Duple Color Image Encryption System Based on 3D Non-equilateral Arnold Transform for IIoT

Huiqing Huang and Zhanchuan Cai, *Senior Member, IEEE*

***Abstract*— The Industrial Internet of Things (IIoT) is to continuously integrate network communication, intelligent analysis and other technologies into every link of the industrial production process, thus greatly improving the manufacturing efficiency. While such systems greatly improve the productivity of the industry, they introduce major safety challenges during the design and operational phases. Therefore, it is necessary to encrypt and protect the information transmitted by the system during the design and runtime stages. This paper focuses on the transmission security of image data in every link of IIoT. Two color images that need to be transmitted can be encrypted into color ciphertext image by using 3D Non-equilateral Arnold Transform (3D-NEAT) and 3D Lorenz System (3D-LS). Different from the traditional algorithm which encrypts one plain image into one ciphertext image, our algorithm encrypts two color images into one color ciphertext image which will cause great confusion to the attacker whom illegally breaks the ciphertext image. First, the proposed method converts two color images with $N \times M$ into a 3D bit-level matrix with size $N \times M \times 48$. Next, 3D-NEAT is applied to permutate the positions of the elements of the resulted 3D bit-level matrix. Then, the permutated 3D bit-level matrix is transformed into three 2D pixel-level images and then diffused by the random diffusion sequences which 3D-LS generates. Finally, the scrambling matrices generated by 3D-LS are used to scramble three diffused 2D pixel-level images and the output is considered as three color components of the encrypted image. The numerical experiments and security analysis show that the proposed image encryption scheme has strong resistance to several known attacks, and yields near-zero correlation and near-eight entropy for the RGB cipher image, and some performance is better than some of the recently proposed image encryption algorithms.**

***Index Terms*—Industrial Internet of Things (IIoT), Duple color image encryption algorithm, 3D Non-equilateral Arnold transform, 3D Lorenz system.**

output is three components of the encrypted image.

I. Introduction

THE rapid development of communication technology has led to the emergence of the Internet of Things (IoT) [1], making the Internet of everything possible. The emergence of the IoT not only brings great convenience to people's life, but also its advantages of the interconnection of everything are very attractive to the industrial field. The combination of industry and the IoT has resulted in the IIoT, it will have a perception, monitoring capability of acquisition, control, sensor and controller, and the analysis of the mobile communications, intelligent technologies such as continuously into the industrial production process each link, finally realizes the traditional industry to a new stage of intelligent [2], [3]. This interconnected environment can greatly improve industrial manufacturing efficiency product quality, reduce cost and resource consumption. On the other hand, a large number of multimedia files, especially image data, are generated in the IIoT, the sharing of these data in industrial big data inevitably involves a lot of confidential data. So, the connections between all different components, both at the physical and network level, present a huge security challenge in IIoT. This challenge is even more critical in applications that exchange large amounts of data with real-time requirements. In order to deal with the privacy and security threats in IIoT, the data captured by IIoT smart devices is encrypted before being transmitted to another IIoT node. In this way, the data transmitted in each node or stored in the cloud is encrypted data, and only authorized users with the correct key can obtain valid information. So, to protect the security of data transmission or storage in the IIoT environment, it is necessary to develop technologies to protect sensitive information continuously.

To protect image information confidentiality and prevent unauthorized users from transmitting sensitive information, the commonly used image information security technologies include image hiding technology [4]–[6] and image encryption technology [7]. Information hiding technology hides confidential information in other information by using data redundancy of information itself and sensory redundancy of human sensory organs. Because plaintext can be hidden in common media, it is difficult for attackers to find the existence of secret information, so that the purpose of secret communication can be effectively achieved. Therefore, in recent years, this technology has attracted the attention of scholars [8]–[12]. In [11], Hassan and Gutub proposed two high-payload embedding methods to achieve high steganographic image quality by using the Hue-Saturation-Value(HSV) color model. Information encryption technology is to use mathematical or physical means to protect electronic information in the process of transmission and storage to prevent information leakage technology. It can effectively avoid disclosing confidential information, so it has always attracted many scholars to study it [13]–[16].

Chaotic systems have such excellent characteristics as pseudo-randomness, ergodicity and high sensitivity to initial conditions and parameters, which are considered to be very suitable for cryptography, because these characteristics are considered to be similar to those of ideal cryptosystem. Since

This work was supported in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2022A1515010263, in part by the Science and Technology Development Fund of Macau under Grant 0052/2020/AFJ and 0059/2020/A2. *(Corresponding author: Zhanchuan Cai.)*

Huiqing Huang is with the School of Mathematics, Jiaying University, Meizhou 514015, China (e-mail: hq-huang2@126.com).

Zhanchuan Cai is with the School of Computer Science and Engineering, Macau University of Science and Technology, Macau 999078, China (email: zccai@must.edu.mo).

Matthews [17] first introduced chaotic systems into image encryption in 1989, many scholars have been attracted to the research of image encryption algorithms based on chaotic systems. In 1998, Fridrich [18] proposed the first permutation-diffusion encryption architecture. Due to the high security of the image encryption algorithm designed by this architecture, this architecture has become the most popular structure and has been adopted by many chaos-based image encryption algorithms [19]. In particular, Arnold transformation (AT) also known as the cat mapping [20], is a chaos system which used widely in the permutation phase of image encryption [21]–[23]. In [21], the cat mapping is extended to generalized cat mapping first, and then the original image pixel positions are scrambled using the generalized cat mapping. Soon after, in order to improve the security level of AT-based method, Zhang *et al.* [22] improved the traditional isometric Arnold transform and scrambled the image with the improved AT. As an independent cryptosystem, AT is not secure enough to be used in most AT-based image encryption schemes due to the periodicity of its output. Therefore, in [23], Wu *et al.* used AT to scramble both the coordinates of image pixels and the pixel values of the corresponding coordinates. In addition, with the security analysis of chaos-based image encryption algorithms, it is found that some schemes are vulnerable to different attack methods [24], [25]. For example, Solak *et al.* [24] cryptanalyzed an image encryption algorithm which is proposed in [18], and found that this algorithm cannot resist chosen-ciphertext attack. Chen *et al.* [25] cryptanalyzed the image encryption algorithm [19] using a chosen-plaintext attack. Therefore, it is very challenging to design a secure and efficient chaos-based image encryption algorithm.

In some cases, it often needs to encrypt two or multiple images with certain relations or a series of pictures of an object to store or transmit simultaneously [26]. Therefore, two or multiple images encryption is widely concerned in the field of image encryption [27], [28]. There is not only a demand for this in practical life, but also a trend in technology development. The multiple image encryption method achieve a significant increase in the number of encrypted images, but also increases the complexity of the encryption system, which greatly increases the efficiency, increases the security of the encryption system. Zhou *et al.* [27] suggested a novel quantum multi-image encryption scheme that is devised by combining quantum 3D Arnold transform and quantum XOR operations with scaled Zhongtang chaotic system. Anand *et al.* [28] presented a new encryption and decryption method for triple color images using 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform.

