# Two-Dimensional Sinusuida-Cosinusuidal-Henon Map for Encryption of Color Image with Higher Security

Satyaprangya Swain [1], Sulochana Parida [2], Tophan Jena [3], RASHMI MANJARI JAYASINGH[4]
[1, 2, 3] Gandhi Institute for Education & Technology, Baniatangi, Khordha, Odisha
[4]NM Institute of Engineering & Technology,Bhubaneswar,Odisha
satyaprangyaswain@giet.edu.in, sulochanaparida@giet.edu.in, tophanjena@giet.edu.in

Abstract: In this paper, a high security color image encryption algorithm is proposed by 2D Sin-Cos-HÃ©non (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 discusion, 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 discuses 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:

$$\begin{cases} x_{i+1} = 1 - \mu \sin^2(\pi x_i) + \sin(\pi y_i), \\ y_{i+1} = \mu \sin(x_i y_i), \end{cases} \quad (1)$$

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.

*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.

*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

$$\lambda = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \cdot f'(x_i). \quad (2)$$

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.

*Key Generation.* Use SHA512 to generate a series of secret keys related to plaintext. Different plaintext can gener- ate 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 $P_{RGB}$:

$$P_{RGB} = [P_R, P_G, P_B]. \quad (3)$$

The generated key is

$$\begin{cases} a = f(hash(P_{RGB}, \text{SHA512})), \\ a_1 = a(1 : 128), \\ a_2 = a(129 : 256), \\ a_3 = a(256 : 384), \\ a_4 = a(385 : 512). \end{cases} \quad (4)$$

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

$$\begin{cases} b_1 = \sum_{i=1}^{128} a_1 \times 2^{-i}, \\ b_2 = \sum_{i=1}^{128} a_2 \times 2^{-i}, \\ b_3 = \sum_{i=1}^{128} a_3 \times 2^{-i}, \\ b_4 = \sum_{i=1}^{128} a_4 \times 2^{-i}. \end{cases} \quad (5)$$

$b_1$ and $b_2$ are the initial value of the chaotic system, bring them into Equation (2), and two chaotic sequences

