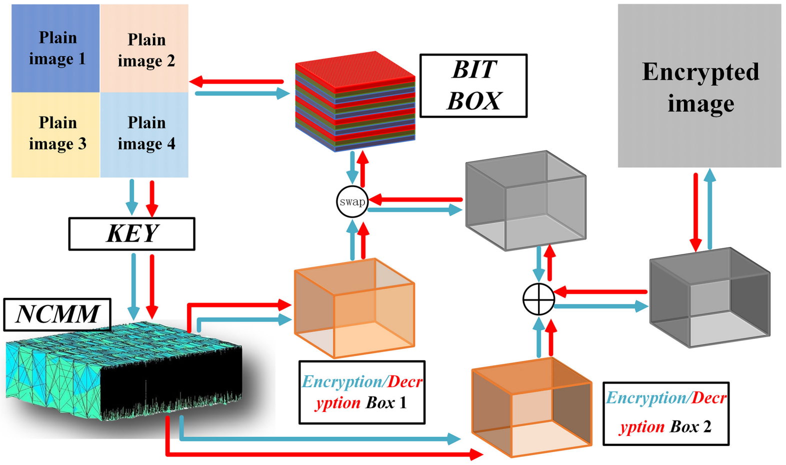
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Networked Chaotic Map Model and Its Applications in Color Multiple Image Encryption

Volume 12, Number 5, October 2020

Yu-jie Sun
Hao Zhang
Chun-peng Wang
Zhen-yu Li
Xing-yuan Wang



DOI: 10.1109/JPHOT.2020.3020307

IEEE photonics SOCIETY
IEEE

Networked Chaotic Map Model and Its Applications in Color Multiple Image Encryption

Yu-jie Sun,[1] Hao Zhang,[2] Chun-peng Wang,[3] Zhen-yu Li,[2]
and Xing-yuan Wang[4]

School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China
College of Information and Computer, Taiyuan University of Technology, Taiyuan 030024, China
School of Cyber Security, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China
School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

DOI:10.1109/JPHOT.2020.3020307

Manuscript received August 16, 2020; accepted August 26, 2020. Date of publication August 31, 2020; date of current version September 17, 2020. This work was supported in part by the National Natural Science Foundation of China under Grants 61702356, 61802212, 61672124, and 61503375) and in part by the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203). *Corresponding author: Hao Zhang (email: zhangh545@126.com).*

Abstract: In this study, a networked spatiotemporal chaotic map model is proposed based on the traditional coupled map lattice system. In addition, the time delay and variable topology parameters are considered to make the system more practical. The chaotic properties are analyzed using a bifurcation diagram, Lyapunov exponents, and entropies. In addition, institute of standards and technology tests are conducted to further analyze the randomness of the system signal. Based on the proposed system, a three-dimensional encryption algorithm is designed to encrypt multiple color images with scrambling and diffusion at the bit level. Several analyses, including histogram analysis, information entropy analysis, correlation analysis, key sensitivity, differential attack analysis, and resistance analyses, are performed to test the effectiveness and robustness of the proposed multiple image encryption algorithm with a networked chaotic map model.

Index Terms: Bit-level, Image encryption, Multiple image, Networked system, Spatiotemporal chaos.

1. Introduction

With the development of computer science and information security theory, data encryption has been widely studied and attracted intense research attention. In particular, as special text data, image encryption technology has become a popular research field [1]–[10]. To encrypt image information effectively, many typical image encryption algorithms have been proposed, such as RSA [11] and DES [12]. However, classical image encryption algorithms are not able to resolve all the problems in modern image processing. Extensive data and the strong correlation between adjacent pixels in images have made it necessary to develop new effective image encryption algorithms.

The emergence of chaos science has inspired researchers in the study of cryptography and chaos-based encryption is an important branch of typical image encryption. Different from the typical image encryption, because of its sensitivity to initial parameters and state values, a chaos system can generate completely different signals with different keys and reproduce these signals for decryption just with chaotic system and initial values. This means less information needs to be stored in the chaos-based encryption and decryption process and the risk of information leakage is lower. In addition, chaos signals are pseudo-random; hence, it is easy to scramble and diffuse plain information with chaotic signals and get satisfactory encryption effect. In a word, chaotic encryption provides a new choice for traditional encryption. In recent years, many effective chaos image encryption algorithms have been proposed [13]– [25].

In the earlier chaos image encryption studies, chaos maps utilized in encryption were always traditional classical maps. These systems have good performances with limited dimensions and detailed structures. However, limited dimensions and well-known properties also decrease the security of such image encryption algorithms. Recently, a useful spatiotemporal map system, called the coupled map lattice (CML), which adds coupling relations to multiple local dimensional maps, has been proposed and utilized in image encryption [26]– [32]. The detailed pattern of CML can be described as follows [26]:

$$\begin{cases} x_{n+1}(i) = (1-\varepsilon(i))f(x_n(i)) + \frac{\varepsilon(i)}{2}[f(x_n(i+1)) + f(x_n(i-1))] \\ f(x) = \mu x(1-x) \end{cases}, \tag{1}$$

where $i = 1, 2 \ldots, L$ is the lattice number, $\varepsilon(i) \in (0, 1)$ is the coupling parameter, $\mu \in (3.57, 4]$ is the control parameter and $f(x) = \mu x(1-x)$ is the Logistic map equation. It should be noticed that indexes of local Logistic map equation in Eq. (1) are $i-1$, i and $i+1$, respectively. This means local lattices are adjacent and the corresponding Eq. (1) is called adjacent CML. Accordingly, CML without above adjacent local map indexes is called non-adjacent CML.

With the CML system, the system dimension and encryption security are improved by the flexibility of the coupling system.

However, it should be noted that the CML's pattern is also fixed by its definition (Eq. (1)) and the topology structure of the whole system can be seen as a regular network. In fact, complex networks in practice are always random coupling. As a result, a networked extension is more practical and can further improve security by randomly coupling the local maps. As far as we know, no literature on this topic has been proposed before. In addition, time delays for the networked system are common; hence, the CML needs to be extended by adding time lags.

Motivated by these discussions, this study proposes a networked chaotic map model with added network time delays to make the system more practical. Because multiple chaos signals can be generated by the networked system at the same time and signals can be applied in the encryption of multiple images and channels, networked chaotic map model (NCMM) system signals are utilized in the encryption of multiple color images. Multiple image encryption is an extension of single image encryption and it can enhance the encryption efficiency and take full advantages of the high dimensional chaotic system signals. In recent years, some research on the multiple image encryptions [33]– [36] are proposed to make this study a hot spot. Based on the motivations and background, the contributions of this study are listed as follows: (1) The NCMM system is a high-dimensional spatiotemporal chaotic system with a random topological structure. (2) The variable topology matrix and added time delay make the system practical and difficult to identify. (3) The 3D spatiotemporal structure of generated signals can be conveniently utilized to deal with the bit space of multiple images and multiple channels in 3D space. (4) Fast scrambling and diffusion methods with NCMM signals can yield satisfactory encryption results. The remainder of this paper is organized as follows. In Section 2, the NCMM is introduced and analyzed. The main multiple image encryption algorithm with NCMM is proposed in Section 3. Section 4 presents a variety of analyses and experiments. Finally, Section 5 concludes the paper.

2. The Networked Chaotic Map Model and Its Dynamical Analysis

In this paper, the networked chaotic map model (NCMM) system can be described by Eq. (2):

$$\begin{cases} x_{n+1}(i) = (1-\varepsilon(i))f(x_n(i)) + \varepsilon(i)Af(x_n(j)) \\ f(x) = \mu x(1-x) \end{cases}, \tag{2}$$

where the parameters are the same as those defined in Eq. (1). The coupling matrix $A = (A_{i,j})_{L\times L}$ has following properties:

$$\begin{cases} A_{i,i} = 0, & i = j \\ A_{i,j} \geq 0, & i \neq j \\ \sum_{j=1,\, j\neq i}^{L} A_{i,j} = \varepsilon(i), & i, j = 1, 2, \ldots, L \end{cases}$$

Remark 1: By fixing $\varepsilon(1) = \varepsilon(2) = \cdots \varepsilon(L) = \varepsilon$, $A_{i,i-1} = A_{i,i+1} = \frac{1}{2}\varepsilon$ and other $A_{i,j} = 0$, the extended NCMM is degraded into the general adjacent CML model; If define $\varepsilon(1) = \varepsilon(2) = \cdots \varepsilon(L) = \varepsilon$, $A_{i,a} = A_{i,b} = \frac{1}{2}\varepsilon$ and other $A_{i,j} = 0$, where a and b are lattice indexes generated by Arnold map with parameter a, then the NCMM is degraded into the non-adjacent CML model.

