

APPLIED RESEARCH

Color Image Encryption Based on LSS-Type Coupled Mapped Lattice

FAN ZHANG  AND **XIAODONG WANG**

Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China
CAS Key Laboratory of On-Orbit Manufacturing and Integration for Space Optics System, Changchun Institute of Optics, Fine Mechanics and Physics,
Chinese Academy of Sciences, Changchun 130033, China

Corresponding author: Fan Zhang (zfan0323@163.com)


This work was supported by the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDA17010205.

ABSTRACT To protect the security of image information in storage or transmission. We present a color image encryption algorithm based on the image features, which are unique to each other. Firstly, 12 pseudo-random sequences are generated based on The Logistic Sine (LSS) coupled mapped lattice. One group of pseudo-random sequences is selected to group the remaining 11 groups of sequences randomly, of which eight groups of sequence data realize the scrambling operation of the bit-level image, and the other three groups learn the image diffusion operation to obtain the encrypted image. The experimental results show that the image encryption algorithm proposed in this paper has ample key space. The number of pixel change rates (NPCR) and unified average change intensity (UACI) are 99.62% and 33.57%, respectively, close to the ideal value. The proposed algorithm effectively resists standard data statistics, cutting, and noise attacks.

INDEX TERMS Image encryption, chaotic system, coupled map lattices.

I. INTRODUCTION

With the significant changes in technologies such as the Internet of Things and big data, digital image transmission and collection have been widely applied in various fields such as military, medical, education, and commerce. The accompanying security, integrity, and anti-interference of digital images are essential. Image encryption processing is an effective method adopted for the problem. The image encryption method mainly uses a key to convert the image into a uniformly distributed signal, independent of the original image and similar to noise. When the recipient does not obtain the correct key, accurate image information cannot be obtained [1], [2], [3], [4], [5]. Under the influence of various adverse factors, such as night, haze and snow weather, the quality of acquired images will be deteriorated significantly. The image restoration methods, such as degradation adaptive neural network or variational decomposition model are as the pre-processing step [6], [7], [8], and then encryption algorithms should minimize the loss of the original image as much as possible to ensure image clarity and effectiveness.

The associate editor coordinating the review of this manuscript and approving it for publication was Abdullah Ilyasu .

Currently, the research direction of image encryption technology has two categories: research on the calculation method of random sequence in the encryption process and the improvement design of the algorithm structure in the encryption process.

The random sequence of the encryption process is generally selected based on chaos theory. Chaotic systems have characteristics such as sensitivity to initial values and pseudo-randomness. Standard chaotic maps mainly include Logistic maps, Tent maps, Henon map, Baker maps, etc [9], [10], [11], [12], [13]. The complexity of chaotic systems determines the security and reliability of encryption algorithms. Conduct in-depth research on the complexity of chaotic systems, including expanding one-dimensional chaotic systems to two-dimensional, three-dimensional, and high-dimensional chaotic systems [14], [15], [16], [17].

Coupled Map Lattice (CML) is a spatiotemporal dynamic system model. It uses lattice sequence number to extend the dimension of chaotic mapping in time domain, which can transform low-dimensional chaotic mapping into hyperchaotic system with more complex dynamic characteristics, and the dimension of this hyperchaotic system is adjustable. CML is widely applied into image encryption because of its advantages of more complex dynamical behavior and

lower computational overhead. Wang et al. [18] proposed a novel spatiotemporal chaos model MCML which changes the structure of CML and the coupling method in different lattices. Zhang et al. [19] proposed a new image encryption algorithm based on the spatiotemporal chaos of the mixed linear–nonlinear coupled map lattices, which has more outstanding cryptography features in dynamics than the logistic map or the system of coupled map lattices does. And the results demonstrate the superior security and high efficiency of the proposed algorithm. Li Tong proposed the S-boxes by the coupled map lattice, using the secondary key for selecting S-box and achieved the nonlinear replacement each round. Pairwise combined the replacement matrix and encrypted two-way to reduce the correlation of the same pixel corresponded to three color components. Obtained initial value of system by combining logistic map and plaintext [20].

Scrambling and diffusion are two prevalent operations for image encryption, while scrambling is to change the pixel positions and diffusion is to change the pixel values. Most existing encryption schemes consider these two operations separately. It may increase the risk of being cracked because it is usually easier to crack a system with two separate operations than to crack the mixture of the operations. To cope with these issues, the research on the algorithm structure of the image encryption process mainly focuses on the joint scrambling and diffusion operation in the encryption process. Wang proposed a novel color image encryption with heterogeneous bit-permutation and correlated chaos. Considering the difference of information amounts between bit-planes, the author employs heterogeneous bit-permutation to reduce computation cost and improve permutation efficiency [21]. Li et al. proposed an approach that jointly permutes and diffuses (JPD) the pixels in a color image for encryption. The hyperchaotic sequence is used to permute and diffuse the pixels in images jointly [22]. Liu et al. put forward simultaneous permutation and diffusion operation (SPDO), which can solve the problem of traditional encryption scheme in which the permutation and diffusion are two independent processes, that leads attackers to crack the two processes separately [23]. An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism is proposed by Jun, which introduced a plain pixel related chaotic orbit perturbing mechanism [24]. Li et al. proposed a novel algorithm that combines hyperchaotic system, dynamic filtering, and bit cuboid operations, namely, DFBC, for image encryption. a diffusion scheme is performed and then the image is transformed to a bit cuboid; and, finally, various types of permutation [25]. The diffusion process can be attacked and the permuted image can be obtained by constructing a special image, the permuted image is get by attacking the diffusion process [26].