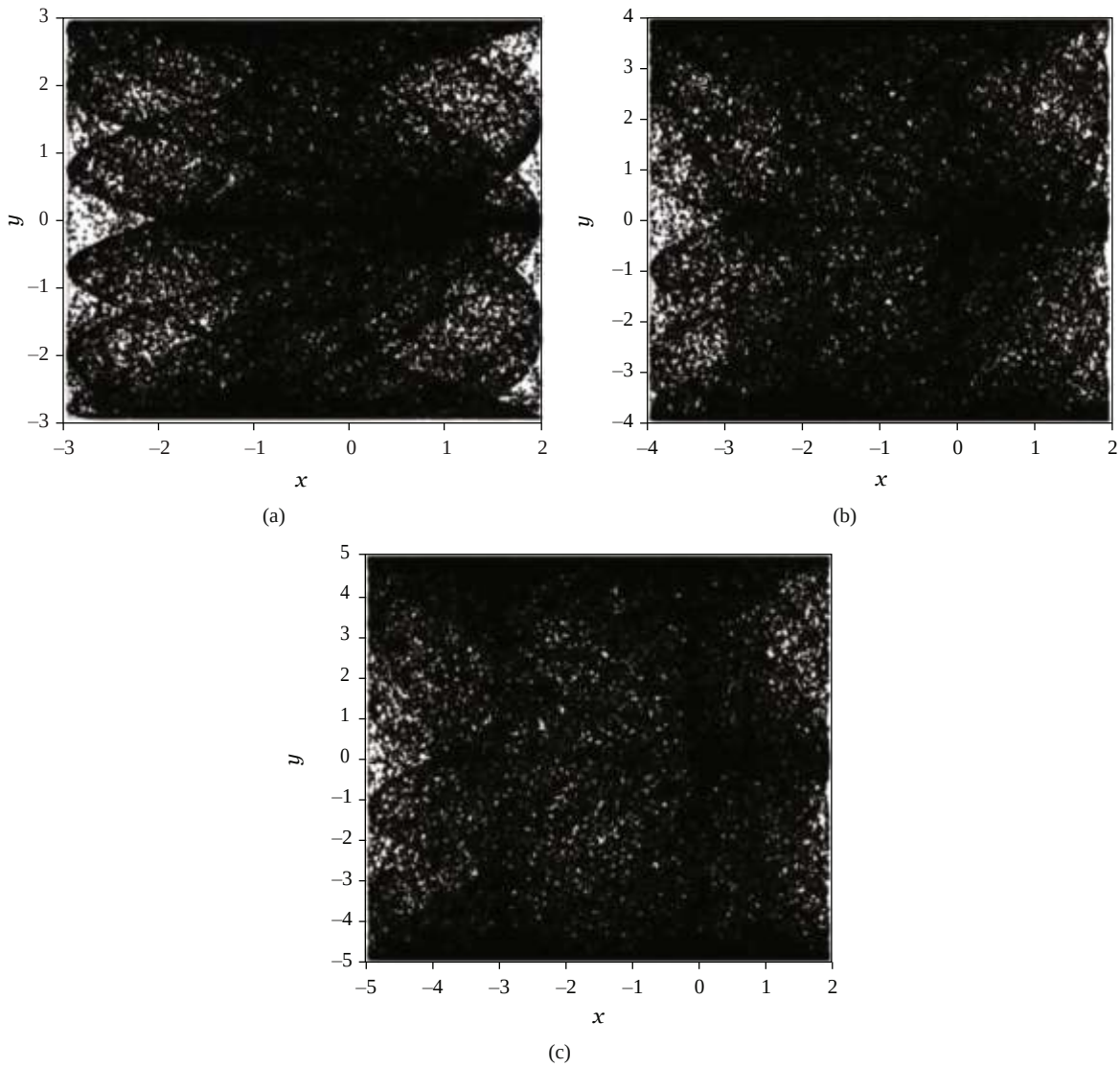



FIGURE 1: 2D-SCH trajectory of different parameters. (a) Trajectory of μ = 3. (b) Trajectory of μ = 4. (c) Trajectory of μ = 5.

are produced which are $x$ and $y$. The size of $x$ is $3N$. The size of $y$ is M.

*Random Scrambling.* Sort the chaotic sequences gener- ated in Section 3.1 from small to large. $x_1$ and $y_1$ are pro- duced. $X$ and $Y$ are defined by

$$X(i) = \text{find}(x_1(i) == x), i \in [1, N],$$
$$Y(i) = \text{find}(y_1(i) == y), i \in [1, 3M]: \quad (6)$$

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

Scrambling the plaintext $P_{RGB}$ and the scrambling matrix $S$ is

$$Q(i, :) = P_{RGB}(Y(i), :), i \in [1, M],$$
$$S_1(:, i) = Q(:, X(i)), i \in [1, 3N], \quad (7)$$
$$S(:, i) = \text{circshift}(S_1(:, i), X(i)):$$

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

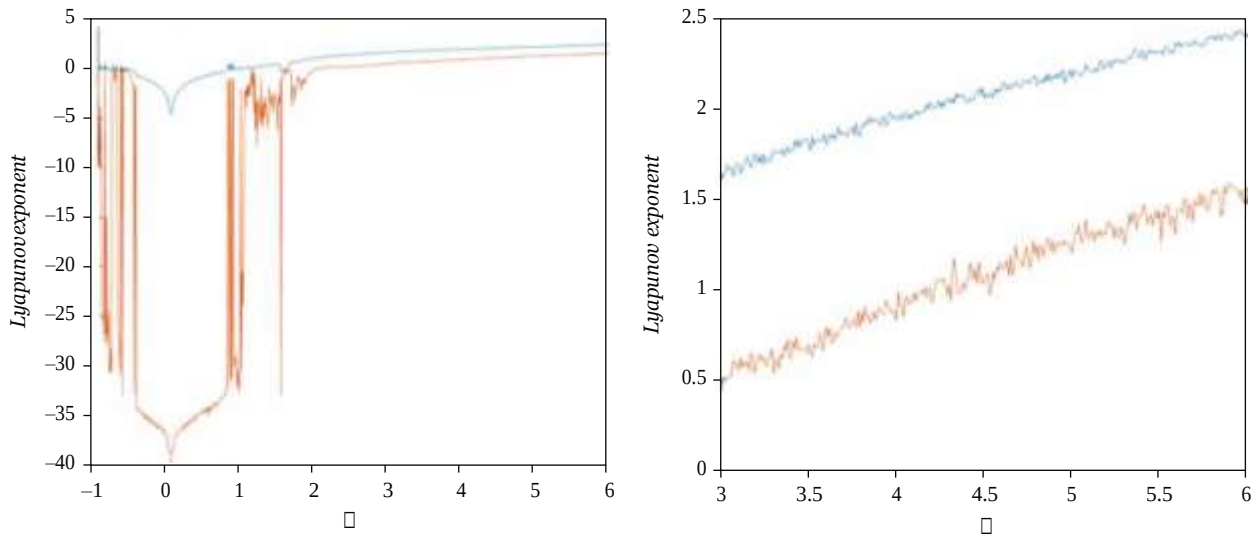
*Location XOR Diffusion.* This section proposes a location XOR diffusion strategy. Determine the starting position of diffusion based on the initial secret key.

