


# Secure Optical Image Communication Using Double Random Transformation and Memristive Chaos

Heping Wen , Jiahao Wu, Linchao Ma, Zhen Liu , Yiting Lin , Limengnan Zhou , Huilin Jian, Wenxing Lin, Linhao Liu, Tianle Zheng, and Chongfu Zhang , *Senior Member, IEEE*

**Abstract**—The issue of information security in photonics environment has attracted more and more attention, especially when the secure communication of optical digital images has become a research hotspot. In this paper, we propose a hybrid encryption scheme for color images in the frequency and spatial domains based on double random transform and memristor hyperchaotic system. Firstly, we decompose the color image into RGB channels and then perform fast fourier transform (FFT) to transform the digital image from the spatial domain to the frequency domain. Secondly, two-phase masks are generated using the memristor hyperchaotic system, and the Fresnel diffraction optical transformation method is performed twice for encryption. Thirdly, the transformation from the frequency domain to the spatial domain is completed using inverse fast fourier transform (IFFT). Finally, the image is permuted and diffused using the chaotic sequences to obtain the final cipher image. Double random phase encryption expands the key space, while the combination of spatial and frequency domains improves the resistance to attacks. Based on cryptanalysis theory, we introduce a dynamic key associated with plain image, which can effectively resist plain attack. The experimental results show that the optical digital image encryption scheme has a large key space, excellent comprehensive performance, and can resist common attacks. In addition, we verify the hardware feasibility and ease of implementation of the proposed algorithm in an embedded optical communication network experimental platform. Therefore, our proposed scheme in this paper is a preferred optical digital image secure communication technology scheme with good application prospects.

**Index Terms**—Optical image encryption, information security, Chaos.

Manuscript received 16 November 2022; revised 20 December 2022; accepted 28 December 2022. Date of publication 30 December 2022; date of current version 23 January 2023. This work was supported in part by the National Science Foundation of China under Grant 62071088, in part by the National Natural Science Foundation of China under Grant 61901096, in part by the Science and Technology Projects of Guangdong Province under Grant 2021A0101180005, in part by Project for Department of Education of Guangdong Province under Grant 2021ZDZX1083, and in part by the Project for Zhongshan Science and Technology under Grant 2021B2062 (*Corresponding authors: Heping Wen; Chongfu Zhang.*)

The authors are with the Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan 528402, China, and also with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: wenheping@uestc.edu.cn; 2019020398117@std.uestc.edu.cn; 2019010004051@stu.zsc.edu.cn; Liuzhen\_zsc@yeah.net; 202004072053@stu.zsc.edu.cn; dreamzlmn@foxmail.com; 1196705632@qq.com; 202003061011@stu.zsc.edu.cn; 202001151017@stu.zsc.edu.cn; 2019010005080@stu.zsc.edu.cn; cfzhang@uestc.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3233129

## I. INTRODUCTION

OPTICAL communication network is a key information infrastructure, and the rapid development of its corresponding technology is revolutionarily changing the way of human work and life. Conversely, the information security of optical network transmission cannot be ignored. Information makes it convenient for people to work or study in daily life as it performs well in transmitting and sharing. Among a wide range of information, digital images have received more attention than others because of the sheer quantity of information and good intuitiveness. Digital image encryption technology is a common method to ensure the confidentiality of images. At this stage, many digital image encryption schemes have been proposed and have achieved good experimental results [1], [2], [3], [4], [5]. However, for one, with the rapid development of technology, the update speed of the algorithm is faster than ever before [6], [7], [8], [9], [10]. Secondly, due to the two-dimensionality of digital images, the redundancy and strong correlation between adjacent pixels are eye-catching [11], [12], [13], [14], [15]. Therefore, information security is facing severe challenges in network communication, which urges us to study more secure digital image encryption schemes [13], [16], [17], [18], [19]. Various mechanisms and methods have been introduced to enhance the security of the algorithm [20], [21], [22], [23].