In this paper, we propose an image encryption system based on 3D-NEAT and 3D-LS for image information transmission in IIoT. The system can encrypt two color images into one color encrypted image, so it can not only ensure the privacy protection of image transmission but also reduce the transmission data. Different from Ref. [23], which uses AT to change the position and value of image pixels in two steps, our scheme first converts two color images into a bit-level 3D matrix, which is permutated by using 3D-NEAT later. In this process, the position of the bit-level 3D matrix elements is scrambled, so that the pixel value of the corresponding pixel-level images changes. The permutated bit-level matrix is then transformed into three pixel-level images. Next, three pixel-level images are diffused and scrambled by 3D-LS. Our scheme also avoids the common cross-talk effects of multi-image encryption since the encryption process is completely reversible, making the decryption process the inverse of the encryption process. The advantages of our scheme are as follows. (1) Two color images are encrypted into one color cipher image, which interferes with the cracking of illegal gainers. (2) Unlike most AT-based image encryption scheme, which only scramble the image, ours changes the pixel value of the image. Therefore, our scheme can protect image information more effectively and safely. (3) The chaotic sequence used in the encryption process and the ciphertext image obtained after encryption have good randomness. The result of NIST SP 800-22 batteries of test for chaotic sequence and encrypted images indicates that they have an ideal degree of randomness. (4) Our algorithm has highly sensitive to the key and plain image. The Mean Square Error (MSE) curve of the key verifies that the proposed scheme is highly sensitive to the key, and the results of Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) show that our algorithm is also very sensitive to the plain image.

This paper is organized as follows. In Section II, we introduce the preliminary works of the proposed algorithm. The duple color image encryption scheme based on 3D-NEAT and 3D-LS are introduced in Section III. Section IV discusses and analyses the numerical experiments and safety performance of the proposed scheme. Finally, the concluding remarks are drawn in Section V.

II. Preliminary Work

A. 3D Non-equilateral Arnold Transformation

Based on Shao and Li's research on 2D non-equilateral Arnold transform [29], [30], Wu *et al.* introduced the 3D-NEAT [see Eq. (1)] and corresponding inverse transformation in [31], as follows:

$$\begin{cases} \begin{pmatrix} x_z \\ y_z \\ z_z \end{pmatrix} = \begin{pmatrix} 1 & b_z & 0 \\ c_z & 1+b_z c_z & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \bmod \begin{pmatrix} N \\ M \\ K \end{pmatrix}, \\ \begin{pmatrix} x_x \\ y_x \\ z_x \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b_x \\ 0 & c_x & 1+b_x c_x \end{pmatrix} \begin{pmatrix} x_z \\ y_z \\ z_z \end{pmatrix} \bmod \begin{pmatrix} N \\ M \\ K \end{pmatrix}, \\ \begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1+b_y c_y & 0 & c_y \\ 0 & 1 & 0 \\ b_y & 0 & 1 \end{pmatrix} \begin{pmatrix} x_x \\ y_x \\ z_x \end{pmatrix} \bmod \begin{pmatrix} N \\ M \\ K \end{pmatrix}. \end{cases} \tag{1}$$

where $c_z = r_z \dfrac{M}{\gcd(N,M)}$, $c_x = r_x \dfrac{K}{\gcd(M,K)}$, $c_y = r_y \dfrac{N}{\gcd(K,N)}$, and $\gcd(\cdot)$ represents the greatest common divisor, $b_x, b_y, b_z, r_x, r_y, r_z$ are any positive integers. And its inverse transformation can be achieved by the following three expressions:

$$\begin{cases} y_x = y_{n+1}, \\ x_x = (x_{n+1} - c_y z_{n+1}) \bmod N, \\ z_x = (z_{n+1} - b_y x_x) \bmod K. \end{cases} \tag{2}$$

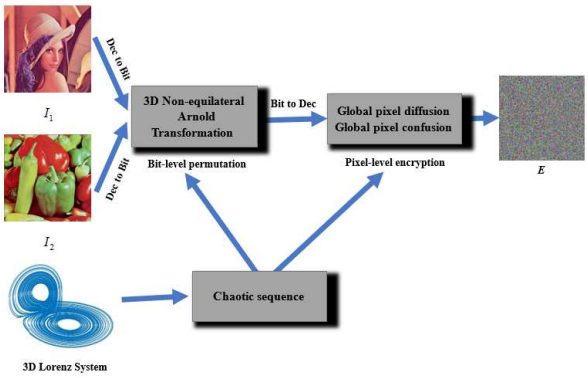


Fig. 1. Flowchart of PDCIEA.

$$\begin{cases} x_z = x_x, \\ z_z = (z_x - c_x y_x) \ mod \ K, \\ y_z = (y_x - b_x z_z) \ mod \ M. \end{cases} \tag{3}$$

$$\begin{cases} z_n = z_z, \\ y_n = (y_z - c_z x_z) \ mod \ M, \\ x_n = (x_z - b_z y_n) \ mod \ N. \end{cases} \tag{4}$$

B. 3D Lorenz System

Lorenz system [32] is a system of nonlinear equations, it can be shown as follows :

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz. \end{cases} \tag{5}$$

where a, b, and c are the control parameters of the Lorenz system. It's in chaotic when $a = 10$, $b = 8/3$, and $c = 28$.

III. Method

The proposed duple color image encryption algorithm is abbreviated as PDCIEA. For convenience, let I_1 and I_2 be two color images with size $N \times M$, and it can be implemented as illustrated in Fig. 1. From the figure, it can be found that the PDCIEA consists of two phases: bit-level image matrix shuffling (BL-IMS) and pixel-level image diffusing-confusing (PL-IDC).

In the BL-IMS stage, we introduce 3D-NEAT to scramble the pixel position in a 3D bit-level image matrix. Firstly, all pixels in each component of the two color images are decomposed into eight binary bits as:

$$b(i,j,k) = \lfloor \frac{p(i,j)}{2^k} \rfloor \mod 2, k = 0, 1, \cdots, 7 \tag{6}$$

where $p(i,j)$ represents the pixel value of the image located on $[i,j]$, and $\lfloor . \rfloor$ represents the rounding down operation. Therefore, through the transformation of Eq. (6), each component of the color image becomes a matrix of size $M \times N \times 8$ with 0 or 1 elements. Then, through matrix superposition, the six component matrices of the two color images are superimposed into a 3D bit-level matrix of size $N \times M \times 48$. After that, it is permutated using 3D-NEAT. After BL-IMS operation, a scrambled 3D bit-level matrix is obtained. This 3D binary

