Hindawi
Complexity
Volume 2022, Article ID 1720842, 16 pages
https://doi.org/10.1155/2022/1720842

*Research Article*

# Novel One-Dimensional Chaotic System and Its Application in Image Encryption

**Zhiqiang Cheng,[1] Wencheng Wang,[2] Yuezhang Dai,[1] and Lun Li[2]**

[1]*School of Physics and Electronic Information, Weifang University, Weifang 261061, China*
[2]*School of Mechanics and Automation, Weifang University, Weifang 261061, China*

Correspondence should be addressed to Lun Li; ll408907652@163.com

Received 2 June 2022; Revised 26 August 2022; Accepted 21 September 2022; Published 18 October 2022

Academic Editor: Rosa M. Lopez Gutierrez



Designing a chaotic system with a simple structure and complex dynamic behavior is one of the main tasks of chaotic cryptography. This paper designs a new 1D chaotic system called 1D two-parameters-sin-cos (1D-TPSC). Compared with high-dimensional chaotic systems, the 1D-TPSC has a simple structure and is easy to implement with software. The Lyapunov exponent analyzes the parameter space of the 1D-TPSC in a chaotic state. Furthermore, using sensitivity analysis, cobweb plot, and bifurcation diagram to verify that the sequence generated by 1D-TPSC has good performance. In addition, the 1D-TPSC has also been applied in chaotic image encryption. Arnold mapping is used to scramble the plaintext, and random XOR is used to diffuse the scrambled image. Simulation experiments show that the method can remarkably resist standard attack methods.

## 1. Introduction

With the rapid development of the Internet, people have more and more methods to obtain information. When digital images are disseminated in public channels as an indispensable communication carrier, the security of image content cannot be guaranteed [1, 2]. Images carry a large amount of intuitive information. Once this information is leaked, it will bring significant damage to personal privacy [3]. Therefore, ensuring the safe transmission of images on the Internet and protecting personal privacy from being leaked is a crucial topic [4, 5].

At present, many image protection algorithms have been proposed. For example, image watermarking technology, image encryption technology, and image steganography technology [6–10]. Image encryption technology is one of the most widely used technologies. It can convert a plaintext image containing much information into a random noise image, and the original plaintext image can be obtained through the correct secret key and decryption system, both of which are indispensable [11, 12]. Due to the high redundancy of the image and the significant adjacent correlation, the traditional AES, DES, RSA, etc. are no longer suitable for image encryption [13]. In recent years, chaos theory has been proven to be very suitable for image encryption. Because of its sensitivity, ergodicity, unpredictability, and other properties, it is very suitable for cryptographic systems to generate secret keys [14, 15]. As more and more chaotic systems are proposed, many chaotic image encryption algorithms have been produced [16, 17]. The structure of the cryptosystem and the way of generating the keystream determine the security of the cryptosystem.

To improve the structure of the cryptographic system and increase its security of the cryptographic system, the chaotic image encryption algorithm is usually proposed in combination with other fields of knowledge; for example, the chaotic image encryption algorithm is based on DNA and RNA theory [18, 19]. Image encryption algorithm based on matrix semitensor product [20, 21], image encryption algorithm based on compressed sensing [22, 23], chaotic image encryption algorithm based on quantum walks [24, 25], and image encryption algorithm based on cellular automata [26] .These algorithms increase the complexity of the algorithm and give the algorithm high security. In

addition, some scholars have proposed many new chaotic systems, which are used to generate the secret key of the cryptographic system to increase the security of the cryptographic system [27–30]. In a new cryptosystem, Kaur et al. used a 7D hyperchaotic map to generate the key stream, which has a large parameter space [27]. Zhang and Han used a 6D hyperchaotic system to generate a random key stream and combined it with DNA technology to propose a color image encryption algorithm, which has good robustness [28]. Li et al. used the fractional 4D hyperchaotic system to generate the keystream of the cryptographic system and discussed the application of this fractional system in image encryption. The experimental results show that the algorithm combined with the fractional 4D hyperchaotic system has higher performance security [29].

Although high-dimensional chaotic systems have higher complexity and more parameter space, due to the complex structure of these high-dimensional chaotic systems, the efficiency of generating key streams is very slow and difficult to achieve in practical applications. Although low-dimensional chaotic systems have a simple structure, their parameter space is minimal. For example, the parameter space of logistic chaotic is (0, 4) [31] and the parameter space of tent mapping is (0, 4) [31]. This will make the cryptosystem have no good ability to resist brute force attacks.

Therefore, this paper proposes a new 1D chaotic system called 1D-TPSC. This chaotic system has a simple structure, two control parameters make its control parameter space very large, and the complex structure displayed by 1D-TPSC, the generated key stream, has high random characteristics. In order to verify the excellent performance of the 1D-TPSC, the 1D-TPSC has been applied to image encryption. In cryptosystems, images are scrambled using Arnold mapping, and random XOR is applied to diffuse the scrambled images. The proposed algorithm can meet the security requirements in one round of encryption.

The rest of the paper is organized as follows. In Section 2, the proposed 1D-TPSC is introduced, and its performance is analyzed. In Section 3, the proposed encryption algorithm based on 1D-TPSC is described. In Section 4, it is verified that the algorithm has high security through some security analysis. Section 5 is a summary of the paper and proposes future work.

## 2. 1D-TPSC

The Sin Map is defined as [32]

$$x_{i+1} = \beta \sin(\pi x_n), \tag{1}$$

where $\beta$ is the control parameter, $x_0$ is the initial value of the chaotic system, and $x \in (-\beta, \beta)$.

There is only one parameter in the Sin Map and using the Sin Map to generate the key stream will result in a small parameter space of the cryptosystem. And the parameter space of Sin Map in a chaotic state is very small. To solve these problems, we propose a new 1D chaotic system called 1D-TPSC, this system has two control parameters, a simple structure can produce complex dynamic behavior, and the 1D-TPSC is described as

$$x_{n+1} = \beta \sin(\pi\mu(1 - x_n) + \cos(\pi x_n + 1)), \tag{2}$$

where $\mu$ and $\beta$ are the two control parameters of 1D-TPSC, $\mu > 0$ and $\beta > 0$. $x_0$ is the initial value of the chaotic system, and $x \in (-\beta, \beta)$.

*2.1. Lyapunov Exponents.* The Lyapunov exponent is a measure of the sensitive dependence of the system on initial conditions [33, 34]. A positive Lyapunov exponent indicates that the system is in a chaotic state. The Lyapunov exponent analysis of the 1D-TPSC is shown in Figure 1. The initial value of the system is selected as $x_0 = 0.98461532023$. When $\beta = 2$, the 1D-TPSC presented a weak chaotic state, and the parameter space in the chaotic state was discontinuous. When $\beta = 4$, the 1D-TPSC presented a weak chaotic state at 0, at $\mu \in (2.9, +\infty)$, the 1D-TPSC is in a chaotic state. With the continuous increase of $\beta$, the chaotic behavior of the 1D-TPSC gradually increased. But at $\mu \in (0, 1.2)$, the chaotic behavior of the 1D-TPSC is always weak, so when choosing parameters, parameters in this interval should be avoided.

*2.2. Bifurcation Diagram.* The bifurcation graph can verify the accuracy of the Lyapunov exponents. The bifurcation graph analysis of the 1D-TPSC is shown in Figure 2. The initial value of the 1D-TPSC is $x_0 = 0.98461532023$. The bifurcation graph verifies that the parameter space of 1D-TPSC described in Section 2.1 is in a chaotic state.

*2.3. Sensitivity Analysis.* Sensitivity analysis is divided into key sensitivity analysis and parameter sensitivity analysis. The initial value sensitivity analysis of the 1D-TPSC is shown in Figure 3, and the parameter sensitivity analysis of the 1D-TPSC is shown in Figure 4. The initial value and parameters of the 1D-TPSC are $x_0 = 0.98461532023$, $\beta = 3.6$, and $\mu = 8.8$. Sensitivity analysis showed that the 1D-TPSC was sensitive to initial values and parameters.

*2.4. Cobweb Diagram.* The chaotic cobweb diagram describes the iterative trajectory of the chaotic system. When the iterative trajectory of the chaotic system is not coincident, in this parameter space, the system has better dynamic behavior, and the generated sequence is random. The cobweb diagram analysis of the 1D-TPSC is shown in Figure 5. The cobweb diagram analysis showed that the trajectories of the series generated by the 1D-TPSC are not coincident, so the 1D-TPSC has good performance ability.

*2.5. 0-1 Test.* The 0-1 test results of 1D-TPSC are shown in Figure 6. When the generated sequence is chaotic, the 0-1 test images exhibit random motion. Conversely, the 0-1 test images are aggregated. It can be seen from Figure 6 that the motion state of 1D-TPSC is a random Brownian motion state, which indicates that the sequence generated by 1D-TPSC is random.

