symmetry

MDPI

Article

Applicable Image Security Based on New Hyperchaotic System

Jingya Wang [1], Xianhua Song [1,2,*], Huiqiang Wang [2] and Ahmed A. Abd El-Latif [3]

[1] School of Science, Harbin University of Science and Technology, Harbin 150080, China; 2020900017@stu.hrbust.edu.cn
[2] School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China; wanghuiqiang@hrbeu.edu.cn
[3] Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt; aabdellatif@nu.edu.eg
* Correspondence: songxianhua@hrbust.edu.cn

Abstract: Hyperchaotic systems are widely applied in the cryptography domain on account of their more complex dynamical behavior. In view of this, the greatest contribution of this paper is that a two-dimensional Sine coupling Logistic modulated Sine (2D-SCLMS) system is proposed based on Logistic map and Sine map. By a series of analyses, including Lyapunov index (LE), 0–1 test, two complexity analysis methods, and two entropy analysis methods, it is concluded that the new 2D-SCLMS map is hyperchaotic with a wider range of chaos and more complex randomness. The new system combined with two-dimensional Logistic-Sine Coupling Mapping (2D-LSCM) is further applied to an image encryption application. SHA-384 is used to generate the initial values and parameters of the two chaotic systems. Symmetric keys are generated during this operation, which can be applied to the proposed image encryption and decryption algorithms. The encryption process and the decryption process of the new image encryption approaches mainly include pixel scrambling, exclusive NOR (Xnor), and diffusion operations. Multiple experiments illustrate that this scheme has higher security and lower time complexity.

Keywords: chaotic systems; hyperchaotic systems; symmetric image encryption; security analysis

Citation: Wang, J.; Song, X.; Wang, H.; Abd El-Latif, A.A. Applicable Image Security Based on New Hyperchaotic System. *Symmetry* **2021**, *13*, 2290. https://doi.org/10.3390/sym13122290

Academic Editor: Christos Volos

Received: 29 October 2021
Accepted: 25 November 2021
Published: 1 December 2021

1. Introduction

Cryptography is a traditional and effective way to protect information security for a long time. According to whether the same key is used in the encryption and decryption processes, encryption can be divided into symmetric encryption and asymmetric encryption. Running symmetric encryption and decryption is relatively faster than the asymmetric encryption and decryption which usually takes a longer time. With the approach of 5G era, the amount of image data in wired and wireless communication nets is in the tens of thousands. Therefore, an efficient symmetric image encryption scheme becomes extremely important for protecting image security during storage and transmission.

Through the years, scholars have proposed multifarious image encryption schemes, such as a series of popularly known confusion and diffusion-based methods [1,2]. The framework structure of confusion and diffusion for image encryption was put forwarded by Fridrich in 1998 [3]. Confusion is usually achieved by permuting pixel control by keys without changing pixel values. Nevertheless, diffusion guarantees that altering one original pixel will cause several encrypted pixels to change.

Multifarious chaotic systems have been extensively applied to diverse fields [4–11] over the years because of their excellent properties [12–15]. Many scholars have designed robust and complex image encryption algorithms by using chaotic systems and the excellent characteristics of chaos [16–25]. When changing the initial parameters of the chaotic map, we can obtain totally different chaotic sequences. However, the premise for applying a chaotic map to image encryption is that it should have a large parameter space. Unfortunately, some classical maps, like Tent and Logistic maps, are chaotic only within a small

scope of parameters. Therefore, it is essential to improve them to generate chaotic maps with more complex properties [26]. Hua et al. [27] proposed 2D-SLMM combined with CMT for image encryption. Zhu et al. [28] designed LSMCL map and combined with the substitution and diffusion methods for image encryption. Although the dimensionalities of these proposed chaotic systems are higher than those of the classical maps, their chaotic trajectories still do not spread over the whole space and their parameter space is not very large. Therefore, a new 2D system with larger parameter space and excellent chaotic properties is put forward.

To strengthen the safety of the chaotic systems and the formation of confusion- and diffusion-based image encryption, we put forward a new Sine-coupling-Logistic-modulated-Sine system based on two one-dimensional maps, which expands the results from one-dimensional to two-dimensional. To verify the better performance of the newly designed 2D-SCLMS map compared to many existing chaotic maps, the dynamics of the newly designed 2D-SCLMS map is analyzed from multiple perspectives, including chaotic trajectory, bifurcation diagram, Lyapunov exponent, two complexity analysis methods [29,30], 0–1 test [31,32], sample entropy, and permutation entropy [33]. Experimental tests show that 2D-SCLMS is a hyperchaotic system and has a wider chaotic range and better randomness.

Besides, a new symmetric encryption scheme using two new chaotic systems, which includes 2D-SCLMS map and 2D-LSCM [34], is further introduced. The procedure of the encryption scheme is realized by pixel scrambling, Xnor, and diffusion. When scrambling, we propose to scramble the image by combining the indices of two chaotic sequences generated by the 2D-SCLMS system. Diffusion consists of two parts, row diffusion and column diffusion. We make use of two other chaotic sequences to perform the row and column diffusion respectively. In addition, the SHA-384 hash is used to produce the initial parameters of two systems, which greatly improves the resistance to known plaintext and chosen plaintext attacks [33,35].

The major contributions of this paper are as follows: (1) A new two-dimensional hyperchaotic map is designed based on Logistic and Sine maps. (2) Various methods, such as chaotic trajectory, Lyapunov exponent, 0–1 test, complexity analysis methods, and two different entropy analysis methods, are used to evaluate the chaotic properties of the new two-dimensional hyperchaotic map. (3) According to the two chaotic maps, a new symmetric encryption scheme for improving image security is proposed.

The rest of this article is arranged as follows. Section 2 states related works. Section 3 proposes the new 2D-SCLMS map and analyzes its chaotic behaviors. Section 4 presents the design of the new pixel scrambling method. Section 5 demonstrates the new symmetric image encryption algorithm. Section 6 describes the corresponding image decryption process. Section 7 presents simulation experiments and safety performance analysis. Section 8 shows color image encryption. Section 9 introduces the application areas of encryption algorithms. Section 10 provides the conclusion.

2. Related Works

This section first introduces two proposed chaotic maps, which constitute the basis for creating the 2D-SCLMS map. Then, another chaotic system 2D-LSCM for image encryption algorithm is described.

2.1. Logistic Map

Pierre François Verhulst denominated this map as the Logistic map [36]. It is known for its complex dynamic properties and has been widely used in different domains. In general, the expression of a 1D Logistic map [37] is

$$x_{i+1} = 4\mu(x_i - {x_i}^2) \tag{1}$$

where $\mu \in (0, 1)$ is the parameter. $x_i \in (0, 1)$, $i = 1, 2, \cdots$.

2.2. Sine Map

A variation of the sine function is Sine map whose input is converted from [0, π] to [0, 1] and whose output range [0, 1] remains unchanged. The expression of the Sine map is described as [38]:

$$x_{i+1} = \lambda \sin(\pi x_i) \tag{2}$$

where $\lambda \in (0, 1)$ is a parameter. $x_i \in (0, 1)$, $i = 1, 2, \cdots$.

2.3. 2D-LSCM

In this paper, 2D-LSCM is used as one of the chaotic systems of the encryption algorithm. The expression of the 2D-LSCM [34] is

$$\begin{cases} z_{i+1} = \sin(\pi(4\alpha(z_i - z_i^2) + (1-\alpha)\sin(\pi w_i))) \\ w_{i+1} = \sin(\pi(4\alpha(w_i - w_i^2) + (1-\alpha)\sin(\pi z_{i+1}))) \end{cases} \tag{3}$$

where $\alpha \in [0, 1]$ is a parameter.

3. 2D-SCLMS Map

We propose a novel Sine-coupling-Logistic-modulated-Sine map, in view of Logistic and Sine maps. To verify the better chaotic performance of the newly 2D-SCLMS map, efficient analysis and comparison are implemented in this section.

3.1. The Newly 2D-SCLMS Map

In fact, Logistic and Sine maps have good chaotic performances only in a suitable range of parameters and they also have some drawbacks, such as simple chaos and small chaotic range. Hence, it is relatively easy to forecast their trajectories using chaotic signal estimation techniques [39,40]. To overcome these drawbacks, a new 2D-SCLMS chaotic map with better chaotic properties is constructed in this paper. It is defined by Equation (4).

$$\begin{cases} x_{i+1} = \sin(4\pi^2(u\sin(4\pi(x_i - x_i^2))) + 4u(y_i - y_i^2)) \\ y_{i+1} = \sin(4\pi^2(u\sin(4\pi(y_i - y_i^2))) + 4u(x_{i+1} - x_{i+1}^2)) \end{cases} \tag{4}$$

where $u > 0.1$ is the parameter. $x_i, y_i \in (-1,1)$, $i = 1, 2, \cdots$.

3.2. Performance Analysis

The 2D-SCLMS map is innovated by combining Logistic and Sine maps and it is expanded to two dimensions. Therefore, the 2D-SCLMS map has more complex chaotic properties and its dynamics will be specified from several aspects.

3.2.1. Chaotic Trajectory

Chaotic trajectory is the motion track of the chaotic map over time for given parameters and initial values. Theoretically, the distribution of trajectories can prove to some extent the randomness of sequences. We set $x_0 = 0.1$, $y_0 = 0.1$, and the corresponding parameters. Figure 1 gives the trajectory diagrams of the newly 2D-SCLMS map, LSMCL, 2D logistic map and 2D-SLMM [28]. It can be obtained that chaotic trajectories of the new 2D-SCLMS map occupy a larger space, indicating that the map has better chaotic and track ergodicity.

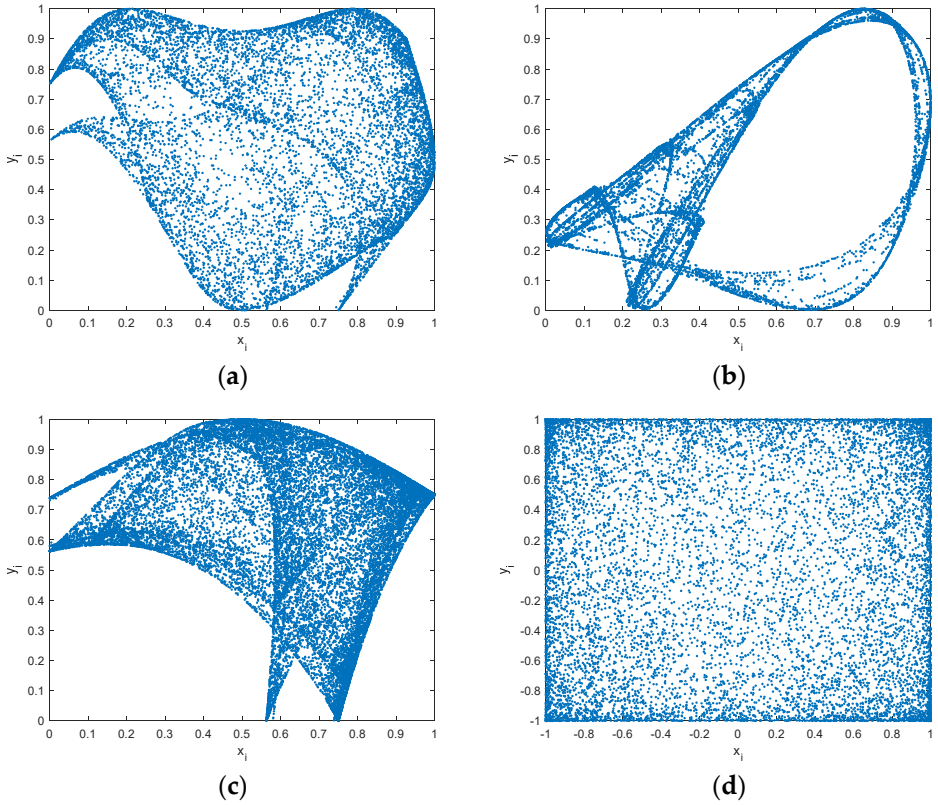


Figure 1. Chaotic trajectory. (**a**) LSMCL with $\alpha = 0.75$, $\beta = 3$; (**b**) 2D logistic map with $\omega = 1.19$; (**c**) 2D-SLMM with $\gamma = 1$, $\eta = 3$; (**d**) 2D-SCLMS with $u = 4$.