Although the proposed system (Eq. (2)) is an extended model of CML, it is still a simple model without time delay. In practice, partial chaotic signals are not transmitted directly to the target node; time delay should be considered. Therefore, the NCMM with time delay can be defined as

$$\begin{cases} x_{n+1}(i) = (1-\varepsilon(i))f(x_n(i)) + (1-\alpha)\varepsilon(i)A_{i,j}f(x_n(j)) + \alpha\varepsilon(i)B_{i,j}f(x_{n-\tau}(j)) \\ f(x) = \mu x(1-x) \end{cases}, \tag{3}$$

where matrices $A = (A_{i,j})_{L\times L}$ and $B = (B_{i,j})_{L\times L}$ represent the coupling matrices with and without time delays, respectively. τ is the time delay and α is the coefficient of delay. The other parameters are defined similarly as the parameters in the system defined in Eq. (2). By considering the networked topology and time delays in the network, the NCMM becomes randomly coupled and practical. To analyze the representative NCMM (Eq. (3)) and apply the results to image encryption, we set L= 8, $\varepsilon(1) = \varepsilon(2) = \cdots \varepsilon(8) = \varepsilon = 0.05$, $\tau = 4$, $\alpha = 0.3$ and

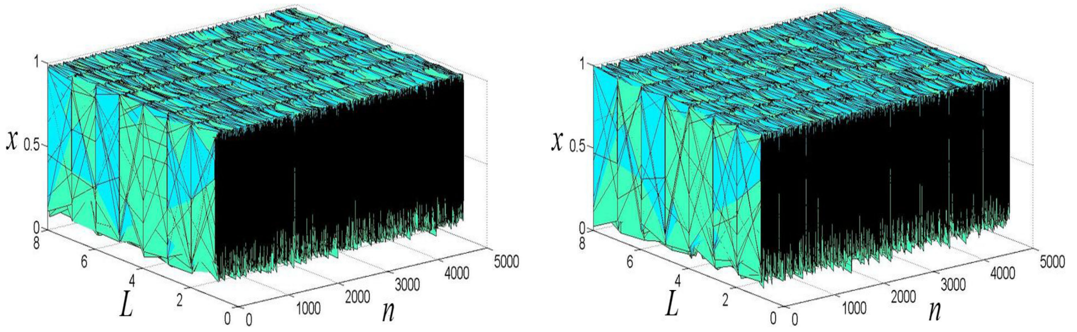
$$A = B = \begin{bmatrix} 0 & 0.2759 & 0.1379 & 0.069 & 0.0344 & 0.069 & 0.1379 & 0.2759 \\ 0.2759 & 0 & 0.2759 & 0.1379 & 0.069 & 0.0344 & 0.069 & 0.1379 \\ 0.1379 & 0.2759 & 0 & 0.2759 & 0.1379 & 0.069 & 0.0344 & 0.069 \\ 0.069 & 0.1379 & 0.2759 & 0 & 0.2759 & 0.1379 & 0.069 & 0.0344 \\ 0.0344 & 0.069 & 0.1379 & 0.2759 & 0 & 0.2759 & 0.1379 & 0.069 \\ 0.069 & 0.0344 & 0.069 & 0.1379 & 0.2759 & 0 & 0.2759 & 0.1379 \\ 0.1379 & 0.069 & 0.0344 & 0.069 & 0.1379 & 0.2759 & 0 & 0.2759 \\ 0.2759 & 0.1379 & 0.069 & 0.0344 & 0.069 & 0.1379 & 0.2759 & 0 \end{bmatrix}$$

With the aforementioned definitions, the derived temporal–spatial dynamic pattern of the NCMM is shown in Fig. 1(a). For comparison, the temporal–spatial dynamic pattern of the adjacent CML is shown in Fig. 1(b).

It can be seen from Fig. 1 that the NCMM has a similar dynamic pattern to CML. However, the coupling relationships became more complex and unpredictable when all the nodes linked. In addition, the time delay also makes the system different from the regular network; it makes the system more practical by taking signal transmission time into consideration.

Considering the Logistic map and first lattices in the NCMM and CML, one can obtain the following bifurcation diagrams and largest Lyapunov exponent diagrams.

From Fig. 2, one can see that the local dynamics in the CML and NCMM are similar. Both the local dynamics in the CML and NCMM are different from that in the classical logistic chaotic map. Obvious periodic windows disappear in the bifurcation diagrams, and similar local bifurcation and



(a) NCMM (b) CML

Fig. 1. Temporal-spatial dynamic pattern of NCMM and CML. (a) NCMM. (b) CML.

Lyapunov exponents can be derived. This means that local chaotic signals in the CML can be replaced with local chaotic signals of the NCMM in applications such as image processing.

To further analyze the dynamical properties of the NCMM with computer simulation and depict the dynamical pattern with detailed data, the entropy analysis is introduced from two aspects. First, the Kolmogorov–Sinai entropy density is used to eliminate the global chaotic properties of the NCMM with L nodes, which can be defined as

$$h = \frac{\sum_{i=1}^{L} \lambda^{+}(i)}{L}, \tag{4}$$

where $\lambda(i)$ is the lyapunov exponent of the ith node and is defined as $\lambda^{+}(i)$ if $\lambda(i)$ is positive. Second, we use the Kolmogorov–Sinai entropy breadth to depict the ratio of positive Lyapunov exponents as

$$h^{+} = \frac{L^{+}}{L}, \tag{5}$$

where L^{+} is the number of NCMM nodes with positive Lyapunov exponents. For comparison, the Kolmogorov–Sinai entropy densities and breadths of adjacent CML and NCMM with time delay are presented as follows, respectively.

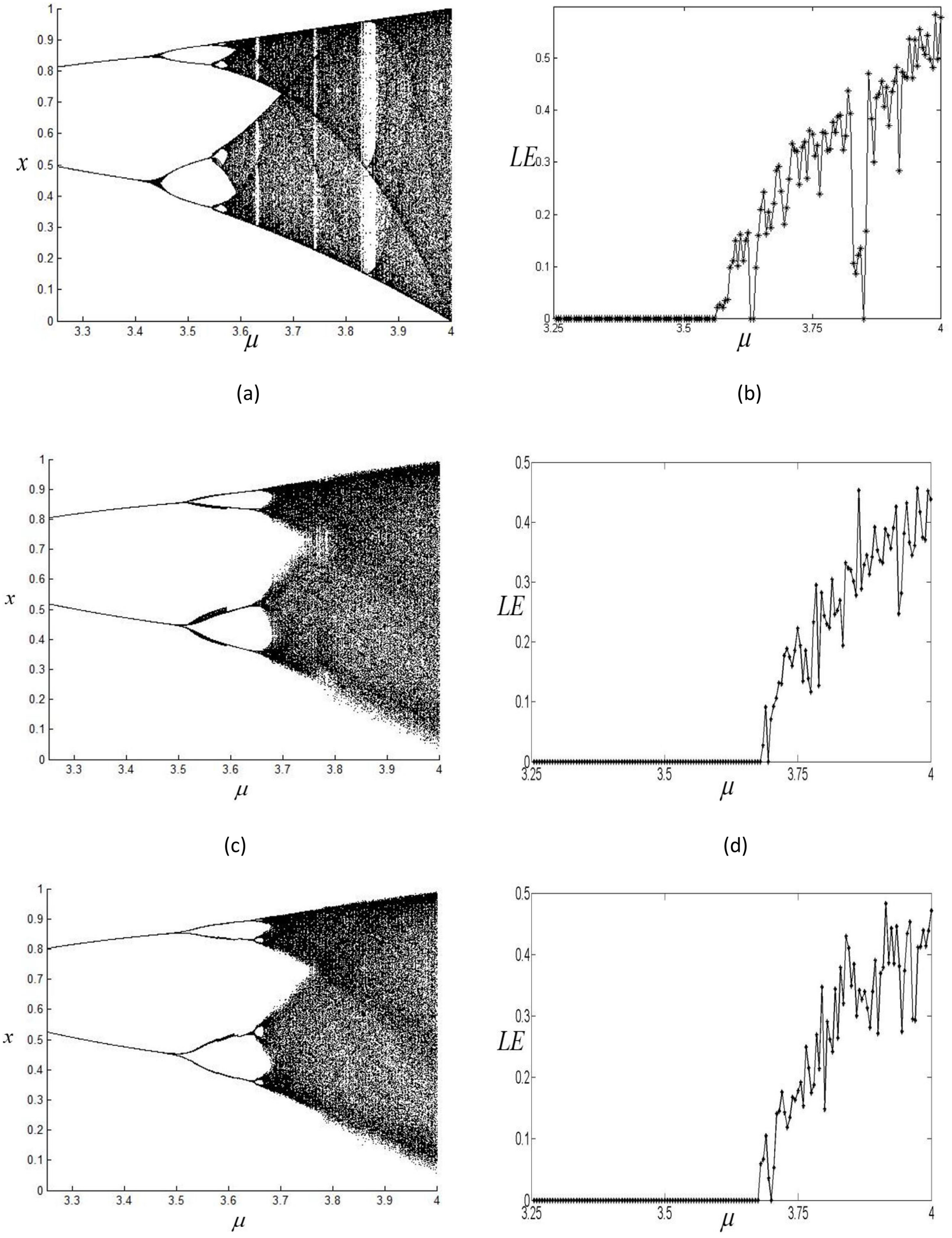
By comparing Fig. 3(c) with Fig. 3(a), it can be seen that the entropy density diagram of NCMM is more convex; the signals contain larger Kolmogorov–Sinai entropy densities than the diagram of CML. In addition, by comparing Fig. 3(d) with Fig. 3(b), it can be seen that there are more smooth areas in the NCMM breadth diagram than the CML breadth diagram. This means that the NCMM generates more chaotic signals with positive Lyapunov exponents under the same conditions. Overall, the NCMM shows better performance than the CML as an indicator of entropy.

In this study, the NIST SP800-22 test was considered to test the randomness of the proposed NCMM. The NIST SP800-22 test includes 15 random test methods to test the statistical characteristics of the time series. If the test result is greater than 0.01, this means that the NCMM passed the test and the randomness is good. The test results of NCMM are listed as follows.