In 2018, Ref. [24] presented a new third-order RLCM-four-elements-based chaotic circuit. The presented memristive chaotic circuit can emerge complex dynamics with chaos, period, coexisting bifurcation modes, and coexisting bubbles. In 2019, Ref. [25] proposed a dual image encryption method based on optical interference and logistic mapping. Experimental results show that this method further improves the security of image encryption on the basis of ensuring its effectiveness and feasibility. In 2020, Ref. [6] proposed a color image encryption scheme based on compressed sensing and dual random transformation. This encryption scheme uses a compression-obfuscation-diffusion encryption structure. The experimental results show a good ability to resist known-plaintext attack (KPA) and chosen-plaintext attack (CPA). Experimental results show that the scheme has a good performance in ensuring information security. Ref. [26] advanced an optical image encryption algorithm based on hyperchaos and public key cryptography. The experimental results show the algorithm in this scheme increases the key space, and reduces the volume and computational complexity of the key, while improving the

computational efficiency. In 2021, some papers are presented, Ref. [27] designed a three-dimensional chaotic system based on memristors. The experimental results show the system has strong superiority, and provide a broader application prospect for chaotic secure communication and image encryption; Ref. [28] proposed a chaotic sequence generation method, correlated with plain and based on cellular neural networks. A dual-channel algorithm for image encryption and decryption was pointed out as well. According to different image parts, digital or optical encryption channels are selected to meet different levels of security requirements; Ref. [14] proposed an asymmetric image encryption method with a basis of HCS, operation at the DNA level and ART concurrently. Under the guidance of this method, key space can be enlarged well enough. Furthermore, because of its high sensitivity to the cipher image, the key space can protect information to a larger extent; Ref. [29] put forward an asymmetric two-color image encryption scheme based on dual random phase encoding and compressed sensing. This scheme effectively improves the security of the image. In summary, although the industry has laid relatively rich theoretical foundations and attained technical achievement in digital image encryption, most of the existing researches are just to perform chaotic systems or optical transformations of digital images on a two-dimensional matrix in the spatial domain of encryption processing.

Aimed at solving the existing problems, this paper proposes a digital color image encryption scheme based on dual random phase encryption and memristive hyperchaotic system. This paper gets an interdisciplinary conclusion by combining optics and chaos. The optical field focuses on encrypting the frequency plane, while the chaotic field specializes in encrypting the spatial domain. The combination of these two fields improves the security of the algorithm. It not only gives full play to the advantages of large capacity and relatively high speed of optical encryption, but also reflects the initial value sensitivity and unpredictability of chaos. By simply using optical encryption, the encryption result is complex and difficult to transmit. Similarly, only chaotic encryption is used, which means only time domain is encrypted, and the quality of encryption will be reduced. In this paper, we use normalization function to realize the conversion between the spatial domain and the frequency domain, thus double random phase encryption and chaotic encryption can be combined. In this experiment, we use the model built by the memristor to generate a chaotic system. Since the resistance of the memristor is affected by magnetic flux and electric charge, it helps to improve the sequence randomness and system complexity. As a circuit element, the memristor can replace the non-linear term in chaotic system and achieve the purpose of simplifying the circuit model. Due to the memory characteristics of the memristor, it is endowed with more complex dynamics than traditional circuits, which increases the difficulty of deciphering digital images. Since each iteration of chaos involves complex integral operations and has high algorithm complexity, the memristive chaotic system is used to iteratively generate a sequence of one-eighth length, and the remaining sequences are combined through certain permutation and combination. This method improves encryption speed while maintaining encryption quality.