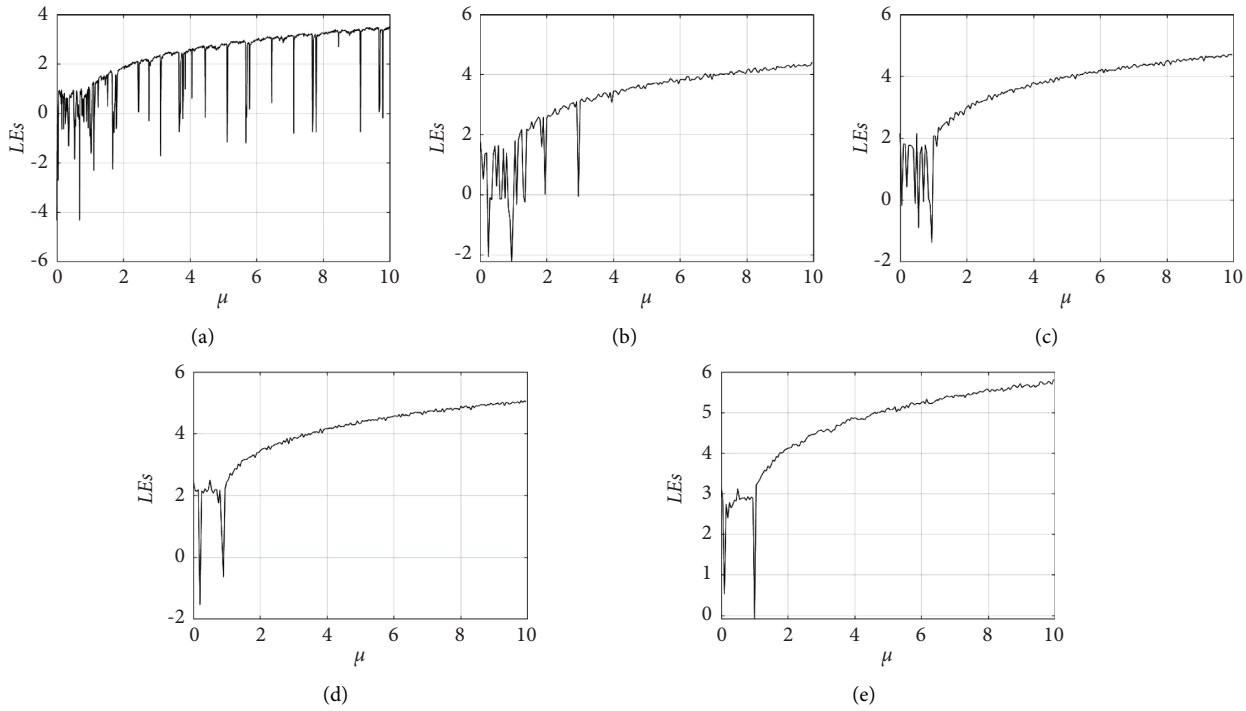



Figure 1: Lyapunov exponents of 1D-TPSC. (a) $\beta = 2$. (b) $\beta = 5$. (c) $\beta = 7$. (d) $\beta = 10$. (e) $\beta = 20$.

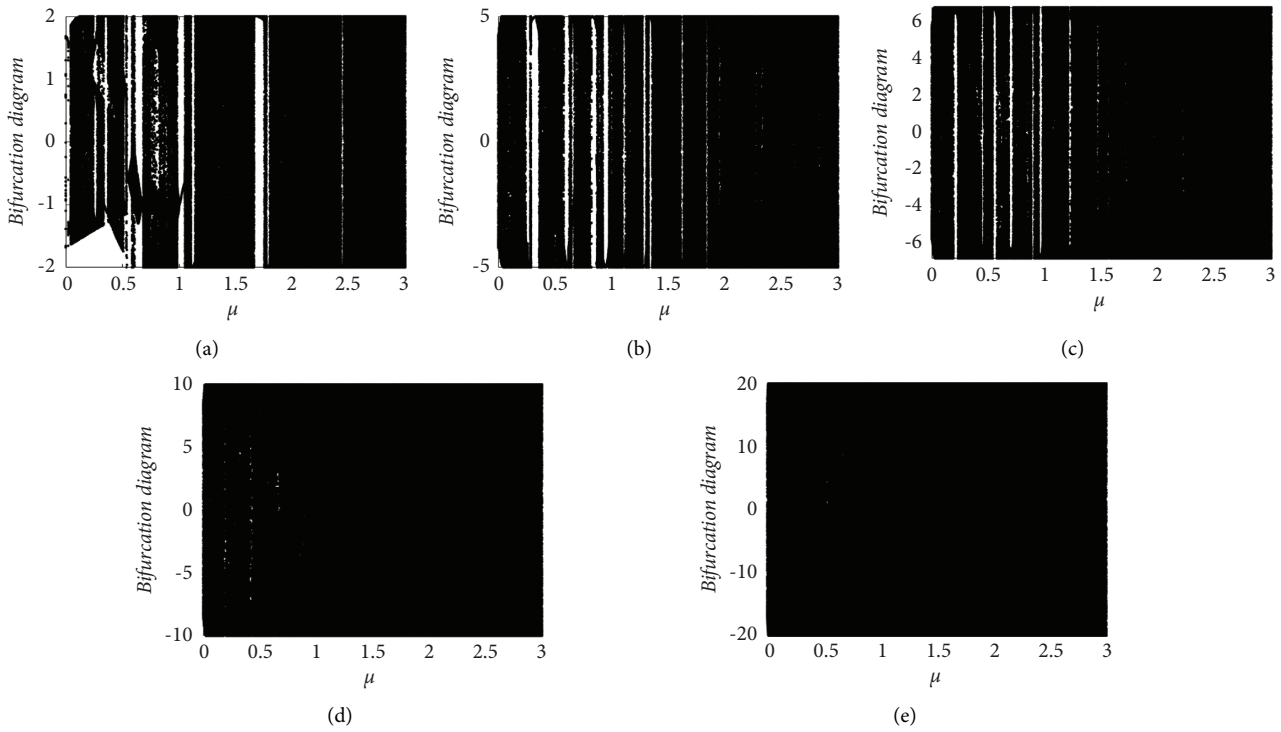



Figure 2: Bifurcation diagrams of 1D-TPSC. (a) $\beta = 2$. (b) $\beta = 5$. (c) $\beta = 7$. (d) $\beta = 10$. (e) $\beta = 20$.

*2.6. Histogram of 1D-TPSC.* Histogram of 1D-TPSC is shown in Figure 7. Figure 7 shows that the sequences produced by 1D-TPSC are uniformly distributed in the middle part of the range, with more values falling at the two ends of the range. In general, the sequences generated by 1D-TPSC are uniformly distributed over its range.

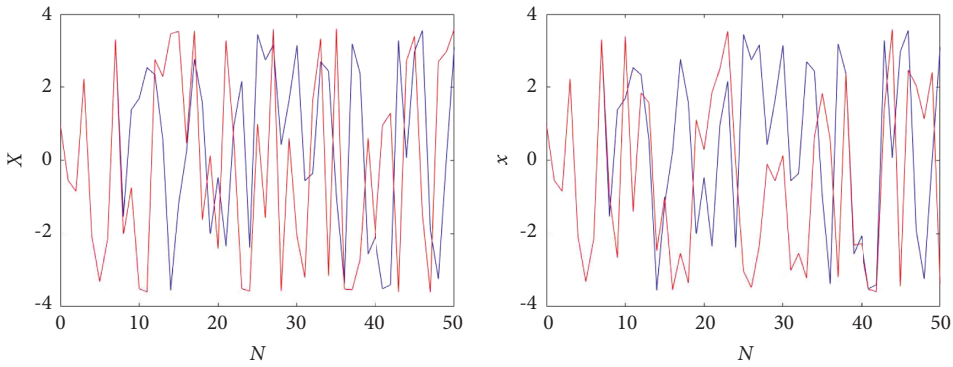



Figure 3: Initial sensitivity analysis. (a) $x_0 = 0.98461532023 + 10^{-15}$. (b) $x_0 = 0.98461532023 - 10^{-15}$.

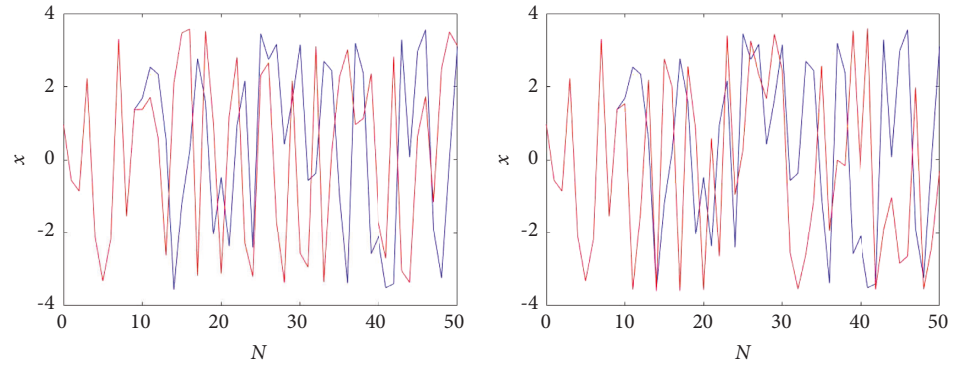



Figure 4: Parameter sensitivity analysis. (a) $\beta = 3.6 + 10^{-15}$. (b) $\mu = 8.8 + 10^{-15}$.

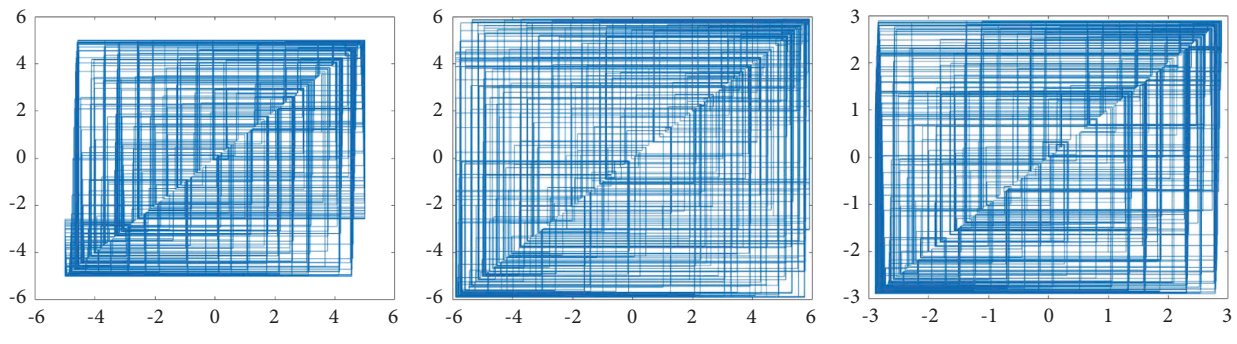



Figure 5: Cobweb diagram. (a) $\mu = 3.9999, \beta = 5.0001$. (b) $\mu = 9.8886, \beta = 5.8967$. (c) $\mu = 7.9634, \beta = 2.8896$.