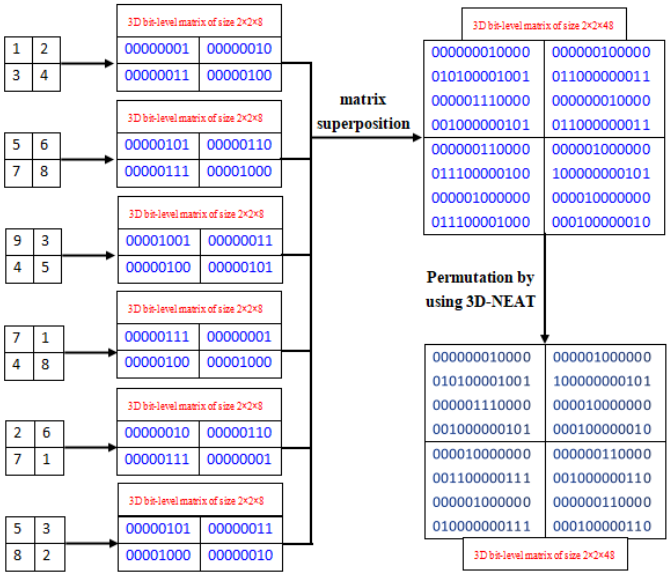


Fig. 2. A numerical example of BL-IMS operation.

image changes the pixel value of the plane image when it is restored in the following steps.

In the PL-IDC stage, we introduce 3D-LS to diffuse and scramble the pixel-level image. Firstly, we split the permutated 3D bit-level matrix into three 3D bit-level matrixes with the size of $N \times M \times 16$, then three 3D bit-level matrixes are converted to three pixel-level images as:

$$g(i,j) = \sum_{k=0}^{15} e(i,j,k) \times 2^k, \tag{7}$$

where $g(i,j)$ represents the pixel value of the pixel-level image located on $[i,j]$. To generate the cipher image, three pixel-level images are diffused and confused using 3D-LS, and then their pixel values are mapped to $[0,1]$.

According to the two-stage process mentioned above, the proposed encryption algorithm has two advantages: first, two color images are encrypted into one color ciphertext image; secondly, unlike the data type of the original image, the pixel value of ciphertext image is between 0 and 1. These increase the difficulty for the decryption of illegal attackers, and the security of the algorithm. The details of encryption are in the following.

Step 1: First, the 3D-LS is iterated large enough L_0 times to generate three random sequences X, Y, Z with the control parameters a, b, c and the initial condition x_0, y_0, z_0. And then we remove the preceding elements and just keep the three sequences of $L = N \times M$ elements that follow, the sequences of these reserved elements are defined as H_1, H_2, H_3, respectively. Next, the generated sequences are transformed into three integer sequences ($U_1, U_2, U_3 \in [0, 65535]$) as follows:

$$\begin{cases} U_1 = \{u_{11}, u_{12}, \cdots, u_{1L}\}, \\ U_2 = \{u_{21}, u_{22}, \cdots, u_{2L}\}, \\ U_3 = \{u_{31}, u_{32}, \cdots, u_{3L}\}, \end{cases} \tag{8}$$

where

$$\begin{cases} u_{1i} = \text{floor}(10^k h_{1i}) \bmod 65536, \\ u_{2i} = \text{floor}(10^k h_{2i}) \bmod 65536, \\ u_{3i} = \text{floor}(10^k h_{3i}) \bmod 65536. \end{cases} \tag{9}$$

Step 2: By intercepting N consecutive elements of sequences X, Y or Z to obtain a sequence $S = \{s_1, s_2, \cdots, s_N\}$. And the sequence corresponding to the sequence S from small to large is S_1. Thus, there exists a shuffling matrix M, which satisfies $S = MS_1'$, and S_1' denotes the transposition of S_1. So, by this way we can construct six shuffling matrixes M_1, M_2, M_3, M_4, M_5, and M_6.

Step 3: The color images I_1, I_2 are decomposed into its red, green, blue components. Six components of two color images are all composed of 8 bit planes. So the two color images are rearranged in bit planes mode to get one 3D bit-plane matrix J with size of $N \times M \times 48$.

Step 4: Six elements are randomly selected from the three integer sequences (U_1, U_2 or U_3) as Arnold parameters b_x, b_y, b_z, r_x, r_y and r_z. Then, the position information of the bit-level cubic J are shuffled by the 3D-NEAT, and obtain shuffled 3D matrix A.

Step 5: Splitting the shuffled 3D matrix A into three 3D bit-plane matrixes B_1, B_2 and B_3 with the size of $N \times M \times 16$, and then three 2D pixel-level images (C_1, C_2 and C_3) can be obtained by using Eq. (7).

Step 6: The three 2D pixel-level images are rearranged into three sequences by column scan, and they are $C_1 = (c_{11}, c_{12}, \cdots, c_{1L})$, $C_2 = (c_{21}, c_{22}, \cdots, c_{2L})$ and $C_3 = (c_{31}, c_{32}, \cdots, c_{3L})$, respectively.

Step 7: Using the three integer sequences U_1, U_2, U_3 to diffuse the sequences C_1, C_2, C_3, so we get three diffused sequences D_1, D_2, D_3.

$$\begin{cases} D_1 = \{d_{11}, d_{12}, \cdots, d_{1L}\}, \\ D_2 = \{d_{21}, d_{22}, \cdots, d_{2L}\}, \\ D_3 = \{d_{31}, d_{32}, \cdots, d_{3L}\}. \end{cases} \tag{10}$$

In Eq. (11), $i = 1, 2, \cdots, L$ and the initial values c_{10}, c_{20}, c_{30}, d_{10}, d_{20}, d_{30} are given value provided as encryption and decryption keys.

Step 8: Rearranging the three sequences D_1, D_2, D_3 into three 2D pixel-level images E_1, E_2, E_3 with a size of $N \times M$, respectively. Then, using the six shuffling matrixes (M_1, M_2, M_3, M_4, M_5, M_6) to shuffle the position information of the three images (E_1, E_2, E_3), and we can obtain three shuffled images G_1, G_2, G_3. Next, the three shuffled images are normalized and the output is considered as the three color components of the encrypted image E.

$$\begin{cases} G_1 = M_1 \times E_1 \times M_2, \\ G_2 = M_3 \times E_2 \times M_4, \\ G_3 = M_5 \times E_3 \times M_6. \end{cases} \tag{12}$$

Algorithm 1 can be referenced for code implementation of PDCIEA. Because PDCIEA is symmetric, so the encryption and decryption keys are the same. And every step of the encryption process is reversible, then decryption is the reverse process of encryption process.