Our encryption scheme is summarized as follows: Firstly, the hyperchaotic Lorenz system is generated from the memristive simulator. Secondly, the two key mask maps for double random encryption and the two-dimensional random sequence for permutation-diffusion are developed from the hyperchaotic Lorenz system. Thirdly, with the help of Double Random Phase Encryption (DRPE) [19], [30], [31], [32], [33], the original image is quickly encrypted, and the original image information is encrypted to the greatest extent. Finally, chaotic encryption performed by using the chaotic scrambling-diffusion encryption structure. This scheme uses the memristive simulator to generate a chaotic system with complex dynamics, which makes the image information more complicated, and more in line with the relevant standards in the practical application fields. Compared with the existing scheme, our scheme has the following advantages:

- The use of memristors to generate billions of resistance hyperchaotic, the performance of the generated sequence is better, and the use of memristors to simplify the model, reducing the amount of calculation
- Digital image encryption combined with double random phase changes, image encryption is introduced into optical changes
- An actual encrypted communication experiment in optical network environment is carried out to further verify the feasibility of the scheme

Through several verifications, the experimental results show that the scheme has high-security performance and encryption efficiency.

## II. RELATED THEORY

### A. Double Random-Phase Encoding

With the in-depth development of research in the field of optics, more and more related technologies have been explored and applied. In the field of image encryption, optical encryption technology has been favored by researchers, because the optical encryption technology has many controllable parameters and the freedom of adjustment of these parameters is high. In the encryption process, optical properties such as focal length, phase, wavelength and diffraction distance are often involved. These parameters enlarge the key space. And because optical encryption has the characteristics of large capacity, it can encrypt more information. Generally, the plain image is scrambled and encoded by optical transformation to realize encryption, such as interference, diffraction. Among the optical image encryption technologies, DRPE is widely used in image encryption. It was first proposed by Refregier and Javidi [6].

The encryption principle of DRPE is briefly described below. The DRPE used in this paper is based on Fresnel diffraction FD for image encryption [34], [35]. The encryption principle process is shown in Fig. 1, original digital image  $P(x, y)$  is placed on the input plane  $\Omega$ . Firstly, it is irradiated by the perpendicular incident light  $\lambda$ . In unit amplitude, the  $P(x, y)$  is modulated by  $RPM_1$  that is close to the input surface of encryption. Next, it reaches the Fresnel diffraction plane  $\Omega_1$  through the Fresnel diffraction transformation at a distance

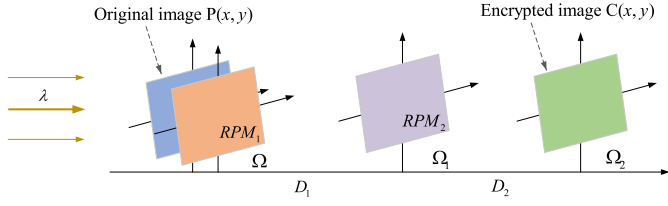


Fig. 1. Process diagram of double random phase encryption based on fresnel diffraction in principle.

of  $D_1$ . After the second  $RPM_2$  encryption, it finally reaches the output plane  $\Omega_2$  through Fresnel diffraction transformation with a distance of  $D_2$ . Encrypted image  $C(x, y)$  is gotten. In Fig. 1,  $RPM_1$  refers to  $\exp[j2\pi\varphi(x, y)]$ , and  $RPM_2$  refers to  $\exp[j2\pi\phi(u, v)]$ .

The entire encryption process formula is:

$$C(x, y) = \text{fft}^{-1}\{\text{fft}\{P(x, y) \times \exp[j2\pi\varphi(x, y)]\} \exp[j2\pi\phi(u, v)]\} \quad (1)$$

where

$$FD\{P(x, y)\} = \frac{\exp(jkD)}{j\lambda D} \iint P(x, y) \times \exp[jk \frac{(m-x)^2 + (n-y)^2}{2D}] dx dy \quad (2)$$

where  $\text{fft}$  and  $\text{fft}^{-1}$  represent the fast fourier transform (FFT) and inverse fast fourier transform (IFFT), respectively.  $D$  is the diffraction distance,  $\lambda$  is the wavelength of light,  $k$  is  $\frac{2\pi}{\lambda}$ ,  $j$  is the imaginary unit,  $(m, n)$  is the coordinates of the  $RPM_1$  pixel and  $(x, y)$  is the coordinates of the original image pixel.  $\varphi(x, y)$  is in the spatial domain, and  $\phi(u, v)$  is in the frequency domain. They are all white noise sequences that are uniformly distributed and independent on  $[0, 1]$ . The encryption scheme theoretically doesn't need to use a lens system for encryption, and can be used for encryption simulation on a computer with simulation software. In addition, since the encrypted data is plural, the data needs to be converted into real values before subsequent encryption processing.

