Research Article

2D Sin-Cos-Henon Map for Color Image Encryption with High Security

Zhiqiang Cheng,1 Wencheng Wang,2 Yuezhang Dai,1 and Lun Li1,2

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

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

Received 1 July 2022; Accepted 12 July 2022; Published 4 August 2022

Copyright © 2022 Zhiqiang Cheng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, a high security color image encryption algorithm is proposed by 2D Sin-Cos-Hénon (2D-SCH) system. A new two-dimensional chaotic system which is 2D-SCH. This system is hyperchaotic. The use of the 2D-SCH, a color image encryption algorithm based on random scrambling and localization diffusion, is proposed. First, the secret key is generated by SHA512 through plaintext. As the initial value of the 2D-SCH system, the secret key is used to generate chaotic sequences. Then, the random scrambling is designed based on chaotic sequences. Finally, a pair of initial points is generated by the secret key; the image diffuses around this point. The ciphertext is obtained by a double encryption. Different from the traditional encryption algorithm, this paper encrypts three channels of color image simultaneously, which greatly improves the security of the algorithm. Simulation results show that the algorithm can resist various attacks.

1. Introduction

With the rapid development of Internet technology, information exchange becomes more and more frequent, and the protection of information becomes more and more important. As an important medium of information exchange, the image has become an important research object of scholars. Many methods are proposed to protect images [1–4], such as image hiding technology, zero-watermarking technology, and image encryption technology [5–9]. Image encryption technology is to convert plaintext into noise image; it is the most commonly used technology.

Because chaotic systems have long-term unpredictability, initial value sensitivity, key sensitivity, and other characteristics, image encryption technology combined with chaotic system has gradually become a hot issue [10–13]. Hua et al. use 2D Logistic-Sine-coupling map in image encryption [14]. Sun et al. proposed an image encryption algorithm combined with 2D nonadjacent coupled map lattice with q [15]. Sharma proposed a new 2D logistic adjusted logistic map and used it in image encryption [16]. Zhang et al. used perceptron-like network and proposed an encryption algorithm based on chaos [17]. The chaotic key stream is used to generate a key matrix, and the image is diffused using the matrix semitensor product technology to complete the encryption [18–20]. In addition, some scholars use DNA technology in image encryption, and these algorithms show good performance [21–23].

Chaos systems are divided into two categories, low-dimensional chaotic systems and high-dimensional chaotic systems [24–27]. Low-dimensional chaotic systems include Logistic and Tent. A low-dimensional chaotic system has a simple structure with only one positive Lyapunov exponent. In Ref. [28], it is pointed out that because of the computer precision problem, low-dimensional chaotic systems have the phenomenon of short period chaos degradation, which seriously destroys its randomness, so the security of chaotic image encryption with low-dimensional chaos is not high. Considering the chaotic system above two-dimensional, the hardware implementation cost is large, and the time of generating chaotic sequence is longer, so it is necessary to develop a low-cost two-dimensional chaotic system. In this
paper, a new 2D-SCH is proposed, this chaotic system has two positive Lyapunov exponents, and chaotic sequences produced take a short time, so it is a hyperchaotic system, and it can be widely used in image encryption.

Recently, many color image encryption algorithms have been proposed. Wang and Sun proposed chaotic image encryption algorithm based on Joseph traversal and cyclic shift function [29]. Xian et al. proposed a new image encryption algorithm combining CDSD and CSBS [30]. The above color image encryption algorithm processes the three channels of the color image separately, so the security of the algorithm is weakened, because the attacker will have three examples of algorithms on basically the same image. This paper proposes a three-channel simultaneous encryption algorithm, which improves the security of the algorithm. On the same image, the attacker will only get an example of the algorithm. Experimental results show that the algorithm proposed in this paper has high security and can resist various attacks.

The main contributions of this paper are as follows:

1. A 2D-SCH is designed; this chaotic system has complex dynamical behavior
2. A cascaded color image encryption algorithm is designed. The three channels of the color image are encrypted at the same time
3. A method of location XOR diffusion is proposed. The starting position of diffusion is not fixed

The rest of this article is as follows. The second section introduces the 2D-SCH, the third section presents the image encryption algorithm, the fourth section analyzes the security of the algorithm, and the fifth section proposes the future work.