Bit-level image encryption method is a common image encryption calculation, which converts the image data into bitmap. And the scrambling and diffusion operations at the bit level can change the position of the pixel and the value of the pixel point at the same time. Compared with the scrambling

and diffusion at the pixel level, the encryption efficiency is effectively improved [27], [28]. Based on the introduction of interdisciplinary DNA sequence encryption mechanisms, base molecules are used as information carriers to achieve image encryption through mathematical transformations or pseudo-DNA calculations. Each pixel of the original image is encoded into four nucleotides by the deoxyribonucleic acid (DNA) coding, then each nucleotide is transformed into its base pair for random time using the complementary rule [29], [30], [31]. Li et al. proposed a novel approach that integrates a hyperchaotic system, pixel-level Dynamic Filtering, DNA computing, and operations on 3D Latin Cubes, namely DFDC, for image encryption [32]. Kalpana proposed the choice of DNA encoding rule, DNA operation and DNA synthetic image creation are all done based on the outcome of various chaotic maps and systems, which has a better ability of resisting statistical and differential attacks on comparison [33]. For any size of the original grayscale image, after being permuted the rows and columns respectively by the arrays generated by piecewise linear chaotic map (PWLCM), each pixel of the original image is encoded by DNA rule [34]. An encryption algorithm combined Intertwining Logistic mapping and dynamic DNA coding is proposed through the simulated annealing algorithm [35].

This article proposes an image encryption algorithm based on bitmap processing and three-dimensional chaotic systems. We are using the Logistic-Sine (LSS) type coupled map lattice to generate 12 groups of pseudo-random sequence. According to the average value of image pixels, we choose a pseudo-random sequence as the key distribution group. The remaining 11 groups are divided into eight groups of scrambling operation sequences and three groups of diffusion operation sequences, where the eight groups of pseudo-random sequences for scrambling operation and the other three groups of pseudo-random sequences are respectively diffused with the scrambling images to obtain encrypted images. The LSS-type chaotic map selected in this article is an improved one-dimensional chaotic system based on Logistic mapping and Sine mapping, which has better chaotic characteristics, more robust security, and more suitable for image encryption.

II. LSS TYPE COUPLED MAP LATTICE

A. COUPLED MAP LATTICE

Coupled Map Lattices (CML) is a typical dynamic system with discrete time, discrete space, and continuous states, specifically described as follows:

$$x_{n+1}(i) = (1 - \varepsilon)f(x_n(i)) + \frac{\varepsilon}{2} \times (f(x_n(i-1)) + f(x_n(i+1))) \quad (1)$$

where n is the time coordinate; $i \in [1, L]$ represents the CML length's grid position. $\varepsilon \in (0,1)$, which is a coupling strength factor and satisfies periodic boundary conditions $x_n(0) = x_n(L)$, $x_n(i)$ represents the i -th grid state value at time n .

B. LSS-TYPE CHAOTIC MAP

This article selects the LSS-type chaotic map, an improved one-dimensional chaotic system based on Logistic and Sine maps. Through dynamic analysis, the LSS-type chaotic system has better chaotic characteristics and is more suitable for image encryption than one-dimensional simple chaotic systems. And The LSS chaotic system is described as follows:

$$X(i + 1) = \text{mod} (rX(i) (1 - X(i)) + (4 - r) \sin(\pi X(i)) / 4, 1) \quad (2)$$

Among them, $r \in (0,4)$ and $X_n \in (0,1)$. For example, when $X(0) = 0.3$ and $r = 1.5$, the sequence trajectory of the LSS chaotic system, as shown in Fig.1, and the output sequence values distribute randomly between (0,1).

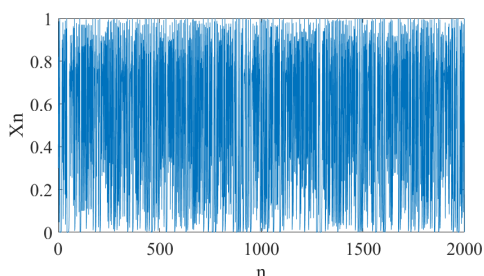


FIGURE 1. LSS chaotic system trajectory, $X(0)=0.3, r=1.5$.

III. ENCRYPTION ALGORITHM AND IMPLEMENTATION

This article uses an LSS-coupled mapped lattice to perform scrambling and diffusion operations on bit images, as shown in Fig.2.