$$j = \text{floor}(b_3 \times 3N),$$
$$i = \text{floor}(b_4 \times M): \quad (8)$$

Determine the value of the initial XOR:

$$c = \text{floor}((0:8 + 0:2b_4) \times 256): \quad (9)$$

Take $(i, j)$ as the center and diffuse to the surroundings.




(a) (b)

FIGURE 2: Lyapunov exponent of 2D-SCH. (a) Lyapunov exponent of μ ∈ ½−1, 6]. (b) Lyapunov exponent of μ ∈ ½3, 6].

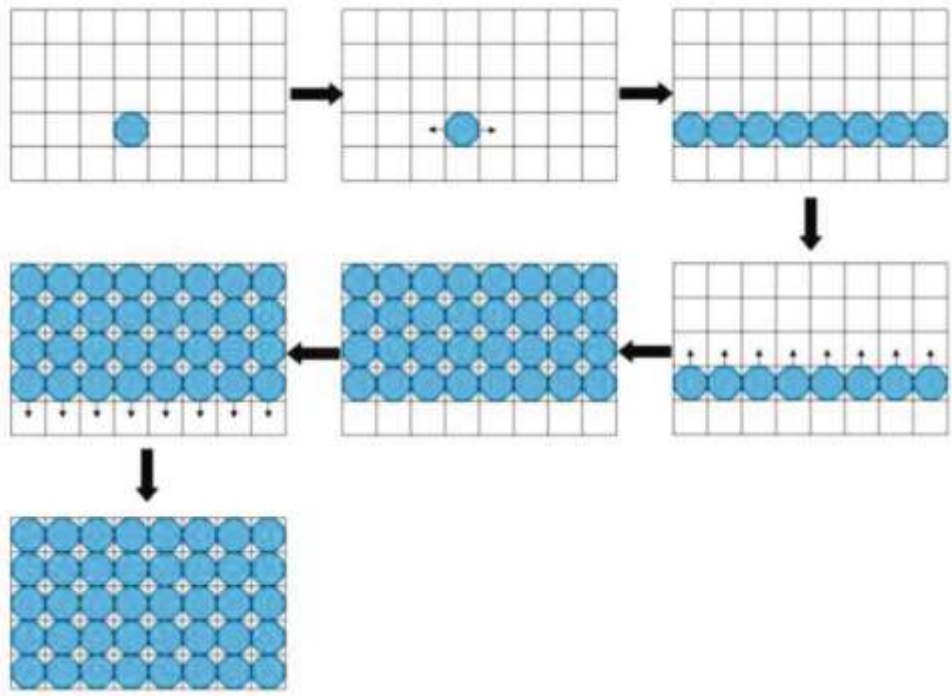


FIGURE 3: Schematic map of location XOR diffusion.