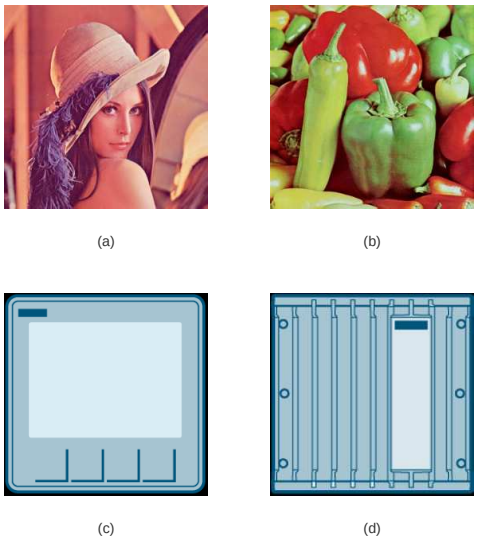


Fig. 3. Color images. (a) "Lena" image, (b) "Peppers" image, (c) "IIDO1" image, (d) "IIDO2" image.

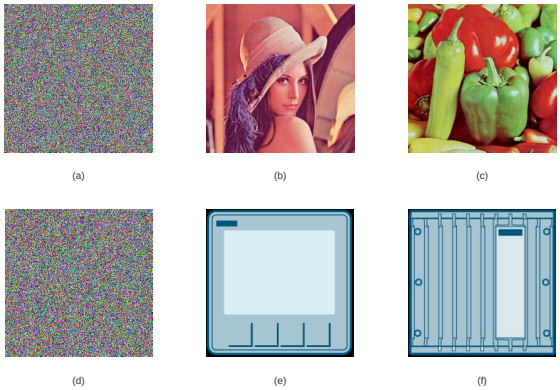


Fig. 4. Encryption and decryption results. (a) Encrypted color image of "Lena" and "Peppers", (b) Decrypted "Lena" image, (c) Decrypted "Peppers" image, (d) Encrypted color image of "IIDO1" and "IIDO2", (e) Decrypted "IIDO1" image, (f) Decrypted "IIDO2" image.

IV. Experimental Results and Analysis

All of the experiments in this section were done on a personal computer, which contains an Intel(R) Core(TM) and 4 Duo CPU i7-8550U @ 1.8GHz, Microsoft Windows 10 system with 8.00GB RAM and Matlab (R2014b) platform. PDCIEA is applied to the color images "Lena" and "Peppers" with the size of 256×256, and two random images selected from Siemens AG Industry's industrial image database objects (IIDOs) [33], [34] shown in Fig. 3. The initial values and parameters of the Eq. (5) are $x_0 = 1.1$, $y_0 = 1.3$, $z_0 = 1.2$, $a = 10$, $b = 8/3$ and $c = 28$. The initial values of Step 6 are $c_{10} = 834$, $c_{20} = 1324$, $c_{30} = 8743$, $d_{10} = 1260$, $d_{20} = 3425$ and $d_{30} = 57786$, respectively. The corresponding encryption and decryption results are shown in Fig. 4.

$$\begin{cases} d_{1i} = \left(\left(d_{1(i-1)} + d_{2(i-1)} + c_{1i} + c_{1(i-1)} + c_{2(i-1)}\right) \mod 65536\right) \oplus c_{3(i-1)} \oplus d_{3(i-1)} \oplus u_{1i}, \\ d_{2i} = \left(\left(d_{2(i-1)} + d_{3(i-1)} + c_{2i} + c_{2(i-1)} + c_{3(i-1)}\right) \mod 65536\right) \oplus c_{1i} \oplus d_{1i} \oplus u_{2i}, \\ d_{3i} = \left(\left(d_{3(i-1)} + d_{1i} + c_{3i} + c_{3(i-1)} + c_{1i}\right) \mod 65536\right) \oplus c_{2i} \oplus d_{2i} \oplus u_{3i}. \end{cases} \tag{11}$$

Algorithm 1 The proposed duple color image encryption algorithm.

Input: Two color images I_1, I_2;
Output: The encrypted image E of I_1 and I_2;

$[N, M] = size(I_1)$;
for $i = 1 : 3$ **do**
  $H_i = dec2bin(I_1(:, :, i), 8)$;
  $H_{3+i} = dec2bin(I_2(:, :, i), 8)$;
end for
for $i = 1 : 6$ **do**
  $J_i = reshape(H_i, N, M, 8)$;
end for
for $i = 1 : 6$ **do**
  $J(:, :, 8 \times (i-1) + 1 : 8 \times i) = J_i$;
end for
$A = Arnold3D(J)$; // The symbol $Arnold3D$ represents the 3D-NEAT
$B = reshape(A, N \times M, 48)$;
for $i = 1 : 3$ **do**
  $C_i = bin2dec(B(:, :, 16 \times (i-1) + 1 : 16 \times i))$;
end for
Diffuse all elements of C_1, C_2 and C_3 with Eq. (11) and obtain three diffused sequences D_1, D_2 and D_3;
for $i = 1 : 3$ **do**
  $E_i = reshape(D_i, N, M)$;
end for
for $i = 1 : 3$ **do**
  $G_i = M_{2(i-1)+1} \times E_i \times M_{2i}$; // Step 2: the shuffling matrixes M_i
end for
for $i = 1 : 3$ **do**
  $E(:, :, i) = G_i$;
end for
Output the encrypted image $E = E/65535$;

A. Statistical Analysis

It is well known that a meaningful image has obvious statistical properties that an attacker can use to attack an encryption system. Therefore, a good encryption algorithm can effectively destroy the statistical characteristics of the original image. To evaluate the performance of our algorithm, some typical statistical analysis methods are adopted in the experiments, such as histogram analysis, correlation analysis and information entropy analysis.

1) Histogram Analysis: The histogram reflects the frequency of each pixel value in an image. A good encryption algorithm will make the histogram of encrypted images completely different from the histogram of the original image, and the encrypted image should have an almost uniform distribution of pixel values.

Fig. 5 gives the histograms of the original images and the

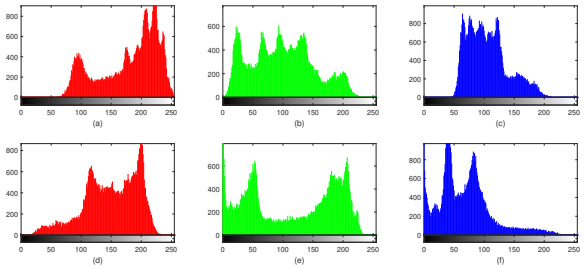


Fig. 5. Histograms of the original images. (a) red component of "Lena", (b) green component of "Lena", (c) blue component of "Lena", (d) red component of "Peppers", (e) green component of "Peppers", (f) blue component of "Peppers".

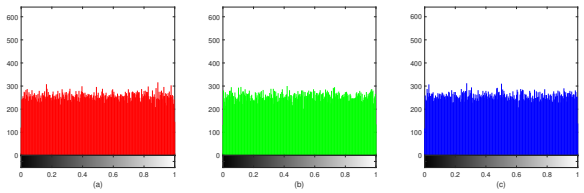


Fig. 6. Histograms of the encrypted color image. (a) red component of the encrypted image, (b) green component of the encrypted image, (c) blue component of the encrypted image.

histograms of the corresponding encrypted image are shown in Fig. 6. It is clear that the histograms of encrypted images differ from the histogram of the original images, and the pixel values of the encrypted image distribute uniformly among the interval of $[0, 1]$.