The specific image encryption algorithm is as follows:

Step 1: Generate LSS coupled map lattice. The color image F contains three data channels, decomposing into 24 bit-images $\{F_1, F_2, \dots, F_{24}\}$. To obtain the initial values $X_1(0), X_2(0) \dots$, and $X_{12}(0)$ for different levels of the coupled mapped lattice, the bit values are calculated using Eq. (3) in each bit level image. The key parameters r of chaotic sequence X_n and the key parameters of coupled mapped lattice ε are obtained using the Hash function. According to Eq. (2), the chaotic sequence X_1 is obtained by iterating $L + M \times 3N$ times where $L = 1000$. And then, the coupling map lattice $X = \{X_1, X_2, \dots, X_{12}\}$ is obtained through Eq. (1). Finally, each group of pseudo-random sequence $[L + 1, L + M \times 3N]$ is extracted as a coupled mapped lattice for image scrambling. Each subsequence has a length of $M \times 3N$.

$$X_i(0) = \text{mod} \left(\sum (F_{2i-1} + F_{2i}) / 2, M \times 3N \right) \quad (3)$$

Step 2: Pseudo-random sequence grouping. From Eq. (4), we obtain the parameter e to get the coupled mapped lattice pseudo-random sequence X_e as the basis for grouping the scrambling and diffusion pseudo-random sequences. The remaining 11 groups of pseudo-random sequences are divided into eight groups of scrambling sequences $\{Z_1, Z_2, \dots, Z_8\}$ and three groups of diffusion sequences

$\{K_1, K_2, K_3\}$.

$$e = \text{mod} \left(\frac{\sum_{i=1}^M \sum_{j=1}^N \sum_{k=1}^3 F(i, j, k)}{M \times 3N}, 12 \right) \quad (4)$$

Step 3: Scramble operation. The RGB three channels of color images with size $M \times N$ are spliced in sequence according to Eq. (5) to obtain an image with size $M \times 3N$; Then decompose the image into bit-level images $\{FB_1, FB_2 \dots FB_8\}$, and convert to a one-dimensional array $\{S_1, S_2 \dots S_8\}$. Sort the scrambled sequence Z_i to get a new ordered sequence $ZP = \{ZP_1, ZP_2 \dots ZP_8\}$, records the position of the value of the sequence Z_i in the sequence ZP_i , giving the serial number $ZT = \{ZT_1, ZT_2 \dots ZT_8\}$. And finally, $ZT = \{ZT_1, ZT_2 \dots ZT_8\}$ sequential scrambled bitmap one-dimensional array $\{S_1, S_2 \dots S_8\}$, giving the scrambled array $\{S'_1, S'_2 \dots S'_8\}$, inversely converted to $M \times 3N$ image array F' .

$$\begin{aligned} F_B(1 : M, 1 : N) &= F_R(1 : M, 1 : N) \\ F_B(1 : M, N + 1 : 2N) &= F_G(1 : M, 1 : N) \\ F_B(1 : M, 2N + 1 : 3N) &= F_B(1 : M, 1 : N) \end{aligned} \quad (5)$$

Step 4: Diffusion operation. Convert the diffusion pseudo-random sequence $\{K_1, K_2, K_3\}$ to two-dimensional arrays with the same dimension as the image F' . According to Eq. (6), we obtain the encrypted image G through the XOR operation between the image data and the diffusion arrays.

$$G(i, j, k) = \text{mod} (F'(i, j, k) \oplus K_k(i, j), 255) \quad (6)$$

The image encryption system in this article belongs to a symmetric encryption system, and the decryption system is identical to the encryption system. We can obtain the decrypted image by reversing the above steps to process the encrypted image.

IV. EXPERIMENTAL RESULTS AND SAFETY MEASUREMENT METHODS

In this section, we do a series of experiments to verify the effectiveness and safety of the proposed image encryption algorithm. As for Fig.3, We select the key parameters $r = 1.5$ and $\varepsilon = 0.5$, which show that the original image cannot be seen from the encrypted image, while the decrypted image can effectively obtain the original image information. We discuss five tests to measure the safety and strength of the algorithm based on the image ‘‘Lena’’, ‘‘Colored Chips’’, ‘‘onion’’, and ‘‘Kobi’’, respectively.

A. KEY SPACE

As we all know, the size of the key space determines the ability of the encryption system to resist brute force attacks. In this encryption algorithm, the keys mainly consist of LSS chaotic mapping parameter r , coupled mapped lattice parameter ε , and sequence initial values $X_1(0), X_2(0), \dots, X_{12}(0)$

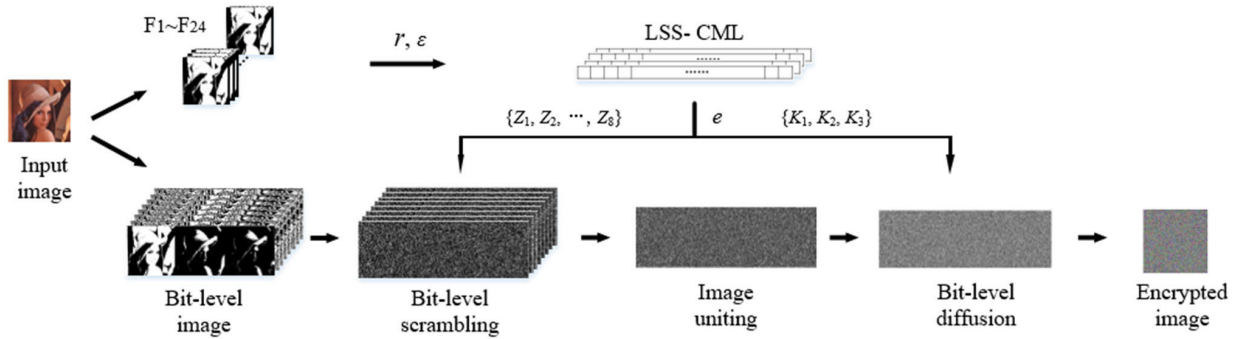


FIGURE 2. The proposed encryption algorithm.