3.2.2. Bifurcation Diagram

The 2D-SCLMS map is chaotic when u is not in the vicinity of 0, which is drawn in Figure 2. However, as we all know, Logistic and Sine maps are in a chaotic state when the parameters are $\mu \in (0.89, 1)$ and $\lambda \in (0.87, 1)$ respectively. Thus, the 2D-SCLMS system exhibits chaos over a larger parameter interval.

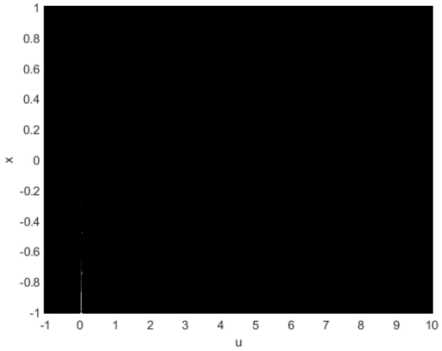


Figure 2. Bifurcation diagram.

3.2.3. Lyapunov Exponent

A significant index to evaluate the dynamical behavior of chaotic maps and a measurable way to represent the sensitivity of chaotic systems to initial values is the Lyapunov exponent. The LE of a 1D dynamic system is represented as

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|f'(x_i)| \tag{5}$$

A positive LE implies that the map is chaotic. A larger LE implies that the system has a better chaotic property. Besides, the number of positive LE of a hyper-chaotic system is not less than two. The LEs of the newly 2D-SCLMS map, LSMCL, 2D logistic map and 2D-SLMM [28] are demonstrated in Figure 3. It reveals that the 2D-SCLMS map has two positive LEs over a broader range of parameters. Therefore, the 2D-SCLMS map has a wider chaos range and more complex chaotic behavior.

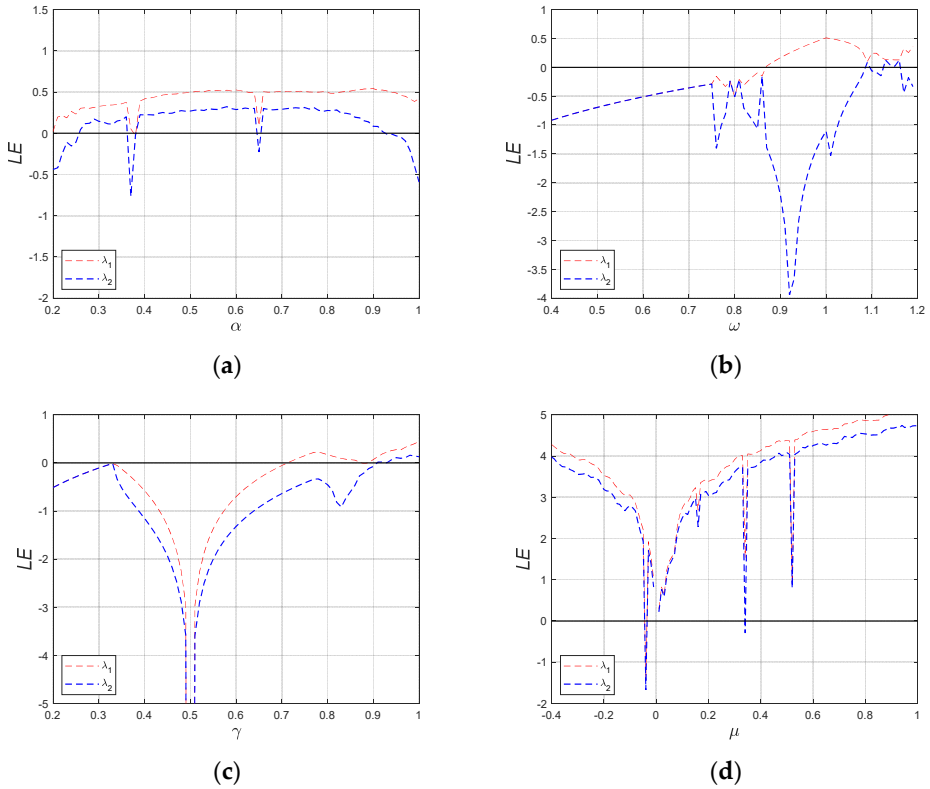


Figure 3. Lyapunov exponent. (**a**) LSMCL with $\beta = 3$; (**b**) 2D logistic map; (**c**) 2D-SLMM with $\eta = 3$; (**d**) 2D-SCLMS.

3.2.4. Complexity Analysis

A momentous index to appraise whether a chaotic sequence is close to a random sequence is the complexity. Under normal circumstances, a higher value of complexity implies that the chaotic sequence is closer to a random sequence. The spectral entropy (SE) complexity algorithm [29] and the C_0 structure complexity algorithm [30] are used to test complexity.

- SE complexity algorithm

The SE value is obtained based on the Shannon entropy algorithm. The process of the algorithm is shown below.

1. In order to make the calculated spectrum more precise, delete the DC part of $\psi(n)$ by Equation (6)

$$\psi(n) = \frac{N\psi(n) - \sum_{n=0}^{N-1} \psi(n)}{N} \tag{6}$$

wherein $n = 0, 1, 2, \ldots, N-1$.

2. Discrete Fourier transform of Equation (6) by Equation (7).

$$\Psi(s) = \sum_{n=0}^{N-1} \psi(n) e^{-j\frac{2\pi}{N}ns} = \sum_{n=0}^{N-1} \psi(n) W_N^{ns} \tag{7}$$

wherein $s = 0, 1, 2, \ldots, N-1$.

3. The sequence $\Psi(s)$ processed by the discrete Fourier transform is calculated by taking the first half of the sequence $\Psi(s)$ and using the Paserval algorithm to compute the power spectrum of one of the specific frequencies by Equation (8).

$$p(s) = \frac{1}{N}|\Psi(s)|^2 \tag{8}$$

where $s = 0, 1, 2, \ldots, N/2-1$. Calculate the total power by Equation (9).

$$p_{tot} = \frac{1}{N}\sum_{s=0}^{N/2-1}|\Psi(s)|^2 \tag{9}$$

The probability of the relative power spectrum is given by Equation (10)

$$P_s = \frac{p(s)}{p_{tot}} = \frac{\frac{1}{N}|\Psi(s)|^2}{\frac{1}{N}\sum_{s=0}^{N/2-1}|\Psi(s)|^2} = \frac{|\Psi(s)|^2}{\sum_{s=0}^{N/2-1}|\Psi(s)|^2} \tag{10}$$

In Equation (10), $\sum_{s=0}^{N/2-1} P_s = 1$.

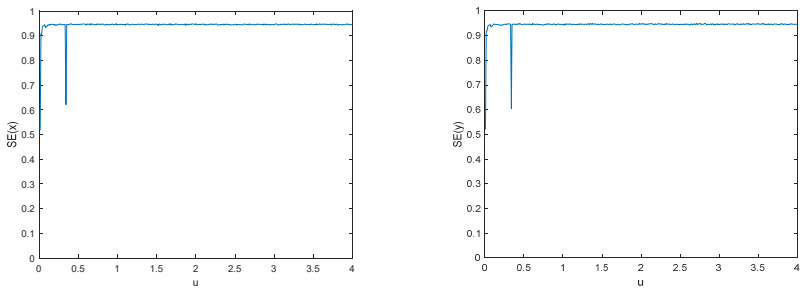
4. Using the above Equations (8)–(10) and combining the concept of Shannon entropy, the spectral entropy *se* of the signal can be found by Equation (11)

$$se = -\sum_{s=0}^{N/2-1} P_s \ln P_s \tag{11}$$

If $P_s = 0$ in the Equation (11), it is defined that $P_s \ln P_s = 0$. The magnitude of the SE tends to $\ln(N/2)$. To facilitate comparative analysis, normalization is implemented

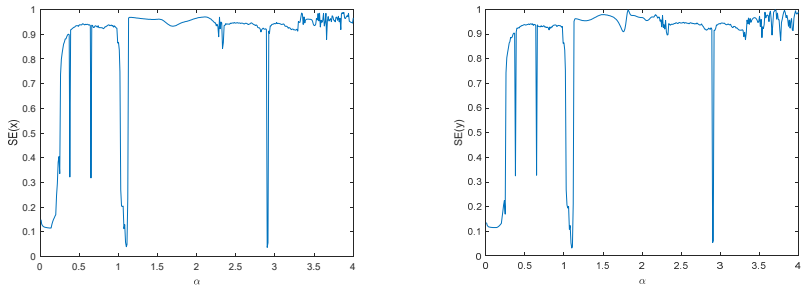
$$SE(N) = \frac{se}{\ln(N/2)} \tag{12}$$

Figure 4 shows the SE of the 2D-SCLMS map and LSMCL. Figure 4a,c are the *SE* values of the x sequence obtained by the 2D-SCLMS system and LSMCL respectively. Figure 4b,d are the *SE* values of the y sequence generated by the 2D-SCLMS map and LSMCL respectively. When $u > 0.35$, the value of SE is around 0.95, which is very close to 1. However, the SE of LSMCL are much smaller than the SE of the 2D-SCLMS map on several small intervals. This indicates that the 2D-SCLMS system has a higher complexity, i.e., the two sequences obtained by the new chaotic system are closer to the random sequence.



(**a**) (**b**)

Figure 4. *Cont.*



(**c**) (**d**)

Figure 4. SEs. (**a**) 2D-SCLMS with u–$SE(x)$; (**b**) 2D-SCLMS with u–$SE(y)$; (**c**) LSMCL with $\beta = 3$, α–$SE(x)$; (**d**) LSMCL with $\beta = 3$, α–$SE(y)$.

- C_0 structure complexity algorithm

The main idea of the C_0 complexity algorithm is to split the sequence into regular and irregular parts and what is wanted is the percentage of the irregular part of the whole chaotic sequence. The specific calculation steps of the C_0 complexity algorithm are as follows.