From Table 1, it can be seen that all test results of NCMM and CML are greater than 0.01, and the corresponding randomness tests are passed. This means that the signals generated by the proposed NCMM are sufficiently good and it can be utilized to replace the classical CML in the encryption applications that require randomness.

3. Color Multiple Image Encryption Algorithm

To test the cryptographic performance, the aforementioned NCMM was applied to multiple image encryption. In the whole encryption, bit signals in multiple images were diffused and scrambled to obtain the encrypted images. It should be noted that three-dimensional pixel or bit distribution is



(a) (b)

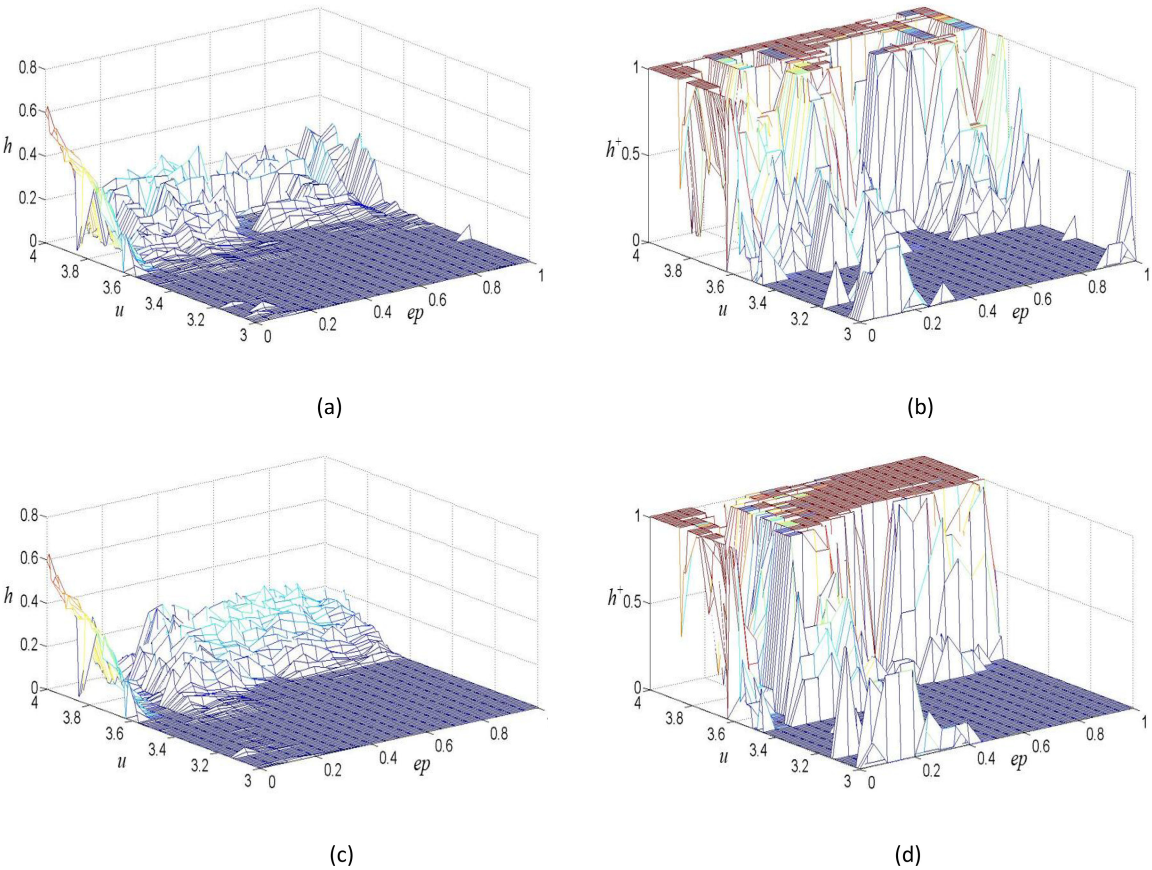
(c) (d)

(e) (f)

Fig. 2. Bifurcation and Largest lyapunov exponent diagrams of CML and NCMM (a) Bifurcation diagrams of Logistic map with μ. (b) Largest lyapunov exponent diagram of Logistic map versus μ. (c) Bifurcation diagrams of CML with μ. (d) Largest lyapunov exponent diagram of CML versus μ. (e) Bifurcation diagrams of NCMM with μ. (f) Largest lyapunov exponent diagram of NCMM versus μ.

more suitable for processing because of the temporal–spatial traits in the NCMM. Consider an encryption consisting of four images as an example. The bit signal three-dimensional decomposition can be depicted as shown in Fig. 4.

From Fig. 4, it can be seen that 8-bit planes compound any R, G, or B plane, and R, G, and B planes compound any color image. Arranging the bit planes of four color images in order (r1, g1,



(a)

(b)

(c)

(d)

Fig. 3. Kolmogorov-Sinai entropy information of NCMM and CML. (a) Entropy density of CML. (b) Entropy breadth of CML. (c) Entropy density of NCMM. (d) Entropy breadth of NCMM.

b1, r2, g2, b2, r3, g3, b3, r4, g4, b4) translates the color images into a three-dimensional bit box. Then, the three-dimensional bit box can be easily scrambled and diffused with the corresponding NCMM key box to obtain the encryption as follows.

In Fig. 5, four color images are translated into a bit box using the process shown in Fig. 4. At the same time, two encryption boxes are generated by the NCMM to scramble and diffuse corresponding bit boxes. Blue lines represents the encryption process and red lines represents the symmetric decryption process in Fig. 5. In addition, $\oplus$ represents the the XOR operation and swap means the swap operation. The detailed steps are as follows.

Step 1: For the four provided $m \times n$ color images P_1, P_2, P_3 and P_4, rearrange the image bits as the bit box A_1 sized $m \times n \times 96$, and reshape $A_1 = reshape(A_1, 1, m \times n \times 96)$.

Step 2: With NCMM, generating an encryption box B_1 sized $m \times n \times 96$. Reshape $B_1 = reshape(B_1, 1, m \times n \times 96)$. Sort the data in B_1 with $sort(\bullet)$ and get the index vector $Index$.

Step 3: From 1 to $m \times n \times 96$,transmit data with the formula $A_2(:, i) = A_1(:, index(i))$ and reshape $A_2 = reshape(A_2, m, n, 96)$.

Step 4: Iterate the logistic map with a plain-text related initial value and obtain the cyclic shift parameters $s(a)$, $s(b)$ and $s(c)$. The parameters are fixed as $a = fix(\bmod(s(a) \times 10^6), m)$, $b = fix(\bmod(s(b) \times 10^6), n)$and $c = fix(\bmod(s(c) \times 10^6), 96)$.

Step 5: Perform the cyclic shift operation as $A_3 =$ circshift$(A_2, [a, b, c])$. Reshape $A_3 = reshape(A_3, 1, m \times n \times 96)$. With NCMM, generate an encryption box B_2 sized

TABLE 1
The Test Results of NIST SP800-22 for NCMM and CML Bit Streams

Test	P-Values of NCMM	Pass or not	P-Values of CML	Pass or not
Frequency (Monobit) test	0.3964	Pass	0.3555	Pass
Frequency test	0.2021	Pass	0.3110	Pass
Runs test	0.5050	Pass	0.2878	Pass
Longest-run-of-ones in a block	0.8225	Pass	0.3871	Pass
Binary matrix rank test	0.1220	Pass	0.0483	Pass
Discrete Fourier transform test	0.2830	Pass	0.6014	Pass
Non-overlapping template matching test	0.2659	Pass	0.0959	Pass
Overlapping template matching test	0.9977	Pass	0.2009	Pass
Maurer's universal statistical test	0.1333	Pass	0.6237	Pass
Liner complexity test	0.1809	Pass	0.1802	Pass
Serial test (p-value1)	0.2596	Pass	0.1536	Pass
Serial test (p-value2)	0.2275	Pass	0.2555	Pass
Approximate entropy test	0.4231	Pass	0.3691	Pass
Cumulative sums test (Forward)	0.9992	Pass	0.9714	Pass
(Backward)	1.0000	Pass	0.9936	Pass
Random excursions test (x=-4)	0.2686	Pass	0.0361	Pass
Random excursions test (x=-3)	0.8633	Pass	0.0992	Pass
Random excursions test (x=-2)	0.9598	Pass	0.4944	Pass
Random excursions test (x=-1)	0.6109	Pass	0.9055	Pass
Random excursions test (x=1)	0.9287	Pass	0.9119	Pass
Random excursions test (x=2)	0.5992	Pass	0.9945	Pass
Random excursions test (x=3)	0.9460	Pass	0.9186	Pass
Random excursions test (x=4)	0.0644	Pass	0.5434	Pass
Random excursions variant test (x=-9)	0.0940	Pass	0.1275	Pass
Random excursions variant test (x=-8)	0.1859	Pass	0.0951	Pass
Random excursions variant test (x=-7)	0.4130	Pass	0.1538	Pass
Random excursions variant test (x=-6)	0.2433	Pass	0.2459	Pass
Random excursions variant test (x=-5)	0.1529	Pass	0.3019	Pass
Random excursions variant test (x=-4)	0.2784	Pass	0.7503	Pass
Random excursions variant test (x=-3)	0.3903	Pass	0.7674	Pass
Random excursions variant test (x=-2)	0.3112	Pass	0.5785	Pass
Random excursions variant test (x=-1)	0.2654	Pass	0.8805	Pass
Random excursions variant test (x=1)	0.2423	Pass	0.4705	Pass
Random excursions variant test (x=2)	0.2537	Pass	0.6146	Pass
Random excursions variant test (x=3)	0.7841	Pass	0.9785	Pass
Random excursions variant test (x=4)	0.5073	Pass	0.9819	Pass
Random excursions variant test (x=5)	0.5525	Pass	0.7713	Pass
Random excursions variant test (x=6)	0.6808	Pass	0.3941	Pass
Random excursions variant test (x=7)	0.4175	Pass	0.3722	Pass
Random excursions variant test (x=8)	0.4043	Pass	0.5193	Pass
Random excursions variant test (x=9)	0.5038	Pass	0.5794	Pass