### B. Memristive Hyperchaotic System

In the field of image encryption, chaotic encryption has been already extensively focused on and utilized. Chaos has the advantages of unpredictability, sensitivity of initial value and uncertainty. With continuous improvement and innovation, it has become more and more mature and safe. Compared with the general chaotic system, the hyperchaotic system presents more complex folding characteristics, better development trajectory and higher security. The general model of hyperchaotic Lorenz system is [6]:

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + rw \end{cases} \quad (3)$$

where  $a, b, c$  and  $r$  are the parameters of the hyperchaotic Lorenz system. When  $a = 10, b = 2.667, c = 28$  and  $-1.52 < r \leq -0.06$ , the system is in hyperchaotic state.

The concept of memristor was first proposed by Professor Cai Shaotang, and the physical model of memristor was discovered in HP laboratory [37]. The birth of memristor provides better assistance for the construction of chaotic system, which can more easily realize the hyperchaotic system. The memristor model adopted in this paper is:

$$q(\varphi) = -a\varphi + 0.5b\varphi|\varphi| \quad (4)$$

where both  $a$  and  $b$  are positive,  $\varphi$  is the magnetic flux of the memristor.

The memristor equation is as follows:

$$W(\varphi) = \frac{dq(\varphi)}{d\varphi} = -a + b|\varphi| \quad (5)$$

The memristor hyperchaotic Lorenz system model adopted in this paper is:

$$\begin{cases} \dot{x} = d(y - x) \\ \dot{y} = -xz + cy + (e + fc)x + kW(w)x \\ \dot{z} = xy + gz \\ \dot{w} = x \end{cases} \quad (6)$$

where  $c, d, e, f, k,$  and  $g$  all are system parameters. This paper selects parameters  $a = 15, b = 0.02, c = -10, d = 35, e = 95, f = -4, k = 1,$  and  $g = -3$ . The phase diagram of hyperchaotic Lorenz attractor generated by memristor system (6) is shown in Fig. 2.

### III. THE PROPOSED ENCRYPTION ALGORITHM

Both DRPE algorithm and chaotic encryption algorithm have their own advantages and disadvantages. Neither the DRPE based on any transformation nor the chaotic encryption based on any structure can not avoid the defects of the algorithm itself. Although DRPE can encrypt a lot of information, its space computational complexity and time operation complexity is high. Chaos is highly sensitive to the key and has good encryption performance. However, the encryption of data is usually only carried out in the spatial domain. Once the encryption is carried out with relatively simple permutation and diffusion structure, the encrypted information is vulnerable to attack. To sum up, the two encryption methods need to be combined together so as to better encrypt the image information. In this way, the advantages of the two encryption methods can be combined to properly make up for their respective disadvantages.

This paper proposes a digital color image encryption scheme based on double random phase and memristor hyperchaotic Lorenz system. Firstly, use memristors to generate chaotic systems. Secondly, apply chaotic systems to generate double random encryption and permutation diffusion random sequences. Thirdly, decompose the original image into RGB sub-images. Perform double random encryption on the three sub-images, and then permute and diffuse these images. Finally, synthesize the encrypted RGB sub-images to obtain the final encrypted color