1. Discrete FFT transform of the sequence $\psi(n)$ by Equation (13)

$$\Psi(s) = \sum_{n=0}^{N-1} \psi(n) e^{-j\frac{2\pi}{N}ns} = \sum_{n=0}^{N-1} \psi(n) W_N^{ns} \tag{13}$$

wherein $s = 0, 1, 2, \ldots, N-1$.

2. Removing the irregular part of $\Psi(s)$, assume that the mean square value of $\{\Psi(s), s = 0, 1, 2, \ldots, N-1\}$ is Equation (14)

$$Q_N = \frac{1}{N} \sum_{s=0}^{N-1} |\Psi(s)|^2 \tag{14}$$

3. Adding a parameter η to the above equation and leaving more than η multiple of that mean square value, assuming the value of the remaining part is zero, i.e.,

$$\widetilde{\Psi}(s) = \begin{cases} \Psi(s), & |\Psi(s)|^2 > \eta Q_N \\ 0, & |\Psi(s)|^2 < \eta Q_N \end{cases} \tag{15}$$

4. Fourier inversion of Equation (15) by Equation (16)

$$\widetilde{\psi}(n) = \frac{1}{N} \sum_{s=0}^{N-1} \widetilde{\Psi}(s) e^{j\frac{2\pi}{N}ns} = \frac{1}{N} \sum_{s=0}^{N-1} \widetilde{\Psi}(s) W_N^{-ns} \tag{16}$$

wherein $n = 0, 1, 2, \ldots, N-1$.

5. The expression of the C_0 complexity measure is Equation (17)

$$C_0(\eta, N) = \frac{1}{\sum_{n=0}^{N-1} |\psi(n)|^2} \sum_{n=0}^{N-1} |\psi(n) - \widetilde{\psi}(n)|^2 \tag{17}$$

The C_0 complexity algorithm developed based on the FFT transform removes the regular part and retains the irregular part. The more irregular parts in the whole sequence, the closer the corresponding time domain signal is to the random sequence.

Figure 5 implies the C_0 complexity algorithm of the 2D-SCLMS map and LSMCL. Figure 5a,c are the C_0 values of the x sequence generated by the 2D-SCLMS map and LSMCL respectively. Figure 5b,d are the C_0 values of the y sequence generated by the

2D-SCLMS map and LSMCL respectively. When $u > 0.35$, the C_0 value of 2D-SCLMS map is very close to 1. However, the C_0 values of LSMCL are small. This indicates that 2D-SCLMS system has a high complexity, that is, the two sequences generated by 2D-SCLMS map are close to random sequences.

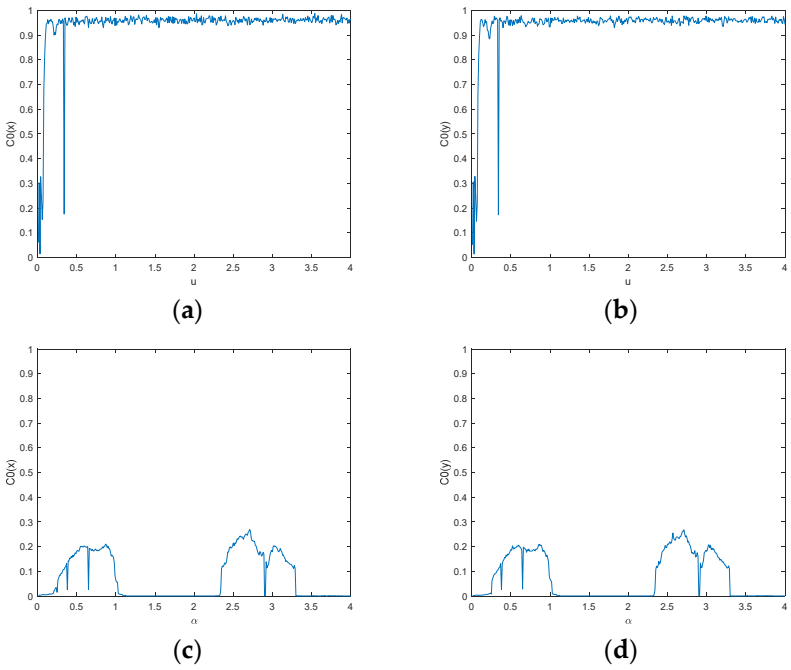


Figure 5. C_0 complexity algorithm. (**a**) 2D-SCLMS with u–$C_0(x)$; (**b**) 2D-SCLMS with u–$C_0(y)$; (**c**) LSMCL with $\beta = 3$, α–$C_0(x)$; (**d**) LSMCL with $\beta = 3$, α–$C_0(y)$.

3.2.5. 0–1 Test

The 0–1 test [31] is an reliable and useful binary algorithm to determine whether a system is chaotic or not, proposed by Gottwald and Melbourne [32]. The 0–1 test is a direct method to determine whether a system is chaotic or not by calculating whether the linear growth rate K_c values of the discrete data transformation variables are close to 1 or 0, without the need of phase space reconstruction.

For a sequence $\varphi(s)$ of length M and any real constant ζ, define two equations,

$$p(s) = \sum_{i=1}^{s} \varphi(i) \cos(i\zeta) \tag{18}$$

$$q(s) = \sum_{i=1}^{s} \varphi(i) \sin(i\zeta) \tag{19}$$

where $s = 1, 2, \ldots, M$.

According to Equations (18) and (19), the expression of the displacement mean squared error is Equation (20)

$$Q(s) = \lim_{M\to\infty} \frac{1}{M} \sum_{i=1}^{s} [p(i) - p(i+s)]^2 + [q(i) - q(i+s)]^2 \tag{20}$$

where $s = 1, 2, \ldots, M$.

It can be seen that it increases linearly with time or that it is bounded, especially, if $p(s)(q(s))$ is Brownian motion, which implies that $Q(s)$ increases linearly with time. If $p(s)(q(s))$ is bounded, which implies that $Q(s)$ is also bounded. Finally, the expression for K_c is Equation (21)

$$K_c = \lim_{s\to\infty} \frac{\log Q(s)}{\log s} \tag{21}$$

A dynamical system is considered non-chaotic when $K_c \approx 0$ and chaotic when $K_c \approx 1$.

For the 2D-SCLMS map, when setting the parameter $u = 3$ and the initial values $x_0 = 0.1$ and $y_0 = 0.5$, the 0–1 test is performed for each of the two sequences generated by the 2D-SCLMS system. We obtain the test results of the (p,q) plot, as shown in Figure 6. The results show that both sequence trajectories are similar to Brownian motion. Moreover, when $0 \leq u \leq 3$, the K_c values of both sequences are close to 1. Therefore, the 2D-SCLMS map is a chaotic system.

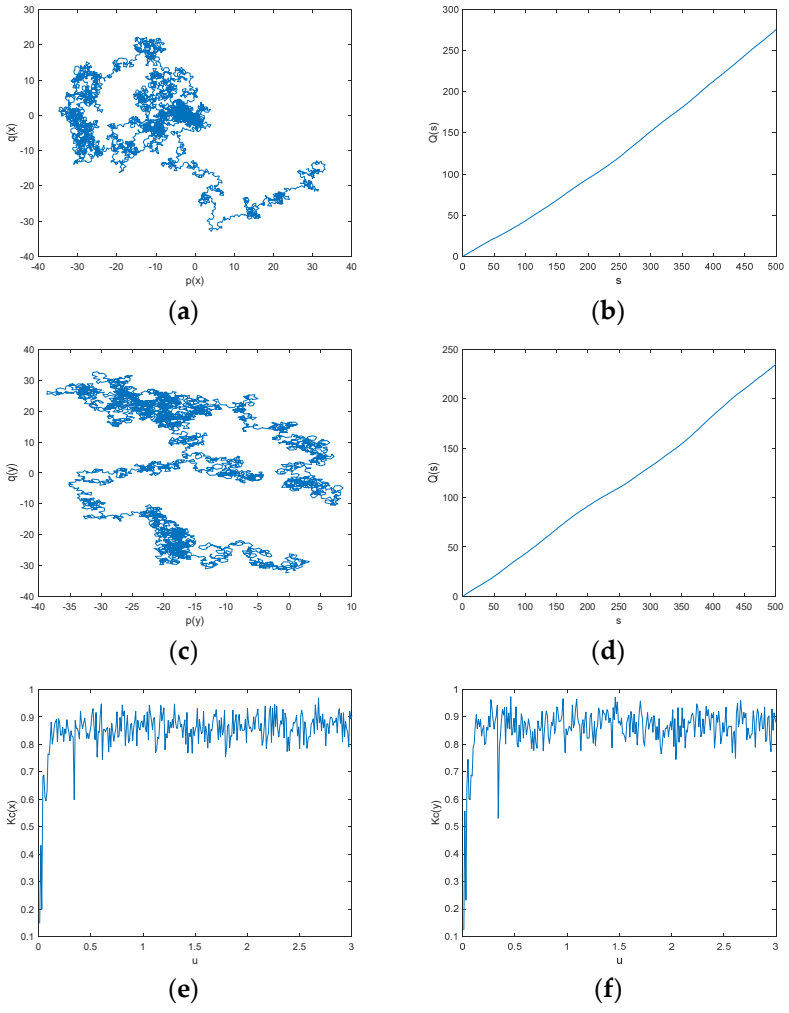


Figure 6. 0–1 test. (**a**) $p(x)$–$q(x)$; (**b**) s–$Q(x)$; (**c**) $p(y)$–$q(y)$; (**d**) s–$Q(y)$; (**e**) u–$K_c(x)$; (**f**) u–$K_c(y)$.

3.2.6. Sample Entropy

A method to assess the complexity of a system is sample entropy. For a sequence $U = \{u(1), u(2), \ldots, u(N)\}$, define parameters s, v.

Reconstructing s dimensional vectors $V(1), V(2), \ldots, V(N\text{-}s + 1)$, where $V(i) = [u(i), u(i + 1), \ldots, u(i + s - 1)]$

$$H_i^s = \frac{H}{N - s} \tag{22}$$

where H is the number of $V(i)$'s that satisfy the condition $d[V(i), V(j)] \leq v$

Find the average of the above equation for all i

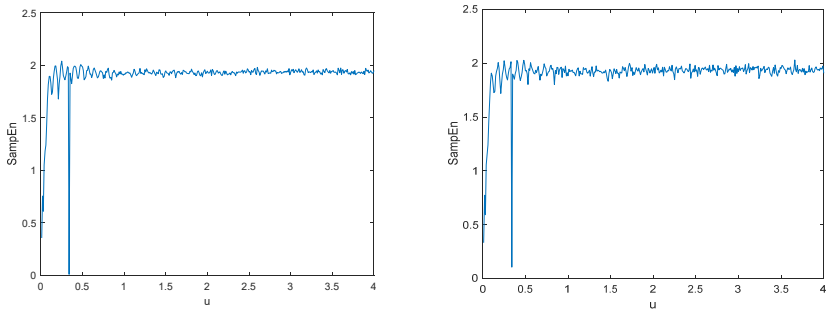
$$H^s(v) = \frac{\sum_{i=1}^{N-s+1} H_i^s(v)}{N - s + 1} \tag{23}$$

Set $g = s + 1$, repeating the above steps, we get $D^g(v)$

Then, the sample entropy is defined as

$$SampEn = -\ln \frac{D^g(v)}{H^s(v)} \tag{24}$$

Figure 7 implies the sample entropy of two sequences generated by the 2D-SCLMS map separately. When $u > 0.35$, the sample entropy is close to 2, which indicates that the two sequences are chaotic sequences and the 2D-SCLMS map is a complex chaotic system.