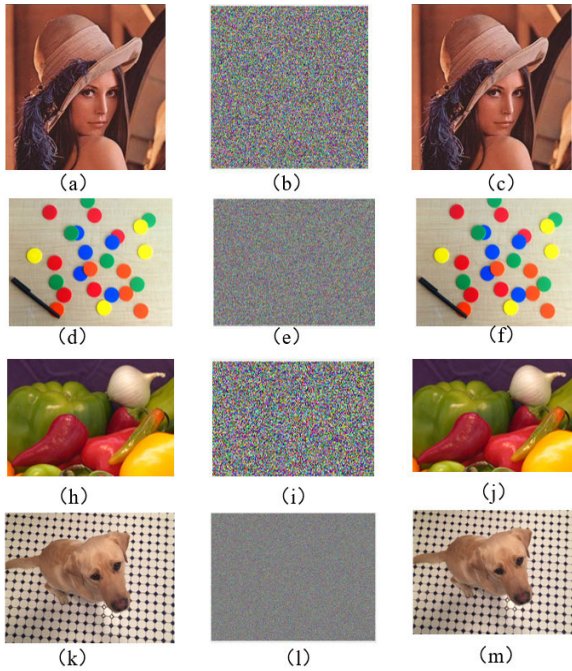


FIGURE 3. Encrypted and decrypted image. The first row is original images, “Lena”, “colored Chips”, “onion”, and “Kobi,” respectively. The second row is encrypted images. The third row is decrypted images.

with the calculation accuracy of 10^{-15} . The designed key space is large enough to withstand exhaustive attacks.

B. SENSITIVITY ANALYSIS

We study the encryption process sensitivity in two aspects: key sensitivity and plaintext sensitivity. It mainly refers to the impact of small changes in the key or plaintext images on the results of encrypted and decrypted images. Usually, the number of pixel change rates (NPCR) and unified average changing intensity (UACI) measure the sensitivity of the encryption process. NPCR is the change rate of pixels in the encrypted image when the value of one pixel in the original image is changed. It measures the percentage of different pixel numbers between the encrypted images while their corresponding authentic images have only one different pixel. UACI calculates the average intensity difference between

the original and encrypted images. The formulations are as follows:

$$\begin{aligned}
 NPCR(C_1, C_2) &= \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N |D(C_1(i, j), C_2(i, j))| \\
 &\quad \times 100\% \\
 UACI(C_1, C_2) &= \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%
 \end{aligned}
 \tag{7}$$

where M and N are the width and height of the image. C_1 and C_2 respectively represent two encrypted images, and $D(\cdot)$ indicates whether two numerical values are the same. If $C_1(i, j) = C_2(i, j)$, then $D(C_1(i, j), C_2(i, j)) = 0$, otherwise $D(C_1(i, j), C_2(i, j)) = 1$. The greater the NPCR and UACI, the greater the difference between C_1 and C_2 . The following analysis is respectively aimed at key sensitivity and plaintext sensitivity.

The key sensitivity mainly includes two parts. The first one is the changes between the encrypted images with different keys, in which the original key introduces a small variable during the encryption process. The second is the impact of introducing minor variable keys in decrypted images during the decryption process. To verify the differences caused by changing key values during the encryption process, we add the variables $\Delta = 10^{-15}$ to each parameter in the original key K and obtain new keys $K1$ and $K2$. Table 1 gives the analysis report for encrypted images with two new keys. We note that slight key differences result in entirely different encrypted images.

TABLE 1. Key sensitivity in the encryption process.

Key	NPCR%	UACI%
$K1 (r+\Delta)$	99.61	33.44
$K2 (e+\Delta)$	99.62	33.52

To verify the impact of introducing small variables in the decrypted process, we decrypt the encrypted image with

new keys $K1$ and $K2$. In contrast, the decryption keys with slight differences cannot correctly decrypt the original image, as shown in Fig 4. The result shows that the algorithm proposed in this article has better key sensitivity during the encryption and decryption processes.

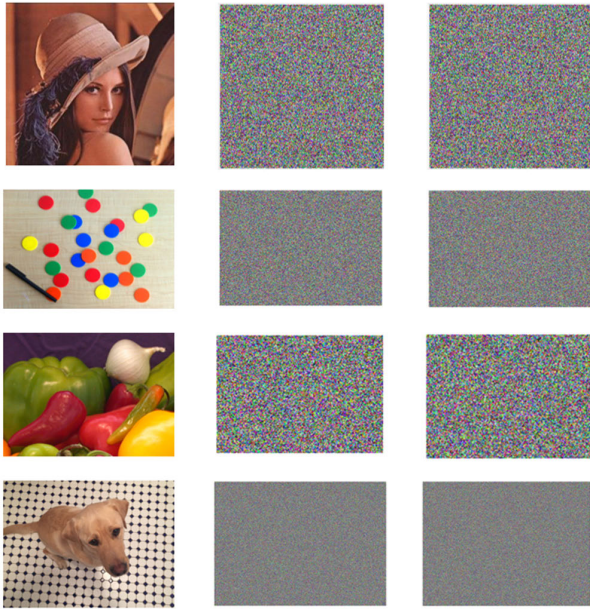


FIGURE 4. Key sensitivity analysis. The first column is the plaintext images, the second and third column are the decrypted image with $K1(r + \Delta)$ and $K2(\epsilon + \Delta)$.