2. 2D-SCH System

A new chaotic system is proposed in this paper. The mathematical analytic formula of the system is as follows:

\[
\begin{align*}
    x_{i+1} &= 1 - \mu \sin^2(\pi x_i) + \sin(\pi y_i), \\
    y_{i+1} &= \mu \sin(x_i y_i),
\end{align*}
\]  

(1)

where \(x_0 \in (0, 1), y_0 \in (0, 1), \) and \(\mu \in [3, 6] \) at this parameter; the system is hyperchaotic with two positive Lyapunov exponents.

2.1. Trajectory. In this section, the trajectory of the 2D-SCH system is described. Choose the parameters \(\mu = 3, \mu = 4, \) and \(\mu = 5 \) and draw their trajectory map which is shown in Figure 1. Trajectory analysis shows that the values of the system distribute almost all places of the plane, which indicates that the system can output more randomly and can take almost all values in the window.

2.2. Lyapunov Exponent. The Lyapunov exponent is an important index to depict chaotic system. When a chaotic system has two or more positive Lyapunov exponents, the system is in a hyperchaotic state. It is defined as

\[
\lambda = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|.
\]  

(2)

Figure 2 shows the Lyapunov exponent in the parameters of \(\mu \in [-1, 6] \) and \(\mu \in [3, 6] \), respectively.

We can see from Figure 2 that when the 2D-SCH system has two positive Lyapunov exponents, under this parameter, the system is in the hyperchaotic state.

Because the 2D-SCH system has good chaos, the 2D-SCH system is used in color image encryption.

3. Color Image Encryption Algorithm

The color image encryption algorithm proposed in this paper is a process of scrambling to diffusion, and it is a two-round encryption algorithm. The size of the color image is \(P \in M \times N; \) the encryption process is shown below.

3.1. Key Generation. Use SHA512 to generate a series of secret keys related to plaintext. Different plaintext can generate different secret keys, because SHA512 is difficult to be cracked, which increases the security of the algorithm. The key is generated as follows:

Suppose the plaintext is \(P \), three channels of \(P \) are \(P_R, P_G, \) and \(P_B, \) and the three channels combined into a new image are \(P_{RGB}: \)

\[
P_{RGB} = [P_R, P_G, P_B].
\]  

(3)

The generated key is

\[
\begin{align*}
    a &= f(\text{hash}(P_{RGB} \text{SHA512})), \\
    a_1 &= a(1 : 128), \\
    a_2 &= a(129 : 256), \\
    a_3 &= a(256 : 384), \\
    a_4 &= a(385 : 512).
\end{align*}
\]  

(4)

In Equation (4), \(\text{hash(x,SHA512)} \) represent \(x \) changed into SHA512. \(f(x) \) stands for converting \(x \) from Hex to Binary. Processing \(a_i:\)

\[
\begin{align*}
    b_1 &= \sum_{i=1}^{128} a_i \times 2^{-i}, \\
    b_2 &= \sum_{i=1}^{128} a_2 \times 2^{-i}, \\
    b_3 &= \sum_{i=1}^{128} a_3 \times 2^{-i}, \\
    b_4 &= \sum_{i=1}^{128} a_4 \times 2^{-i}.
\end{align*}
\]  

(5)

\(b_1 \) and \(b_2 \) are the initial value of the chaotic system, bring them into Equation (2), and two chaotic sequences
are produced which are \( x \) and \( y \). The size of \( x \) is \( 3N \). The size of \( y \) is \( M \).

3.2. Random Scrambling. Sort the chaotic sequences generated in Section 3.1 from small to large. \( x_1 \) and \( y_1 \) are produced. \( X \) and \( Y \) are defined by

\[
X(i) = \text{find}(x_1(i) == x), \quad i \in [1, N],
\]

\[
Y(i) = \text{find}(y_1(i) == y), \quad i \in [1, 3M].
\]

In Equation (6), \( \text{find}(x_1(i) == x) \) represents the position of \( x_1(i) \) in \( x \).

Scrambling the plaintext \( P_{\text{RGB}} \) and the scrambling matrix \( S \) is

\[
Q(i, :) = P_{\text{RGB}}(Y(i), :), \quad i \in [1, M],
\]

\[
S_1(:, j) = Q(:, X(j)), \quad i \in [1, 3N],
\]

\[
S(:, j) = \text{circshift}(S_1(:, j), X(i)).
\]

In Equation (7), \( \text{circshift}(x, b) \) represents that the vector \( x \) is cyclically shifted to the right by \( b \) positions.