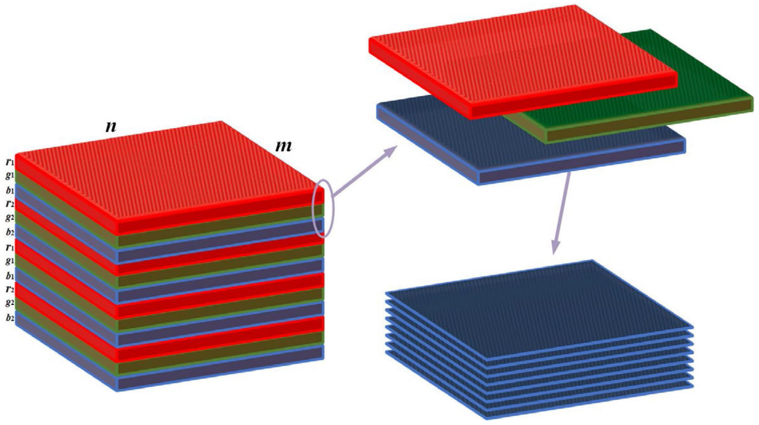


Fig. 4. Multiple images bit signal three-dimensional decomposition.

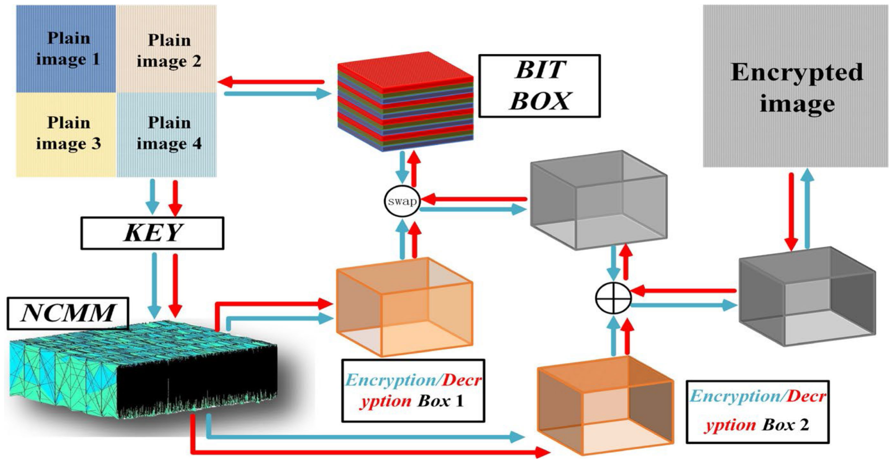


Fig. 5. Multiple images encryption/decryption flow chart with NCMM.

$m \times n \times 96$. Reshape B_2=$reshape(B_2, 1, m \times n \times 96)$. Then perform the XOR operations $A_3(1) = A_3(1) \oplus B_2(1) \oplus A_3(m \times n \times 96)$ and $A_3(i) = A_3(i) \oplus B_2(i) \oplus A_3(i-1)$ twice.

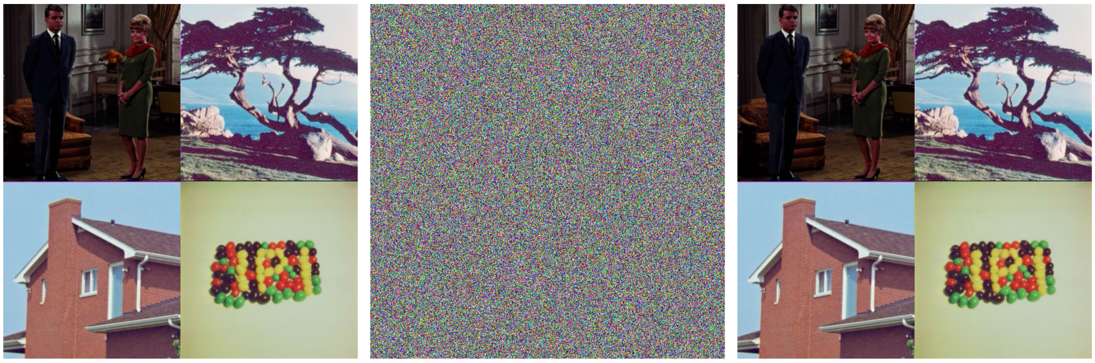
Step 6: Reshape the bit box and recover the color images with bit planes in accordance with different color channels. Then the encryption process is completely completed.

Where $reshape(\bullet)$, $fix(\bullet)$, mod$(\bullet)$, circshift$(\bullet)$, $sort(\bullet)$ and $index(\bullet)$ are all standard Matlab functions. Because the encryption algorithm is symmetrical, the image can be totally recovered with a symmetrical decryption method. Detailed encryption and decryption results are presented in the following sections.

4. Color Multiple Image Encryption Algorithm

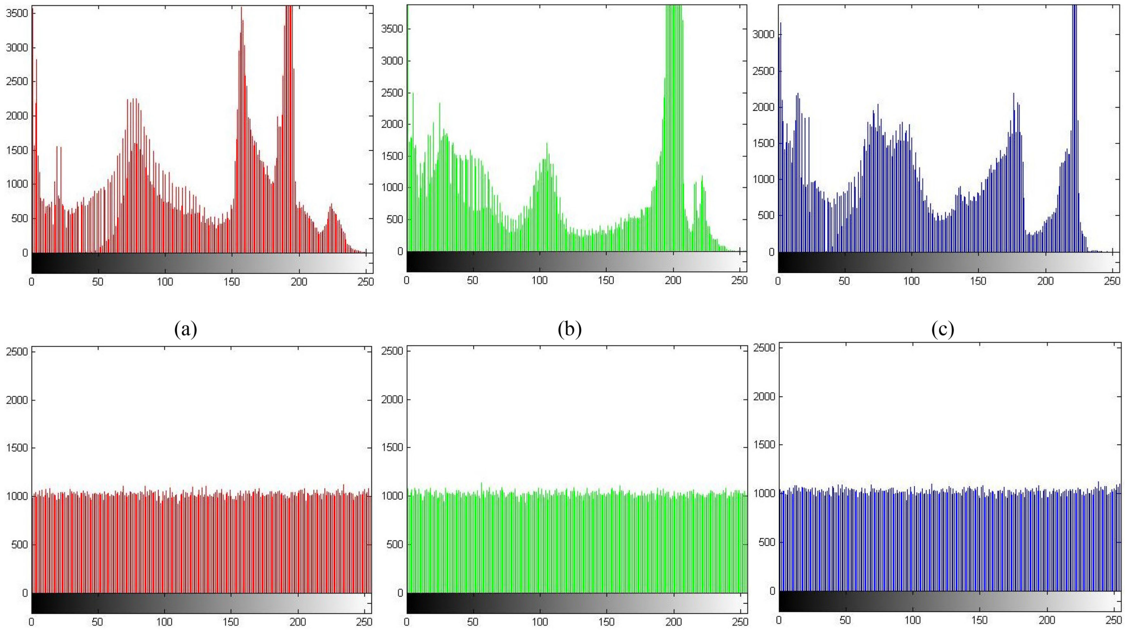
In this section, tests to analyze the multiple image encryption algorithm are reported. Simulations were performed using the MATLAB 2014a software on a Thinkpad L470 laptop with an Intel-Core, i7-7500U, X64 CPU, 16 GB RAM, and Windows 10 operation system (64 bit). Multiple images cover “Couple.bmp”, “House.bmp”, “Tree.bmp” and “Bean.bmp” sized 256 × 256 from the USC-SIPI image database. The hybrid encryption and decryption results are shown in Fig. 6.

Fig. 6(a) shows a combined image of multiple plain images. With the proposed method, Fig. 6(a) is encrypted as shown in Fig. 6(b), and no plaintext information can be observed. With the symmetrical decryption method, the encrypted image in Fig. 6(b) is completely recovered, as shown in Fig. 6(c).



(a) (b) (c)

Fig. 6. Encryption and decryption results: (a) Multiple plain images. (b) Encrypted hybrid images. (c) Decrypted images.



(a) (b) (c)

(d) (e) (f)

Fig. 7. Histograms of plaintext images and ciphertext images (a) Red component of Fig. 6(a). (b) Green component of Fig. 6(a). (c) Blue component of Fig. 6(a). (d) Red component of Fig. 6(b). (e) Green component of Fig. 6(b). (f) Blue component of Fig. 6(b).

4.1 Plaintext and Ciphertext Histogram Analysis

To analyze the image encryption properties, histograms were utilized to determine the pixel distribution. For a robust image encryption algorithm, pixels of the encrypted images are almost equally distributed, and no concentrated pixel distribution can be observed in the histogram. Taking the plaintext image in Fig. 6(a) and the encrypted image in Fig. 6(b) as an example, the derived histograms for different channels are shown as follows.