(**a**) (**b**)

Figure 7. Sample entropy. (**a**) *u–SampEn*(x); (**b**) *u–SampEn*(y).

3.2.7. Permutation Entropy

A valid way to test the complexity of chaotic sequences is permutation entropy (PE) [33]. The range of PE is from 0 to 1. A larger PE indicates that the generated chaotic sequence is more complex.

In Figure 8, the PE value is very close to 1, which explains that the 2D-SCLMS system is a complex chaotic system.

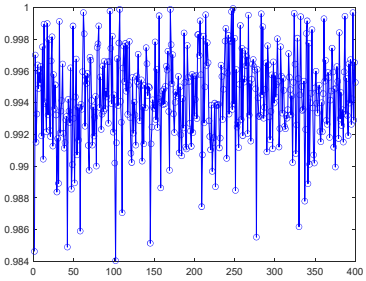


Figure 8. Permutation entropy.

In summary, this paper proposes a hyperchaotic system based on two existing chaotic maps, which has a larger parameter space and better chaotic properties than some existing chaotic maps. Based on this, the hyperchaotic system can be applied to encryption to provide convenience and security for image transmission. Therefore, a new symmetric image encryption algorithm based on this system is proposed in the paper.

4. Pixel Scrambling

Two matrices A, B are arranged in ascending order by columns to produce two position index matrices A_1, B_1. Let A_1 be the row index and B_1 be the column index, combined together to permute the matrix P. In this section, the 6×6 matrix is used as an example and the results are shown in Figure 9.

$$[\sim, A_1] = sort(A) \tag{25}$$

$$[\sim, B_1] = sort(B) \tag{26}$$

$$P_1 = scramble(P, [A_1, B_1]) \tag{27}$$

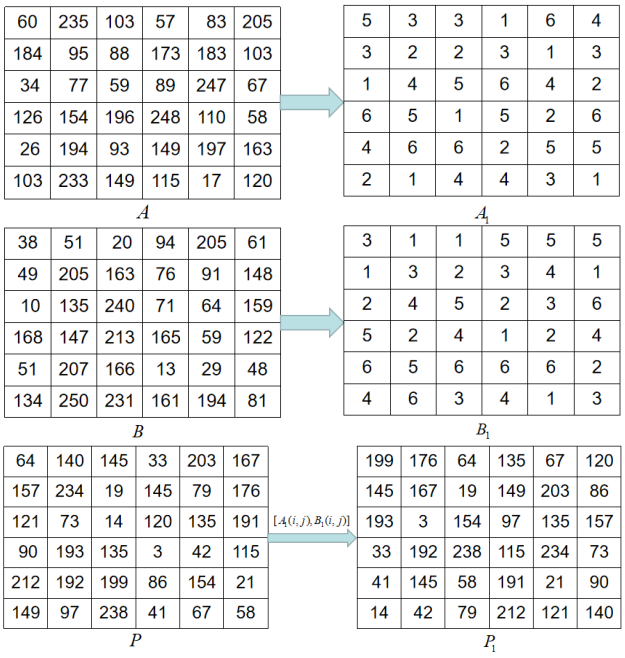


Figure 9. Pixel scrambling.

5. Image Encryption Algorithm

The paper expounds the symmetric encryption scenario based on 2D-LSCM and new 2D-SCLMS system and Figure 10 is the flowchart. The encryption step mainly includes pixel scrambling, Xnor, and diffusion.

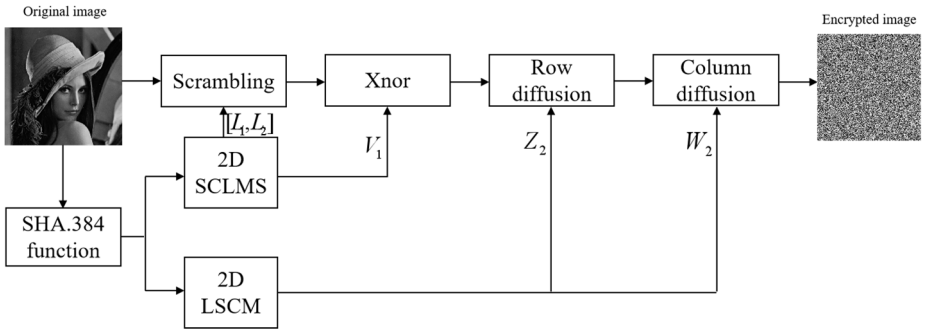


Figure 10. The encryption flowchart.

1. Generation of keys

To heighten the safety of the scenario and the relevance of keys to original image. The hash is utilized to create initial parameters of the two systems. The hash 384 algorithm is used to acquire a 384-bit hash value that can be converted into a sequence of 48 binary values $k_1, k_2, \ldots, k_{48}$. These values are computed by Equation (28)

$$\begin{cases} x_0 = mod((k_1 + k_2 + k_3 + k_4 + k_5 + k_6 + k_7 + k_8 + k_9 + k_{10}), 256)/256 + x_0' \\ y_0 = mod((k_{11} + k_{12} + k_{13} + k_{14} + k_{15} + k_{16} + k_{17} + k_{18} + k_{19} + k_{20}), 256)/256 + y_0' \\ u = mod((k_{21} + k_{22} + k_{23} + k_{24} + k_{25} + k_{26} + k_{27} + k_{28} + k_{29} + k_{30}), 256)/256 + u' \\ z_0 = mod((k_{31} + k_{32} + k_{33} + k_{34} + k_{35} + k_{36}), 256)/256 + z_0' \\ w_0 = mod((k_{37} + k_{38} + k_{39} + k_{40} + k_{41} + k_{42}), 256)/256 + w_0' \\ \alpha = mod((k_{43} + k_{44} + k_{45} + k_{46} + k_{47} + k_{48}), 256)/256 + \alpha' \end{cases} \quad (28)$$

where the parameters x_0', y_0', u', z_0', w_0', α' are symmetric keys.

2. Pixel scrambling

The initial values (x_0, y_0, u) are brought into the 2D-SCLMS map for MN + 500 iterations to generate two chaotic sequences x_n, y_n. The first 500 iterations are discarded in order to eliminate transient effects. First, the two sequences are processed separately to obtain two new sequences U, V.

$$\begin{aligned} u_i &= floor(mod(x_i \times 10^{10}, 256)) \\ v_i &= floor(mod(y_i \times 10^{10}, 256)) \end{aligned} \tag{29}$$

U, V sequences are converted to matrices U_1, V_1 respectively. The sequence U_1, V_1 are sorted in ascending order by each column to generate two position indexes L_1, L_2. As introduced in Section 4, let L_1 be the row index and L_2 be the column index, and combine them together to disrupt the original image matrix P to generate P_1.

3. Xnor

Perform the Xnor operation on matrix P_1 and matrix V_1 to generate matrix P_2.

$$P_2 = 255 - \mathrm{mod}(bitxor(V_1, P_1), 256) \tag{30}$$

4. Diffusion of rows

The initial values (z_0, w_0, α) are brought into the 2D-LSCM for MN + 500 iterations to generate two chaotic sequences z_n, w_n. The first 500 iterations are discarded in order to eliminate transient effects.

$$\begin{aligned} a_i &= round(mod(z_i \times 10^{14}, 256)) \\ b_i &= ceil(mod(w_i \times 10^{14}, 256)) \end{aligned} \tag{31}$$

A, B sequences are converted to matrices Z_2, W_2 respectively.

For the first column of P_2, $P_3(i, 1)$ is calculated via Equation (32)

$$P_3(i,1) = \mathrm{mod}(P_2(i,1) + P_2(i,N) + Z_2(i,1), 256) \tag{32}$$

For the other column of P_2, $P_3(i, j)$ is calculated using Equation (33)

$$P_3(i,j) = \mathrm{mod}(P_2(i,j) + P_3(i,j-1) + Z_2(i,j), 256) \tag{33}$$

5. Diffusion of columns

For the first row of P_3, $P_4(1, j)$ is calculated by Equation (34)

$$P_4(1,j) = \mathrm{mod}(P_3(1,j) + P_3(M,j) + W_2(1,j), 256) \tag{34}$$

For the other column of P_3, $P_4(i, j)$ is calculated by Equation (35)

$$P_4(i,j) = \mathrm{mod}(P_3(i,j) + P_4(i-1,j) + W_2(i,j), 256) \tag{35}$$

6. Image Decryption

The specific step is described below and drawn in Figure 11.

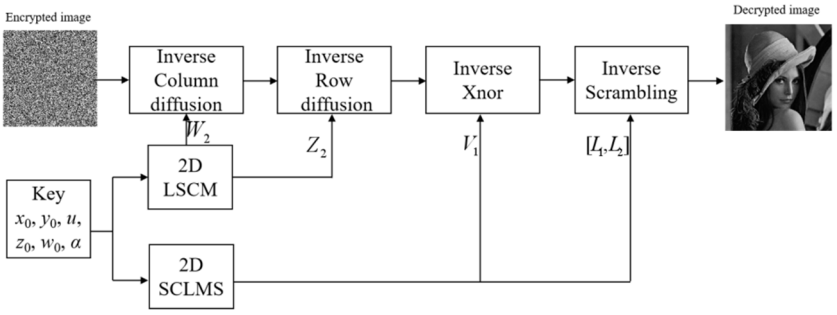


Figure 11. The decryption flowchart.

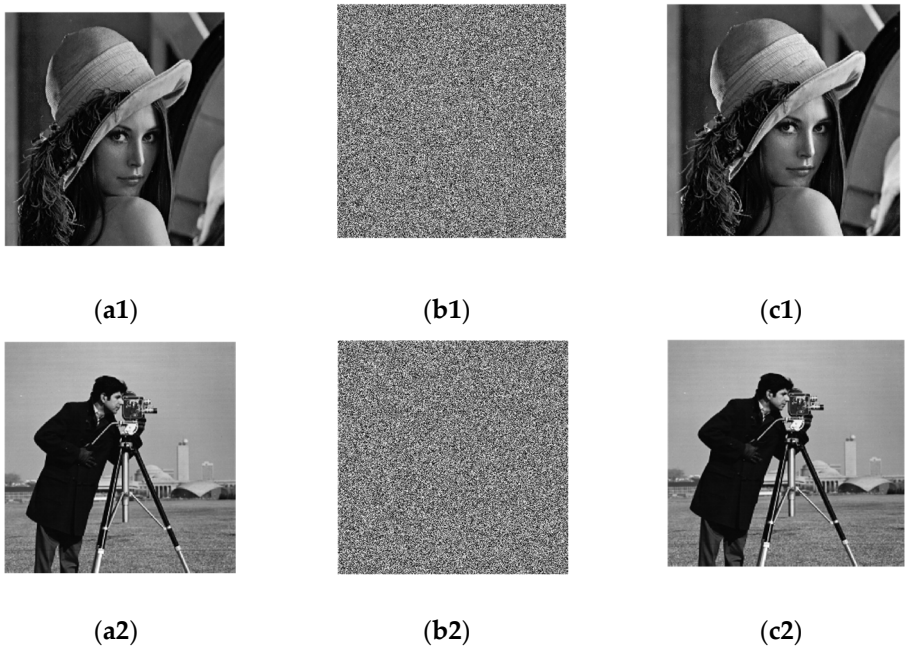
The image is obtained by performing the inverse operations of column diffusion, row diffusion, Xnor, and pixel scrambling on the ciphertext image in turn.