3.3. Location XOR Diffusion. This section proposes a location XOR diffusion strategy. Determine the starting position of diffusion based on the initial secret key.

\[
j = \text{floor}(b_3 \times 3N),
\]

\[
i = \text{floor}(b_4 \times M).
\]

Determine the value of the initial XOR:

\[
c = \text{floor}((0.8 + 0.2b_4) \times 256).
\]

Take \((i, j)\) as the center and diffuse to the surroundings.
The diffusion steps are

\begin{align*}
C(i, j) &= \text{bitxor}(S(i, j), c), \\
C(s, j) &= \text{bitxor}(S(s, j), C(s - 1, j)), s \in i + 1 : M, \\
C(s, j) &= \text{bitxor}(S(s, j), C(s + 1, j)), s \in i - 1 : -1 : 1, \\
C(s, t) &= \text{bitxor}(S(s, t), C(s, t - 1)), s \in 1 : M, t \in j + 1 : 3N, \\
C(s, t) &= \text{bitxor}(S(s, t), C(s, t + 1)), s \in 1 : M, t \in j - 1 : -1 : 1, \\
\end{align*}

and finally, get the ciphertext \( C \):

\begin{align*}
C_R &= C(1 : 1 : N), \\
C_G &= C(1 + N : 2N), \\
C_B &= C(1 + 2N : 3N).
\end{align*}

The three channels of color images are obtained by processing the ciphertext \( C \).

Figure 3 shows the steps of the location XOR diffusion.
Figure 4: Encryption and decryption of Goldhill and Fruits. (a) Plaintext of Goldhill. (b) Ciphertext of Goldhill. (c) Decryption of Goldhill. (d) Plaintext of Fruits. (e) Ciphertext of Fruits. (f) Decryption of Fruits.
3.4. Decryption Algorithm. The algorithm proposed in this paper is a symmetric image encryption algorithm; each part of the encryption is reversible.

Decrypt the key $a$ generated by Equation (4) and ciphertext $C$; the decryption steps are as follows:

Step 1 (reverse process of diffusion).

$$S(i, j) = \text{bitxor}(C(i, j), c),$$

$$S(s, j) = \text{bitxor}(C(s, j), C(s - 1, j)), s \in i + 1 : M,$$

$$S(s, j) = \text{bitxor}(C(s, j), C(s + 1, j)), s \in i - 1 : -1 : 1,$$

$$S(s, s) = \text{bitxor}(C(s, s), C(s - 1, s), C(s + 1, s)), s \in 1 : M, s \in j + 1 : 3N,$$

$$S(s, s) = \text{bitxor}(C(s, s), C(s - 1, s), C(s + 1, s)), s \in 1 : M, s \in j - 1 : -1 : 1.$$

Step 2 (reverse process of scrambling).

$$S_s(i, j) = \text{circshift}(S(i, j), 3N - X(i)),$$

$$Q(s, X(i)) = S_s(i, j), i \in [1, 3N],$$

$$P_{RGB}(Y(i), :) = Q(i, :], i \in [1, M].$$

Step 3 (the three channels of plaintext).

$$P_R = P_{RGB}(:, 1 : N),$$

$$P_G = P_{RGB}(:, 1 + N : 2N),$$

$$P_B = P_{RGB}(:, 1 + 2N : 3N).$$

4. Simulation and Performance Analysis

4.1. Simulation. Figure 4 shows Goldhill_color_576x720 and Fruits_color_480x512, the two rounds of encryption and decryption process.

4.2. Secret Key Space Analysis. This paper uses the SHA512 to produce the secret key, and then, the secret key space is

$$\text{space} = 2^{512} > 2^{100}.$$  

As mentioned in Refs. [31, 32], the algorithm is sufficient to resist violent attacks when the secret key space exceeds $2^{100}$, so the algorithm proposed in this paper is sufficient to resist violent attacks.

4.3. Secret Key Sensitive Analysis. The key $a$ in this article is generated by SHA512, and $a$ is divided into several keys. One of the keys $b_1$ is processed to obtain the wrong key $b'_1 = b_1 + 10^{-14}$. Use the wrong key to restore the image. Take Lena_color_512x512 as an example. The results are shown in Figure 5.

It can be seen from Figure 5 that the secret key in this paper is sensitive, and even if a small change is made to the secret key, the plaintext cannot be obtained through the decryption algorithm.