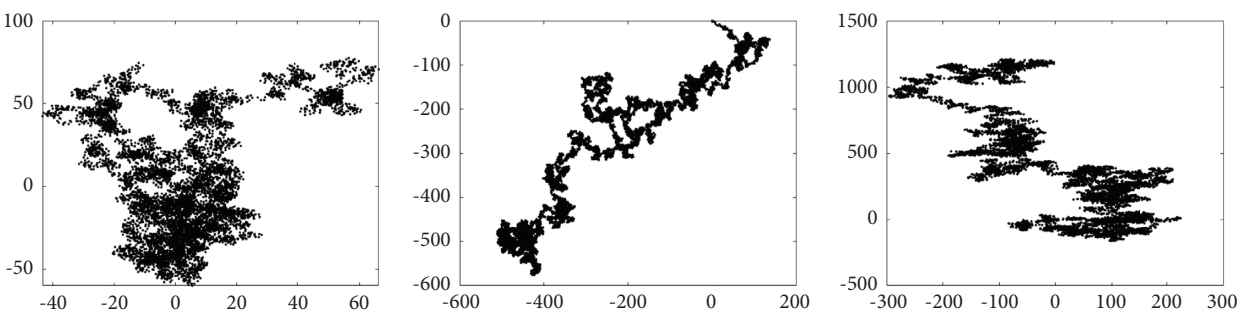



Figure 6: Continued.

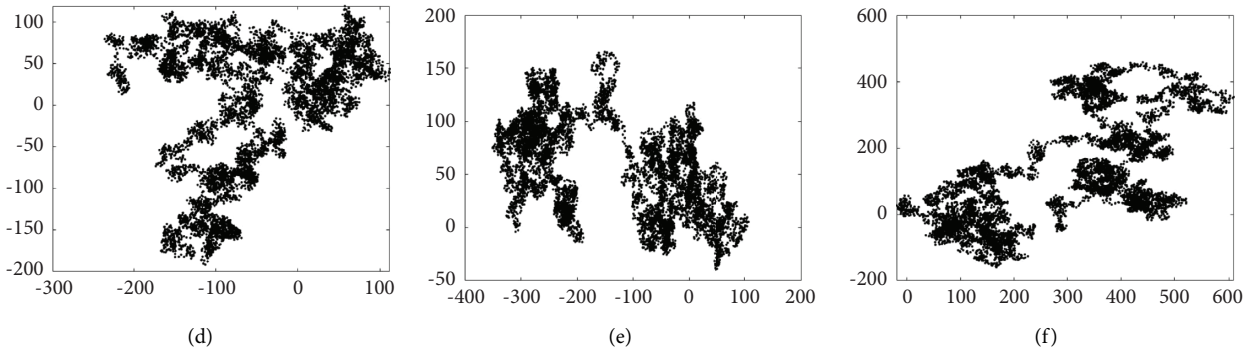



Figure 6: 0-1 test with different parameters. (a) $\beta = 2$, $\mu = 6$. (b) $\beta = 5$, $\mu = 6$. (c) $\beta = 10$, $\mu = 6$. (d) $\beta = 5$, $\mu = 9$. (e) $\beta = 5$, $\mu = 15$. (f) $\beta = 8$, $\mu = 8$.

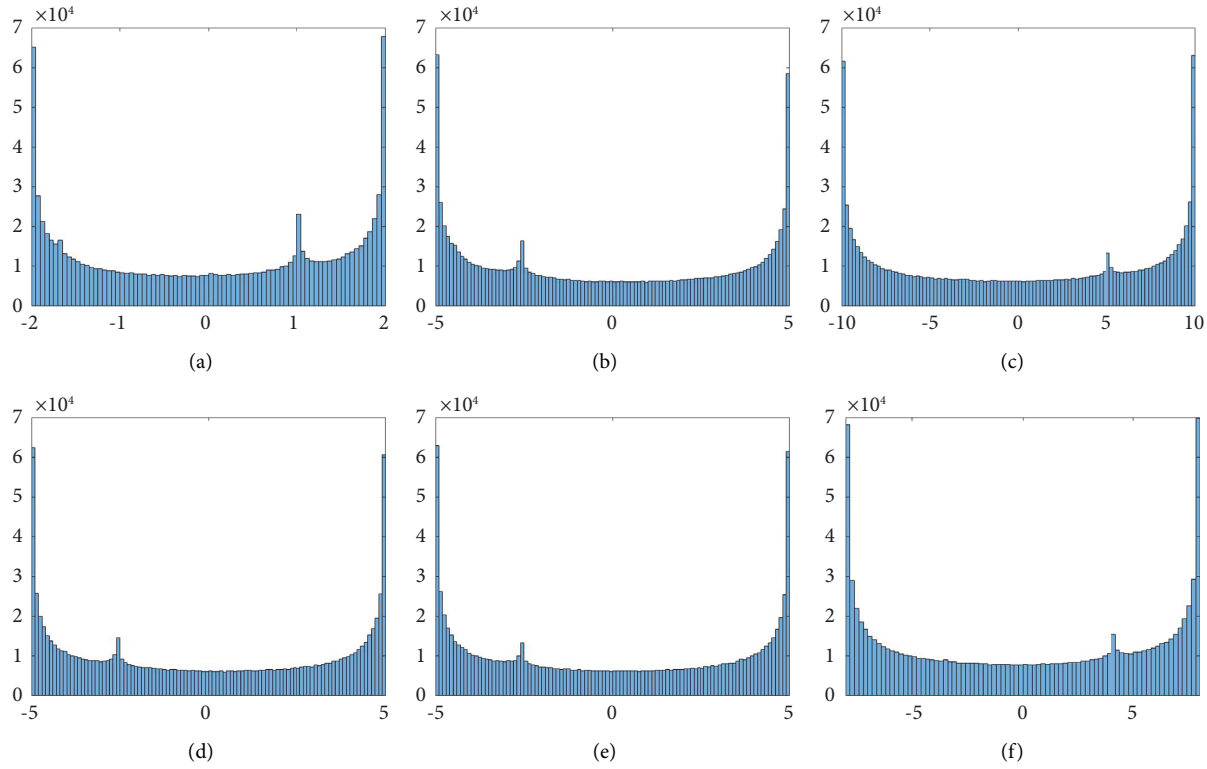



Figure 7: Histogram of 1D-TPSC with different parameters. (a) $\beta = 2$, $\mu = 6$. (b) $\beta = 5$, $\mu = 6$. (c) $\beta = 10$, $\mu = 6$. (d) $\beta = 5$, $\mu = 9$. (e) $\beta = 5$, $\mu = 15$. (f) $\beta = 8$, $\mu = 8$.

*2.7. NIST 800-22 Test.* NIST 800-22 test [35] results of 1D-TPSC are shown in Table 1. Table 1 shows that the sequences generated by 1D-TPSC passed all NIST tests, which indicated that the generated sequences had better randomness, and it is more suitable for cryptosystems.

## 3. Description of Encryption Algorithm (IM-TPSC)

Based on the 1D-TPSC, a new image encryption algorithm is proposed. This algorithm is a scrambling-to-diffusion process. The description of the algorithm is as follows:

Input: plaintext image $P(M \times N)$.

Output: ciphertext image $C$.

Step 1: the revision key of the IM-TPSC is generated using a hash function. Among them, the plaintext $P$ is the input of HASH-256. Generate a 256 bit key $k_1$. $k_1$ is divided into 16 groups, each group is

$$k_2(i) = \sum_{j=16\times i-15}^{16\times i} k_1(j), \quad i = 1, 2, 3, \ldots, 16. \tag{3}$$

The resulting revision key is

Table 1: NIST 800-22 test of 1D-TPSC.

| Test | $P$-val | Pass or no pass |
|---|---|---|
| Block frequency | 0.6890 | Pass |
| Rank | 0.0005 | Pass |
| Linear complexity | 0.1865 | Pass |
| Runs | 0.4372 | Pass |
| Universal | 0.1626 | Pass |
| Longest run of ones | 0.8343 | Pass |
| Nonoverlapping template matching | 0.7399 | Pass |
| Spectral | 0.3504 | Pass |
| Serial | 0.7399 | Pass |
| Frequency | 0.3115 | Pass |
| Overlapping template matching | 0.2429 | Pass |
| Approximate entropy | 0.4372 | Pass |
| Random excursions variant | 0.8043 | Pass |
| Random excursions | 0.2535 | Pass |
| Cumulative sums | 0.3924 | Pass |

$$\begin{cases} K_1 = \dfrac{\left(k_2(1)+k_2(2)+k_2(3)+k_2(4)\right)}{10^2}, \\ K_2 = \dfrac{\left(k_2(5)+k_2(6)+k_2(7)+k_2(8)\right)}{10^2}, \\ K_3 = \dfrac{\left(k_2(9)+k_2(10)+k_2(11)+k_2(12)\right)}{10^2}, \\ K_4 = \dfrac{\left(k_2(13)+k_2(14)+k_2(15)+k_2(16)\right)}{10^2}. \end{cases} \tag{4}$$

Step 2: given the initial keys of the cryptosystem $\rho_1, \rho_2, \rho_3$, according to the revised key, the new keys are generated as

$$\begin{cases} \varphi_1 = \rho_1 + \upsilon_1 - \upsilon_4, \\ \varphi_2 = \rho_2 + \upsilon_2, \\ \varphi_3 = \rho_3 + \upsilon_3, \end{cases} \tag{5}$$

where

$$\begin{cases} \upsilon_1 = x_{20} \mapsto x_{n+1} = \left(\dfrac{3.99+K_1}{10^3}\right) x_n(1-x_n), x_1 = K_1, n = 1,2,\ldots,20, \\ \upsilon_2 = x_{20} \mapsto x_{n+1} = \left(\dfrac{3.99+K_2}{10^3}\right) x_n(1-x_n), x_1 = K_2, n = 1,2,\ldots,20, \\ \upsilon_3 = x_{20} \mapsto x_{n+1} = \left(\dfrac{3.99+K_3}{10^3}\right) x_n(1-x_n), x_1 = K_3, n = 1,2,\ldots,20, \\ \upsilon_4 = x_{20} \mapsto x_{n+1} = \left(\dfrac{3.99+K_4}{10^3}\right) x_n(1-x_n), x_1 = K_4, n = 1,2,\ldots,20. \end{cases} \tag{6}$$

Step 3: generate the key stream of the cryptosystem by the equation,

$$X\colon\ x_{n+1} = \beta \sin\left(\pi\mu(1-x_n) + \cos(\pi x_n + 1)\right), \tag{7}$$

where in (6), $x_1 = \varphi_1, \beta = \varphi_2, \mu = \varphi_3, n = 1,2,\ldots,MN$. The size of $X$ is $1 \times MN$.