Plaintext sensitivity mainly refers to the sensitivity of an encrypted image to the change of pixels in a plaintext image. In other words, there will exist differences between plaintext images and encrypted images if the value of a pixel in the plaintext image is changed. Currently, the plaintext sensitivity is analyzed mainly through resisting differential attacks. This article randomly selects a pixel in the original image and replaces the value with 0. We could obtain the encrypted image $G1$ after the same encryption process. Table 2 shows the NPCR and UACI analysis report compared with the original encrypted image G . The results in this table show that the NPCR and UACI performance of the proposed algorithm is better than the considered algorithms.

C. HISTOGRAM ANALYSIS

Image histogram is a statistical table of image pixel distribution, which reflects the distribution of image pixel value information. The horizontal coordinate of the histogram represents the pixel value, and the vertical coordinate represents the number of that pixel value in the entire image. The histogram is an important feature of the image. In general, the histogram of image is irregular. A well-designed encryption scheme will break the shape, and the histogram of the encrypted image should be as flat as possible. Fig 5 shows the histograms of plaintext images and encrypted images, respectively.

TABLE 2. Plaintext sensitivity in the encryption process.

Algorithm	NPCR	UACI
Lena	99.62	33.57
Colored Chips	99.62	33.39
Onion	99.65	33.34
Kobi	99.61	33.51
Ref.7	99.61	31.62
Ref.11	99.58	33.44
Ref.17	99.60	33.53
Ref.18	99.61	33.48

From the figure, we can see that different plaintext images have different histograms. The pixel distribution of plaintext image histograms is relatively concentrated and has apparent characteristics. For example, onion's color is bright and rich, so the histogram is relatively uniform and there are more pixels with smaller numbers. As the color chips image is much whiter and brighter, so there are more pixel values between 100 and 255. When we study the histograms of all channels of the encrypted image, we can find that they look almost identical, which is significantly different from the plaintext image histogram. In particular, the height of all pixel values is roughly the same, indicating that the distribution of pixel values in each channel of the encrypted image is very uniform. This graph reveals that the proposed algorithm can effectively resist histogram statistical analysis attacks.

D. CORRELATION COEFFICIENTS OF ADJACENT PIXELS

There is a high degree of correlation between adjacent pixels of the image, including horizontal, vertical, and diagonal directions. Theoretically, there is no correlation between adjacent pixels of the encrypted image. Eq. (8) measures the correlation between adjacent image pixels.

$$CC = \frac{\sum_{i=1}^N \left[\left(x_i - \frac{1}{N} \sum_{i=1}^N x_i \right) \times \left(y_i - \frac{1}{N} \sum_{i=1}^N y_i \right) \right]}{\sqrt{\left[\sum_{i=1}^N \left(x_i - \frac{1}{N} \sum_{i=1}^N x_i \right)^2 \right] \times \left[\sum_{i=1}^N \left(y_i - \frac{1}{N} \sum_{i=1}^N y_i \right)^2 \right]}} \tag{8}$$

In this paper, we plot the correlations of 2000 random pairs of adjacent pixels in the horizontal, vertical, and diagonal directions from the plaintext image and encrypted images respectively, as shown in Fig 6, as shown in Figure 6. For each image, the pixels in the R, G, and B channels are drawn in red, green, and blue, respectively. In the second column, we can find that most pairs of pixels are distributed along a diagonal line, indicating a strong correlation in the plaintext image. However, in the third, fourth and fifth columns, we can see that the points fill the entire plane on R, G and B channels, showing a weak correlation in the encrypted image. This diagram proves that the algorithm proposed in this paper can effectively break the correlation existing in the original image.

Table 3 shows the correlation coefficients of plaintext images and encrypt images in horizontal, vertical and