The diffusion steps are

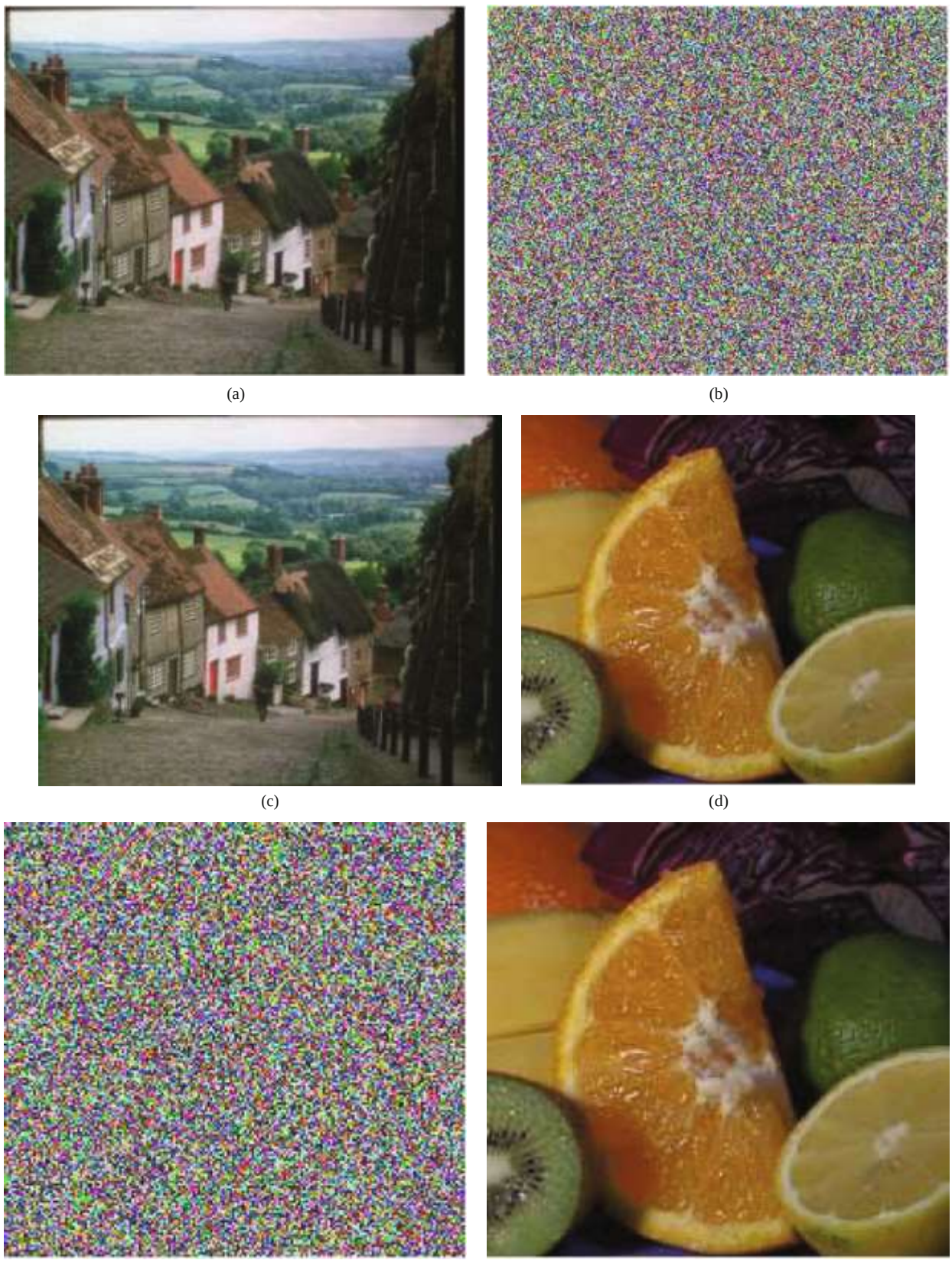
$$
\begin{aligned}
&C(i,j) = \text{bitxor}(S(i,j), c),\\
&C(s,j) = \text{bitxor}(S(s,j), C(s-1,j)), s \in i+1:M,\\
&C(s,j) = \text{bitxor}(S(s,j), C(s+1,j)), s \in i-1:-1:1,\\
&C(s,t) = \text{bitxor}(S(s,t), C(s,t-1)), s \in 1:M, t \in j+1:3N,\\
&C(s,t) = \text{bitxor}(S(s,t), C(s,t+1)), s \in 1:M, t \in j-1:-1:1,
\end{aligned}
\tag{10}
$$

and finally, get the ciphertext $C$:

$$
\begin{aligned}
&C_R = C(:,1:N),\\
&C_G = C(:,1+N:2N),\\
&C_B = C(:,1+2N:3N):
\end{aligned}
\tag{11}
$$

The three channels of color images are obtained by processing the ciphertext $C$.

Figure 3 shows the steps of the location XOR diffusion.



(a) (b) (c) (d) (e) (f)

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.

(a) (b)

FIGURE 5: Key sensitivity analysis. (a) Restored of the correct key. (b) Restored of the wrong key.

*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).

$$\begin{aligned}
&S(i, j) = \text{bitxor}(C(i, j), c),\\
&S(s, j) = \text{bitxor}(C(s, j), C(s-1, j)), s \in i+1 : M,\\
&S(s, j) = \text{bitxor}(C(s, j), C(s+1, j)), s \in i-1 : -1 : 1,\\
&S(s, t) = \text{bitxor}(C(s, t), C(s, t-1)), s \in 1 : M, t \in j+1 : 3N,\\
&S(s, t) = \text{bitxor}(C(s, t), C(s, t+1)), s \in 1 : M, t \in j-1 : -1 : 1:
\end{aligned} \quad (12)$$

*Step 2* (reverse process of scrambling).