Step 4: Arnold mapping is described as,

$$\begin{bmatrix} f_{n+1} \\ g_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} f_n \\ g_n \end{bmatrix} \bmod M. \tag{8}$$

Generate the parameters and times of Arnold mapping by

$$\begin{cases} a = \text{floor}\left(X(M) \times 10^6\right)\text{mod}10^2 + 10, \\ b = \text{floor}\left(X(N) \times 10^7\right)\text{mod}10^2 + 10, \\ r = \text{floor}\left(X(M+1) \times 10^8\right)\text{mod}10^2 + 10. \end{cases} \tag{9}$$

Step 5: the plaintext image $P$ is used as the input of Arnold mapping, and the parameters of Arnold mapping are $a, b, r$ , then a scrambling matrix $S$ can be generated.

Step 6: generate the starting position $Q$ of the diffusion and the diffusion matrix $D$:

$$\begin{cases} Q = \text{floor}\left(X(\text{MN}) \times 10^9\right)\text{mod}\,(M+N), \\ D = \text{floor}\left(X \times 10^{10}\right)\text{mod}256. \end{cases} \tag{10}$$

Step 7: Diffusion is described as

(1) $C[Q] = D[Q] \oplus S[Q]$.
(2) $C[Q+1] = D[Q+1] \oplus S[Q+1] \oplus C[Q]$.
(3) $C[i] = D[i] \oplus S[i] \oplus C[i-1] \oplus C[i-2], \quad i = Q+2, Q+3, Q+4, \ldots, \text{MN}$.
(4) $C[Q-1] = (D[Q-1] + S[Q-1] + C[Q])\text{mod}256$.
(5) $C[i] = (D[i] + S[i] + C[i+1] + C[i+2])\text{mod}256$. $i = Q-2, Q-3, Q-4, \ldots, 1$.

Example 1:

$$\begin{aligned} D &= (170, 87, 247, 78, 84, 121, 126, 72, 116, 132), \\ S &= (104, 115, 1, 38, 25, 58, 208, 45, 236, 152), \end{aligned} \tag{11}$$

Set $Q = 6$, we can get $C$ by Step 7:

$$\begin{aligned} &C(6) = D(6) \oplus S(6) = 121 \oplus 58 = 67, \\ &C(7) = D(7) \oplus S(7) \oplus C(6) = 126 \oplus 208 \oplus 67 = 237, \\ &\begin{cases} C(8) = D(8) \oplus S(8) \oplus C(7) \oplus C(6) = 72 \oplus 45 \oplus 67 \oplus 237 = 203, \\ \vdots \\ C(10) = D(10) \oplus S(10) \oplus C(9) \oplus C(8) = 132 \oplus 152 \oplus 190 \oplus 203 = 105, \end{cases} \\ &C(5) = (D(5) + S(5) + C(6))\text{mod}256 = (84 + 25 + 67)\text{mod}256 = 176, \\ &\begin{cases} C(4) = (D(4) + S(4) + C(5) + C(6))\text{mod}256 = (78 + 38 + 176 + 67)\text{mod}256 = 103, \\ \vdots \\ C(1) = (D(1) + S(1) + C(2) + C(3))\text{mod}256 = (170 + 104 + 64 + 15)\text{mod}256 = 97, \end{cases} \\ &C = (97, 64, 15, 103, 176, 67, 237, 203, 190, 105). \end{aligned} \tag{12}$$

## 4. Performance Analysis

*4.1. Visualization of Grayscale Images.* The visual analysis of IM-TPSC is shown in Figures 8–10. The selected initial keys are $\rho_1 = 0.132465, \rho_2 = 5.21345, \rho_3 = 11.2314533$. Visual analysis shows that the IM-TPSC is visually secure.

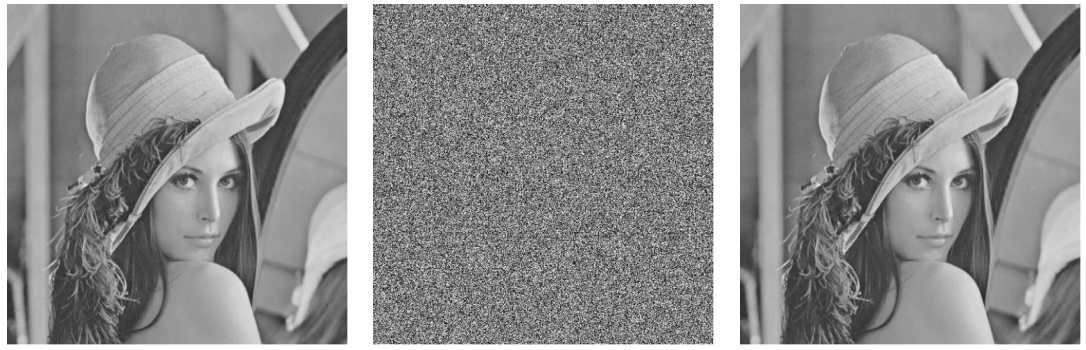
*4.2. Robustness Analysis.* Encrypted images are subject to noise and cropping attacks during transmission. Therefore, the encryption algorithm needs to resist a certain degree of noise attack and tailoring attacks. The robustness analysis of the IM-TPSC is shown in Figures 11 and 12. We add varying degrees of noise and missing data to test the robustness of the algorithm.

Figures 11 and 12 show that even if the plaintext is attacked by some noise or some information is lost, some features of the plaintext image can still be obtained through the decryption algorithm, indicating that the IM-TPSC has good robustness, and can resist noise attacks and clipping attacks.

*4.3. Histogram Analysis.* The histogram analysis of IM-TPSC is shown in Figures 13 and 14. It shows that the histogram distribution of plaintext is uneven, and the histogram distribution of ciphertext is uniform. This indicates that the attacker cannot obtain adequate information from the ciphertext to crack the algorithm, so the proposed encryption algorithm has a strong ability to resist statistical attacks.

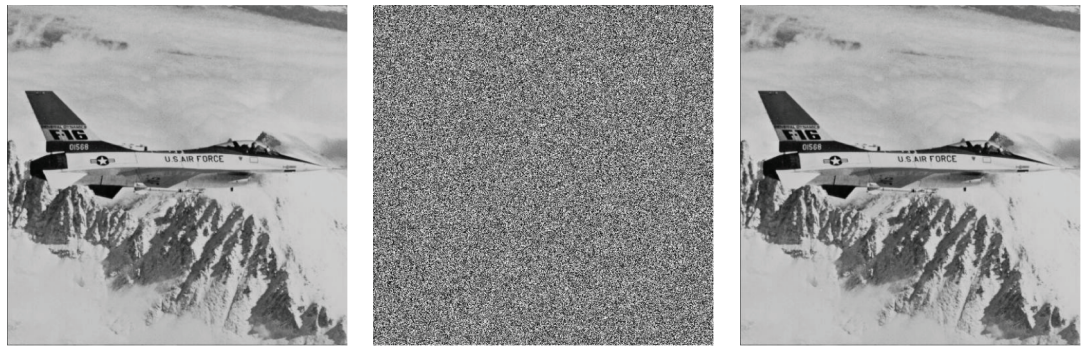
*4.4. Chosen Plaintext Attack Analysis.* Use the formula $P(i,j) \oplus P1(i,j) = C(i,j) \oplus C1(i,j)$ to verify whether the proposed algorithm is resistant to chosen plaintext attacks. If the equation does not hold, it indicates that the algorithm has a good ability to resist the chosen plaintext attack. The ability of IM-TPSC to resist the chosen plaintext attack is shown in Figure 15.

Figure 15 shows that IM-TPSC has good resistance to a chosen plaintext attack. Beyond that, it is reported in Ref. [36] that when the secret key is related to the plaintext, the algorithm can resist the chosen plaintext attack. The chosen plaintext attack is the most potent attack among the four classic attack methods (Ciphertext only, Known plaintext, Chosen plaintext, and Chosen ciphertext), so IM-TPSC can resist the classical attack way.