7. Experimental Results and Performance Analysis

To confirm the performance of the new symmetric encryption programme, all experiments are conducted on a PC with AMD Ryzen 2.00 GHz CPU, 8 G RAM, and 1 TB hard disk with Window 10 Ultimate system. This experiment is operated by MATLAB R2020a software. The selected images in this paper are all 512 × 512 in size.

7.1. Simulation Results

In this paper, we set the parameters x_0', y_0', z_0', w_0', and α' all to 0 and $u' = 1$. Six images are selected for testing. In Figure 12, each column is respectively the original, ciphertext and decrypted image. All the cipher images resemble noise and all of them can be decrypted successfully, which illustrates that the encryption algorithm is extremely secure.



(**a1**) (**b1**) (**c1**)

(**a2**) (**b2**) (**c2**)

Figure 12. *Cont.*

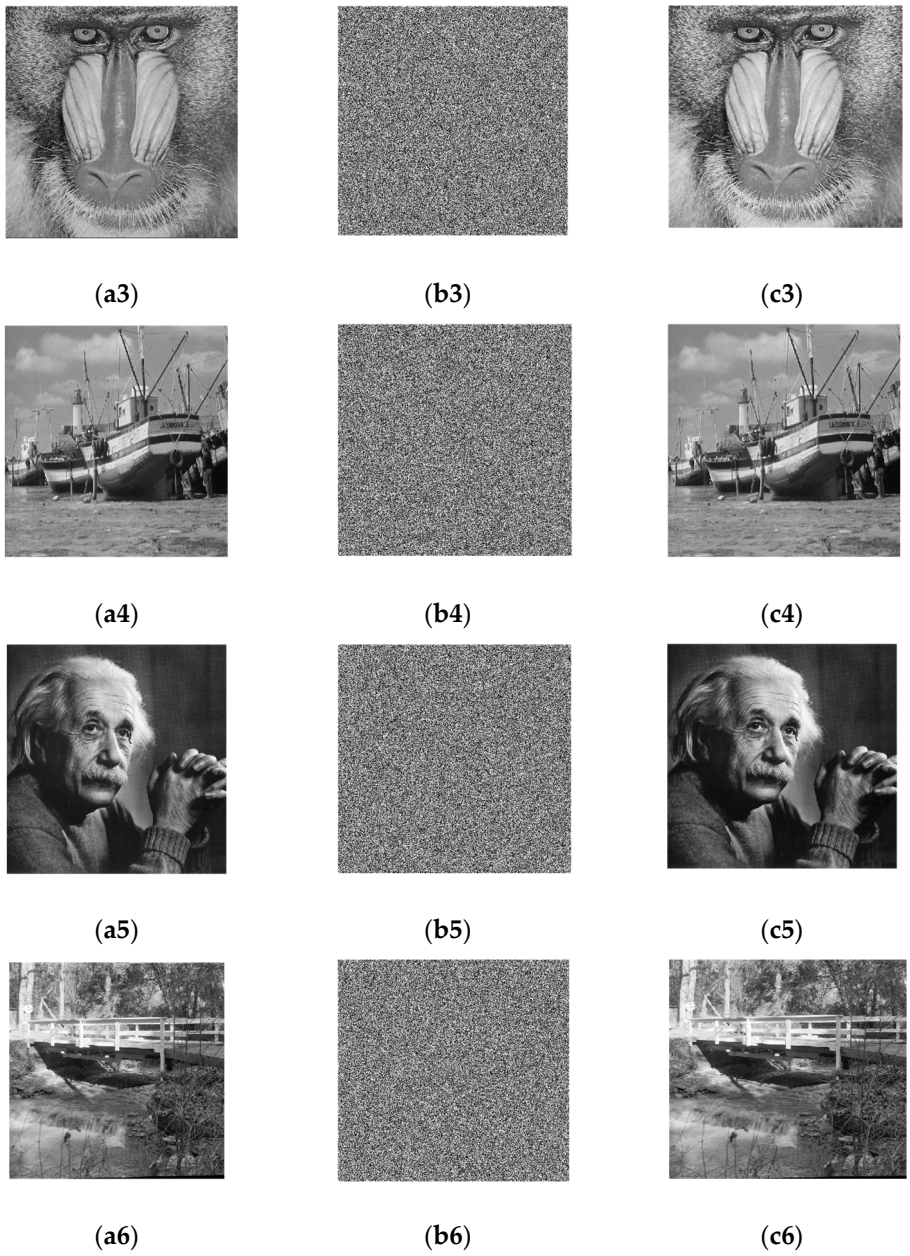


Figure 12. Illustration of image encryptions and decryptions. (**a1**–**a6**) Plain images; (**b1**–**b6**) Encrypted images; (**c1**–**c6**) Decrypted images.

7.2. Running Time (Complexity)

To verify that the new encryption scheme is practical and efficient, we calculated the time for the encryption algorithm and the decryption algorithm in Table 1. Table 1 demonstrates that the new encryption algorithm takes less time, which illustrates that the algorithm is practical and efficient. Table 2 shows the running time comparison between the encryption algorithm proposed in this paper and other encryption algorithms. It can be seen from Table 2 that the scheme proposed in this paper has an acceptable speed.

Table 1. Running time of encryption and decryption algorithms (unit: s).

Image	Lena	Couple	Cattle	Boat	Average
Encryption	0.5769	0.5858	0.6556	0.6426	0.615225
Decryption	0.6137	0.6136	0.6352	0.6519	0.6286

Table 2. The average running time of different encryption schemes (unit: s).

Scheme	Encryption Time	Microprocessor/RAM/O.S
Ref. [41]	11.005	2.53 GHz, 2 GB RAM, Windows 7 and Matlab R2012b
Ref. [42]	0.497	1.9 GHz, 4 GB RAM, Windows 7 and MATLAB 7.9
Ours	0.615	2.00 GHz, 8 GB RAM and 1 TB hard disk with, Window 10 and MATLAB R2020a

7.3. Information Entropy (IE)

Shannon proposed the entropy criterion in [43]. It is an indispensable tool [44] for testing the randomness of images before and after encryption. The expression of information entropy [45] is

$$H(s) = -\sum_{i=0}^{2^8-1} p(s_i) \log_2 p(s_i) \tag{36}$$

In Equation (36), $p(s_i)$ is the probability of s_i. Theoretically, the ideal value of IE is 8.

We test the IE of the new encryption scenario and compare it with other encryption algorithms on "Boat" image. For the IE, Table 3 demonstrates that the original image is around 7, while the encrypted image is almost nearly 8. Table 4 demonstrates that our scheme has the largest entropy value, which explains that the ciphertext image has better randomness.

Table 3. IE of multiple images.

Image	Lena	Couple	Cameraman	Boat	Einstein	Cattle
Plain	7.3920	7.2010	7.0480	7.1914	7.2655	7.3579
Encryption	7.9994	7.9993	7.9994	7.9993	7.9993	7.9993

Table 4. IE of different schemes.

Image	Ref. [27]	Ref. [41]	Ref. [42]	Ours
Boat	7.9959	7.99928	7.9980	7.9993

7.4. Key Space Analysis

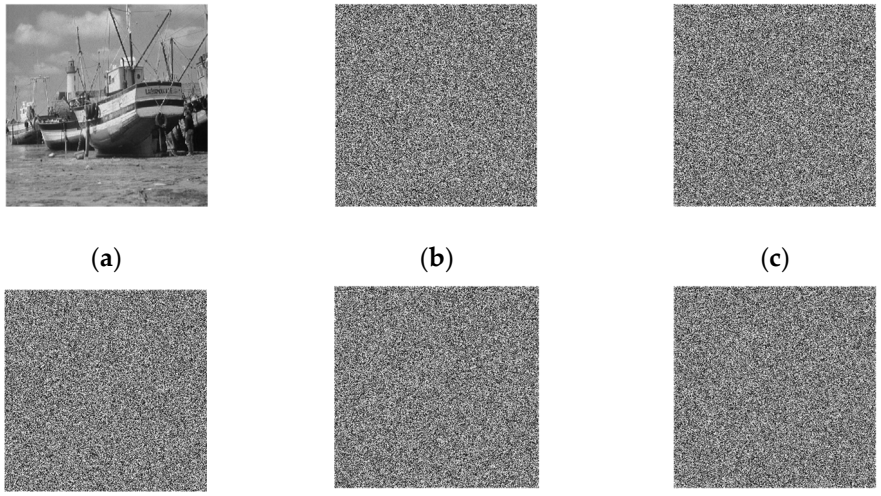
An excellent encryption scenario with a key space greater than 2^{100} is considered sufficient to oppose the most usual violent attack [46]. Then, the key of this scenario consists of a 384-bit hash values and initial keys x_0', y_0', u', z_0', w_0', α'. Suppose the calculation accuracy is 10^{-14}, the key space of this algorithm is $10^{14\times6} = 10^{84}$. In addition to that, we have the 384-bit stream generated by SHA-384, so the entire key space is resistant to violent attack.

7.5. Key Sensitivity Analysis

A slight change of key causes the decrypted image to be completely different. We encrypt the "Boat" using the correct key. After that, any one of these keys is changed slightly. Figure 13 displays the images under different key decryption. When keys change very little, the decrypted images resemble noise, which indicates that this scenario is extremely sensitive to all keys.