4.4. Histogram Analysis. Histogram analysis is to calculate the distribution of pixel values of plaintext and ciphertext. Generally, the distribution of plaintext histograms is uneven, and the distribution of ciphertext histograms obtained by a secure encryption algorithm is uniform; otherwise, the attacker will get some plaintext information through the histogram distribution of ciphertexts and crack the algorithm (Figure 6).
Figure 6: Continued.
It can be seen from Figure 6 that the distribution of the ciphertext histogram after the algorithm in this paper is uniform. Therefore, the algorithm proposed in this paper has a good ability to resist statistical attacks.

4.5. Correlation Analysis. Correlation analysis is another important indicator of statistical analysis. Correlation analysis includes horizontal correlation analysis, vertical correlation analysis, and object correlation analysis.
The calculation formula is as follows:

\[ r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \]  

(16)

\[ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \]  

(17)

\[ D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \]  

(18)

\[ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \]  

(19)

Table 1 shows the correlation analysis of plaintexts and ciphertexts. Experimental results show that the proposed algorithm can reduce the correlation of adjacent pixels.

Taking Lena as an example, Table 2 shows the comparison results of the correlation of adjacent pixels. Compared with Refs. [13, 33–37], we can see that the correlation between the adjacent pixels of the ciphertext obtained by the encryption algorithm in this paper is smaller, so this algorithm has higher security and can resist statistical attacks.

4.6. Different Attack. Differential attack refers to an attacker attacking a plaintext image and observing the transformation of the ciphertext to find a way to crack the algorithm. Differential attacks have two important indicators: number of pixel change rate (NPCR) and uniform average changing intensity (UACI); their calculation formula is

\[ \text{NPCR} = \frac{\sum_{i,j} E(i, j)}{M \times N} \times 100\% \]  

(20)

\[ \text{UACI} = \frac{1}{M \times N} \left[ \sum_{i,j} \left| C_1(i, j) - C_2(i, j) \right| \right] \times 100\% \]  

(21)

The theoretical values of NPCR and UACI are 99.6093% and 33.4635%, respectively. Change a bit on a pixel value of the plaintext to obtain an encrypted image, and compare it with the original encrypted image. Calculate the values of NPCR and UACI by the two encrypted images. In this paper, random selection of 100 sets of points for testing and the average value is taken. The calculation results are shown in Table 3.

Table 4 shows NPCR and UACI comparison with Refs. [13, 33–35, 37, 38]. The comparison results show that the proposed NPCR and UACI are closer to the theoretical value, so this algorithm has higher security.

4.7. Information Entropy Analysis. Information entropy represents the degree of confusion of information distribution. The bigger the information entropy, the more chaotic the information distribution. Conversely, the smaller the information entropy, the more uniform the information distribution. The calculation formula is as follows:

\[ H(s) = \sum_{i=0}^{2^r-1} p(s_i) \log_2 \frac{1}{p(s_i)} \]  

(22)

The theoretical value of information entropy is 8. Using the above formula, the entropy test is performed on the plaintext and ciphertext of the algorithm in this paper. The test results are shown in Table 5.

Table 6 presents a comparison with Refs. [33–35, 37, 38]. The comparison results show that the proposed NPCR and UACI are closer to the theoretical value, so this algorithm has higher security.

4.8. Time Analysis. The system environment is as follows: win7 system, CPU: 5210U, and Matlab R2019a. Taking Lena_color (512x512) as an example, the time analysis of the proposed encryption algorithm is shown in Table 7, and the time comparison results with some algorithms are shown in Table 7.
Time complexity analysis shows that the algorithm proposed in this paper runs faster and is more suitable for promotion in industrial production.

5. Conclusion

This paper designs a 2D-SCH chaotic system, which is a hyperchaotic system. This system has low implementation cost and short time to generate chaotic sequence. Therefore, 2D-SCH chaotic system is used in image encryption. A location XOR diffusion algorithm is proposed, which obtains ciphertext after two rounds of operations. Unlike the common color image encryption, the algorithm designed in this paper encrypts three channels at the same time, which increases the security of the algorithm. Simulation and performance analysis show that the algorithm designed in this paper can resist various attacks.

In future work, the authors intend to implement the algorithm in hardware so that the algorithm can be used in industrial production and make the encryption algorithm more secure and robust.

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 National Natural Science Foundation of China (61802212).

References