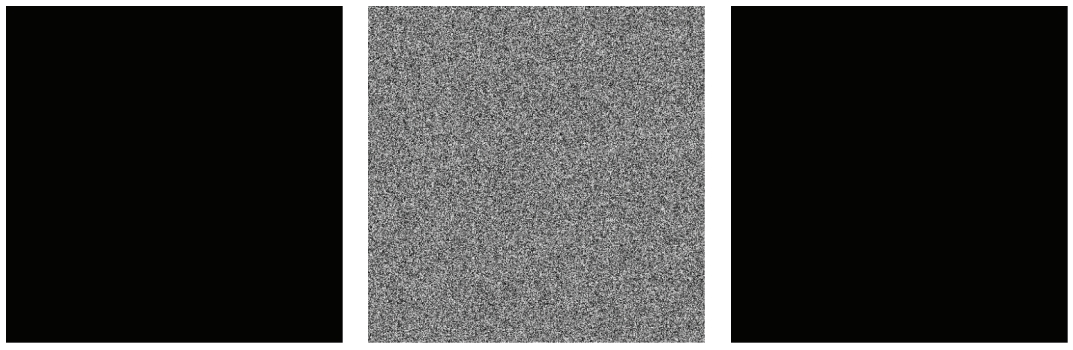
(a) (b) (c)

Figure 8: Encrypt and decrypt image of Lena. (a) Lena. (b) Encrypted Lena. (c) Decrypted Lena.




(a) (b) (c)

Figure 9: Encrypt and decrypt image of plane. (a) Plane. (b) Encrypted plane. (c) Decrypted plane.



(a) (b) (c)

Figure 10: Encrypt and decrypt image of all-black. (a) All-black. (b) Encrypted all-black. (c) Decrypted all-black.

*4.5. Differential Attack Analysis.* NPCR and UACI are two evaluation indicators to evaluate the ability of the algorithm to resist differential attack. It is reported in Ref. [37] that when the size of the image is $256 \times 256$, if the NPCR exceeds 99.5693, the UACI is between 33.2824 and 33.6447, indicating that the algorithm is resistant to differential attacks. When the size of the image is $512 \times 512$, if the NPCR exceeds 99.5893, the UACI is between 33.3730 and 33.5541, indicating that the algorithm is resistant to differential attacks. Differential attack analysis is shown in Table 2. The experimental results show that the proposed algorithm has a good ability to resist differential attacks.

*4.6. Key Sensitivity.* The secret key of the cryptosystem should be robust; that is, the original plaintext image cannot be obtained through the decryption system if the secret key changes slightly. The key sensitivity analysis of the IM-TPSC is shown in Figure 16. The initial keys are $\rho_1 = 0.132465, \rho_2 = 5.21345, \rho_3 = 11.2314533$. The slightly changed key is

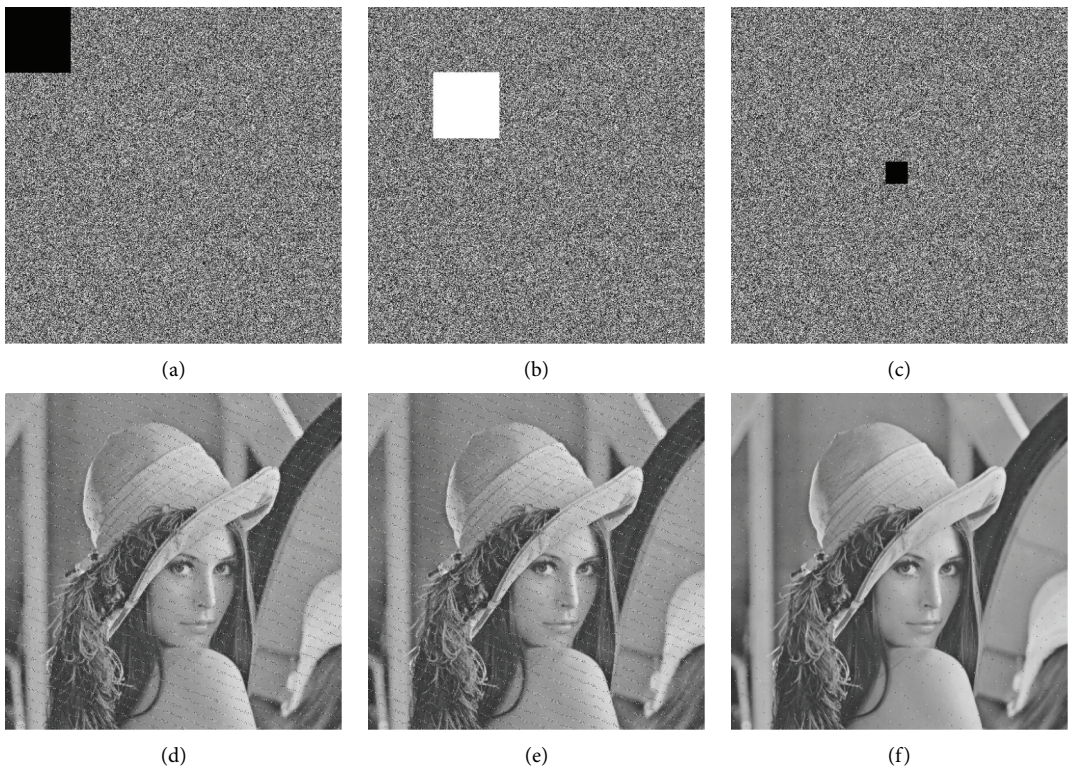



Figure 11: Clipping attack. (a) Clipping attack 1. (b) Clipping attack 2. (c) Clipping attack 3. (d) Decrypt of attack 1. (e) Decrypt of clipping attack 2. (f) Decrypt of clipping attack 3.

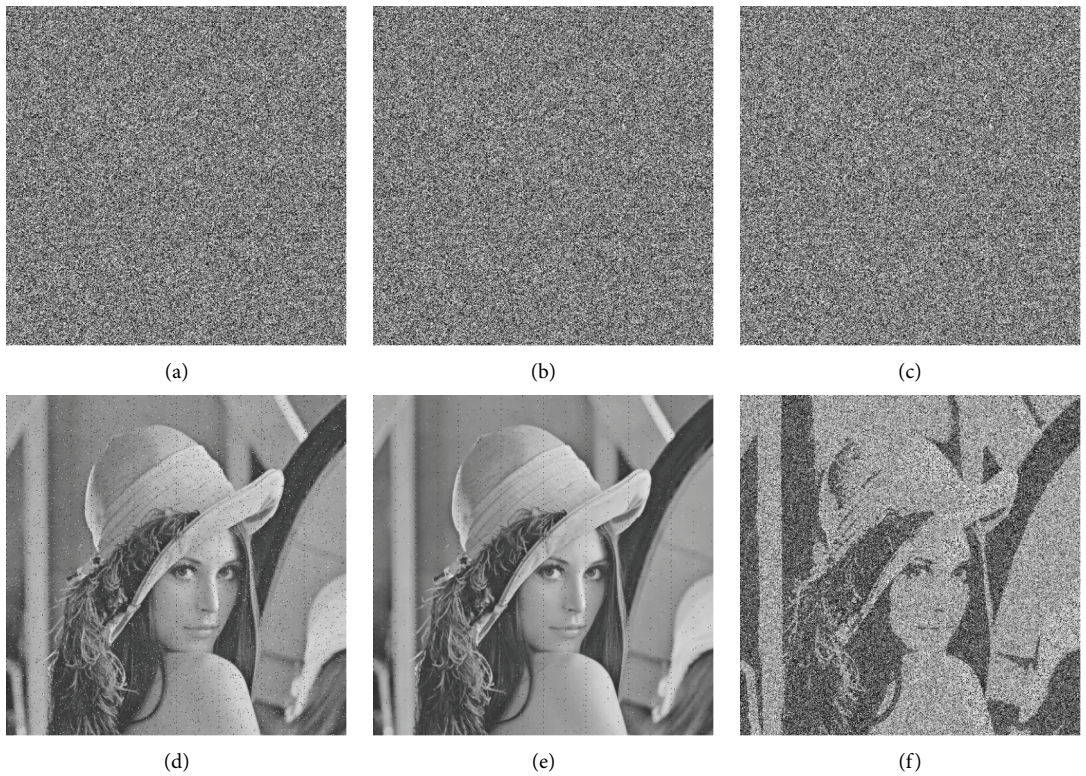



Figure 12: Noise attack. (a) 0.01 salt & pepper. (b) 0.001 salt & pepper. (c) 0.01 Gaussian. (d) Decrypt of 0.01 salt & pepper. (e) Decrypt of 0.001 salt & pepper. (f) Decrypt of 0.01 Gaussian.

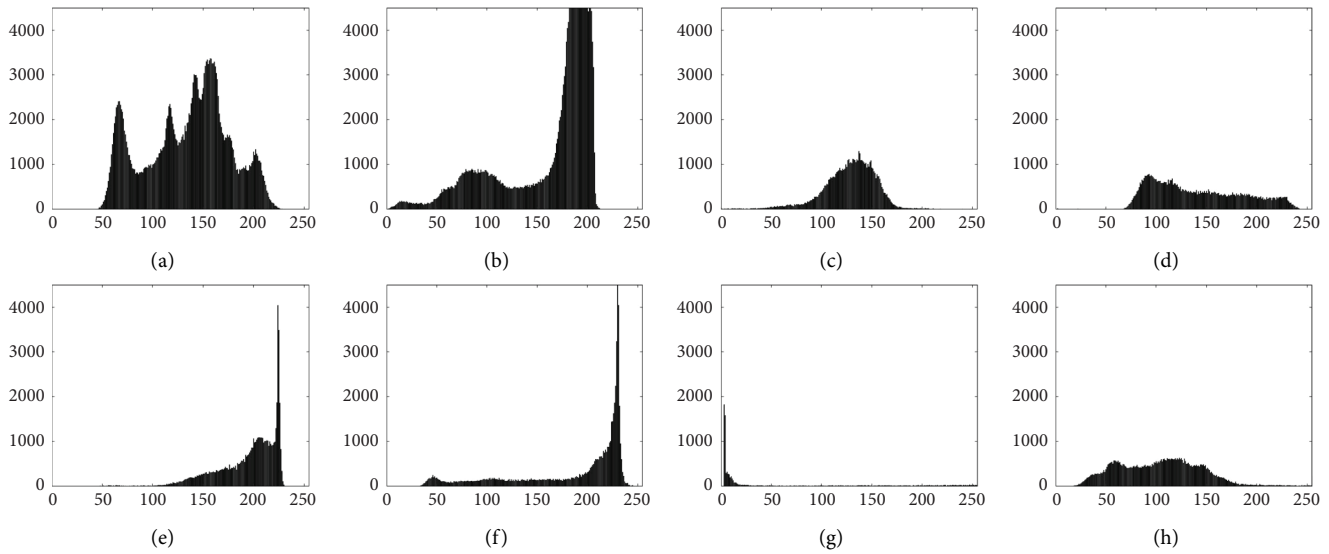



Figure 13: Histogram analysis for plaintext. (a) Lena. (b) Plane. (c) 5.1.09. (d) 5.1.10. (e) 5.1.11. (f) 5.1.12. (g) 5.1.13. (h) 5.1.14.