Figs. 7(a)–(c) are histograms of the plaintext images shown in Fig. 6(a) for the R, G, and B components, respectively. It can be observed that plaintext pixels are not evenly distributed, and obvious peaks and troughs can be seen in Figs. 7(a)–(c). By contrast, ciphertext pixels are evenly

TABLE 2
Information Entropies of Multiple Encrypted Images

Image	R component	G component	B component
Couple	7.9967	7.9974	7.9972
House	7.9970	7.9973	7.9970
Tree	7.9973	7.9973	7.9971
Bean	7.9974	7.9974	7.9968

TABLE 3
Information Entropies Comparisons of LENA IMAGE

Algorithm	R component	G component	B component
Our algorithm	7.9973	7.9974	7.9970
[5]	7.9893	7.9896	7.9903
[6]	7.3894	7.5280	7.5173
[15]	7.9974	7.9972	7.9968
[25]	7.9968	7.9969	7.9975

distributed in Figs. 7(d)–(f), and no obvious peak or trough can be seen. This shows that the encryption is effective in resisting the statistical analysis of pixels.

4.2 Information Entropy Analysis

In the previous section, the entropy was utilized to test the signals of the NCMM. Similarly, the image information can also be analyzed using information entropy. For any given information source m, information entropy can be defined by the following formula:

$$h(m) = \sum_{i=0}^{l-1} p(m_i) log \frac{1}{p(m_i)}, \tag{6}$$

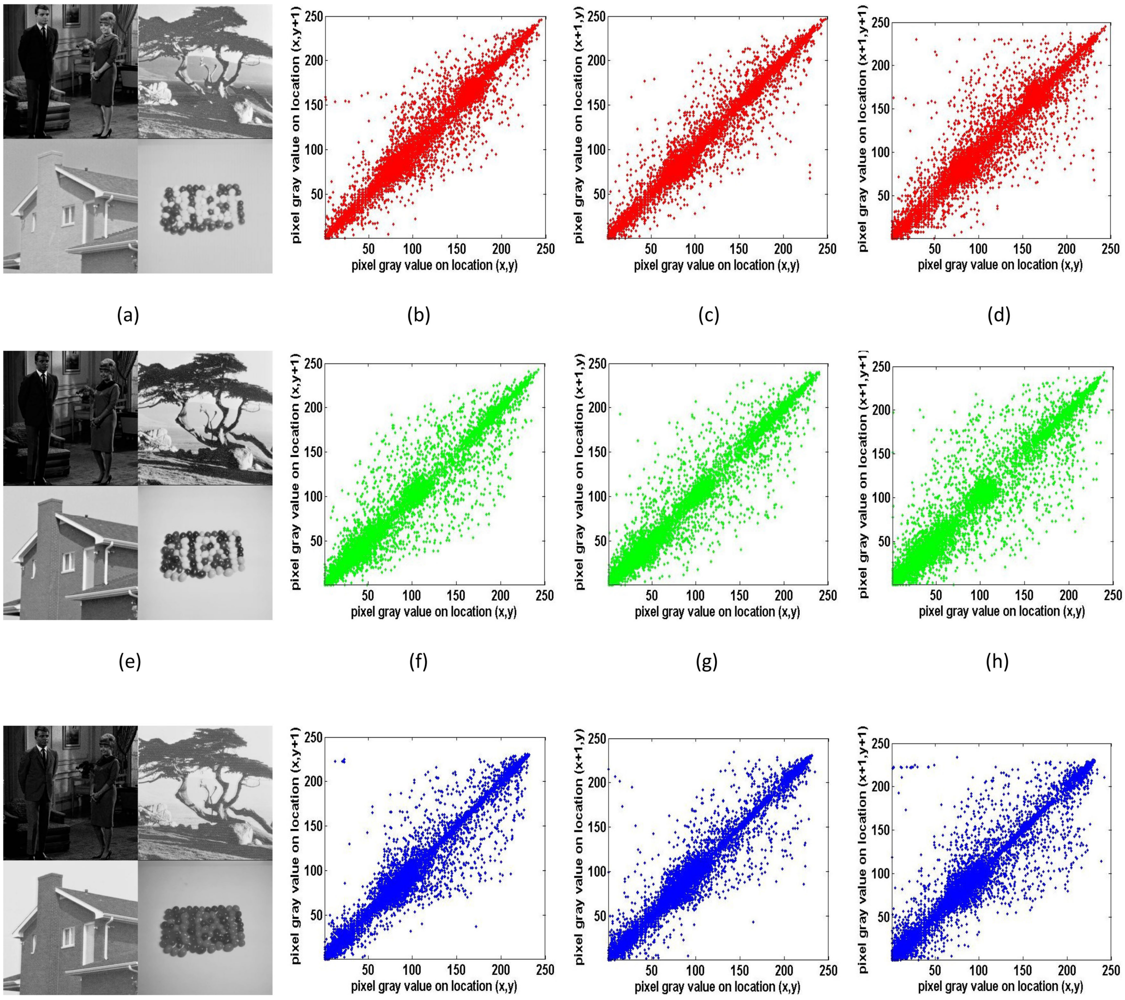
where l is the number of symbols and $p(m_i)$ represents the probability of the ith symbol. For information entropy, the ideal value can be calculated as 8, which means that the information entropy of an image encrypted with a robust algorithm should be close to 8. For the provided example, the entropies for different images are shown in the following table.

From Table 2, it can be observed that entropies for different images after the encryption process are all closed to the ideal value, and the algorithm is robust. It should be noticed that even though this paper focus on the multiple image encryption, the encryption algorithm can also be applied in single image encryption as a special case of multiple image encryption. For example, the information entropy analysis for Lena image and some comparisons are listed in following Table 3.

From Table 3, it can be seen that our algorithm is the information entropies are all closed to 8. In addition, the information entropy of our algorithm is higher compared with listed references. These mean that the proposed algorithm is robust enough to resist possible entropy attack and analysis.

4.3 Correlation Analysis of Adjacent Pixels

For general plaintext images, adjacent pixel series are significantly related to each other; correlation information can easily be utilized to attack the encryption algorithm. Generally, the correlation of adjacent pixel series in a plaintext image is close to 1, and the correlation of adjacent pixel series in a ciphertext image after encryption is close to 0. For any given image pixel series, $a = \{a_i\}$ and



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

(e) (f) (g) (h)

(i) (j) (k) (l)

Fig. 8. Adjacent pixel correlation of the multiple images (a) R channel, (b) Horizontal of (a), (c) Vertical of (a), (d) Diagonal of (a), (e) G channel, (f) Horizontal of (e), (g) Vertical of (e), (h) Diagonal of (e), (i) B channel, (j) Horizontal of (i), (k) Vertical of (i), (l) Diagonal of (i).

$b = \{b_i\}$, correlations can be calculated with following equations:

$$r_{ab} = \frac{\text{cov}(a, b)}{\sqrt{D(a)}\sqrt{D(b)}}, \tag{7}$$

where $\text{cov}(a, b) = \frac{1}{N}\sum_{i=1}^{N}[a_i - E(a)][b_i - E(b)]$, $D(a) = \frac{1}{N}\sum_{i=1}^{N}[a_i - E(a)]^2$and $E(a) = \frac{1}{N}\sum_{i=1}^{N} a_i$. To validate the correlation results, adjacent pixel series in the plaintext image and ciphertext image were selected in three different directions (horizontal, vertical, and diagonal). The detailed results are shown in Fig. 8 and Fig. 9.

Fig. 8 depicts the correlations of the color plaintext images for the three channels in different directions. Fig. 9 depicts the correlations of the ciphertext images after encryption. From Figs. 8(a)–(d), it can be seen that the adjacent pixels of the hybrid images in the horizontal direction are far related and closed. Adjacent pixel coordinates are located near the diagonal. Some results can be found in the vertical and diagonal directions from Figs. 8(e)–(h) and Figs. 8(i)–(l), respectively. Meanwhile, it can be seen from Figs. 9(a)–(d) that adjacent pixel coordinates of hybrid images after encryption in the horizontal direction are randomly distributed. Some results can be found