7.6. Histogram Analysis

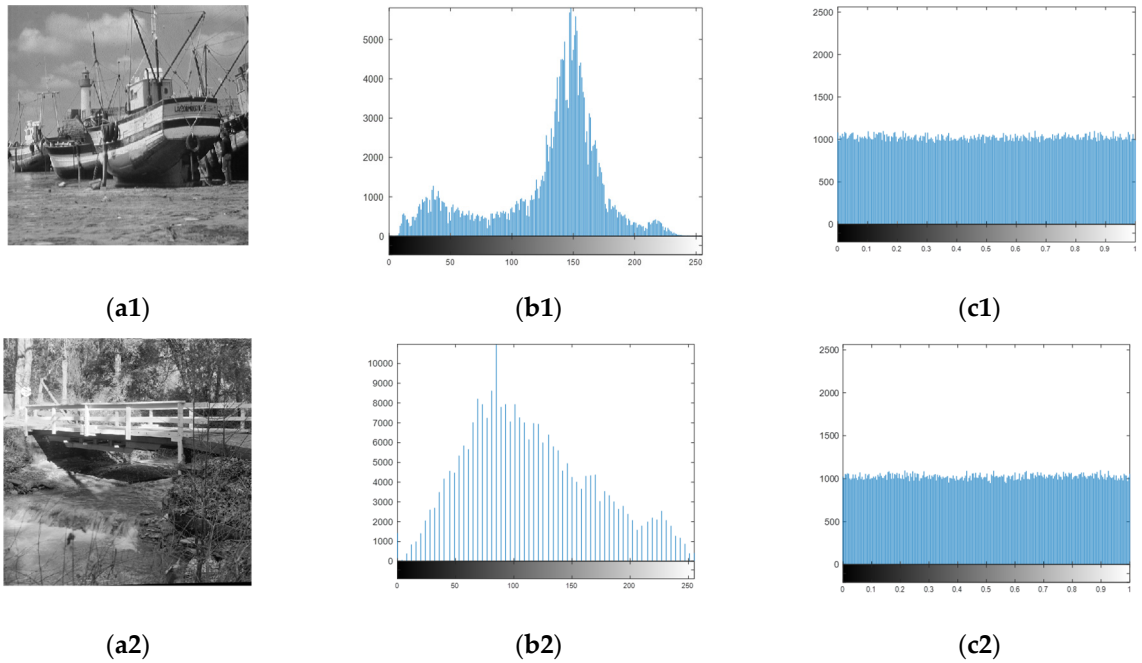
Normally, the histogram is nearly flat to resist statistical attacks. Obviously, the histogram of ciphertext images tends to be uniformly distributed in Figure 14, which indicates that this scenario is resistant to statistical attacks.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 13. Key sensitivity analysis. (**a**) Image decrypted with correct keys; (**b**) Decrypted image when $x_0{}'$ changes to $x_0{}' + 10^{-9}$; (**c**) Decrypted image when $y_0{}'$ changes to $y_0{}' + 10^{-9}$; (**d**) Decrypted image when u' changes to $u' + 10^{-9}$; (**e**) Decrypted image when $z_0{}'$ changes to $z_0{}' + 10^{-9}$; (**f**) Decrypted image when $w_0{}'$ changes to $w_0{}' + 10^{-9}$.



(**a1**) (**b1**) (**c1**)

(**a2**) (**b2**) (**c2**)

Figure 14. *Cont.*

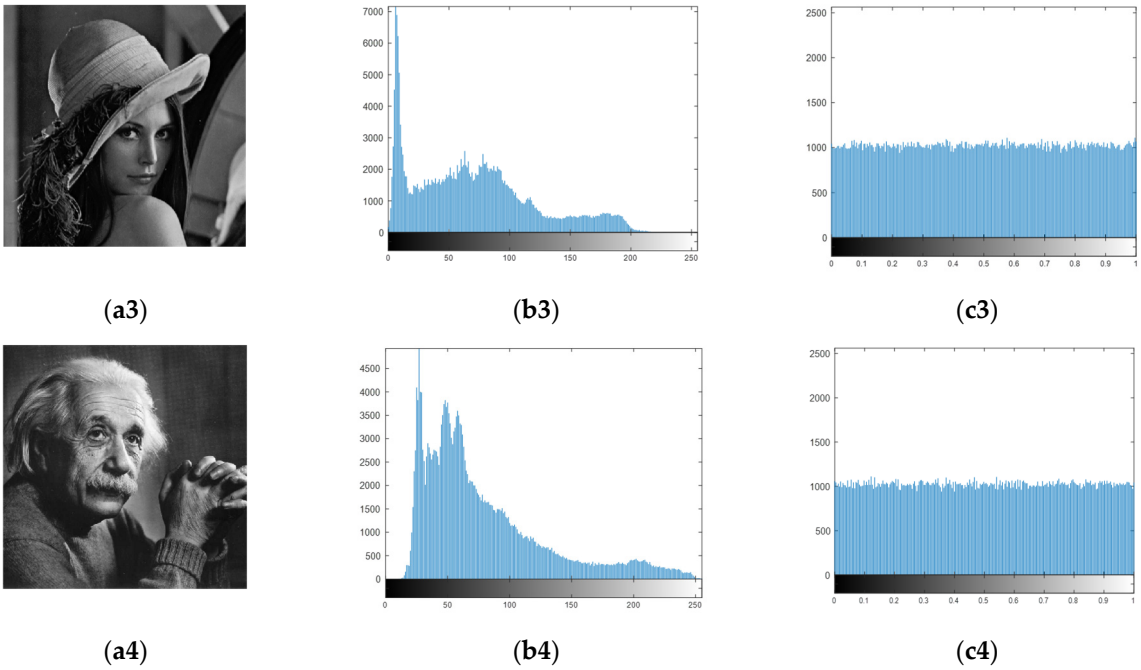


Figure 14. Histogram analysis. (**a1**–**a4**) Plain images; (**b1**–**b4**) Plain image histograms; (**c1**–**c4**) Encrypted image histograms.

7.7. Chi-Square Analysis

This paper utilizes a quantitative way to calculate the resistance of encryption scenario to statistical attacks, i.e., the chi-square test [47], whose expression is Equation (37).

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0} \tag{37}$$

where v_i is frequency occupied by grayscale value i. $v_0 = MN/256$. Table 5 shows the chi-square calculation results, where the first and second rows show the chi-square results of the encrypted and plain images, respectively. The chi-square of all encrypted images is less than 293.25 [34], which indicates that the encryption scheme is sufficient to defend against statistical attacks.

Table 5. Chi-square.

Image	Lena	Couple	5.2.10	Cattle	Boat
Chi-square	232.9199	261.8418	229.6328	262.5801	259.3848
	270,681.8	298,865.2	118,561.8	187,692.2	383,969.7

7.8. Correlation Analysis

The meaning of encryption is to decrease the correlation, which is expressed in Equations (38)–(41). This section arbitrarily selects 10,000 pairs of adjacent pixels x, y from the plain and encrypted images and calculates them in horizontal, vertical, and diagonal directions.

$$\rho_{xy} = \frac{1}{\sqrt{D(x)D(y)}} cov(x, y) \tag{38}$$

$$\mathrm{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{39}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{40}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{41}$$

Table 6 lists the correlation coefficients of multiple images. Table 7 compares the correlation coefficients of different encryption algorithms for the "Boat" image. Figure 15 reveals the correlation of the plain and ciphertext images of "Lena". The correlation of the plain image is diagonal in all directions, i.e., the correlation of the original image is very high. The correlation of the ciphertext image is scattered throughout the image, that is, the correlation of the ciphertext image is vastly abated, which demonstrates that the encryption scenario is very good.

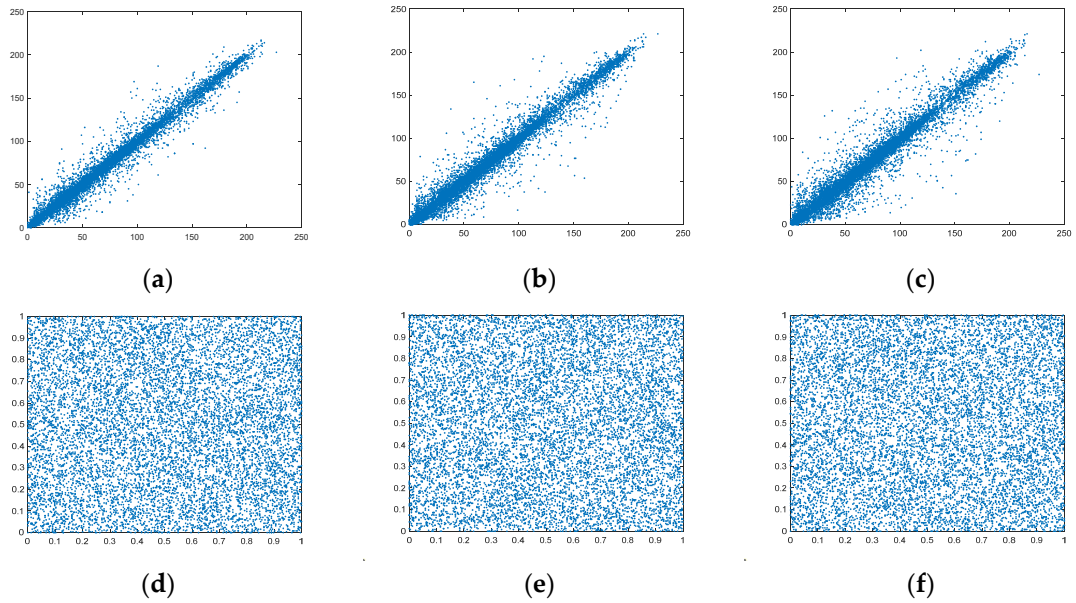


Figure 15. Correlation. (**a**) Plain image horizontal correlation; (**b**) Plain image vertical correlation; (**c**) Plain image diagonal correlation; (**d**) Encrypted image horizontal correlation; (**e**) Encrypted image vertical correlation; (**f**) Encrypted image diagonal correlation.

Table 6. Correlation coefficient of multiple images.

Image	Horizontal	Vertical	Diagonal
Lena	0.9840 0.0037	0.9835 −0.00027	0.9717 0.001
Cameraman	0.9853 0.0004	0.9870 −0.00006	0.9765 −0.00035
Boat	0.9833 0.0012	0.9727 0.000587	0.9617 −0.00003
Couple	0.9624 0.0046	0.9650 −0.00062	0.9386 0.000345
Einstein	0.9687 −0.0049	0.9644 0.0034	0.9548 −0.0013
Cattle	0.8573 0.0018	0.9103 0.0031	0.8423 0.000611

Table 7. Correlation coefficients of Boat for multiple algorithms.

Direction	Horizontal	Vertical	Diagonal
Ref. [27]	−0.0295	−0.015	−0.0224
Ref. [41]	0.009480	0.004406	−0.010305
Ref. [42]	−0.0100	−0.0124	−0.0185
Ours	0.0012	0.000587	−0.00003

7.9. Differential Attack Analysis

The value of pixel change rate (NPCR) [48,49] and the unified average change intensity (UACI) [50] are utilized to determine the ability of the new scheme against differential attacks, which are given by

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |Sign(C_1(i,j) - C_2(i,j))| \tag{42}$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{2^8 - 1} \tag{43}$$

The ideal NPCR and UACI values are respectively 0.996094 and 0.334635 for 256 gray level images [51,52]. Table 8 lists the NPCR and UACI values of the new scenario for several images and they are both approach desired value. The UACI of the new scenario is closer to 33.4635% than other algorithms in Table 9. Thus, this scenario is forceful against differential attacks.

Table 8. NPCR and UACI of multiple images.

Image	NPCR	UACI
Lena	0.996235	0.334444
Einstein	0.996117	0.334894
5.2.10	0.996239	0.334401
Cattle	0.996246	0.334874
Boat	0.995869	0.334856
Cameraman	0.996155	0.334441
Mean	0.9961435	0.3346517

Table 9. NPCR and UACI of Boat for different schemes.