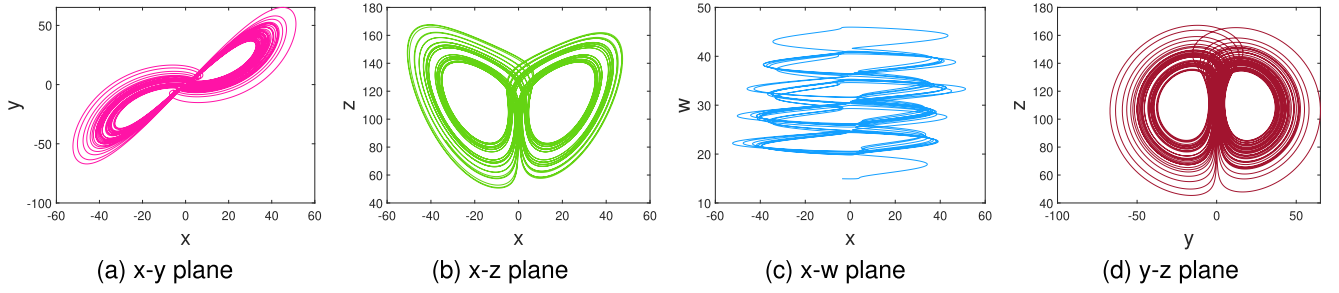


Fig. 2. Memristive hyperchaotic attractor phase diagram.

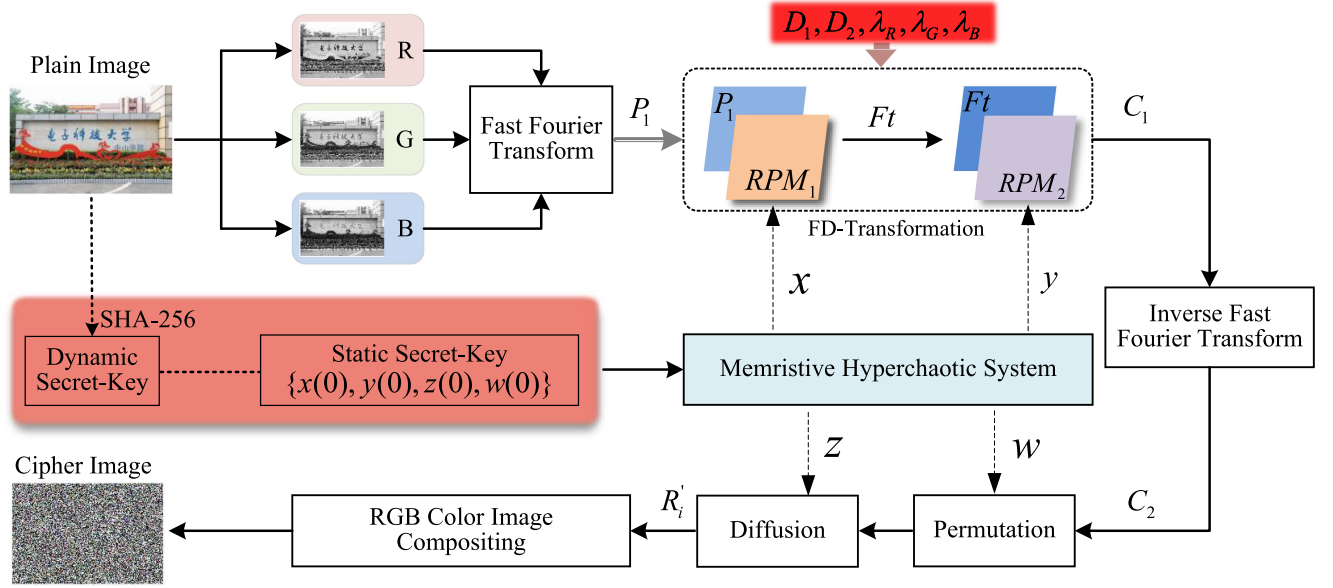


Fig. 3. The flowchart of DRPE and hyperchaotic Lorenz encryption generated by a memristor.

image. The specific steps of the encryption algorithm are as follows:

*Step 1. Memristive chaotic encryption sequences:* The key of the cryptosystem in this paper consists of two parts: Dynamic Secret-key and Static Secret-key. The dynamic secret-key is determined by a hash function that dynamically generates a 256-bit hash value based on the plaintext. The static secret-keys are the four initial values of the memristive hyperchaos, and the wavelength  $k$  and diffraction distance  $D$  in Fresnel diffraction, respectively. The specific key space is  $\{hash256, x(0), y(0), z(0), w(0), D_1, D_2, \lambda_R, \lambda_G, \lambda_B\}$ .