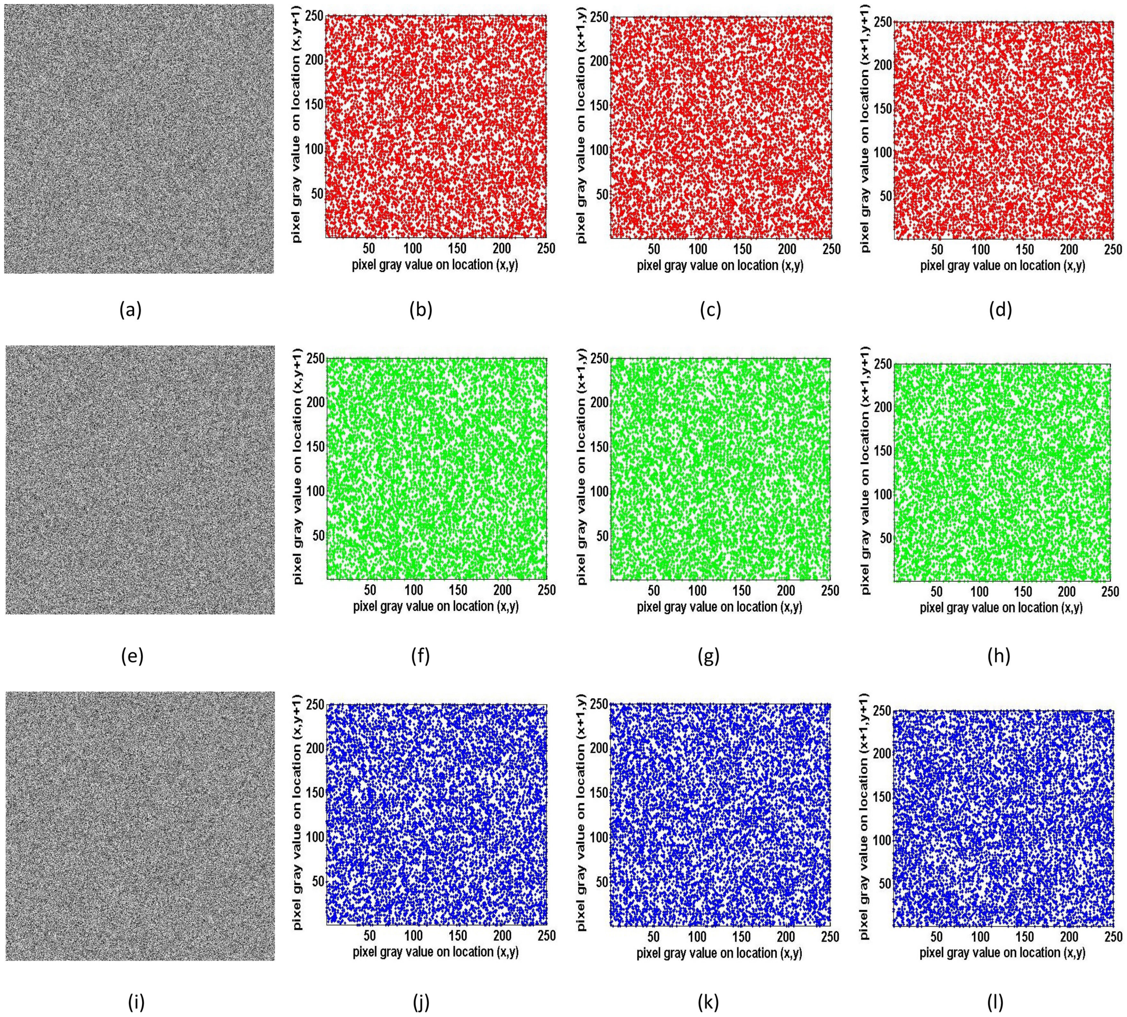


Fig. 9. Adjacent pixel correlation of the encrypted multiple images (a) R channel, (b) Horizontal of (a), (c) Vertical of (a), (d) Diagonal of (a), (e) G channel, (f) Horizontal of (e), (g) Vertical of (e), (h) Diagonal of (e), (i) B channel, (j) Horizontal of (i), (k) Vertical of (i), (l) Diagonal of (i).

in the vertical and diagonal directions from Figs. 9(e)–(h) and Figs. 9(i)–(l), respectively. This means that the correlations of the ciphertext images are effectively reduced after encryption. The corresponding correlations of individual images are shown in Table 3.

It can be seen that the correlations of the plaintext image are close to 1 and the correlations of the ciphertext image are close to 0 after the encryption. This indicates that the encryption with NCMM is sufficiently robust to resist statistical analysis.

4.4 Differential Attack Analysis

To test the resistance to possible attacks, some values, such as the number of pixels change rate (NPCR) and unified average changing intensity (UACI), were utilized to evaluate the encryption algorithm. Generally, the ideal values of NPCR and UACI are 99.6094% and the ideal value of UACI is 33.4635%, respectively. After changing one bit value in the position (10,10), the derived hybrid differential attack analysis images are shown in Fig. 10.

Based on a small change in the position (10,10), cipher images in Fig. 10(b) and Fig. 10(c) are derived. From Fig. 10(d), it can be seen that the small change in Fig. 10(a) makes the cipher

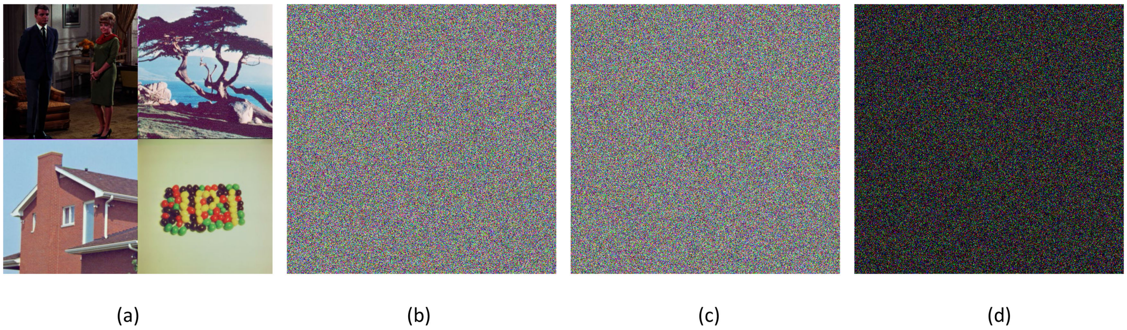


Fig. 10. Hybrid differential attack analysis images (a) Hybrid image, (b) Cipher image, (c) Cipher image with tiny change, and (d) Subtraction image of (b) and (c).

images totally different. Corresponding to Fig. 10, NPCRs of the red, green, and blue channels are 99.6163%, 99.6162%, and 99.6090%, respectively. Conversely, the UACIs of the red, green, and blue channels are 33.4663%, 33.4272%, and 33.5492%, respectively. Both the NPCRs and UACIs are close to their ideal values, which means that the algorithm is robust.

4.5 Key Sensitivity Analysis

It can be seen that the encryption result is very sensitive to small changes in the plaintext. In fact, a robust encryption algorithm should also be sensitive to small changes in the system key. For the system parameters μ and coupling strength ε in the NCMM, after adding a small change 10^{-15} to these keys, sensitive analysis images are shown in Fig. 11.

Fig. 11 shows the sensitive analysis results of the proposed encryption algorithm with the NCMM. From Fig. 11(b) and Fig. 11(c), it can be seen that the original image in Fig. 11(a) is successfully encrypted with different parameters μ, and it can be observed from the subtraction image in Fig. 11(d) that the encrypted images in Fig. 11(b) and Fig. 11(c) are completely different. With the correct key μ, Fig. 11(b) is successfully recovered. However, with the correct key μ, Fig. 11(c) cannot be decrypted. Similarly, Fig. 11(b) cannot be recovered to the correct image. This means that the proposed encryption algorithm with NCMM is also sensitive to small changes of the key. From Fig. 11(e), Fig. 11(f), Fig. 11(j) and Fig. 11(k), same conclusions can be derived for the other key ε with the key μ. This means the algorithm has good key sensitivity to multiple sub-keys. To further test the key sensitivity, the MSE(Mean Square Error) and PSNR(Peak Signal to Noise Ratio) are calculated for the decrypted image Fig. 11(c) with a tiny modified parameter μ. Results are shown in the Table 5.

It is exhibited that for both the compounded image and every sub-image, MSE values are very large and PSNR values are smaller than 10, this means the decrypted images with tiny modified parameter are unacceptable and the key sensitivity is robust. Similar to the entropy analysis, in order to compare our algorithm with existing research, the MSE and PSNR analysis is done in the Lena image to show the performance. The comparisons are listed as following Table 6.

From Table 6, it is exhibited that MSE values are all very large and PSNR values are all smaller than 10. In addition, our algorithm has larger MSE values and smaller PSNR values in most comparisons with listed references. These mean the algorithm is very sensitive to keys and it is robust to resist to possible key attacks.

4.6 Key Space Analysis

It is exhibited that the key space should be large enough for a robust encryption algorithm. In this paper, there exist L initial valuses $x_0(i)$and parameters $\varepsilon(i)$, $1 \le i \le L$, other parameters are defined as $0 \le a \le 1$, $3.569 < \mu \le 4$. Assume that the computational accuracy of the computer is set as