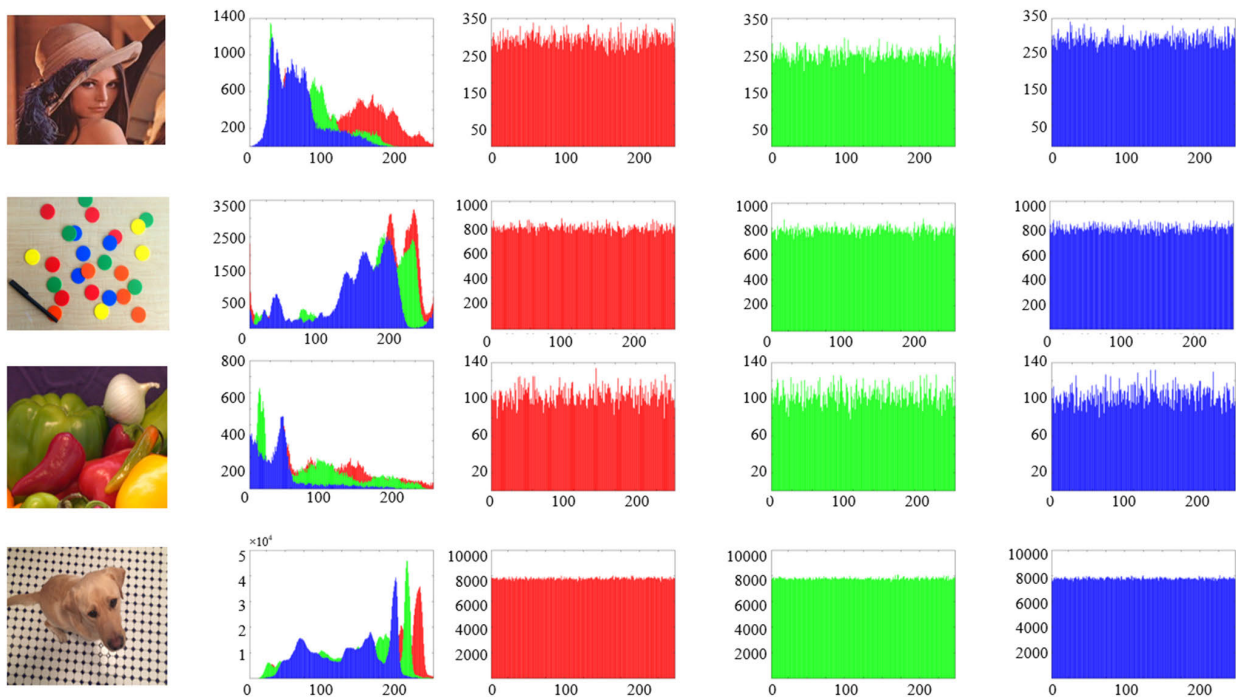


FIGURE 5. Histogram analysis. The first column is plaintext image, the second column is histograms on R, G, and B channels, the third column is encrypted image histograms on R, G, and B channels, respectively.

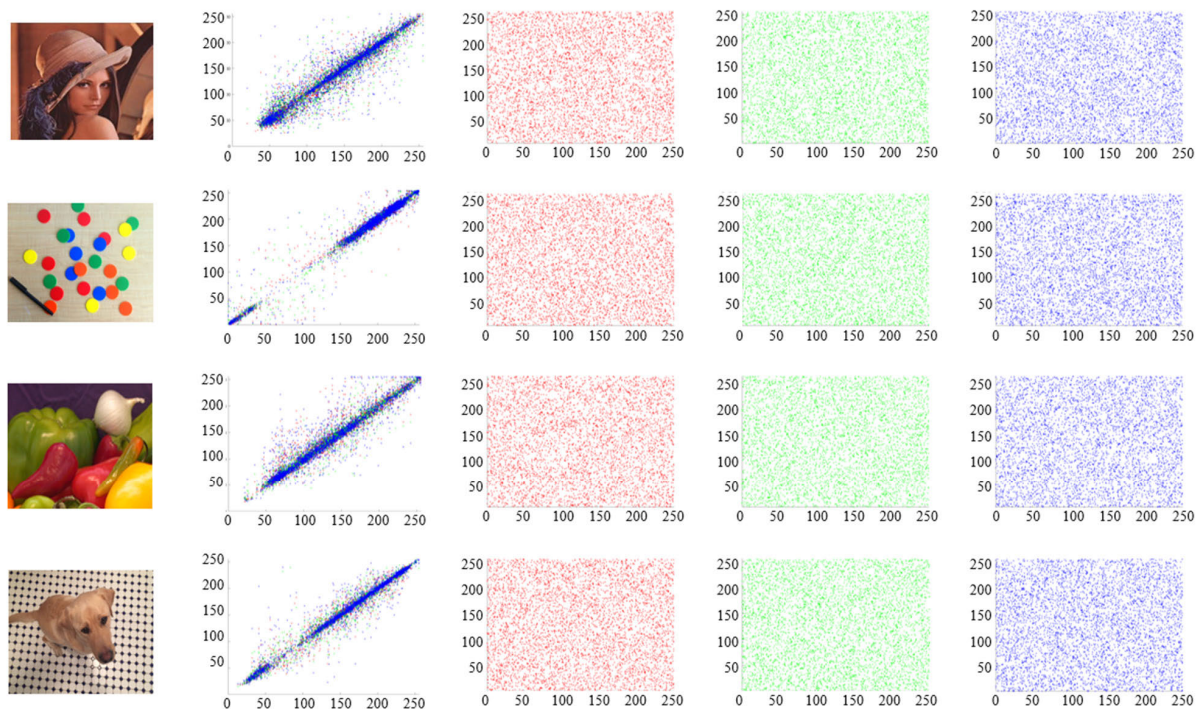


FIGURE 6. Correlation distributions for a color image. The first column is plaintext images, the second column is the correlations of plain images in horizontal, vertical, and diagonal directions. The third, fourth, fifth columns are the correlations of encrypted images in horizontal, vertical, and diagonal directions.

diagonal directions, respectively. From the table, we can find that the correlation of plaintext images is close to 1, which indicating that there is a strong correlation. In contrast, the

correlation of all encrypt images is very low, close to 0, which indicating that the algorithm in this paper effectively reduces the correlation of adjacent pixels in plaintext images.

TABLE 3. Correlation coefficient analysis.

