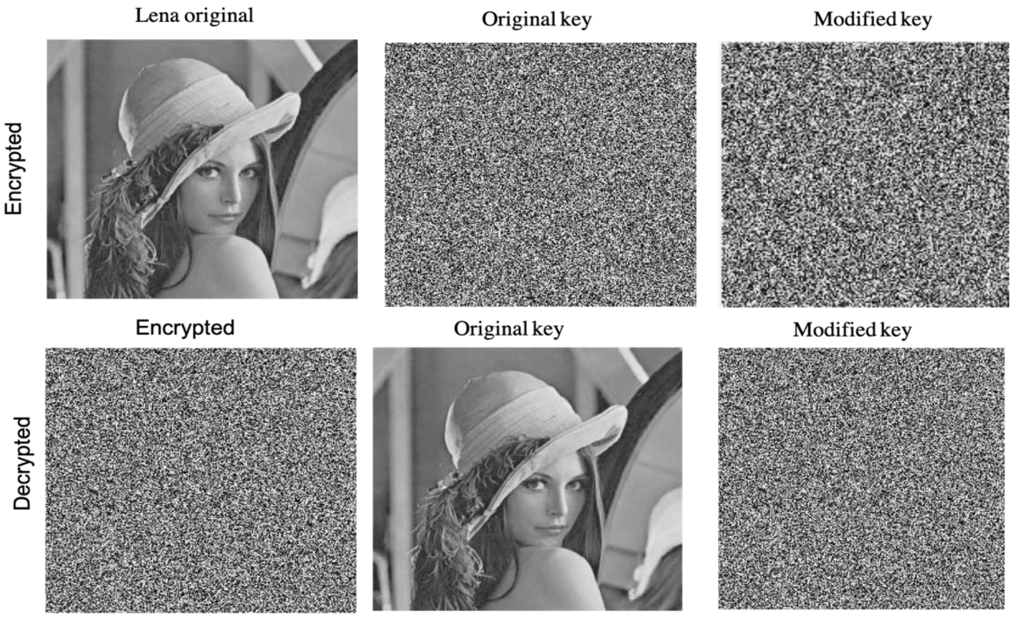


Fig. 13. Key sensitivity test for encryption and image encryption

4.2.6 Evaluation Of Key Space

To evaluate the algorithm resistance to brute-force attacks, the entire key space is determined and presented in Table 4. The proposed scheme key space consists of the set of initial conditions $(x\_1, x\_2, x\_3\ )$ and parameters $(\lambda_1, r_1,\ \beta_1,\ \lambda_2, r_2,\ \beta_2,\ \lambda_3, r_3,\ \beta_3)$ of the two chaotic systems. For a machine with a precision of $10^{-15}$the key space is calculated as follows $[\![(10]\!]^{15})^{8}\ = 10^{180}$, which is sufficiently large. This situation allows us to deduce that our proposed algorithm is capable of resisting brute force attacks. In addition, a comparison of this encryption scheme with other chaotic image encryption schemes is carried out. The results shown in Table 4 indicate that the key space of this algorithm is also larger than that of other algorithms.

Table 4. Comparison of the key space of the proposed algorithm with other algorithms

Algorithm	Key space
[14]	10^{75}
[40]	10^{90}
[41]	10^{105}
Proposed scheme	10^{10}

4.2.7 Evaluation Of Image Encryption Time

Execution time is an important measure for guaranteeing the efficiency of an encryption algorithm. By evaluating the execution time of the entire encryption process for the two images under consideration, we obtained 1.255517 seconds and 1.567479 seconds for the Lena and Cameraman images respectively. However, it should be noted that the encryption execution time for the Lena image is comparable to the work presented in the literature. The result illustrated in Table 6 shows that the proposed algorithm is faster than the authors' image encryption schemes.

Table 5. Encryption execution time analysis

Algorithm	Execution time (s)
[42]	2.792
[43]	2.9
[44]	4.601
[45]	7.788
[46]	4.821
Proposed scheme	0.99

5 Conclusion

In this article, we propose a new one-dimensional discrete chaotic map for enhancing the security of chaos-based encryption systems. The proposed discrete system combines a nonlinear polynomial structure with a sinusoidal term, controlled by several independent parameters, which allows for a wider chaotic range and improved dynamic complexity. A detailed analysis of its chaotic properties, including bifurcation diagrams, the Lyapunov exponent, sensitivity to initial conditions and parameters, and approximate entropy, confirms the robust chaotic nature of the proposed map. Building on the advantages of the new map, we use it to develop an image encryption algorithm. The scheme is based on a permutation operation and two diffusion operations, driven three times by the new map. Experimental results and security analyses, including the study of histograms, correlations between adjacent pixels, key sensitivity, and NPCR and UACI metrics, demonstrate that the proposed algorithm offers good performance and strong resistance to statistical and differential attacks.