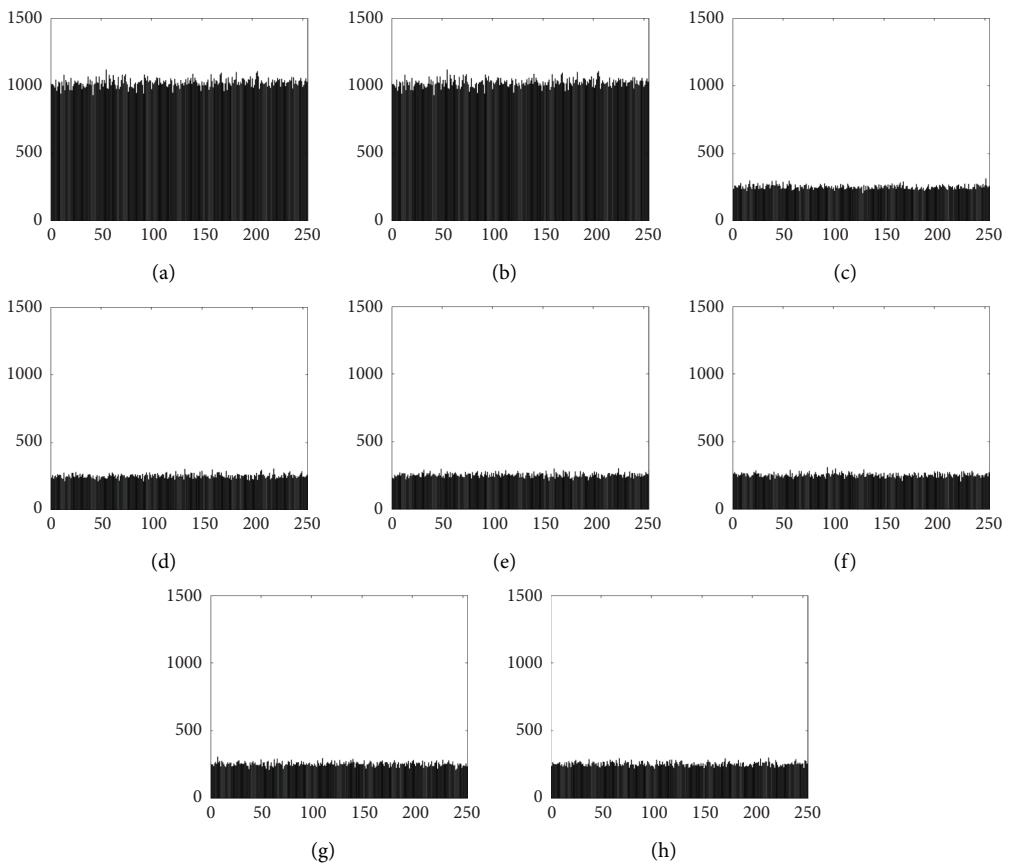



Figure 14: Histogram analysis for ciphertext. (a) Lena. (b) Plane. (c) 5.1.09. (d) 5.1.10. (e) 5.1.11. (f) 5.1.12. (g) 5.1.13. (h) 5.1.14.

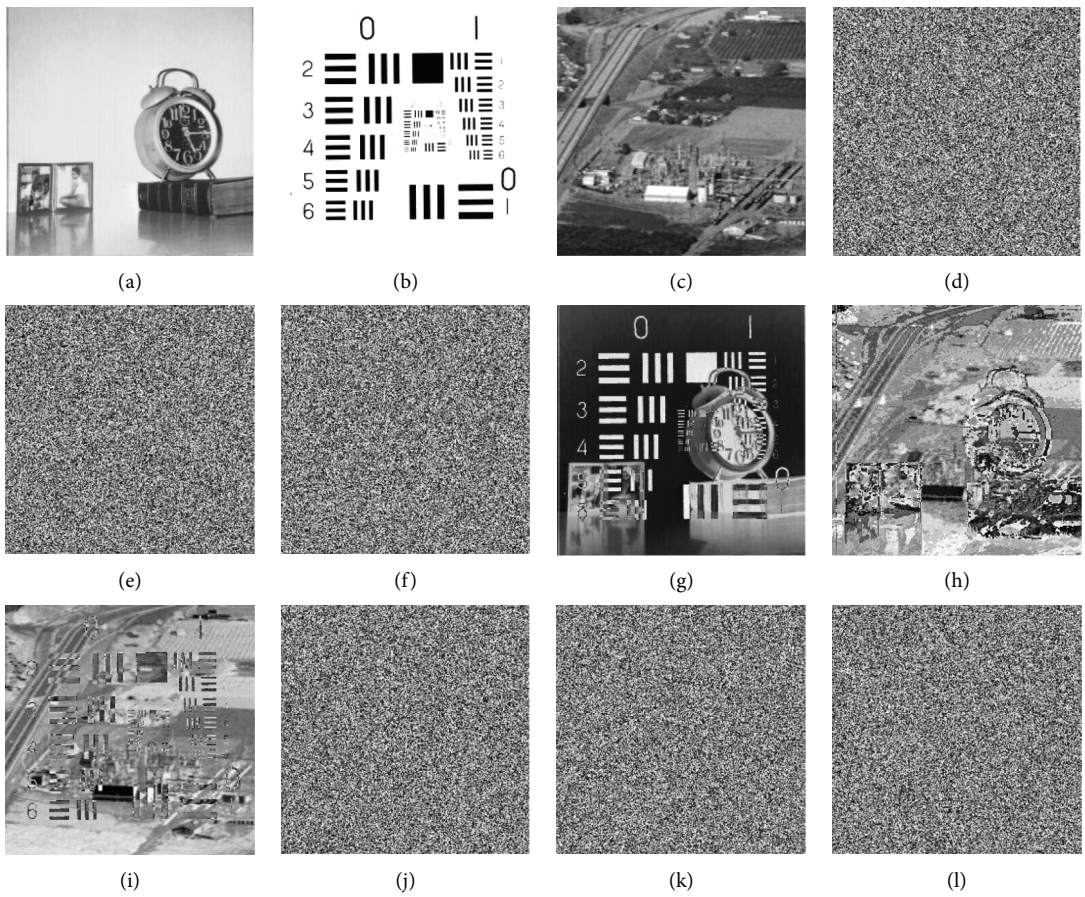


Figure 15: Chosen plaintext attack analysis. (a) 5.1.09. (b) 5.1.10. (c) 5.1.11. (d) Encrypted 5.1.09. (e) Encrypted 5.1.10. (f) Encrypted 5.1.11. (g) 5.1.09 xor 5.1.10. (h) 5.1.09 xor 5.1.11. (i) 5.1.10 xor 5.1.11. (j) Encrypted 5.1.09 xor encrypted 5.1.10. (k) Encrypted 5.1.09 xor encrypted 5.1.11. (l) Encrypted 5.1.10 xor encrypted 5.1.11.

Table 2: Differential attack analysis of IM-TPSC.

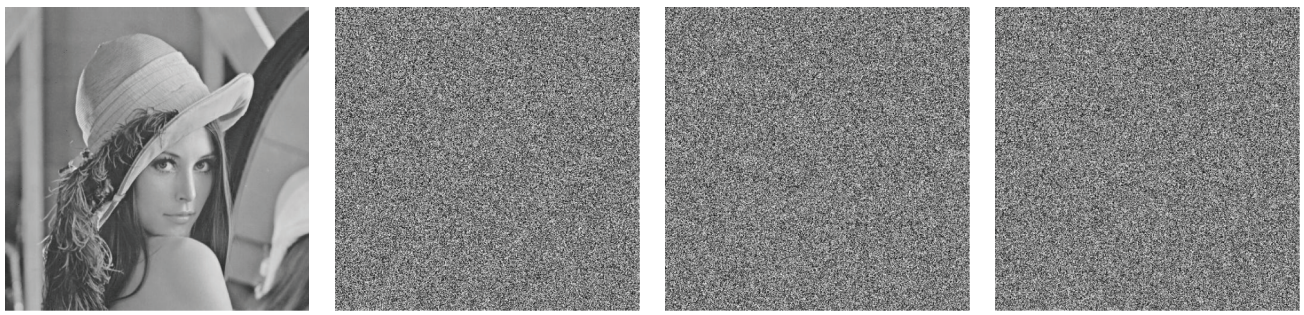
| Image | NPCR (%) | Pass or no pass | UACI (%) | Pass or no pass |
|---|---|---|---|---|
| Lena | 99.6055 | Pass | 33.4325 | Pass |
| Plane | 99.6002 | Pass | 33.4730 | Pass |
| Black | 99.6158 | Pass | 33.4565 | Pass |
| White | 99.5992 | Pass | 33.4325 | Pass |
| 5.1.09 | 99.6022 | Pass | 33.5235 | Pass |
| 5.1.10 | 99.6038 | Pass | 33.4963 | Pass |
| 5.1.11 | 99.6099 | Pass | 33.4664 | Pass |
| 5.1.12 | 99.6002 | Pass | 33.5099 | Pass |
| 5.1.13 | 99.6108 | Pass | 33.5317 | Pass |
| 5.1.14 | 99.6121 | Pass | 33.4780 | Pass |

$$N\rho_1 = 0.132465 + 10^{-15},$$
$$N\rho_2 = 5.21345 + 10^{-15},$$
$$N\rho_2 = 5.21345 + 10^{-15}.$$

*4.7. Key Space.* The key of IM-TPSC includes the initial key $\rho_1, \rho_2, \rho_3$ and the revised key $k_1$. If the calculation accuracy of the computer is $10^{-15}$, then the key space of the IM-TPSC is $2^{256} \times 10^{15} \times 10^{15} \times 10^{15} \approx 2^{405}$. The keyspace of the IM-TPSC is compared with other algorithms which are shown in Table 3, this algorithm is more secure and can resist brute force attacks [38].