$$S_1(:, i) = \text{circshift}(S(:, i), 3N - X(i)),$$

$$\begin{aligned}
&Q(:, X(i)) = S_1(:, i), i \in [1, 3N],\\
&P_{RGB}(Y(i), :) = Q(i, :), i \in [1, M]:
\end{aligned} \quad (13)$$

*Step 3* (the three channels of plaintext).

$$\begin{aligned}
P_R &= P_{RGB}(:, 1 : N),\\
P_G &= P_{RGB}(:, 1+N : 2N),\\
P_B &= P_{RGB}(:, 1+2N : 3N):
\end{aligned} \quad (14)$$

## 4. Simulation and Performance Analysis

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

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

$$\text{space} = 2^{512} > 2^{100}: \quad (15)$$

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.

*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 $b' = b_1 + 10^{-14}$. 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.

*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).

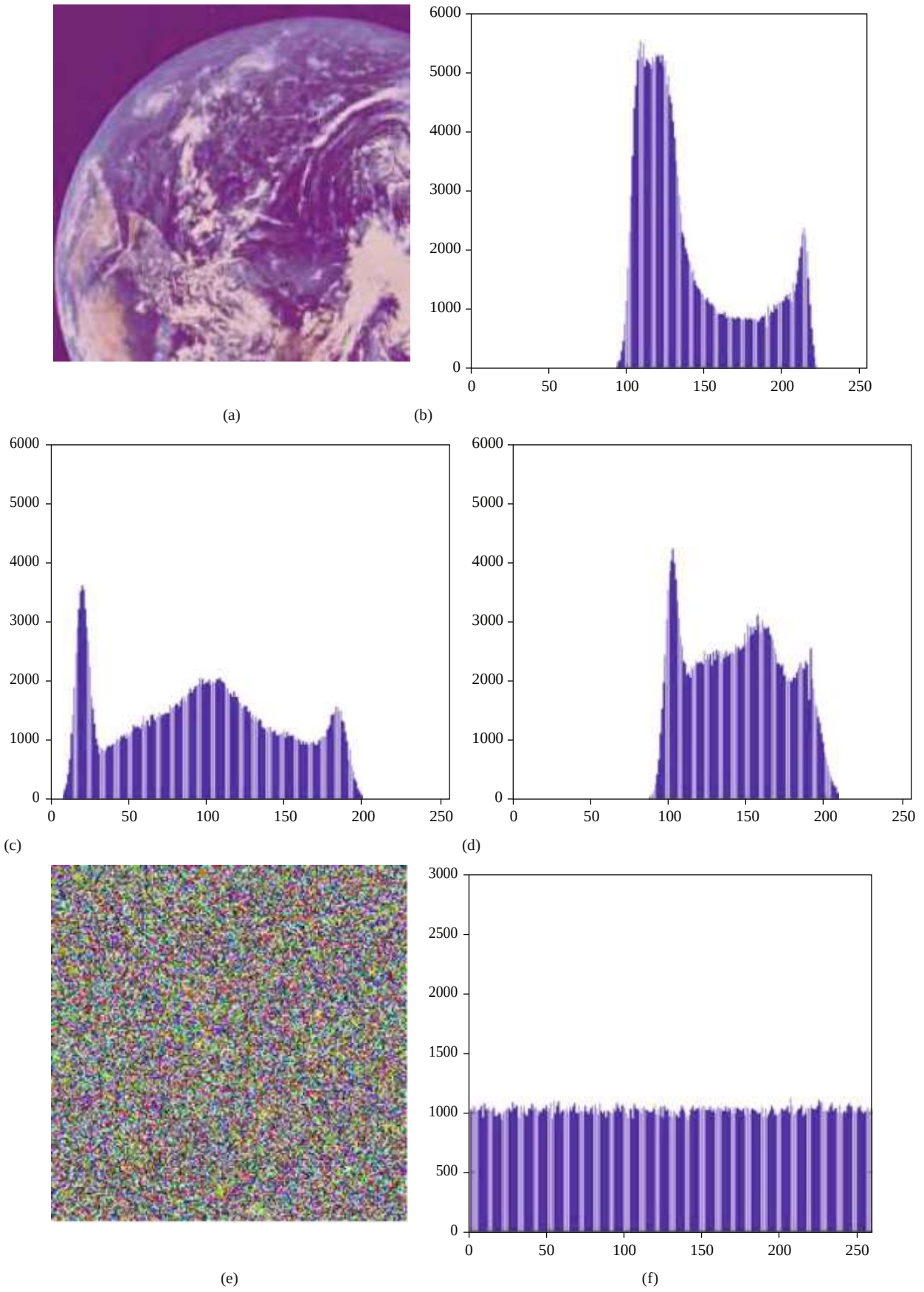



FIGURE 6: Continued.