Algorithm	IMAGE	Direction		
		horizontal	vertical	diagonal
Lena	plaintext	0.9796	0.9656	0.9491
	encrypted	0.0050	-0.0021	0.0034
Colored Chips	plaintext	0.9898	0.9889	0.9829
	encrypted	0.0020	-0.0050	0.0074
Onion	plaintext	0.9815	0.9902	0.9707
	encrypted	0.0098	0.0033	-0.0089
Kobi	plaintext	0.9911	0.9910	0.9812
	encrypted	0.0050	0.0042	-0.0078
Ref.7	plaintext	0.9412	0.9699	0.9380
	encrypted	0.0045	-0.0011	-0.0039
Ref.11	plaintext	0.9757	0.9365	0.9018
	encrypted	0.0077	-0.0090	0.0178
Ref.17	plaintext	0.9670	0.9491	0.9543
	encrypted	-0.0033	-0.0051	-0.0048
Ref.18	plaintext	0.9670	0.9491	0.9543
	encrypted	-0.0069	-0.0059	-0.0055

E. THE INFORMATION ENTROPY

The information entropy represents the uncertainty of random variables. The greater the information entropy, the stronger the randomness and the higher the security of the image. The formula is as follows:

$$H = - \sum_{i=0}^L p(i) \log p(i) \tag{9}$$

The L represents the grayscale level, and $p(i)$ represents the probability of a pixel value of i . For images with a gray level of 256, the theoretical maximum of information entropy is 8. This paper calculates the information entropy of channels R, G, and B of the encrypted image, as shown in Table 4.

TABLE 4. Information entropy calculation.

Algorithm	CHANNEL R	Channel G	Channel B
Lena	7.9971	7.9969	7.9978
Colored Chips	7.9991	7.9990	7.9991
Onion	7.9939	7.9932	7.9934
Kobi	7.9999	7.9999	7.9999
Ref.7	7.9971	7.9974	7.9973
Ref.11	7.9917	7.9916	7.9917
Ref.17	7.9993	7.9993	7.9992
Ref.18	7.9974	7.9970	7.9971

The results in Table 4 show the encrypted image information entropy obtained by the algorithm proposed in this paper is close to the theoretical value with solid randomness. The highest entropy value is 7.9999 in the image ‘‘Kobi’’, which is better than the value in the reference. All these results demonstrate that the proposed algorithm can effectively resist the information entropy attacks and ignore information leakage in the encryption process.

F. NOISE AND CUTTING ATTACKS

In digital image transmission, there will be noise interference or information loss. A compelling image encryption

algorithm must cope with external interference effectively, recover the original image, and have robustness. The following analyzes noise interference and Cutting attacks, respectively.

The 0.01, 0.1, and 0.5 salt and pepper noise are added to the encrypted image. Fig 7 shows the decrypted image obtained by the algorithm in this paper. We can receive most plaintext image information after adding noise to the encrypted image, which effectively resists noise attacks.

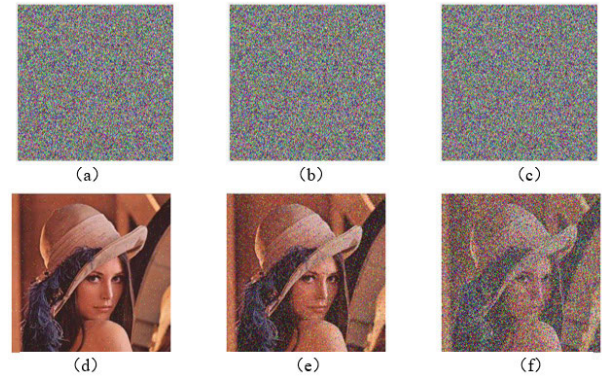


FIGURE 7. Noise attack results. (a)-(c) cipher images with 0.01%, 0.1%, 0.5% salt and pepper noise. (d)-(f) the decrypted images from the first row.

We first crop 8%, 15%, 31%, and 62% pixels at the encrypted image, respectively, and then decrypt the image using the proposed process. The result is shown in Fig 8. As the figure shows, our algorithm can obtain the most plaintext information and resist cutting attacks.

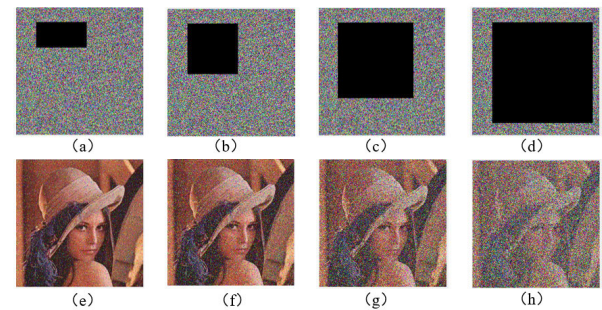


FIGURE 8. Attacks cropping attack results. (a)-(d) cipher images with 8%, 15%, 31%, and 62% data loss. (e)-(h) the decrypted images from the first row.

V. CONCLUSION

This paper proposes an image encryption algorithm based on an LSS-type coupled mapped lattice. To effectively resist known and selected plaintext attacks, the key stream of the CML is obtained based on the LSS chaotic map, respectively. The experimental results show that the image encryption algorithm proposed in this paper has ample key space that can effectively resist violent attacks. The number of pixel change rates (NPCR) and unified average change intensity (UACI) are 99.62% and 33.57%, respectively, close to the ideal value. The above-experimental results demonstrate that the image

encryption algorithm can effectively resist histogram attacks, information entropy attacks, and noise and cutting attacks, which have better security and robustness. All these experimental results benefit from the characteristics of the LSS-type CML chaotic system: (1) the LSS-type CML chaotic system that generates a chaotic sequence for subsequent encryption operations which has more complex dynamical behavior and lower computational overhead, (2) introduce the color images information into the initial values of the chaotic system, each image has its own unique chaotic sequence, (3) the joint scrambling and diffusion operations is promising for color image encryption. we will study how to accelerate the proposed scheme using GPUs in the future and be implemented on iOS and Android.