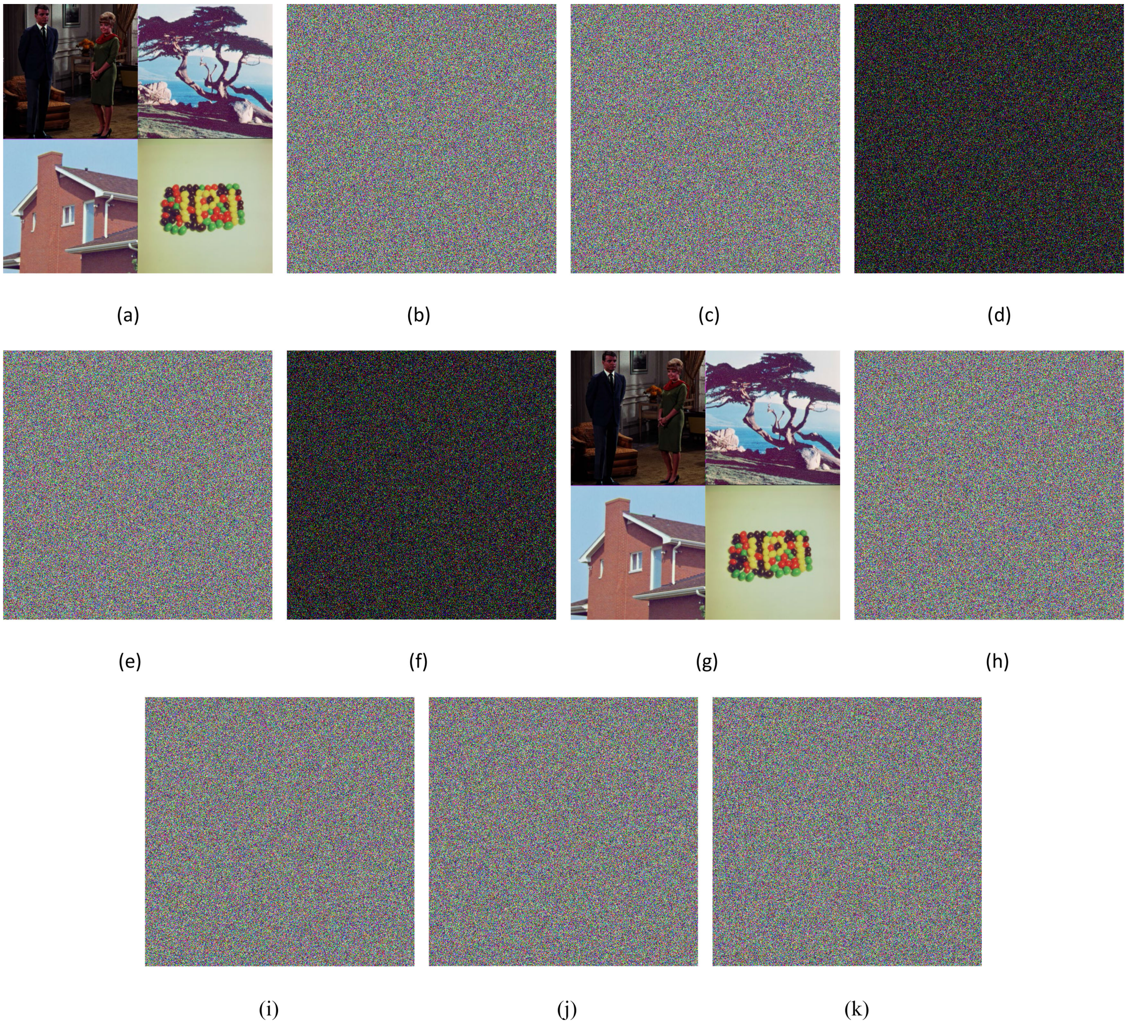


Fig. 11. Key sensitive analysis of hybrid image: (a) Original image, (b) Encrypted image of (a), (c) Encrypted image of (a) with modified μ, (d) Subtraction image of (b) and (c), (e) Encrypted image of (a) with modified ε, (f) Subtraction image of (b) and (e), (g) Decrypted image of (a) with correct μ and ε, (h) Decrypted image of (c) with u, (i) Decrypted image of (b) with modified u, (j) Decrypted image of (e) with ε, (k) Decrypted image of (b) with modified ε.

$10^{-15}$and L= 8, the key space is $S_{\text{key}} = 10^{15\times(2\times8+1+4-3.569)} \approx 2^{868}$. Obviously, the key space S_{key} is much larger than 2^{100}, so it is large enough to resist possible force attack effectively.

4.7 Resistance Analysis to Salt-and-Pepper Noise

After encryption, the image may also be tampered with in the storage procedure. To test the resistance of the proposed algorithm to external disturbances, different levels of salt-and-pepper noises were added to the cipher images. With these noises, the recovered images can be seen in Fig. 12.

From Figs. 12(a)–(c), it seems that different levels of noise have no obvious difference. However, the corresponding recovered images are obvious from Figs. 12(d)–(f). Although higher-level noise makes the recovered image less clear, it should be pointed out that all encrypted images with noise are successfully recovered. This means that the proposed encryption algorithm with NCMM is robust to resist noise attacks.

TABLE 4
Correlations of the Plaintext Image (PI) and Ciphertext Image (CI)

Image	Component	Correlation coefficient	Direction to calculation correlation		
			Horizontal	Vertical	Diagonal
Couple	Red	PI	0.9508	0.9482	0.9044
		CI	-0.000035	0.01	-0.0089
	Green	PI	0.9573	0.9220	0.8956
		CI	-0.0498	-0.0305	0.0334
	Blue	PI	0.9428	0.9275	0.8917
		CI	-0.00032	0.0163	0.0046
House	Red	PI	0.9404	0.9655	0.9059
		CI	-0.0215	-0.0109	0.0042
	Green	PI	0.9598	0.9824	0.9289
		CI	0.008	-0.0211	0.0283
	Blue	PI	0.9777	0.9808	0.9649
		CI	-0.0548	-0.0508	-0.0187
Tree	Red	PI	0.9475	0.9592	0.9162
		CI	-0.0074	-0.0024	0.008
	Green	PI	0.9368	0.9655	0.9260
		CI	-0.0066	0.0122	-0.0526
	Blue	PI	0.9458	0.9622	0.9316
		CI	-0.0116	0.0378	-0.0111
Bean	Red	PI	0.9742	0.9786	0.9548
		CI	0.0353	-0.0084	0.0419
	Green	PI	0.9756	0.0038	-0.0025
		CI	0.0091	-0.0094	-0.023
	Blue	PI	0.9886	0.9894	0.9746
		CI	-0.0124	0.0175	-0.0166

TABLE 5
MSE and PSNR of Decrypted Images

Image	Image F.11(c)	Part 1	Part2	Part 3	Part4
MSE	10683	15451	8330	9928	9025
PSNR	7.8548	6.2504	8.9695	8.1868	8.6161

TABLE 6
MSE and PSNR of Lena Image

Analysis Test	Component	Our algorithm	[23]	[25]
MSE	R	10566	10464.9	7385.1
	G	9010	8800.42	8698.7
	B	7014	7119.13	9580.0
PSNR	R	7.8917	7.93344	9.1080
	G	8.5838	8.68577	8.7362
	B	9.6714	9.60653	8.3167

4.8 Resistance Analysis to Cropping Attack

Similar to the resistance to noise analysis, the analysis of cropping is also useful to test the resistance to possible image tampering. For an encrypted hybrid image, assuming that different percentages of image information are lost, the recovered images are shown in Fig. 13.

From Figs. 13(a)–(c), it can be seen that different percentages of image information are lost. From Figs. 13(d)–(f), it can be observed that the more information lost, the less clear is the recovered image. However, regardless of the percentage of image information lost, the image information

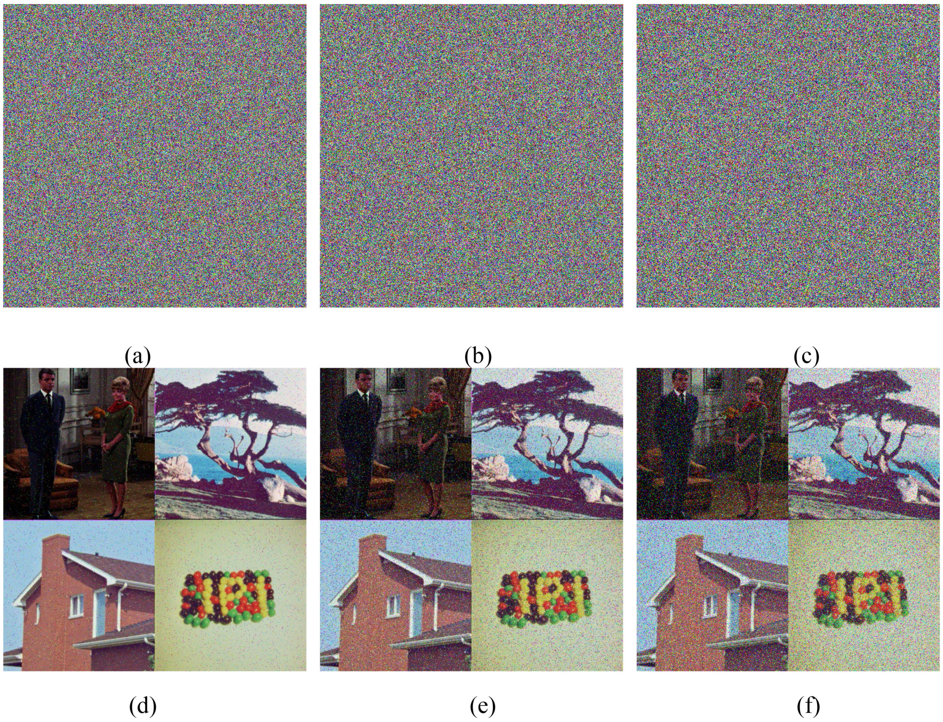


Fig. 12. Encrypted and decrypted images with salt-and-pepper noise: (a) Encrypted image with noise intensity 0.01, (b) Encrypted image with noise intensity 0.05, (c) Encrypted image with noise intensity 0.1, (d) Decrypted image of (a), (e) Decrypted image of (b), (f) Decrypted image of (c).