In addition, we use the chi-square test to quantitatively test the uniformity of histogram. The chi-square test has the form:

$$\chi^2 = \sum_{i=0}^{255} \frac{(k_i - \bar{k})^2}{\bar{k}}, \tag{13}$$

where k_i represents the number of occurrences of the pixel value i, and $\bar{k}$ is the expected frequency. So, as smaller as the χ^2 is, the more evenly distributed the image is.

To be consistent with the data type of the original image, first the encrypted image is converted to 8-bit data type in this test. Table I shows the χ^2 values of the original images and their corresponding encrypted image. It is clear from Table I that the χ^2 values of each component of the encrypted image are much smaller than the original images. This indicates that the distribution of the histogram of the encrypted image is uniform, therefore, it is impossible for the attacker to obtain the valid information of the original image by analyzing the histogram of the encrypted image.

2) Correlation Analysis: As is known to all, adjacent pixels of a meaningful image are highly correlated in each direction, and this feature makes statistical attacks possible. To analyze the correlation of the original images and encrypted image, we introduce the correlation coefficient C_{xy} between two

TABLE I
VALUES OF χ^2 FOR THE ORIGINAL AND ENCRYPTED IMAGES.

	Original "Lena" image			Original "Peppers" image			Encrypted color image		
	R	G	B	R	G	B	R	G	B
χ^2	65012	30363	92313	54389	35625	85311	390	391	381

TABLE II
CCAP IN EACH COMPONENT OF THE ORIGINAL AND ENCRYPTED IMAGES.

	Original "Lena" image			Original "Peppers" image			Encrypted color image		
	R	G	B	R	G	B	R	G	B
Horizontal	0.9792	0.9732	0.9555	0.9660	0.9792	0.9625	-0.0008	0.0012	0.0002
Vertical	0.9591	0.9448	0.9262	0.9626	0.9739	0.9526	-0.0003	0.0009	-0.0008
Diagonal	0.9393	0.9300	0.9038	0.9318	0.9540	0.9204	0.0003	0.0005	-0.0001

TABLE III
COMPARISON OF CCAP FOR EACH COMPONENT OF THREE ENCRYPTED IMAGES BY DIFFERENT ENCRYPTION ALGORITHMS.

	PDCIEA			[35]			[28]			[36]	[37]
	R	G	B	R	G	B	R	G	B		
Horizontal	-0.0008	0.0012	0.0002	0.0027	0.0034	0.0046	-0.0169	-0.0238	-0.0261	-0.0003	0.0017
Vertical	-0.0003	0.0009	-0.0008	-0.0013	-0.0034	0.0038	-0.0057	-0.0046	-0.0064	-0.0013	-0.0011
Diagonal	0.0003	0.0005	-0.0001	-0.0039	-0.0021	0.0013	-0.0300	-0.0510	-0.0012	-0.0066	-0.0013

adjacent pixels (CCAP) to measure the degree of correlation in a specific direction.

$$C_{xy} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\sum_{i=1}^{N}(x_i - \bar{x})^2)(\sum_{i=1}^{N}(y_i - \bar{y})^2)}} \tag{14}$$

where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$.

We randomly chosen 8000 pairs of two adjacent pixels from the original image and the cipher image. The correlation coefficient of two adjacent pixels in the original images and their corresponding encrypted image are listed in Table II. And the CCAP of encrypted image by our scheme were compared with those of [28], [35], [36], as shown in Table III. Fig. 7 shows the correlation of two vertical adjacent pixels of the original images, and the correlation of two vertical adjacent pixels of encrypted image are shown in Fig. 8. From the results, we can find that the correlation coefficient of adjacent pixels in each direction of the encrypted image is close to 0, while that of adjacent pixels in each direction of the original images is close to 1, which means that our algorithm can effectively resist statistical attacks.

3) Information Entropy: Information entropy can measure the degree of uncertainty and randomness of information source. For images, $H(s)$ is used to measure the confusion of an image and measure the uniformity of gray value distribution. Let s denote the information source, the formula for calculating information entropy $H(s)$ is expressed as follows:

$$H(s) = -\sum_{i=0}^{L-1} p(s_i)\log_2 p(s_i), \tag{15}$$

where $p(s_i)$ represents the probability of s_i. For a 256 level grayscale image, when the occurrence frequency of each pixel value of ciphertext is equal, the theoretical value is 8.

Table IV lists the information entropy of each component of the original images and encrypted images, and the information entropy of PDCIEA and other encryption schemes are listed in Table V. From these data, we can find that the information entropy of each component of the encrypted image is close to 8, and the information entropy of each component of encrypted image by PDCIEA is larger than those of [38] and [39]. Those mean the PDCIEA has a good property of information entropy.

TABLE V
COMPARISON OF $H(s)$ FOR EACH COMPONENT OF ENCRYPTED IMAGES BY DIFFERENT ENCRYPTION ALGORITHMS.

	Encrypted color image		
	R	G	B
PDCIEA	7.9954	7.9954	7.9955
[38]	7.9898	7.9898	7.9908
[39]	7.9896	7.9893	7.9896
[40]	7.9974	7.9976	7.9975
[41]	7.9977	7.9980	7.9992
[42]	7.9969	7.9974	7.9968

4) Local Shannon entropy: We introduce the local Shannon entropy [43] to measure the randomness of the cipher image, because the global Shannon entropy is sometimes unable to measure the real randomness of the image, and it can be defined by:

$$\overline{H_{(k,T_B)}}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{16}$$

where $S_1, S_2, \cdots, S_k$ are random selection of non-overlapping blocks image with T_B pixels from the test image and $H(S_i)(i = 1, 2, \cdots, k)$ are calculated by Eq. (15).

In this test, we randomly select $k = 30$ non-overlapping blocks image with $T_B = 1936$ pixels from the encrypted image. It can be seen from the conclusion of Ref. [43],

TABLE IV
$H(s)$ VALUES OF EACH COMPONENT OF THE ORIGINAL AND ENCRYPTED IMAGES.

	Original "Lena" image			Original "Peppers" image			Encrypted color image		
	R	G	B	R	G	B	R	G	B
$H(m)$	7.2412	7.5767	6.9171	7.3356	7.6122	7.1604	7.9954	7.9954	7.9955

the confidence interval of $(30, 1936)$-local Shannon entropy should be between $[7.901901305, 7.903037329]$, with respect to α-level confidence of 0.05. The values of local Shannon entropy for color encrypted image are listed in Table VI, it can see from Table VI that our algorithm provides a random-like encrypted image, which has a ideal random degree.

TABLE VI
THE TEST OF LOCAL SHANNON ENTROPY FOR ENCRYPTED IMAGE
$(k = 30, T_B = 1936, \alpha = 0.05)$.