	NPCR	UACI
Ref. [27]	0.996209	0.336018
Ref. [41]	0.996100	0.334412
Ref. [42]	0.996102	0.335367
Ours	0.995869	0.334856

7.10. Local Shannon Entropy

The local Shannon entropy can better express the randomness of the local image and can overcome some drawbacks of the global Shannon entropy. For each image P, arbitrarily choose k non-overlapping sub-images S_i, $i = 1, 2, \ldots, k$. T_B pixels are arbitrarily chosen for every sub-image. The local Shannon information entropy is calculated as follows:

$$\overline{LH_{k,T_B}}(P) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{44}$$

In Equation (44), $H(S_i)$ shows the IE of sub-image S_i. We set $k = 30$, $T_B = 7936$ in this paper. When the confidence interval is 0.05, the local Shannon entropy is in the interval of

[7.901901305, 7.903373329] [34]. Table 10 lists the local Shannon entropy of multiple images whose results pass the experiment, i.e., the randomness of the local image is good.

Table 10. Local Shannon entropy.

Image	Local Entropy	Result
Lena	7.9025	Pass
Cameraman	7.9027	Pass
Boat	7.9024	Pass
Cattle	7.9026	Pass
Einstein	7.9028	Pass
5.2.10	7.9027	Pass

7.11. Cropping Attack

Remove some pixels from the encrypted image and see if it can be decrypted is the cropping attack. In this section, we test "Lena". Figure 16 presents the decrypted images after cutting 1/64, 1/16 and 1/4, respectively. Even if 1/4 of the data is cut off, the decrypted image still displays information from the original image, which illustrates that this scheme is highly resistant to clipping attack.

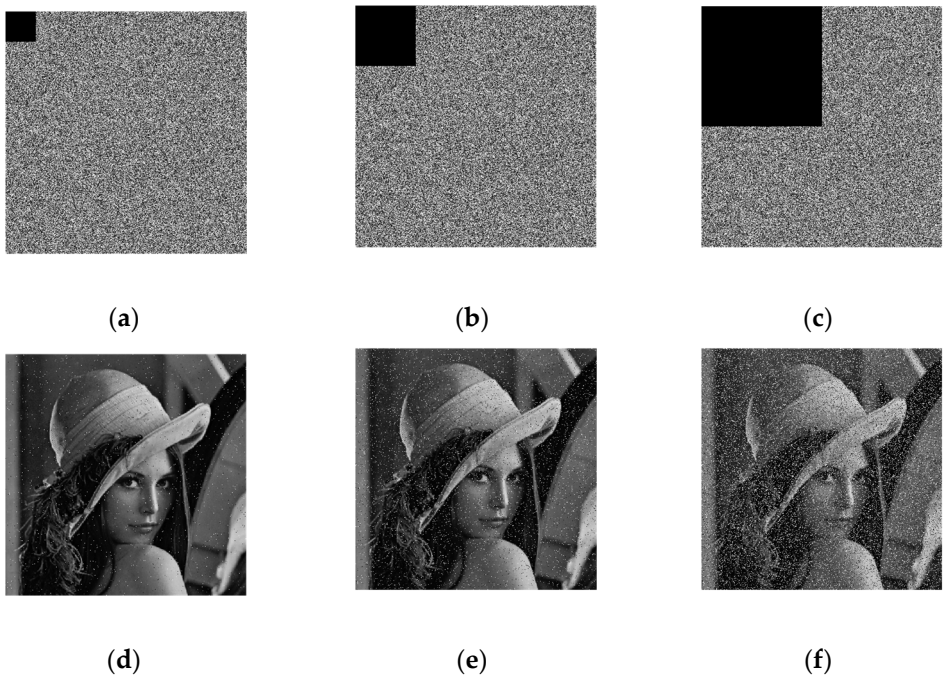
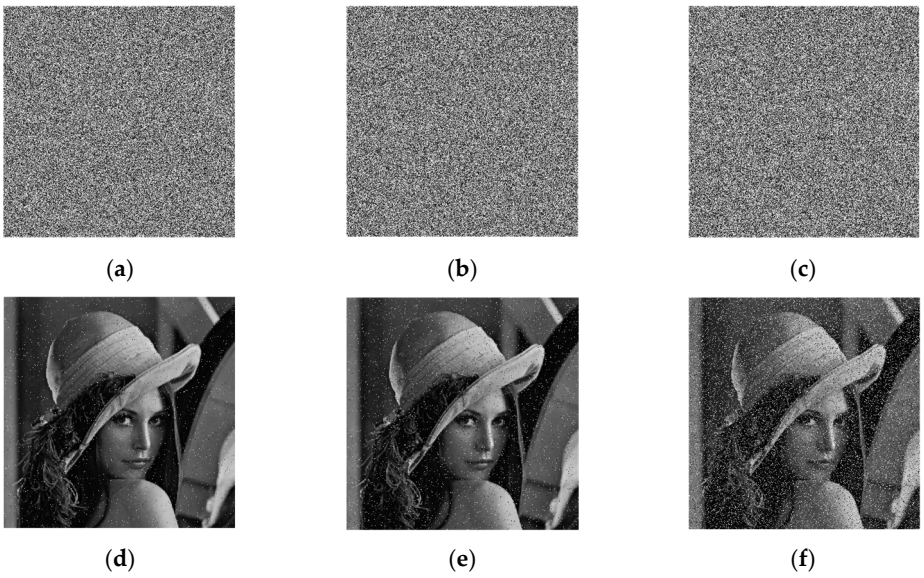


Figure 16. Cropping attack. (**a**) Crop 1/64; (**b**) Crop 1/16; (**c**) Crop 1/4; (**d**) Decrypted image of crop 1/64; (**e**) Decrypted image of crop 1/16; (**f**) Decrypted image of crop 1/4.

7.12. Noise Attack

Inevitably, images are affected during transmission by noise that causes data loss. We take the noise of pepper and salt as an example to show the robustness of the proposed encryption algorithm, whose noise strengths are 0.005, 0.01, and 0.05, respectively. Even with the addition of 0.05 noise, the decrypted image still displays information from the original image in Figure 17, which indicates that this scheme is highly resistant to noise attacks.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 17. Noise attack. (**a**) 0.005 noise; (**b**) 0.01 noise; (**c**) 0.05 noise; (**d**) Decrypted image with 0.005 noise; (**e**) Decrypted image with 0.01 noise; (**f**) Decrypted image with 0.05 noise.

8. Color Image Encryption

The encryption algorithm proposed in this paper can be used not only for grayscale images, but also for color images. The flowchart of color image encryption is given in Figure 18. Unlike grayscale images, color images are divided into three channels, R, G, and B. Each channel is encrypted separately and finally combined to obtain the cipher image.

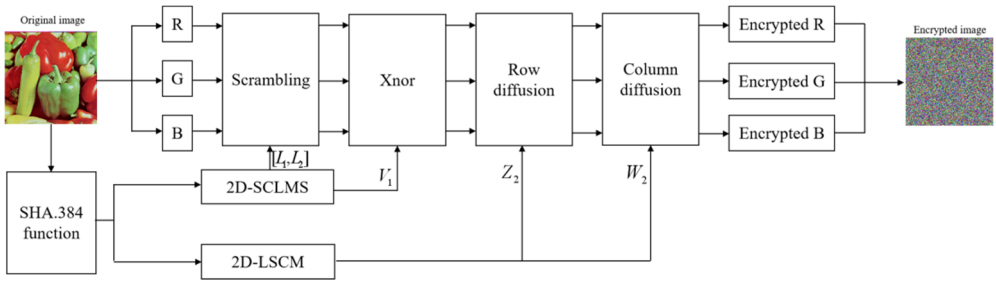
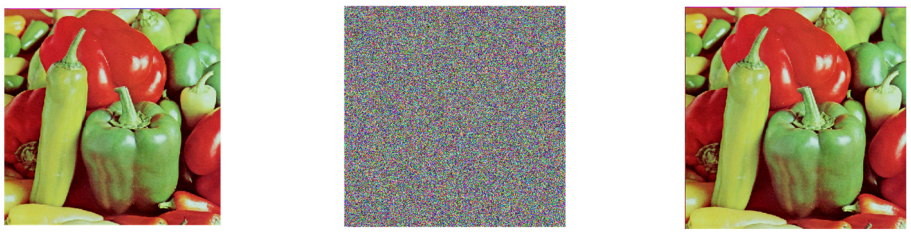


Figure 18. The color image encryption flowchart.

We take the "Peppers" image as an example. The original image, cipher image, and decrypted image are shown in Figure 19. From the figure, we can see that the cipher image is similar to noise, and no information from the original image is obtained. This indicates that the encryption algorithm proposed in this paper works well and is applicable to color images.



(**a**) (**b**) (**c**)

Figure 19. Color image. (**a**) Plain image; (**b**) Cipher image; (**c**) Decrypted image.

When the color image is divided into three channels, R, G, and B, the encryption of each channel is the same as that of the gray image. Therefore, the security tests are not re-demonstrated in detail.

9. Application Areas of Encryption Algorithms

The high efficiency and securer performance of the proposed symmetric encryption algorithm make it possible to apply in many military, commercial, and even daily-use fields. Herein, we itemize several typical applications.

1. E-mail

Image data in e-mails are usually transmitted over non-secure channels, such as the Internet. The widespread use of the Internet has also made encrypting e-mail with sensitive information a very important application in recent years.

2. Electronic money

Electronic money, as a new means of financial transactions, must make the transactions authenticated but untraceable. Transactions must be authenticated so that both parties involved in the transaction are not deceived. Transactions must be untraceable so that each party's privacy is protected. In practice, however, if there is no special protocol to support collaboratively, these requirements are difficult to achieve.

3. Authentication server

The authentication server solves the security problem between two communities at different endpoints in the network. Two groups must be able to exchange keys, and at the same time must ensure that they are talking to the correct counterparty, not an imposter. The authentication server implements these functions through various protocols that rely on encryption mechanisms.

4. Smart card

A smart card contains a microcomputer as well as a small amount of storage space. In general, smart cards are mostly used on various forms of credit. Other types of smart cards are used for access to computers or building access control, etc. Smart cards use encryption technology because it allows certain important operations to be performed, such as modifying bank accounts and accessing secure environments.

5. Internet of Things

In the Internet of Things, the use of smart mobile devices to transfer images in large amounts of data has become increasingly common, such as photos of criminal suspects, medical photos of patients, military photos, etc. The image data captured by some end devices or IoT nodes is related to the private information of users. To protect these image data, image encryption schemes provide a convenient and secure method for the confidentiality of image conversion and storage in IoT systems.

10. Conclusions

The paper mainly introduces a new 2D-SCLMS map based on Logistic and Sine maps. A series of tests, such as Lyapunov exponent, 0–1 test, two complexity analysis methods, and two entropy analysis methods, are used to conclude that the 2D-SCLMS map is hyperchaotic with a broader chaotic range and better randomness. This paper further designs a symmetric image encryption algorithm using 2D-SCLMS map and 2D-LSCM. The encryption algorithm is used under the permutation-diffusion framework which combines pixel scrambling, Xnor, and diffusion. In addition, it uses the hash to create the initial parameters of two systems, which greatly improves the resistance to known plaintext and chosen plaintext attacks. Finally, the simulation experiments of time complexity, key space and sensitivity, information entropy and local Shannon entropy and correlation coefficient demonstrate the large key space, high security, and low time complexity of the new encryption scheme.