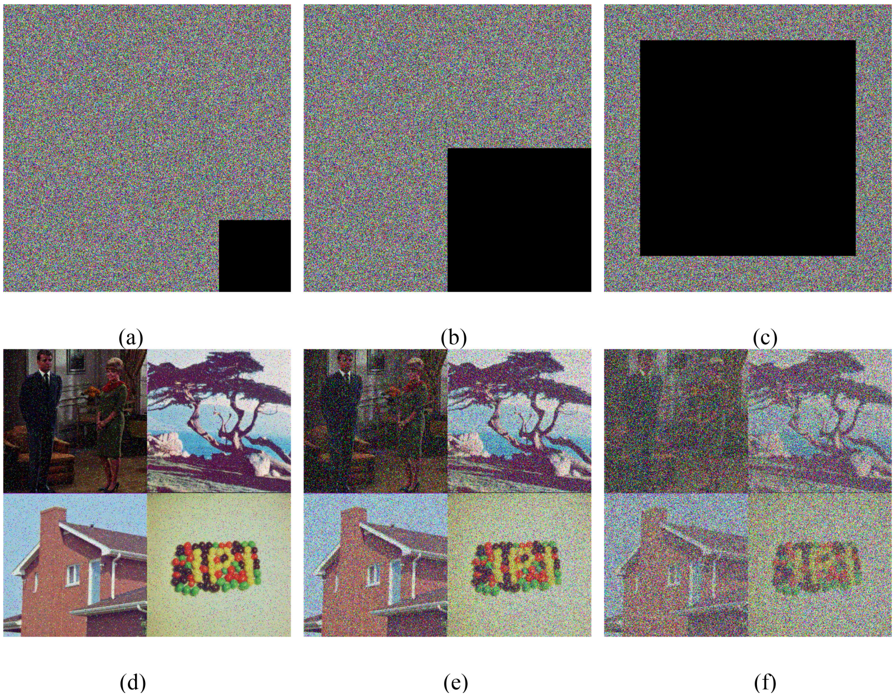


Fig. 13. Encrypted and decrypted images with information loss: (a) Encrypted image with 6.25% information loss, (b) Encrypted image with 12.5% information loss, (c) Encrypted image with 56.25% information loss, (d) Decrypted image of (a), (e) Decrypted image of (b), and (f) Decrypted image of (c).

can be easily recovered after decryption. This means that the proposed encryption algorithm with NCMM has good resistance to information loss.

5. Conclusion

In this study, the spatiotemporal chaotic system CML was extended to the NCMM with network topology analysis. From experiments, it was found that the NCMM has chaotic properties similar to those of CML and shows better performance as an indicator of entropy. To make the system practical, time delays were added to the system model, and NIST random tests were performed. With the proposed system, a 3D color image encryption algorithm was designed to deal with the plaintext information at the bit level. After the encryption, information entropy, correlation analysis, key sensitivity, differential attack analysis, noise attack, and cropping attack analyses were conducted to demonstrate the algorithm's performance. Both the theoretical analysis and numerical simulation results show that multiple image encryption with NCMM is effective and robust. It should be noticed that, multiple images encryption is far related to the big data and complex computation, and the parallel computing and processing with the multipath signals from NCMM are necessary. So in the future, we will focus on the parallel data processing of the proposed system and improve the image encryption efficiency by combing the compressing technology.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[2] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform," *IEEE Trans. Image Process.*, vol. 1, no. 2, pp. 205–220, Apr. 1992.

[3] J. K. Hu and F. L. Han, "A pixel-based scrambling scheme for digital medical images protection," *J. Netw. Comput. Appl.*, vol. 32, no. 4, pp. 788–794, 2009.

[4] Z. Zhong, J. Chang, M. G. Shan, and B. G. Hao, "Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption," *Opt. Commun.*, vol. 285, no. 1, pp. 18–23, 2012.

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

[6] D. C. Mishra, R. Sharma, S. Suman, and A. Prasad, "Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold transform," *J. Inf. Secur. Appl.*, vol. 37, pp. 65–90, 2017.

[7] Y. S. Zhang *et al.*, "Low-cost and confidentiality-preserving data acquisition for internet of multimedia things," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3442–3451, Oct. 2018.

[8] M. Khan, F. Masood, A. Alghafis, M. Amin, and S. I. B. Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *Plos One*, vol. 14, 2019, Art. no. e0225031.

[9] Y. S. Zhang, P. Wang, H. Huang, Y. W. Zhu, D. Xiao, and Y. Xiang, "Privacy-assured FogCS: Chaotic compressive sensing for secure industrial big image data processing in fog computing," *IEEE Trans. Ind. Inform.*, to be published, doi: 10.1109/TII.2020.3008914.

[10] M. Khan, F. Masood, and A. Alghafis, "Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system," *Neural Comput. Appl.*, vol. 32, pp. 11837–11857, 2020.

[11] C. S. Chen, T. Wang, Y. Z. Kou, X. C. Chen, and X. Li, "Improvement of trace-driven I-Cache timing attack on the RSA algorithm," *J. Syst. Softw.*, vol. 86, no. 1, pp. 100–107, 2013.

[12] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM J. Res. Develop.*, vol. 38, no. 3, pp. 243–250, 1994.

[13] Q. Zhang and X. P. Wei, "RGB color image encryption method based on Lorenz chaotic system and DNA computation," *IETE Tech. Rev.*, vol. 30, no. 5, pp. 404–409, 2013.

[14] M. K. Mandal, M. Kar, and S. K. Singh. "Symmetric key image encryption using chaotic Rossler system," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2145–2152, 2014.

[15] X. Y. Wang and H. L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–61, 2015.

[16] C. H. Li, G. C. Luo, and K. Qin, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, 2017.

[17] Y. Zhong, L. F. Chen, and W. W. Gan, "Image encryption system based on joint transformation correlation and ptychography," *IEEE Photon. J.*, vol. 12, no. 2, Apr. 2020, Art. no. 2400110.

[18] Y. L. Luo *et al.*, "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Process.*, vol. 161, pp. 227–247, 2019.

[19] R. Z. Li, Q. Liu, and L. F. Liu, "Novel image encryption algorithm based on improved logistic map," *IET Image Process.*, vol. 13, no. 1, pp. 125–134, 2019.

[20] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *J. Inf. Secur. Appl.*, vol. 45, pp. 117–130, 2019.

[21] Z. Zhu, C. Wu, and J. Wang, “A novel 3D vector decomposition for color-image encryption,” *IEEE Photon. J.*, vol. 12, no. 2, Apr. 2020, Art. no. 7800614.

[22] N. Munir, M. Khan, Z. Wei, A. Akgul, M. Amin, and I. Hussain, “Circuit implementation of 3D chaotic self-exciting single-disk homopolar dynamo and its application in digital image confidentiality,” *Wireless Netw.*, 2020. [Online]. Available: https://doi.org/10.1007/s11276-020-02361-9

[23] T. U. Haq and T. Shah, “12×12 S-box design and its application to RGB image encryption,” *Optik*, vol. 217, 2020, Art. no. 164922.

[24] G. Y. Luan, A. C. Li, and Z. G. Chen, “Asymmetric optical image encryption with silhouette removal using interference and equal modulus decomposition,” *IEEE Photon. J.*, vol. 12, no. 2, Apr. 2020, Art. no. 6900508.

[25] U. Arshad, M. Khan, S. Shaukat, M. Amin, and T. Shah, “An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation,” *Physica A: Statistical Mechanics Appl.*, vol. 546, 2020, Art. no. 123458.

[26] Y. Q. Zhang and X. Y. Wang, “Spatiotemporal chaos in Arnold coupled logistic map lattices,” *Nonlinear Anal.-Model. Control*, vol. 18, no. 4, pp. 526–541, 2013.

[27] X. J. Wu, Y. Li, and J. Kurths, “A new color image encryption scheme using CML and a fractional-order chaotic system,” *Plos One*, vol. 10, no. 3, 2015, Art. no. e0119660.

[28] X. Y. Wang, H. L. Zhang, and X. M. Bao, “Color image encryption scheme using CML and DNA sequence operations,” *Biosystems*, vol. 144, pp. 18–26, 2015.

[29] R. Bechikh, H. Hermassi, E. Abd, and A. Ahmed, “Breaking an image encryption scheme based on a spatiotemporal chaotic system,” *Signal Process.-Image Commun.*, vol. 39, pp. 151–158, 2015.

[30] X. J. Wu, K. S. Wang, and X. Y. Wang, “Color image DNA encryption using NCA map-based CML and one-time keys,” *Signal Process.*, vol. 148, pp. 272–287, 2018.

[31] H. P. Wen, S. M. Yu, and J. H. Lue, “Breaking an image encryption algorithm based on DNA encoding and spatiotemporal Chaos,” *Entropy*, vol. 21, no. 3, 2019, Art. no. 246. [Online]. Available: https://doi.org/10.3390/e21030246

[32] Y. He, Y. Q. Zhang, and X. Y. Wang, “A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system,” *Neural Comput. Appl.*, vol. 32, no. 1, pp. 247–260, 2020.

[33] M. R. Abuturab, “A superposition based multiple-image encryption using Fresnel-Domain high dimension chaotic phase encoding,” *Opt. Lasers Eng.*, vol. 129, 2020, Art. no.106038.

[34] H. Zhang, X. Q. Wang, X. Y. Wang, and P. F. Yan, “Novel multiple images encryption algorithm using CML system and DNA encoding,” *IET Image Process.*, vol. 14, pp. 518–529, 2020.

[35] X. L. He, H. Tao, and L. J. Zhang, “Single-shot optical multiple-image encryption based on polarization-resolved diffractive imaging,” *IEEE Photon. J.*, vol. 11, 2019, Art. no. 3900812.

[36] K. A. K. Patro and B. Acharya, “A novel multi-dimensional multiple image encryption technique,” *Multimedia Tools Appl.*, vol. 79, pp. 12959–12994, 2020.