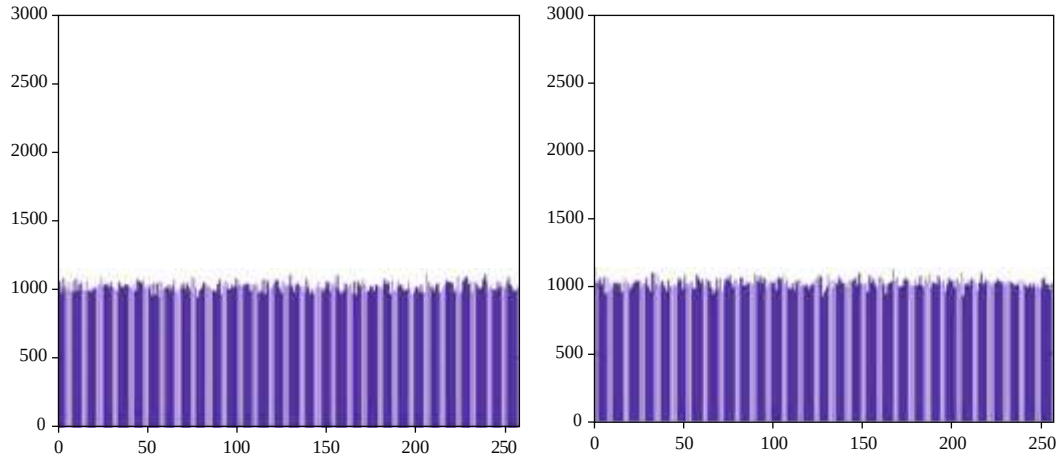



FIGURE 6: Histogram analysis. (a) Plaintext of 2.1.11_color. (b) Histogram of 2.1.11_R. (c) Histogram of 2.1.11_G. (d) Histogram of 2.1.11_B. (e) Ciphertext of 2.1.11_color. (f) Histogram of ciphertext 2.1.11_R. (g) Histogram of ciphertext 2.1.11_G. (h) Histogram of ciphertext 2.1.11_B.

TABLE 1: Correlation coefficients of images.

| Image | Plaintext | | | Proposed | | |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Lena_color_R | 0.9797 | 0.9892 | 0.9696 | -0.0005 | 0.0002 | 0.0001 |
| Lena_color_G | 0.9688 | 0.9823 | 0.9553 | -0.0009 | 0.0003 | -0.0003 |
| Lena_color_B | 0.9325 | 0.9573 | 0.9180 | -0.0009 | 0.0014 | -0.0007 |
| Goldhill_color_R | 0.9782 | 0.9731 | 0.9593 | 0.00001 | 0.0017 | -0.0013 |
| Goldhill_color_G | 0.9815 | 0.9839 | 0.9707 | 0.0013 | 0.0004 | 0.0019 |
| Goldhill_color_B | 0.9837 | 0.9845 | 0.9729 | 0.0009 | -0.0001 | -0.0012 |
| Fruits_color_R | 0.9915 | 0.9916 | 0.9832 | 0.0033 | 0.0024 | -0.0049 |
| Fruits_color_G | 0.9860 | 0.9853 | 0.9704 | 0.0022 | -0.0003 | -0.0022 |
| Fruits_color_B | 0.9510 | 0.9316 | 0.8824 | 0.0049 | -0.0019 | 0.0021 |

TABLE 2: Comparison of correlation coefficients.

| Lena | | H | V | D |
|---|---|---|---|---|
| Proposed | R | -0.0005 | 0.0002 | 0.0001 |
| | G | -0.0009 | 0.0003 | -0.0003 |
| | B | -0.0009 | 0.0014 | -0.0007 |
| Ref. [33] | R | -0.0003 | 0.0012 | -0.0017 |
| | G | -0.0007 | 0.0012 | 0.0021 |
| | B | 0.0018 | 0.0101 | 0.0023 |
| Ref. [34] | R | -0.0014 | 0.0024 | -0.0023 |
| | G | 0.0002 | 0.0007 | -0.0004 |
| | B | 0.0026 | -0.0019 | -0.0074 |
| Ref. [13] | R | -0.0029 | 0.0013 | -0.0026 |
| | G | -0.0032 | -0.0032 | -0.0039 |
| | B | 0.0040 | -0.0018 | 0.0012 |
| Ref. [35] | | 0.0006 | -0.0017 | -0.0008 |
| Ref. [36] | | 0.0013 | 0.0022 | 0.0006 |
| Ref. [37] | | -0.0747 | -0.0015 | -0.0013 |