References

[1] R. Sneyers, «Climate chaotic instability: Statistical determination and theoretical background,» *Environmetrics,* vol. 8, no. 5, pp. 517–532, 1997.

[2] X. Zeng, R. A. Pielke, and R. Eykholt, «Chaos theory and its applications to the atmosphere,» *Bulletin of the American Meteorological Society,* vol. 74, no. 4, pp. 631–644, 1993.

[3] A. Serletis and P. Gogas, «Purchasing power parity, nonlinearity and chaos,» *Applied Financial Economics,* vol. 10, no. 6, pp. 615–622, 2000, doi: 10.1080/096031000437962.

[4] M. Maqableh, A. Samsudin, and M. A. Alia, «New hash function based on chaos theory (CHA-1),» *International Journal of Computer Networks & Security,* vol. 8, no. 2, pp. 20–26, 2008.

[5] M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Bouridane, «Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption,» *Communications in Nonlinear Science and Numerical Simulation,* vol. 18, no. 8, pp. 2035–2047, 2013, doi: 10.1016/j.cnsns.2012.12.018.

[6] A. Hasheminejad and M. Rostami, «A novel bit-level multiphase algorithm for image encryption based on PWLCM chaotic map,» *Optik,* vol. 184, pp. 205–213, 2019, doi: 10.1016/j.ijleo.2019.03.065.

[7] S. E. Borujeni and M. S. Ehsani, «Modified logistic maps for cryptographic application,» *Applied Mathematics,* vol. 6, no. 5, pp. 773–782, 2015, doi: 10.4236/am.2015.65073.

[8] R. L. Rivest, A. Shamir, and L. Adleman, «A method for obtaining digital signatures and public-key cryptosystems,» *Communications of the ACM,* vol. 21, no. 2, pp. 120–126, 1978.

[9] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, «A novel image encryption/decryption scheme based on integrating multiple chaotic maps,» *AIP Advances,* vol. 10, no. 7, Art. no. 075017, 2020, doi: 10.1063/5.0009225.

[10] X. Wang, S. Wang, N. Wei, and Y. Zhang, «A novel chaotic image encryption scheme based on hash function and cyclic shift,» *IETE Technical Review,* vol. 36, no. 1, pp. 39–48, 2018, doi: 10.1080/02564602.2017.1393352.

[11] X. Wu, H. Shi, M. Ji'e, S. Dua, and L. Wang, «A novel image compression and encryption scheme based on conservative chaotic system and DNA method,» *Chaos, Solitons & Fractals,* vol. 172, Art. no. 113492, 2023, doi: 10.1016/j.chaos.2023.113492.

[12] S. Zhu, X. Deng, W. Zhang, and C. Zhu, «Secure image encryption scheme based on a new robust chaotic map and strong S-box,» *Mathematics and Computers in Simulation,* vol. 207, pp. 322–346, 2023, doi: 10.1016/j.matcom.2022.12.025.

[13] V. Patidar, N. K. Pareek, and K. K. Sud, «A new substitution–diffusion-based image cipher using chaotic standard and logistic maps,» *Communications in Nonlinear Science and Numerical Simulation,* vol. 14, no. 7, pp. 3056–3075, 2009, doi: 10.1016/j.cnsns.2008.11.005.

[14] J. Zhao, S. Wang, and Y. Chang, «A novel image encryption scheme based on an improper fractional-order chaotic system,» *Nonlinear Dynamics,* vol. 80, pp. 1721–1729, 2015, doi: 10.1007/s11071-015-1911-x.

[15] S. Amina and F. K. Mohamed, «An efficient and secure chaotic cipher algorithm for image content preservation,» *Communications in Nonlinear Science and Numerical Simulation,* vol. 60, pp. 12–32, 2018, doi: 10.1016/j.cnsns.2017.12.017.

[16] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, «A chaotic-based encryption/decryption framework for secure multimedia communications,» *Entropy,* vol. 22, no. 11, Art. no. 1253, 2020, doi: 10.3390/e22111253.

[17] J. Oravec, L. Ovsenik, and J. Papaj, «An image encryption algorithm using logistic map with plaintext-related parameter values,» *Entropy,* vol. 23, no. 11, Art. no. 1373, 2021, doi: 10.3390/e23111373.

[18] W. Wen, Y. Li, and X. Zhang, «Secure image encryption scheme based on chaotic maps and bit-level permutation,» *Entropy,* vol. 25, no. 8, Art. no. 1124, 2023, doi: 10.3390/e25081124.

[19] A. Kanso and M. Ghebleh, «A refinement of the logistic map for cryptographic applications,» *Franklin Open,* vol. 12, Art. no. 100333, 2025, doi: 10.1016/j.fraope.2025.100333.

[20] Y. Zhou, L. Bao, and C. L. P. Chen, «A new 1D chaotic system for image encryption,» *Signal Processing,* vol. 97, pp. 172–182, 2014, doi: 10.1016/j.sigpro.2013.10.034.