Firstly, use the memristor constructed to generate the sequence and mask required for encryption. Secondly, sample the corresponding spatial domain and frequency domain coordinates according to the plain image size. Thirdly, construct an environment for DRPE, which is the initial value of the parameters. Set diffraction wavelength  $\lambda$  and diffraction distance  $D$ . These parameters are used as part of the keys, and these keys can be set to different values for different sub-images. Fourthly, calculating the SHA-256 value of the plain image, slightly disturb the initial value of the hyperchaotic system so that different plains have different keys, which can improve the ability to resist CPA.

The specific formulas are as follows:

$$\begin{cases} \dot{x}(0) = x(0) + (s_1 \oplus s_2 \oplus s_3 \oplus s_4)/256/1000 \\ \dot{y}(0) = y(0) + (s_5 \oplus s_6 \oplus s_7 \oplus s_8)/256/1000 \\ \dot{z}(0) = z(0) + (s_9 \oplus s_{10} \oplus s_{11} \oplus s_{12})/256/1000 \\ \dot{w}(0) = w(0) + (s_{13} \oplus s_{14} \oplus s_{15} \oplus s_{16})/256/1000 \end{cases} \quad (7)$$

where  $x(0), y(0), z(0)$  and  $w(0)$  are the initial parameters of the hyperchaotic system.  $\dot{x}(0), \dot{y}(0), \dot{z}(0)$  and  $\dot{w}(0)$  are the initial values after disturbance.  $\oplus$  is bitwise XOR operation and  $s_i$  represents the hash value of the plain image.

*Step 2. Fast fourier transform:* First, the plaintext image is divided into RGB channel subgraphs, and each subgraph is encrypted separately. Here we take the R-channel submap as an example. Then the FFT is used to change the image from the spatial domain to the frequency domain to obtain the image  $P_1$  in the frequency domain.  $P_1$  will be subjected to double random phase change in the optical domain in the next step. The equation can be defined as follows:

$$P_1 = \text{fft}(P) \quad (8)$$

where  $P$  refers to the original image to be encrypted,  $P_1$  is a fourier-transformed matrix.



*Step 3. The first double random-phase encoding:* Multiply the preprocessed sub-image  $P_1$  in the frequency domain with the phase mask  $RPM_1$ . Then, complete double random encryption through the angular spectrum propagation function.

The equation can be defined as follows:

$$\begin{cases} Rt_1 = \exp(2\pi j \times \text{mask}_1) \\ Fai_1 = P_1 \cdot Rt_1 \\ Ft = h_2(fx, fy, D_1, \lambda_1) \cdot Fai \end{cases} \quad (9)$$

where  $\text{mask}_1$  refers to the random phase mask  $RPM_1$ ,  $Fai_1$  is the result of  $P_1$  and  $Rt_1$  point multiplication.  $h_2(\cdot)$  represents the angular spectrum propagation function,  $(fx, fy)$  represents the frequency domain coordinate position.  $Rt_1$  represents the value of  $\text{mask}_1$ .  $D_1$  is the Fresnel diffraction distance and  $\lambda_1$  is the single-amplitude incident light wavelength.  $Ft$  is the first randomly encrypted image.

*Step 4. The second double random-phase encoding:* The image after double random encryption is multiplied by the phase mask  $RPM_2$ , and then multiplied by the angular spectrum propagation function to realize the second random phase encryption.