TABLE 3: Average NPCR and UACI values between two ciphertexts.

| Image | NPCR (%) | UACI (%) |
|---|---|---|
| Lena_color_R | 99.6023 | 33.4610 |
| Lena_color_G | 99.6092 | 33.4563 |
| Lena_color_B | 99.6111 | 33.4783 |
| Goldhill_color_R | 99.6536 | 33.4568 |
| Goldhill_color_G | 99.6036 | 33.4632 |
| Goldhill_color_B | 99.6102 | 33.4652 |
| Fruits_color_R | 99.6046 | 33.4863 |
| Fruits_color_G | 99.6123 | 33.4446 |
| Fruits_color_B | 99.5326 | 33.4789 |

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.

TABLE 4: NPCR and UACI comparison with other algorithms (%).

| Proposed | Average | Ref. [33] | Ref. [34] | Ref. [13] | Ref. [35] | Ref. [37] | Ref. [38] |
|---|---|---|---|---|---|---|---|
| NPCR | 99.6075 | 99.6099 | 99.9948 | 99.6100 | 99.6100 | 99.6500 | 99.6200 |
| UACI | 33.4652 | 33.5510 | 33.3616 | 33.5000 | 33.3600 | 33.5100 | 33.4000 |

TABLE 5: Information entropy of images.

| Image | Plain | Proposed |
|---|---|---|
| Lena_color_R | 7.2530 | 7.9993 |
| Lena_color_G | 7.5951 | 7.9993 |
| Lena_color_B | 6.9685 | 7.9994 |
| Goldhill_color_R | 7.6100 | 7.9995 |
| Goldhill_color_G | 7.5544 | 7.9995 |
| Goldhill_color_B | 7.5539 | 7.9996 |
| Fruits_color_R | 7.5381 | 7.9992 |
| Fruits_color_G | 7.3435 | 7.9994 |
| Fruits_color_B | 6.7969 | 7.9992 |

TABLE 6: Information entropy comparison.

| Channels | Proposed | Ref. [33] | Ref. [34] | Ref. [35] | Ref. [37] | Ref. [38] |
|---|---|---|---|---|---|---|
| R | 7.9993 | 7.9977 | 7.9973 | 7.9951 | 7.9974 | 7.9970 |
| G | 7.9993 | 7.9968 | 7.9969 | 7.9965 | 7.9968 | 7.9970 |
| B | 7.9994 | 7.9969 | 7.9971 | 7.9829 | 7.9970 | 7.9976 |

TABLE 7: Time efficiency analysis.

| Algorithms | Proposed | Ref. [35] | Ref. [37] | Ref. [38] | Ref. [39] |
|---|---|---|---|---|---|
| Time/s | 2.31 | 12.23 | 21.94 | 2.68 | 19.14 |

The calculation formula is as follows:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (16)$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \quad (17)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \quad (18)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad (19)$$

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 it can resist statistical attacks.

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

$$\mathrm{NPCR} = \frac{\sum_{i,j} E(i,j)}{M \times N} \times 100\%, \quad (20)$$

$$\mathrm{UACI} = \frac{1}{M \times N}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%: \quad (21)$$

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.

*Information Entropy Analysis.* Information entropy rep- resents the degree of confusion of information distribution. The bigger the information entropy, the more chaotic the information distribution. Conversely, the smaller the infor- mation entropy, the more uniform the information distribu- tion. The calculation formula is as follows:

$$H(s) = \sum_{i=0}^{2^L-1} p(s) \log_2 \frac{1}{p(s)}: \quad (22)$$

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] of Lena. The experimental results show that the information entropy of the algorithm proposed in this paper is closer to 8, so this algorithm has higher security.

*Time Analysis.* The system environment is as follows: win7 system, CPU: 5210 U, 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.

## References

[1] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, "Construction of s-boxes using different maps over elliptic curves for image encryption," *IEEE Access*, vol. 9, pp. 157106–157123, 2021.

[2] X. Zhang and J. Tian, "Multiple-image encryption algorithm based on genetic central dogma," *Physica Scripta*, vol. 97, no. 5, article 055213, 2022.

[3] Z. X. Wang, K. Y. Sha, and X. L. Gao, "Digital watermarking technology based on LDPC code and chaotic sequence," *IEEE Access*, vol. 10, pp. 38785–38792, 2022.

[4] 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.

[5] 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.

[6] 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.