[21] A. Dinu, Image Encryption Using Chaotic Maps, 2025.

[22] J. Xie, C. Yang, Q. Xie, and L. Tian, «An encryption algorithm based on transformed logistic map,» in *Proc. Int. Conf. Network Security, Wireless Communications and Trusted Computing,* Wuhan, China, pp. 111–114, 2009, doi: 10.1109/NSWCTC.2009.201.

[23] Z. Hua, Y. Zhou, and H. Huang, «Cosine-transform-based chaotic system for image encryption,» *Information Sciences,* vol. 480, pp. 403–419, 2019, doi: 10.1016/j.ins.2018.12.048.

[24] X. Zhang *et al.,* «Chaos-based color image encryption with JPEG compression,» 2025.

[25] Z. Kalsoubé, A. H. Ahamat, Y. K. Mahamoud, and P. Woafo, «Chaos in new polynomial discrete logistic maps with fractional derivative and applications for text encryption,» *Applied Mathematics & Information Sciences,* vol. 17, pp. 807–816, 2023.

[26] J. C. Sprott, *Chaos and Time-Series Analysis*. Oxford, UK: Oxford University Press, 2003.

[27] S. H. Strogatz, Nonlinear Dynamics and Chaos, 2nd ed. Boulder, CO, USA: Westview Press, 2015.

[28] E. Ott, Chaos in Dynamical Systems, 2nd ed. Cambridge, UK: Cambridge University Press, 2002.

[29] G. Alvarez and S. Li, «Some basic cryptographic requirements for chaos-based cryptosystems,» International Journal of Bifurcation and Chaos, vol. 16, pp. 2129–2151, 2006.

[30] S. M. Pincus and A. L. Goldberger, «Physiological time-series analysis: What does regularity quantify?» American Journal of Physiology, vol. 266, pp. H1643–H1656, 1994.

[31] X.-Y. Wang, «New chaotic encryption algorithm based on chaotic sequence and plaintext,» IET Information Security, vol. 8, pp. 213–216, 2014.

[32] S. Lian, J. Sun, and Z. Wang, «A block cipher based on a suitable use of the chaotic standard map,» Chaos, Solitons & Fractals, vol. 26, pp. 117–129, 2005, doi: 10.1016/j.chaos.2004.11.096.

[33] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, «New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix,» Electronics, vol. 10, Art. no. 910, 2021, doi: 10.3390/electronics10091066.

[34] J. Wu, X. Liao, and B. Yang, «Image encryption using 2D Hénon–sine map and DNA approach,» Signal Processing, vol. 153, pp. 11–23, 2018, doi: 10.1016/j.sigpro.2018.06.008.

[35] R. Subramani, B. Emin, S. T. Kingni, and A. Akgül, «Image encryption application and security analysis based on semiconductor lasers,» Optik, vol. 287, Art. no. 171164, 2023.

[36] D. I. M. Setiadi and N. Rijati, «Image encryption using 2D cascaded logistic map and permutation–substitution operations,» Computation, vol. 11, Art. no. 178, 2023, doi: 10.3390/computation11090178.

[37] D. S. Malik and T. Shah, «Color multiple image encryption scheme based on 3D chaotic maps,» Mathematics and Computers in Simulation, vol. 178, pp. 646–666, 2020.

[38] X. Wang, L. Liu, and Y. Zhang, «A novel chaotic block image encryption algorithm,» Optics and Lasers in Engineering, vol. 66, pp. 10–18, 2015, doi: 10.1016/j.optlaseng.2014.08.005.

[39] B. Stoyanov and K. Kordov, «Image encryption using Chebyshev map and rotation equation,» Entropy, vol. 17, pp. 2117–2139, 2015, doi: 10.3390/e17042117.

[40] H. Zhu, L. Dai, Y. Liu, and L. Wu, «A three-dimensional bit-level image encryption algorithm with Rubik's cube method,» Mathematics and Computers in Simulation, vol. 185, pp. 754–770, 2021.

[41] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, «Image encryption with double spiral scans and chaotic maps,» Security and Communication Networks, Art. ID 8694678, 2019, doi: 10.1155/2019/8694678.

[42] A. Arab, M. J. Rostami, and B. Ghavami, «An image encryption method based on chaos system and AES algorithm,» Journal of Supercomputing, vol. 75, pp. 6663–6682, 2019.

[43] G. Zhang and Q. Liu, «A novel image encryption method based on total shuffling scheme,» Optics Communications, vol. 284, pp. 2775–2780, 2011.

[44] R. Parvaz and M. Zarebnia, «A combination chaotic system and application in color image encryption,» Optics and Laser Technology, vol. 101, pp. 30–41, 2018.

[45] C. Zhu, G. Wang, and K. Sun, «Cryptanalysis and improvement on an image encryption algorithm using a chaos-based S-box,» Symmetry, vol. 10, Art. no. 313, 2018.