	$\overline{H_{(30,1936)}}(S)$	Result
Encrypted image		
R	7.902702	SUCCESS
G	7.901942	SUCCESS
B	7.902869	SUCCESS

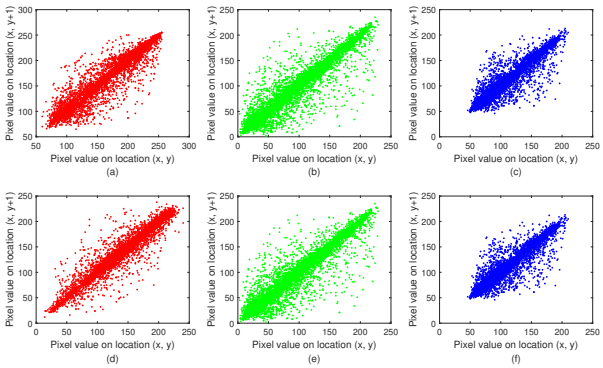


Fig. 7. Correlation of two vertical adjacent pixels in (a) red component of "Lena", (b) green component of "Lena", (c) blue component of "Lena", (d) red component of "Peppers", (e) green component of "Peppers", (f) blue component of "Peppers".

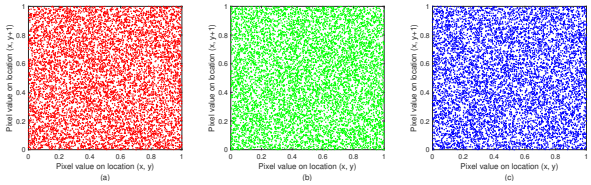


Fig. 8. Correlation of two vertical adjacent pixels in (a) red component of the encrypted image, (b) green component of the encrypted image, (c) blue component of the encrypted image.

B. Key Sensitive Analysis

The key sensitive is one of the important criteria to measure the security of an encryption algorithm. Key sensitivity means that for the same encrypted image with a small change of the keys, the corresponding decrypted images are completely different. Here, we test the sensitivity of PDCIEA to the key from the decryption process. We introduce the mean square error (MSE) to measure the influence of key perturbation on the encrypted image. It measures the degree of difference between two images, which is defined as:

$$MSE = \frac{1}{3MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3}(I(i,j,k) - H(i,j,k))^2, \quad (17)$$

where N and M are the sizes of the images. For two images, a larger MSE value indicates a greater difference between two images. In the process of decryption, the MSE curves corresponding to the decrypted images and the original images when only key x_0 is changed are shown in Figs. 9 (a-b), and the MSE curves corresponding to only key y_0 changes are shown in Figs. 9 (c-d). See from the MSE curves, we can find that the MSE value is close to 0 only if the key is completely correct, and the other cases are very large. This means that even small changes in the key will not produce the correct decryption results unless the key is completely correct. Therefore, the proposed encryption algorithm has high key sensitivity.

C. Key Space Analysis

A good encryption algorithm should be a sufficiently large key space to make the brute force attack impossible. For a cryptosystem, the larger the key space, the better the resistance to brute force attacks. The key of our algorithm includes a, b, c, x_0, y_0, z_0, c_{10}, c_{20}, c_{30}, d_{10}, d_{20} and d_{30}. Where the parameters (a, b, c) and initial values (x_0, y_0, z_0) of 3D Lorenz system are double, and c_{10}, c_{20}, c_{30}, d_{10}, d_{20} and d_{30} are 16-bit integers. And that the computer's calculation accuracy is 10^{16}, so the total key space $S \approx 7.9228 \times 10^{124}$. The comparison with other algorithms in key space is shown in Table VII, which shows that PDCIEA has larger key space than other algorithms, and has a large enough key space to resist brute force attacks.

D. Differential Analysis

In general, an attacker may make slight changes to the plain image, and then observe the changes in the cipher image to find some meaningful relationship between the plain image and the cipher image. This is the attack method of a chosen-plaintext attack, also known as a differential attack. And plaintext sensitivity is that small changes in the plaintext image

TABLE VII
COMPARISON OF KEY SPACE.

Algorithm	PDCIEA	[35]	[38]	[44]
Key space	7.9228×10^{124}	6.5536×10^{48}	10^{60}	4.295×10^{71}

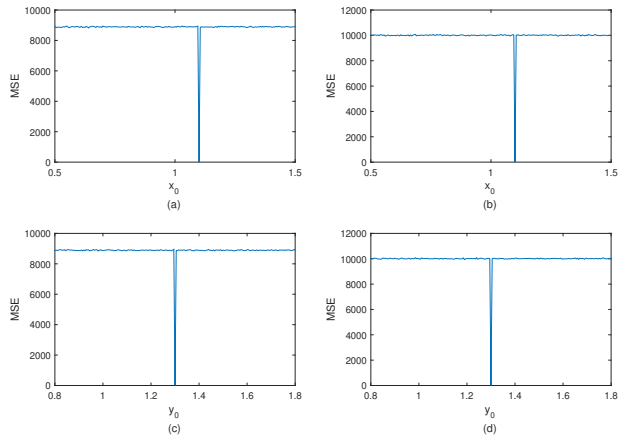


Fig. 9. MSE curves for x_0 and y_0. (a) "Lena", (b) "Peppers", (c) "Lena", (d) "Peppers".

will lead to a completely different ciphertext image. Therefore, the algorithm can effectively resist differential attacks if it is sensitive to plaintext. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are presented to test the sensitivity of encryption algorithms to plaintext. Mathematically, the formulas for the calculation of the values of NPCR and UACI are as follows [45]:

$$NPCR = \frac{\sum_{i,j} D_{R,G,B}(i,j)}{N \times M} \times 100\% \tag{18}$$

$$UACI = \frac{\sum_{i,j} |C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)|}{N \times M \times H} \times 100\% \tag{19}$$

respectively, where $C_{R,G,B}(i,j)$ and $C'_{R,G,B}(i,j)$ are each component of the cipher images before and after one pixel of the plain image is changed, H represents the largest allowed pixel value in the image and $M \times N$ is the size of the image.

$$D_{R,G,B}(i,j) = \begin{cases} 0 & if \quad C_{R,G,B}(i,j) = C'_{R,G,B}(i,j), \\ 1 & if \quad C_{R,G,B}(i,j) \neq C'_{R,G,B}(i,j). \end{cases} \tag{20}$$

The values of NPCR and UACI of one pixel change of plaintext image in our algorithm are shown in Table VIII. The NPCR and UACI test results of one pixel change of the original "Lena" image are listed in columns 2 through 4 of Table VIII, and the columns 5 through 7 of Table VIII list the values of NPCR and UACI of one pixel change of the original "Peppers" image. As Table VIII shown, the NPCR values of three components of the images no less than 0.9739 and the UACI values no less than 0.3255. This means that a small change in the plaintext image will cause at least 97.39% pixel value change in the ciphertext image. In other words, our algorithm is very sensitive to plaintext, so it can effectively resist selective plaintext attack and differential attack.