[7] 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*, p. 1, 2021.

[8] Y. Li, T. Zhang, and Y. Zhang, "Adaptive control of the chaotic system via singular system approach," *Journal of Applied Mathematics*, vol. 2014, 6 pages, 2014.

[9] X. Wang, Y. Su, C. Luo, and C. Wang, "A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling," *PLoS One*, vol. 15, no. 7, p. e0236015, 2020.

[10] C. Xu, J. Sun, and C. Wang, "An image encryption algorithm based on random walk and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 30, no. 4, p. 2050060, 2020.

[11] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, "Colour image encryption scheme based on enhanced quadratic chaotic map," *IET Image Processing*, vol. 14, no. 1, pp. 40–52, 2020.

[12] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[13] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[14] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[15] Y. Sun, H. Zhang, X. Wang, X. Q. Wang, and P. F. Yan, "2D non-adjacent coupled map lattice with q and its applications in image encryption," *Applied Mathematics and Computation*, vol. 373, p. 125039, 2020.

[16] M. Sharma, "Image encryption based on a new 2D logistic adjusted logistic map," *Multimedia Tools and Applications*, vol. 79, no. 1-2, pp. 355–374, 2020.

[17] Y. Zhang, A. Chen, Y. Tang, J. Dang, and G. Wang, "Plaintext-related image encryption algorithm based on perceptron-like network," *Information Sciences*, vol. 526, pp. 180–202, 2020.

[18] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Processing*, vol. 183, p. 108041, 2021.

[19] C. Zou, X. Wang, and H. Li, "Image encryption algorithm with matrix semi-tensor product," *Nonlinear Dynamics*, vol. 105, no. 1, pp. 859–876, 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] V. F. Signing, G. G. Tegue, M. Kountchou et al., "A cryptosystem based on a chameleon chaotic system and dynamic DNA coding," *Chaos, Solitons and Fractals*, vol. 155, p. 111777, 2022.

[22] M. Yildirim, "Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit," *Chaos, Solitons and Fractals*, vol. 155, p. 111631, 2022.

[23] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, 2020.

[24] L. Liu, M. Lei, and H. Bao, "Event-triggered quantized quasi-synchronization of uncertain quaternion-valued chaotic neural networks with time-varying delay for image encryption," *IEEE Transactions on Cybernetics*, pp. 1–12, 2022.

[25] A. A. Karawia and Y. A. Elmasry, "New encryption algorithm using bit-level permutation and non-invertible chaotic map," *IEEE Access*, vol. 9, pp. 101357–101368, 2021.

[26] N. Iqbal, R. A. Naqvi, M. Atif et al., "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[27] S. Jing, Y. Guo, and W. Chen, "Meaningful ciphertext encryption algorithm based on bit scrambling, discrete wavelet transform, and improved chaos," *IET Image Processing*, vol. 15, no. 5, pp. 1053–1071, 2021.

[28] C. Li, T. Xie, Q. Liu, and G. Cheng, "Cryptanalyzing image encryption using chaotic logistic map," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1545–1551, 2014.

[29] X. Wang and H. Sun, "A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function," *Optics and Laser Technology*, vol. 122, p. 105854, 2020.

[30] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Optics and Lasers in Engineering*, vol. 134, p. 106202, 2020.

[31] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[32] H. Liu, Y. Zhang, A. Kadir, and Y. Xu, "Image encryption using complex hyper chaotic system by injecting impulse into parameters," *Applied Mathematics and Computation*, vol. 360, pp. 83–93, 2019.

[33] R. Hosseinzadeh, M. Zarebnia, and R. Parvaz, "Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral," *Optics and Laser Technology*, vol. 120, p. 105698, 2019.

[34] X. Kang, A. Ming, and R. Tao, "Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 6, pp. 1595–1607, 2019.

[35] S. M. Basha, P. Mathivanan, and A. B. Ganesh, "Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map," *Optik*, vol. 259, p. 168956, 2022.

[36] Z. Zhu, C. Wu, J. Wang, K. Hu, and X. D. Chen, "A novel 3D vector decomposition for color-image encryption," *IEEE Photonics Journal*, vol. 12, no. 2, pp. 1–14, 2020.

[37] P. Mathivanan, "QR code based color image stego-crypto technique using dynamic bit replacement and logistic map," *Optik*, vol. 225, p. 165838, 2021.

[38] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color image encryption algorithm based on hyper-chaos and DNA computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020.

[39] X. Wang, Y. Su, C. Luo, F. Nian, and L. Teng, "Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate," *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 13845–13865, 2022.