Among them, the information entropy of encrypted images using the proposed encryption algorithm can reach 7.9994 at best, which is very close to 8 and better than other related algorithms. The correlation coefficient of the cipher image can even reach -0.00003, which is far smaller than the correlation coefficients obtained using other encryption algorithms. Besides, various attacks, e.g., differential, cropping, and noise attacks, are also analyzed and the conclusions illustrate that this algorithm is also resistant to various attacks. Finally, the value of UACI can reach 33.4651%, which is very small from the standard value and can still recover the original image well when a quarter of the image is cropped off.

In the future, we intend to focus on the verification of the hyperchaotic systems from the perspective of theoretical analysis. Moreover, we remain interested in the practical combination of the proposed image encryption schemes with Internet of Things applications to effectively protect the security of images during the transmission of Internet of Things.

Author Contributions: Formal analysis, J.W.; funding acquisition, X.S. and H.W.; investigation, X.S.; methodology, J.W. and X.S.; resources, A.A.A.E.-L.; validation, H.W.; visualization, J.W.; writing—original draft, J.W.; writing—review & editing, X.S. and A.A.A.E.-L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Postdoctoral Research Foundation of China (2018M631914) and the Heilongjiang Provincial Postdoctoral Science Foundation (CN) (LBH-Z17042).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F.; Altameem, A.; Lee, M. Image encryption using a synchronous permutation-diffusion technique. *Opt. Lasers Eng.* **2017**, *90*, 146–154. [CrossRef]
2. Essaid, M.; Akharraz, I.; Saaidi, A.; Mouhib, A. A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. *Procedia Comput. Sci.* **2018**, *127*, 539–548. [CrossRef]
3. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos* **1998**, *8*, 1259–1284. [CrossRef]
4. Drybin, Y.A.; Sadau, S.V.; Sadau, V.S. Digital model of a pseudo-random number generator based on a continuous chaotic system. *Informatica* **2021**, *17*, 36–47. [CrossRef]
5. Li, X.; Feng, Z.; Zhang, Q.; Wang, X.; Xu, G. Scaling of attractors of a multiscroll memristive chaotic system and its generalized synchronization with sliding mode control. *Int. J. Bifurc. Chaos* **2021**, *31*, 2150007. [CrossRef]
6. Setoudeh, F.; Sedigh, A.K. Nonlinear analysis and minimum l2-norm control in memcapacitor-based hyperchaotic system via online particle swarm optimization. *Chaos Solitons Fractals* **2021**, *151*, 111214. [CrossRef]
7. Benrhouma, O.; Hermassi, H.; Abd El-Latif, A.A.; Belghith, S. Chaotic watermark for blind forgery detection in images. *Multimed. Tools Appl.* **2016**, *75*, 8695–8718. [CrossRef]
8. Yan, X.; Wang, S.; Abd El-Latif, A.A.; Niu, X. Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. *Multimed. Tools Appl.* **2015**, *74*, 3231–3252. [CrossRef]
9. Abd El-Latif, A.A.; Yan, X.; Li, L.; Wang, N.; Peng, J.L.; Niu, X. A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption. *Opt. Laser Technol.* **2013**, *54*, 389–400. [CrossRef]
10. Belazi, A.; El-Latif, A.; Rhouma, R.; Belghith, S. Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference, Security Symposium, Dubrovnik, Croatia, 24–28 August 2015; pp. 606–610.
11. El-Latif, A.; Abd-El-Atty, B.; Abou-Nassar, E.M.; Venegas-Andraca, S.E. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Opt. Laser Technol.* **2019**, *124*, 105942. [CrossRef]
12. Yue, W.; Yang, G.; Jin, H.; Noonan, J.P. Image encryption using the two-dimensional logistic chaotic map. *J. Electron. Imaging* **2012**, *21*, 013014.
13. Wang, X.; Gao, S. Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Inf. Sci.* **2020**, *507*, 16–36. [CrossRef]
14. El-Latif, A.; Abd-El-Atty, B.; Amin, M.; Iliyasu, A.M. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **2020**, *10*, 1930. [CrossRef]
15. Tsafack, N.; Sankar, S.; Abd-El-Atty, B.; Kengne, J.; El-Latif, A. A new chaotic map with dynamic analysis and encryption application in internet of health things. *IEEE Access* **2020**, *8*, 137731–137744. [CrossRef]
16. AlShaikh, M.; Laouamer, L.; Nana, L.; Pascu, A.C. Efficient and robust encryption and watermarking technique based on a new chaotic map approach. *Multimed. Tools Appl.* **2017**, *76*, 8937–8950. [CrossRef]
17. Kanso, A.; Ghebleh, M. A novel image encryption algorithm based on a 3D chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 2943–2959. [CrossRef]

18. Li, C.; Zhang, Y.; Xie, E.Y. When an attacker meets a cipher-image in 2018: A year in review. *J. Inf. Secur. Appl.* **2019**, *48*, 102361. [CrossRef]
19. Liu, H.; Wang, X. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.* **2010**, *59*, 3320–3327. [CrossRef]
20. Li, L.; Abd-El-Atty, B.; Abd El-Latif, A.A.; Ghoneim, A. Quantum color image encryption based on multiple discrete chaotic systems. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; pp. 555–559.
21. Sambas, A.; Vaidyanathan, S.; Tlelo-Cuautle, E.; Abd-El-Atty, B.; Abd El-Latif, A.A.; Guillén-Fernández, O.; Sukono; Hidayat, Y.; Gundara, G. A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption. *IEEE Access* **2020**, *8*, 137116–137132. [CrossRef]
22. Yang, T.; Wang, Z.; Fang, J.A. Image encryption using chaotic coupled map lattices with time-varying delays. *Commun. Nonlinear Sci. Numer. Simul.* **2010**, *15*, 2456–2468.
23. Amin, M.; Abd El-Latif, A.A. Efficient modified RC5 based on chaos adapted to image encryption. *J. Electron. Imaging* **2010**, *19*, 013012. [CrossRef]
24. Wong, K.W.; Kwok, B.S.H.; Law, W.S. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **2010**, *372*, 2645–2652. [CrossRef]
25. Zhou, Q.; Wong, K.W.; Liao, X.; Xiang, T.; Hu, Y. Parallel image encryption algorithm based on discretized chaotic map. *Chaos Solitons Fractals* **2008**, *38*, 1081–1092. [CrossRef]
26. Alawida, M.; Samsudin, A.; Teh, J.S.; Alkhawaldeh, R.S. A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* **2019**, *160*, 45–58. [CrossRef]
27. Hua, Z.; Zhou, Y.; Pun, C.M.; Chen, C.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
28. Zhu, H.; Zhao, Y.; Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **2019**, *7*, 14081–14098. [CrossRef]
29. Sun, J. 2D-SCMCI Hyperchaotic Map for Image Encryption Algorithm. *IEEE Access* **2021**, *9*, 59313–59327. [CrossRef]
30. Yang, F.; Mou, J.; Yan, H.; Hu, J. Dynamical analysis of a novel complex chaotic system and application in image diffusion. *IEEE Access* **2019**, *7*, 118188–118202. [CrossRef]
31. Gottwald, G.A.; Melbourne, I. The 0–1 Test for Chaos: A review. In *Chaos Detection and Predictability*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 221–247.
32. Gottwald, G.A.; Melbourne, I. Testing for chaos in deterministic systems with noise. *Phys. D Nonlinear Phenom.* **2008**, *212*, 100–110. [CrossRef]
33. Xu, Q.; Sun, K.; Cao, C.; Zhu, C. A fast image encryption algorithm based on compressive sensing and hyperchaotic map. *Opt. Lasers Eng.* **2019**, *121*, 203–214. [CrossRef]
34. Shengtao, G.; Tao, W.; Shida, W.; Xuncai, Z.; Ying, N. A Novel Image Encryption Algorithm Based on Chaotic Sequences and Cross-Diffusion of Bits. *IEEE Photonics J.* **2020**, *13*, 1–15. [CrossRef]
35. Wang, X.; Su, Y. Image encryption based on compressed sensing and DNA encoding. *Signal Process.—Image Commun.* **2021**, *95*, 116246. [CrossRef]
36. Jason, A.C.G. Structure of the parameter space of the hénon map. *Phys. Rev. Lett.* **1993**, *70*, 2714–2717.
37. May, R.M. Simple mathematical models with very complicated dynamics. *Nature* **1976**, *261*, 459–467. [CrossRef] [PubMed]
38. Rehman, M.U.; Shafique, A.; Khalid, S.; Hussain, I. Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps. *IEEE Access* **2021**, *9*, 52277–52291. [CrossRef]
39. Arroyo, D.; Rhouma, R.; Alvarez, G.; Li, S.; Fernandez, V. On the security of a new image encryption scheme based on chaotic map lattices. *Chaos Interdiscip. J. Nonlinear Sci.* **2008**, *18*, 033112. [CrossRef] [PubMed]
40. Xiaofu, W.; Songgeng, S. A general efficient method for chaotic signal estimation. *IEEE Trans. Signal Process.* **1999**, *47*, 1424–1428.
41. Farah, M.A.; Farah, A.; Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dyn.* **2020**, *99*, 3041–3064. [CrossRef]
42. Belazi, A.; Abd El-Latif, A.A.; Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **2016**, *128*, 155–170. [CrossRef]
43. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
44. Li, C.; Lin, D.; Feng, B.; Lü, J.; Hao, F. Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *IEEE Access* **2018**, *6*, 75834–75842. [CrossRef]
45. Abd El-Latif, A.A.; Abd-El-Atty, B.; Mazurczyk, W.; Fung, C.; Venegas-Andraca, S.E. Secure data encryption based on quantum walks for 5G Internet of Things scenario. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 118–131. [CrossRef]
46. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
47. Liu, L.; Jiang, D.; An, T.; Guan, Y. A plaintext-related dynamical image encryption algorithm based on permutation-combination-diffusion architecture. *IEEE Access* **2020**, *8*, 62785–62799. [CrossRef]
48. Jiang, D.; Liu, L.; Zhu, L.; Wang, X.; Rong, X.; Chai, H. Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. *Signal Process.* **2021**, *188*, 108220. [CrossRef]

49. Nestor, T.; De Dieu, N.J.; Jacques, K.; Yves, E.J.; Iliyasu, A.M.; El-Latif, A.; Ahmed, A. A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem. *Sensors* **2020**, *20*, 83. [CrossRef] [PubMed]
50. Zhao, C.F.; Ren, H.P. Image encryption based on hyper-chaotic multi-attractors. *Nonlinear Dyn.* **2020**, *100*, 679–698. [CrossRef]
51. Chen, J.; Zhu, Z.L.; Zhang, L.B.; Zhang, Y.; Yang, B.Q. Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. *Signal Process.* **2018**, *142*, 340–353. [CrossRef]
52. Ye, G.; Pan, C.; Huang, X.; Mei, Q. An efficient pixel-level chaotic image encryption algorithm. *Nonlinear Dyn.* **2018**, *94*, 745–756. [CrossRef]