TABLE VIII
NPCR AND UACI VALUES FOR ENCRYPTING TWO TEST IMAGES.

	"Lena"			"Peppers"		
	R	G	B	R	G	B
$NPCR$	0.9739	0.9740	0.9740	0.9995	0.9996	0.9996
$UACI$	0.3237	0.3248	0.3255	0.3328	0.3329	0.3336

E. NIST SP 800-22 Batteries of Test

The National Institute of Standards and Technology (NIST) has released a test suite for randomness testing of random number and pseudo-random number generators [46]. This test method can be used to analyze the uncertainty of chaotic sequence in the encryption system and the randomness between the encrypted image pixels. The parameters of NIST SP 800-22 tests in Table IX.

TABLE IX
NIST SP 800-22 PARAMETERS.

Parameters	Value
Block frequency Test-Block length (M)	128
Non-overlapping Template-Block length (m)	9
Overlapping Template-Block length (m)	9
Approximate Entropy Test-Block length (m)	10
Serial Test-Block length (m)	16
Linear Complexity Test-Block length (M)	500

The results of NIST SP 800-22 tested on chaos sequences generated through 3D-LS and the pixels of encrypted image are shown in Table X. As can be seen from the table, the P-value for all the tests being above 0.01, which indicates that the chaotic sequence generated by 3D-LS and the encrypted image obtained after encryption have good randomness.

TABLE X
NIST SP 800-22 RESULTS.

Test parameters	P-value	
	3D-LS	Encrypted image
ApproximateEntropy	0.228878	0.213309
BlockFrequency	0.534146	0.122325
CumulativeSums-I	0.350485	0.739918
CumulativeSums-II	0.739918	0.911413
FFT	0.035174	0.350485
Frequency	0.440538	0.534146
LinearComplexity	0.213309	0.739918
LongestRun	0.122325	0.066882
NonOverlappingTemplate	0.911413	0.911413
OverlappingTemplate	0.568989	0.350485
Rank	0.122325	0.213309
Runs	0.350485	0.213309
Serial-I	0.534146	0.035174
Serial-II	0.122325	0.739918

F. Computational Complexity Analysis

The computational complexity of the proposed algorithm is determined by significant operations required to complete the encryption/decryption process over two colour images with the size of $N \times M$, such as 3D-NEAT, XORing and scrambling operations. For two colour images with the size of $N \times M$, there are $6 \times N \times M$ pixels in the plain image, in the process of 3D-NEAT, the transformation object is bit element, so the complexity for 3D-NEAT is $O(48 \times N \times M)$. In the process of diffusion and confusion scheme, the XORing and scrambling

TABLE XI
THE COMPUTATIONAL COMPLEXITY OF THE PROPOSED ALGORITHM AND OTHER SCHEMES.

Algorithm	PDCIEA	Ref. [40]	Ref. [47]
Computational complexity	$O(48 \times N \times M)$	$O(12 \times N \times M)$	$O(24 \times N \times M)$

operations are pixel level, the complexity for XORing and scrambling needs $O(6 \times N \times M)$. Moreover, chaotic sequences required during encryption/decryption process, which are generated by 3D-LS, and it takes up the complexity of $O(3 \times N \times M)$. Therefore, the overall computational complexity for the proposed scheme is $O(48 \times N \times M)$. Table XI reveals that the computational complexity of the proposed scheme is bigger than these schemes in Refs. [40], [47].

V. CONCLUSION

In this paper, we propose a new image encryption system for IIoT. In particular, the proposed scheme can encrypt two color images into one encrypted image, which can not only protect the privacy of the image but also reduce the amount of image information. The proposed system aims at realizing efficient and secure image transmission in IIoT. 3D-NEAT is applied to permute the positions of the elements of the 3D bit-level matrix calculated by converting the pixel values of the components of color images into binary values. At last, we get the cipher image by diffusing and scrambling the permutated 3D bit-level matrix using the chaos sequence generated from 3D-LS. To verify the feasibility and effectiveness of the system, we have carried out many numerical experiments and security analysis on the encryption system proposed in this paper. According to the test results, the proposed image encryption system has good security performance, which can effectively resist various common attacks, such as brute force attacks and chosen-plaintext attacks, and some performance is better than other image encryption algorithms proposed in recent years.

REFERENCES

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[2] H. Mouratidis, V. Diamantopoulou, "A Security Analysis Method for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4093–4100, 2018.

[3] Z. Xia, L. Jiang, X. Ma, W. Yang, P. Ji, N. Xiong, "A Privacy-Preserving Outsourcing Scheme for Image Local Binary Pattern in Secure Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 629–638, 2020.

[4] W. Zhang, H. Wang, D. Hou, N. Yu, "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation," *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469–1479, 2016.

[5] A. Gutub, F. Al-Shaarani, "Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons," *Arabian Journal for ence and Engineering*, vol. 45, pp. 26312644, 2020.

[6] F. S. Hassan, A. Gutub, "Efficient Image Reversible Data Hiding Technique Based on Interpolation Optimization," *Arabian Journal for Science and Engineering*, vol. 46, pp. 84418456, 2021.

[7] J. Chen, L. Chen, Y. Zhou, "Universal chosen-ciphertext attack for a family of image encryption schemes," *IEEE Transactions on Multimedia*, 2020, doi: 10.1109/TMM.2020.3011315.

[8] F. S. Hassan, A. Gutub, "Efficient reversible data hiding multimedia technique based on smart image interpolation," *Multimedia Tools and Applications*, vol. 79, pp. 3008730109, 2020.

[9] F. S. Hassan, A. Gutub, "Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, pp. 2017–2030, 2022.

[10] A. A. Gutub, "Adopting counting-based secret-sharing for e-Video Watermarking allowing Fractional Invalidation," *Multimedia Tools and Applications*, vol. 81, no. 7, pp. 9527–9547, 2022.

[11] F. S. Hassan, A. Gutub, "Improving data hiding within colour images using hue component of HSV colour space," *CAAI Transactions on Intelligence Technology*, vol. 7, no. 1, pp. 56–68, 2022.

[12] A. K. Sahu, A. Gutub, "Improving grayscale steganography to protect personal information disclosure within hotel services," *Multimedia Tools and Applications*, 2022, https://doi.org/10.1007/s11042-022-13015-7.

[13] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, G. Wang, H. Harry, S. Baik, "Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689, 2018.

[14] B. O. Al-Roithy, A. Gutub, "Remodeling randomness prioritization to boost-up security of RGB image encryption," *Multimedia Tools and Applications*, vol. 80, pp. 2852128581, 2021.

[15] A. Gutub, B. O. Al-Roithy, "Varying PRNG to improve image cryptography implementation," *Journal of Engineering Research*, vol. 9, no. 3A, pp. 153183, 2021.