The equation can be defined as follows:

$$\begin{cases} Rt_2 = \exp(2j \times \text{mask}_2) \\ Fai_2 = Ft \cdot Rt_2 \\ C_1 = h_2(fx, fy, D_2, \lambda_2) \cdot Fai_2 \end{cases} \quad (10)$$

where  $\text{mask}_2$  refers to the random phase mask  $RPM_2$ ,  $Fai_2$  is the result of  $Ft$  and  $Rt_2$  point multiplication.  $Rt_2$  represents the value of  $Ft$ ,  $Rt_2$  represents the Fresnel diffraction distance,  $\lambda_2$  represents the single-amplitude incident light wavelength,  $C_1$  represents the second randomly encrypted image.

*Step 5. Inverse fast fourier transform:* Use abs function and floor function to realize the conversion from plural cipher to real cipher. In the end, use the IFFT function to convert pixel values in  $C_1$  to  $[0, 256]$ .

The equation can be defined as follows:

$$C_2 = \text{fft}^{-1}(\text{floor}(\text{abs}(C_1))) \quad (11)$$

where  $\text{floor}(\cdot)$  rounds the element of  $C_1$  to the nearest integer toward minus infinity,  $\text{abs}(\cdot)$  takes absolute value of  $C_2$ .  $\text{Normalize}(\cdot)$  masks the value of  $C_2$  between 0 and 255,  $C_2$  represents the DRPE encrypted image.

*Step 6. Permutation:* Use the ascending function  $\text{sort}(\cdot)$  in Matlab to arrange the pixel values of a chaotic matrix from small to large, and record the sorted coordinate position  $[\text{index}H, \text{index}W]$ . Take  $[\text{index}H, \text{index}W]$  as the new coordinates of the pixels of the image to be encrypted. The permutation operation does not change the pixel value, only the pixel value position. The formula is summarized as follows:

$$\sum_{i=1}^H \sum_{j=1}^W U = \dot{C}_2 [\text{index}H(i), \text{index}W(j)] \quad (12)$$

where  $\dot{C}_2$  is the image to be encrypted,  $U$  is the cipher image after permutation.  $H$  and  $W$  are the height and width of the color images  $C_2$  and  $U$ , respectively.  $\text{index}H(i)$ ,  $\text{index}W(j)$  respectively refers to the row random sequence and column random sequence used for permutation.

*Step 7. Diffusion:* Use a chaotic random sequence  $S$  of length  $H \times W$  prepared in step1, set the first pixel of the cipher image  $R_1 = 0$ , then calculate the sum of  $S_1, U_1, R_1$  and perform a modulo operation on the sum to obtain the second cipher pixel  $R_2$ . Where  $U_1$  is the first pixel of image  $U$  to be encrypted, and  $S_1$  is the first pixel of the random sequence  $S$ . cipher pixel  $R_i$  can be sequentially obtained through the iterative relationship. In order to make the plain information completely hide in the cipher pixels, reverse diffusion is required, that is,  $i$  is diffused from  $H \times W$  to 1. The specific formula for two diffusions is as follows:

$$\begin{cases} R_i = (R_{i-1} + S_i + U_i) \bmod 256 & i \in [1, H \times W] \\ R'_i = (R_{i+1} + S_i + U_i) \bmod 256 & i \in [H \times W, 1] \end{cases} \quad (13)$$

where  $U$  is the image before diffusion,  $R_i$  is the image after modulus diffusion, and  $R'_i$  is the final cipher after encryption of the R channel subgraph of the plain image.  $S$  is the random chaotic sequence,  $\bmod$  is the modulus operator, and the calculation result is between 0 and 256. The range of  $H \times W$  values depends on the length and width of  $P$ .

*Step 8. RGB color image compositing:* Repeat the above steps again to obtain the ciphers of the clear image G and B channel subgraphs, respectively. Call the cat function to synthesize the three encrypted sub-images of RGB into the final color-encrypted image.