REFERENCES

- [1] X. Wang and H. Sun, "A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function," *Opt. Laser Technol.*, vol. 122, Feb. 2020, Art. no. 105854.
- [2] P. Singh, B. Acharya, and R. K. Chaurasiya, "Low-area and high-speed hardware architectures of LBlock cipher for Internet of Things image encryption," *J. Electron. Imag.*, vol. 31, no. 3, p. 31, May 2022.
- [3] H. Huang, Y. Chen, and D. Cheng, "Plaintext-related image encryption scheme based on chaos and game of life," *J. Electron. Imag.*, vol. 31, no. 1, Feb. 2022, Art. no. 013031.
- [4] H. Zhao, S. Xie, J. Zhang, and T. Wu, "Efficient image encryption using two-dimensional enhanced hyperchaotic Henon map," *J. Electron. Imag.*, vol. 29, no. 2, Mar. 2020, Art. no. 023007.
- [5] G. Atali and E. Sonmez, "Efficient chaos-based image encryption approach for secure communication," *J. Electron. Imag.*, vol. 30, no. 2, Apr. 2021, Art. no. 023026.
- [6] J. Zhang, Y. Cao, Z.-J. Zha, and D. Tao, "Nighttime dehazing with a synthetic benchmark," in *Proc. 28th ACM Int. Conf. Multimedia*, Oct. 2020, pp. 2355–2363.
- [7] Y. Liu, Z. Yan, S. Chen, T. Ye, W. Ren, and E. Chen, "NightHazeFormer: Single nighttime haze removal using prior query transformer," in *Proc. 31st ACM Int. Conf. Multimedia*, Oct. 2023, pp. 4119–4128.
- [8] Y. Liu, Z. Yan, J. Tan, and Y. Li, "Multi-purpose oriented single nighttime image haze removal based on unified variational retinex model," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 4, pp. 1643–1657, Apr. 2023.
- [9] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019.
- [10] Z. L. Shanshan and Z. Hongli, "Image grey level encryption based on cat map," *J. Comput. Appl.*, vol. 41, no. 4, pp. 1148–1152, 2021.
- [11] X. Zhang, Z. Luo, and C. Gao, "A digital image encryption algorithm based on chaotic sequences," *Comput. Appl. Eng. Educ.*, vol. 42, no. 19, pp. 61–62, 2006.
- [12] A. Zhu, L. Li, and M. Chen, "An improved BMP image encryption algorithm based on logistic map," in *Proc. Int. Conf. Comput. Commun. Technol. Agricult. Eng.*, vol. 3, Jun. 2010, pp. 576–578.
- [13] C. Hou, X. Liu, and S. Feng, "Quantum image scrambling algorithm based on discrete baker map," *Modern Phys. Lett. A*, vol. 35, no. 17, Jun. 2020, Art. no. 2050145.
- [14] Z. Xiangqiu and Y. Ruisong, "Chaotic image encryption algorithm based on improved Logistic map," *Comput. Eng.*, vol. 47, no. 11, p. 9, 2021.
- [15] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.
- [16] U. Erkan, A. Toktas, and Q. Lai, "2D hyperchaotic system based on schaffer function for image encryption," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 119076.
- [17] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2943–2959, Jul. 2012.
- [18] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Sci. Rep.*, vol. 10, no. 1, p. 9784, Jun. 2020.
- [19] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
- [20] L. Tong and Z. Xuefeng, "Color image encryption algorithm based on coupled map lattice," *Appl. Res. Comput.*, vol. 34, p. 10, Jan. 2017.
- [21] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.
- [22] T. Li, J. Shi, and D. Zhang, "Color image encryption based on joint permutation and diffusion," *J. Electron. Imag.*, vol. 30, no. 1, Feb. 2021, Art. no. 013008.
- [23] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE Access*, vol. 8, pp. 27361–27374, 2020.
- [24] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism," *Opt. Exp.*, vol. 21, no. 23, p. 27873, 2013.
- [25] X. Li, Z. Xie, J. Wu, and T. Li, "Image encryption based on dynamic filtering and bit cuboid operations," *Complexity*, vol. 2019, pp. 1–16, Feb. 2019.
- [26] L. Liu, Z. Zhang, and R. Chen, "Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos," *IEEE Access*, vol. 7, pp. 126450–126463, 2019.
- [27] A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map," *Optik*, vol. 184, pp. 205–213, May 2019.
- [28] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.
- [29] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1240–1248, Sep. 2012.
- [30] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, Jun. 2016.
- [31] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, Mar. 2019.
- [32] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes," *Entropy*, vol. 21, no. 3, p. 319, Mar. 2019.
- [33] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," *Optik*, vol. 126, no. 24, pp. 5703–5709, Dec. 2015.
- [34] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012.
- [35] J. Yang and H. Wu, "Color image encryption algorithm based on chaotic system and dynamic DNA coding and operation," *Comput. Eng.*, vol. 44, no. 2, pp. 151–157, 2018.



FAN ZHANG was born in Jilin, China, in 1993. She received the master's degree from Tsinghua University, in 2018.

She is currently an Assistant Researcher Fellow with Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences. Her research interests include space optical remote sensing imaging and information processing technology.



XIAODONG WANG was born in Jilin, China, in 1970. He received the Ph.D. degree in optical engineering from Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun, China, in 2003.

He is currently a Researcher with Changchun Institute of Optics, Fine Mechanics and Physics. His research interests include space optical remote sensing imaging and information processing technology.