*4.8. Correlation Analysis.* Usually, the attacker will use a certain amount of pixel values to infer the distribution of the remaining pixel values through statistical analysis. This requires that the adjacent pixel correlation of the ciphertext has a very low correlation. The correlation analysis of the IM-TPSC is shown in Figure 17.

When the correlation of the images is small, the images show a divergent state. Visually, the adjacent pixels of the ciphertext have little correlation. The quantitative analysis results of the correlation are shown in Table 4, and the correlation calculation formula is



(a) (b) (c) (d)

Figure 16: Key sensitivity analysis. (a) Decrypted image with a correct key (b) Decrypted image with the wrong key of $N\rho_1$. (c) Decrypted image with the wrong key of $N\rho_2$. (d) Decrypted image with the wrong key of $N\rho_3$.

Table 3: Comparison of key space.

| Algorithms | IM-TPSC | Ref. [39] | Ref. [40] | Ref. [41] |
|---|---|---|---|---|
| Key space | $2^{405}$ | $2^{376}$ | $2^{256}$ | $2^{128}$ |

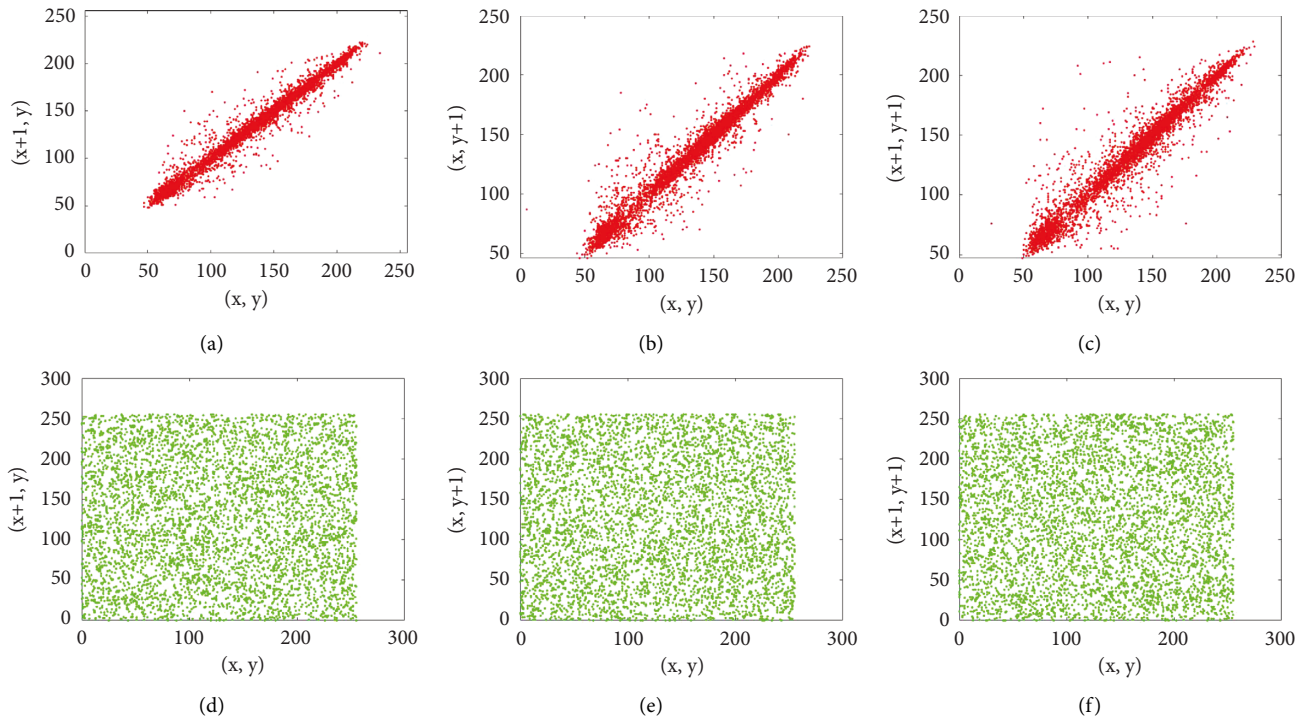



Figure 17: Correlation analysis for IM-TPSC of Lena. (a) Horizontal of plaintext. (b) Vertical of plaintext. (c) Diagonal of plaintext. (d) Horizontal of ciphertext. (e) Vertical of ciphertext. (f) Diagonal of ciphertext.

$$r_\rho = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x) \cdot D(y)}}. \tag{13}$$

Table 5 shows that the correlation of the ciphertext is very small, close to 0. It is shown that the IM-TPSC reduces the correlation between adjacent pixels of the image. In addition, the comparison results with some new algorithms ([42]) are shown in Table 5. Neighboring pixels are less correlated, so IM-TPSC is more secure and more resistant to statistical attacks.

*4.9. Information Entropy Analysis.* Information entropy reflects the uncertainty of information. Information entropy is described as

$$H = \sum_{i=0}^{255} p(g_i) \log_2 \frac{1}{p(g_i)}. \tag{14}$$

The theoretical value of information entropy is 8. When the information entropy is closer to 8, it indicates that the information distribution is more chaotic. The

Table 4: Correlation coefficients of IM-TPSC.

| Image | Plaintext | | | Ciphertext | | |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Lena | 0.9710 | 0.9847 | 0.9588 | −0.0001 | −0.0004 | −0.0008 |
| Plane | 0.9663 | 0.9641 | 0.9370 | 0.0002 | −0.0015 | −0.0012 |
| Black | 1 | 1 | 1 | 0.0027 | 0.0003 | −0.0008 |
| White | 1 | 1 | 1 | 0.0011 | 0.0025 | 0.0014 |
| 5.1.09 | 0.9020 | 0.9390 | 0.9037 | −0.0042 | −0.0072 | −0.0030 |
| 5.1.10 | 0.9050 | 0.8602 | 0.8213 | 0.0059 | −0.0027 | −0.0024 |
| 5.1.11 | 0.9571 | 0.9366 | 0.8927 | −0.0029 | 0.0065 | 0.0045 |
| 5.1.12 | 0.9565 | 0.9741 | 0.9389 | 0.0038 | −0.0010 | 0.0039 |
| 5.1.13 | 0.8722 | 0.8667 | 0.7562 | 0.0027 | −0.0028 | −0.0082 |
| 5.1.14 | 0.9466 | 0.8984 | 0.8529 | −0.0001 | −0.0028 | 0.0017 |

Table 5: Correlation coefficients of IM-TPSC.

| Algorithms | IM-TPSC | Ref. [42] | Ref. [43] | Ref. [44] | Ref. [45] |
|---|---|---|---|---|---|
| Horizontal | −0.0001 | −0.0005 | −0.0031 | 0.0020 | 0.0084 |
| Vertical | −0.0004 | 0.0008 | −0.0293 | 0.0038 | −0.0039 |
| Diagonal | −0.0008 | −0.0032 | 0.0077 | −0.0018 | −0.0013 |

information entropy analysis of the IM-TPSC is shown in Table 6. In addition, the comparison results with some new algorithms ([42]) are shown in Table 7. The information entropy analysis of the IM-TPSC shows that the information entropy of ciphertext is closer to the theoretical value than that of plaintext. Therefore, the IM-TPSC can make information distribution more chaotic. The comparison results with the information entropy of some new algorithms show that the information entropy of this paper is closer to the theoretical value, so the IM-TPSC has better security.

The local information entropy represents the characteristics of the local distribution of information and can represent the chaotic degree of the local information distribution. The local information entropy analysis of the IM-TPSC is shown in Table 8. The results of local information entropy analysis show that the ciphertext information obtained by the IM-TPSC is not only chaotic globally but also locally, so the IM-TPSC has better security.

*4.10. Efficiency Analysis.* The operating environment of the proposed algorithm is windows 10, MATLAB 2021a, i3-10105, 4 cores, 6 MB cache. Efficiency analysis of the proposed algorithm is shown in Table 9.

Efficiency analysis shows that the algorithm proposed in this paper has good efficiency. The proposed algorithm not only has high security but also high efficiency, which is very suitable for practical applications.

*4.11. Visualization of Color Images.* IM-TPSC is generalized from gray image encryption to color image encryption [50]. The three channels of the color image are encrypted respectively and the ciphertext color image is synthesized. A visual analysis of color image encryption is shown in Figure 18. Visually, the ciphertext image does not contain any plaintext information. This shows that IM-TPSC also has high security in color images.