[16] H. Huang, D. Cheng, "A secure image compression-encryption algorithm using dct and hyperchaotic system," *Multimedia Tools and Applications*, 2022, https://doi.org/10.1007/s11042-021-11796-x.

[17] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[18] Fridrich and Jiri, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation & Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[19] Z. Hua, S. Yi, Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, no. mar., pp. 134–144, 2018.

[20] V. Arnold, A. Avez, *Problemes Ergodiques De La Mećanique Classique*, Paris, France: Gauthier-Villars, 1967.

[21] Z. Ma, S. Qiu, "An image cryptosystem based on general cat map," *Journal on Communications*, vol. 24, no. 2, pp. 51–57, 2003.

[22] Q. Zhang, M. Shen, Y. Zhai, "3D Chaotic Cat Map Based Digital Image Encryption Method," *Journal of Data Acquisition & Processing*, vol. 22, no. 3, pp. 292–298, 2007.

[23] J. Wu, Z. Liu, J. Wang, L. Hu, S. Liu, "A compact image encryption system based on arnold transformation," *Multimedia Tools and Applications*, , no. 6, pp. 1–15, 2020.

[24] E. Solak, C. Cokal, O. Yildiz, "CRYPTANALYSIS OF FRIDRICH'S CHAOTIC IMAGE ENCRYPTION," *International Journal of Bifurcation and Chaos*, vol. 20, no. 5, pp. 1405–1413, 2010.

[25] Y. Chen, C. Tang, R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal processing*, vol. 167, no. Feb., pp. 107286.1–107286.12, 2020.

[26] Q. Wang, Q. Guo, J. Zhou, "Double image encryption based on linear blend operation and random phase encoding in fractional Fourier domain," *Optics Communications*, vol. 285, no. 21-22, pp. 4317–4323, 2012.

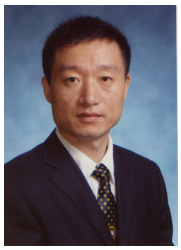
[27] N. Zhou, X. Yan, H. Liang, X. Tao and G. Li, "Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system," *Quantum Information Processing*, vol. 17, no. 12, pp. 338, 2018.

[28] A. Joshi, D. Kumar, A. Gaffar, D. Mishra, "Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform," *Optics and Lasers in Engineering*, vol. 133, pp. 106139, 2020, https://doi.org/10.1016/j.optlaseng.2020.106139.

[29] L. Shao, Z. Qin, H. Gao and X. Heng, "2-Dimension Non Equilateral Image Scrambling Transformation," *Acta Electronica Sinica*, vol. 35, no. 7, pp. 1290–1294, 2007.

[30] Y. Li, Q. Feng, F. Zhou, Q. Li, "2-D Arnold transformation and non-equilateral image scrambling transformation," *Computer Engineering and Design*, vol. 30, no. 13, pp. 3133–3135, 2009.
[31] C. Wu and X. Tian, "3-Dimensional Non-equilateral Arnold Transformation and its Appl ication in Image Scrambling," *Journal of Computer-Aided Design & Computer Graphics*, vol. 22, no. 10, pp. 1831–1840, 2010.
[32] E. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.
[33] N. Hurrah, N. Loan, S. Parah, J. Sheikh, K. Muhammad, A. de Macedo, V. de Albuquerque, "INDFORG: Industrial Forgery Detection using Automatic Rotation Angle Detection and Correction," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3630–3639, 2021.
[34] Siemens AG Industry, "Industrial image database," 2022. [Online]. Available: https://www.automation.siemens.com/bilddb/search.aspx. Accessssed on: September 17, 2022.
[35] H. Huang, S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Processing*, vol. 11, no. 4, pp. 211–216, 2017.
[36] B. Abd-El-Atty, A. Abd El-Latif, S. Venegas-Andraca, "An encryption protocol for NEQR images based on one-particle quantum walks on a circle," *Quantum Information Processing*, vol. 18, no. 9, 2019.
[37] H. Huang, Y. Chen, D. Cheng, "Plaintext-related image encryption scheme based on chaos and game of life," *Journal of Electronic Imaging*, vol. 31, no. 1, pp. 013031, 2021, https://doi.org/10.1117/1.JEI.31.1.013031.
[38] H. Huang, "Novel Scheme for Image Encryption Combining 2D Logistic-Sine-Cosine Map and Double Random-Phase Encoding," *IEEE Access*, vol. 7, no. 1, pp. 177988–177996, 2019.
[39] M. Sahari, I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 723–744, 2018.
[40] N. Chidambaram, P. Raj, T. Karruppuswamy, R. Amirtharajan, "Advanced framework for highly secure and cloud-based storage of colour images," *IET Image Processing*, vol. 14, no. 13, pp. 3143–3153, 2020.
[41] Y. Hu, Q. Li, D. Ding, L. Jiang, Z. Yang, H. Zhang, Z. Zhang, "Multiple coexisting analysis of a fractional-order coupled memristive system and its application in image encryption," *Chaos, Solitons & Fractals*, vol. 152, 2021, https://doi.org/10.1016/j.chaos.2021.111334.
[42] M. Zarebnia, R. Parvaz, "Image encryption algorithm by fractional based chaotic system and framelet transform," *Chaos, Solitons & Fractals*, vol. 152, 2021, https://doi.org/10.1016/j.chaos.2021.111402.
[43] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.
[44] H. Huang, S. Yang, R. Ye, "An efficient symmetric image encryption by using a novel 2D chaotic system," *IET Image Processing*, vol. 14, no. 6, pp. 1157–1163, 2020.
[45] S. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Processing*, vol. 92, no. 5, pp. 1202–1215, 2012.
[46] R. Sivaraman, S. Rajagopalan, J. Rayappan, R. Amirtharajan, "Ring oscillator as confusion-diffusion agent: a complete trng drove image security," *IET Image Processing*, vol. 14, no. 13, pp. 2987–2997, 2020.
[47] X. Chai, X. Fu, Z. Gan, Y. Lu, Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

Huiqing Huang received the Ph.D. degree from the Department of Mathematics, Shantou University, Shantou, China, in 2018. From 2020 to 2021, he was a Visiting Scholar with the Macau University of Science and Technology, Macau, China. He is currently a lecturer with the College of Mathematics, Jiaying University, China. His research interests include chaos cryptography, information security, and image processing. He has authored over 10 papers in journals and refereed conference.



Zhanchuan Cai (Senior Member, IEEE) received the Ph.D. degree in computer software and theory from Sun Yat-sen University, Guangzhou, China, in 2007. He is currently a Professor with the School of Computer Science and Engineering, Macau University of Science and Technology, Macau, China, where he is also with the State Key Laboratory of Lunar and Planetary Sciences at Macau University of Science and Technology. He has authored over 100 papers in journals and refereed conference. His research interests include image processing and computer graphics, intelligent information processing, multimedia information security, and remote sensing data processing and analysis.