Table 6: Information entropy of IM-TPSC.

| Image | Plaintext | Ciphertext |
|---|---|---|
| Lena | 7.2185 | 7.9994 |
| Plane | 6.7059 | 7.9993 |
| Black | 0 | 7.9993 |
| White | 0 | 7.9993 |
| 5.1.09 | 6.7093 | 7.9972 |
| 5.1.10 | 7.3118 | 7.9970 |
| 5.1.11 | 6.4523 | 7.9970 |
| 5.1.12 | 6.7057 | 7.9973 |
| 5.1.13 | 1.5483 | 7.9970 |
| 5.1.14 | 7.3424 | 7.9971 |

Table 7: Information entropy comparison of Lena.

| Algorithms | IM-TPSC | Ref. [42] | Ref. [43] | Ref. [44] | Ref. [45] |
|---|---|---|---|---|---|
| Information entropy | 7.9994 | 7.9987 | 7.9993 | 7.9973 | 7.9973 |

Table 8: Local information entropy.

| Image | Local information entropy | Result |
|---|---|---|
| Lena | 7.9028 | Pass |
| Plane | 7.9029 | Pass |
| Black | 7.9021 | Pass |
| White | 7.9029 | Pass |
| 5.1.09 | 7.9026 | Pass |
| 5.1.10 | 7.9020 | Pass |
| 5.1.11 | 7.9022 | Pass |
| 5.1.12 | 7.9025 | Pass |
| 5.1.13 | 7.9029 | Pass |
| 5.1.14 | 7.9029 | Pass |

Table 9: Efficiency analysis of the image $512 \times 512$.

| Methods | Time/s |
|---|---|
| 1D-TPSC | 1.0231 |
| Ref. [46] | 1.3300 |
| Ref. [47] | 13.5600 |
| Ref. [48] | 2.0400 |
| Ref. [49] | 1.9000 |


Figure 18: Visualization of color images. (a) Color Lena ($512 \times 512$). (b) Encrypted color Lena. (c) Decrypted color Lena. (d) Color plane ($512 \times 512$). (e) Encrypted color plane. (f) Decrypted color plane.

## 5. Conclusion and Outlook

In this paper, a new one-dimensional chaotic system is designed called 1D-TPSC. Through the Lyapunov exponent, bifurcation graph, sensitivity analysis, spider graph, and NIST test, it is verified that the key stream generated by one-dimensional TPSC has good randomness and is very suitable for cryptosystems. In addition, one-dimensional TPSC is a chaotic system with a simple structure and complex dynamic behavior. It has two control parameters, and cryptosystems that use 1D-TPSC to generate the keystream have a larger key space. An image encryption algorithm based on 1D-TPSC is designed. Through key analysis, statistical analysis, robustness analysis, efficiency analysis, and other methods, it is verified that the proposed encryption algorithm has high security and can resist common attacks such as brute force attacks, statistical attacks, and noise attacks.

Although 1D-TPSC exhibits good performance, its parameter space in a chaotic state is not globally continuous, and this structure will limit the design of secret keys in cryptosystems. Therefore, in future work, we will improve 1D-TPSC so that its parameter space in the chaotic state is globally continuous.

## Data Availability

The data used to support the findings of this study are included within the article.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This research was supported by the Natural Science Foundation of Shandong Province (ZR2020KF033).

## References

[1] C. Welba, D. Ramachandran, A. Noura et al., "Josephson junction model: FPGA implementation and chaos-based encryption of sEMG signal through image encryption technique," *Complexity*, vol. 2022, pp. 1–14, Article ID 4510236, 2022.

[2] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Information Sciences*, vol. 507, pp. 16–36, 2020.

[3] A. N. Kengnou Telem, C. Feudjio, B. Ramakrishnan, H. B. Fotsin, and K. Rajagopal, "A simple image encryption based on binary image affine transformation and zigzag process," *Complexity*, vol. 2022, Article ID 3865820, 22 pages, 2022.

[4] W. Xingyuan, G. Suo, Y. Xiaolin, Z. Shuang, and W. Mingxu, "A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system," *International Journal of Bifurcation and Chaos*, vol. 31, no. 01, Article ID 2150003, 2021.

[5] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, "Analytic study of a novel color image encryption method based on the chaos system and color codes," *Complexity*, vol. 2021, pp. 1–19, Article ID 5499538, 2021.

[6] F. Yu, S. Qian, X. Chen et al., "Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map," *Complexity*, vol. 2021, pp. 1–21, Article ID 6683284, 2021.

[7] C. Wang, B. Ma, Z. Xia, J. Li, Q. Li, and Y. Q. Shi, "Stereoscopic image description with trinion fractional-order continuous orthogonal moments," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 4, pp. 1998–2012, 2022.

[8] B. Ma and Y. Q. Shi, "A reversible data hiding scheme based on code division multiplexing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1914–1927, 2016.

[9] Q. Li, X. Wang, B. Ma et al., "Concealed attack for robust watermarking based on generative model and perceptual loss," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 8, pp. 5695–5706, 2022.

[10] X. Wang, X. Wang, B. Ma, Q. Li, and Y. Q. Shi, "High precision error prediction algorithm based on ridge regression predictor for reversible data hiding," *IEEE Signal Processing Letters*, vol. 28, pp. 1125–1129, 2021.

[11] S. Gao, R. Wu, X. Wang et al., "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Processing*, vol. 202, Article ID 108745, 2023.

[12] Z. Li, C. Peng, W. Tan, and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, pp. 1–18, Article ID 8824915, 2021.

[13] F. H. Hsiao, "Applying 3DES to chaotic synchronization cryptosystems," *IEEE Access*, vol. 10, pp. 1036–1050, 2022.

[14] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[15] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Optics & Laser Technology*, vol. 121, Article ID 105777, 2020.

[16] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[17] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, 2016.

[18] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[19] D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation," *Entropy*, vol. 23, no. 3, p. 361, 2021.

[20] X. Wang and S. Gao, "Application of matrix semi-tensor product in chaotic image encryption," *Journal of the Franklin Institute*, vol. 356, no. 18, pp. 11638–11667, 2019.

[21] X. Wang and S. Gao, "A chaotic image encryption algorithm based on a counting system and the semi-tensor product," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10301–10322, 2021.

[22] Y. Shi, Y. Hu, and B. Wang, "Image encryption scheme based on multiscale block compressed sensing and Markov model," *Entropy*, vol. 23, no. 10, p. 1297, 2021.

[23] P. Ping, X. Yang, X. Zhang, Y. Mao, and H. Khalid, "Generating visually secure encrypted images by partial block pairing-substitution and semi-tensor product compressed sensing," *Digital Signal Processing*, vol. 120, Article ID 103263, 2022.

[24] Y. Su and X. Wang, "A robust visual image encryption scheme based on controlled quantum walks," *Physica A: Statistical Mechanics and Its Applications*, vol. 587, Article ID 126529, 2022.

[25] C. H. Lin, J. X. Wu, P. Y. Chen et al., "Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity," *IEEE Access*, vol. 9, pp. 118624–118639, 2021.

[26] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[27] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, p. 147, 2020.

[28] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13841–13864, 2021.

[29] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4D hyperchaotic memristive system and application in color image encryption," *Eurasip Journal on Image and Video Processing*, vol. 2019, no. 1, 2019.

[30] M. Taheri, C. Zhang, Z. R. Berardehi, Y. Chen, and M. Roohi, "No-chatter model-free sliding mode control for synchronization of chaotic fractional-order systems with application in image encryption," *Multimedia Tools and Applications*, vol. 81, no. 17, pp. 24167–24197, 2022.

[31] X. Wang and M. Zhang, "An image encryption algorithm based on new chaos and diffusion values of a truth table," *Information Sciences*, vol. 579, pp. 128–149, 2021.

[32] B. Yosefnezhad Irani, P. Ayubi, F. Amani Jabalkandi, M. Yousefi Valandar, and M. Jafari Barani, "Digital image scrambling based on a new one-dimensional coupled Sine map," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2693–2721, 2019.

[33] H. Zang, X. Zhao, and X. Wei, "Construction and application of new high-order polynomial chaotic maps," *Nonlinear Dynamics*, vol. 107, no. 1, pp. 1247–1261, 2022.

[34] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Mendez-Ramirez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.

[35] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Information Sciences*, vol. 550, pp. 13–26, 2021.

[36] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[37] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology," *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[38] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, and C. Cruz-Hernandez, "Suggested integral analysis for chaos-based image cryptosystems," *Entropy*, vol. 21, no. 8, p. 815, 2019.

[39] X. Wang, N. Guan, and P. Liu, "A selective image encryption algorithm based on a chaotic model using modular sine arithmetic," *Optik*, vol. 258, Article ID 168955, 2022.

[40] Y. Ding, Z. Duan, and S. Li, "2D arcsine and sine combined logistic map for image encryption," *The Visual Computer*, 2022.

[41] X. Xu and S. Chen, "An optical image encryption method using hopfield neural network," *Entropy*, vol. 24, no. 4, p. 521, 2022.

[42] N. R. Pour and M. Yaghoobi, "A new method in encryption of gray scale images using chaos game representation," *Multimedia Tools and Applications*, vol. 81, no. 20, pp. 29653–29672, 2022.

[43] P. Ayubi, S. Setayeshi, and A. M. Rahmani, "Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, vol. 52, Article ID 102472, 2020.

[44] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps," *Optics & Laser Technology*, vol. 143, Article ID 107326, 2021.

[45] J. Wang, X. Zhi, X. Chai, and Y. Lu, "Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 16087–16122, 2021.

[46] A. Banik, D. S. Laiphrakpam, A. Agrawal, and R. Patgiri, "Secret image encryption based on chaotic system and elliptic curve cryptography," *Digital Signal Processing*, vol. 129, Article ID 103639, 2022.

[47] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018.

[48] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2020.

[49] P. Parida, C. Pradhan, X. Z. Gao, D. S. Roy, and R. K. Barik, "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," *IEEE Access*, vol. 9, pp. 76191–76204, 2021.

[50] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. Lopez-Gutierrez, and O. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.