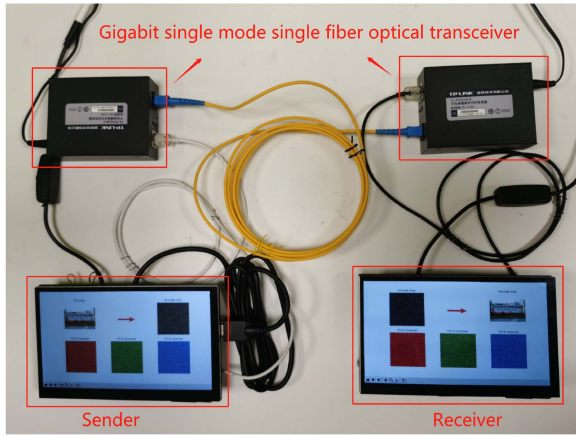
$$C = \text{cat}(3, R'_i, G'_i, B'_i) \quad (14)$$

where  $C$  is the final cipher.  $R'_i$  is the cipher of the plain image R channel,  $G'_i$  is the cipher of the plain image G channel, and  $B'_i$  is the cipher of the B channel.

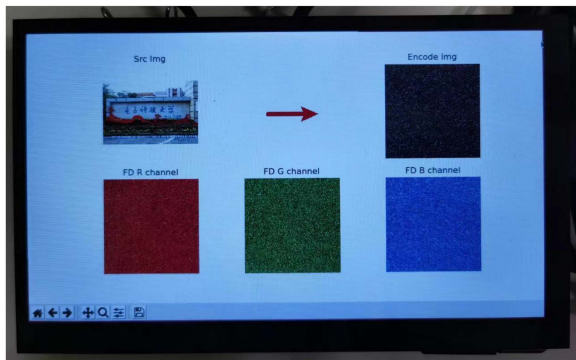
#### IV. EXPERIMENTAL VERIFICATION AND DISCUSSION

To verify our security analysis, we selected an image with a standard size of  $512 \times 512$  as a test image for the experiment. We conduct simulation verification on the proposed image cryptosystem which is executed on a PC with MATLAB r2018b. The running PC is installed with Windows 10 64-bit operating system with Intel (R) Core (TM) i7-8565 U CPU @ 1.80 GHz 1.99 GHz and 8 GB memory. In order to prove that the encryption scheme of this paper has a good encryption effect, we selected some pictures from ‘‘Ground Truth Database’’ and ‘‘USC-SIPI Image Database’’ as the test objects [38], [39].

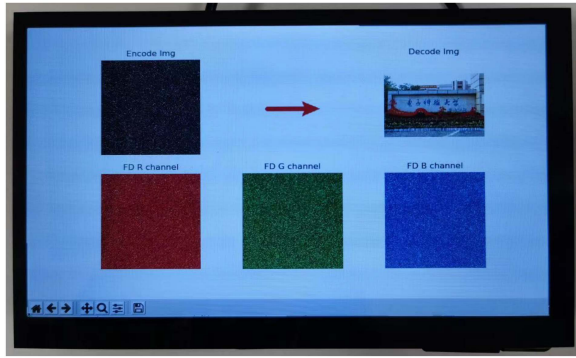
Based on these, in order to prove that the encryption scheme proposed in this paper is effective and applicable, we further verified it on the experiment platform for optical access network based on ARM-embedded system. This security correspondence platform of digital images in the optical access network is mainly composed of two ARM embedded system devices and an optical transceiver TP-LINKTL-FC311A-3 in one mode and fiber. The maximum transmission distance can reach about 10KM, and the maximum transmission rate is about 155Mbit/s. The development motherboard used in the ARM-embedded system is Raspberry Pie 4B, and the chip adopts Broadcom BCM2711 in a Cortex - A72 structure. And kernel version is 32-bit Linux 5.4, which is equipped with a displayer in 3.5 in liquid crystal display. Peer to Peer technology is applied to data communication. The



(a)



(b)



(c)

Fig. 4. Experiment result in Optical Access Network secure communication platform: (a) The overall physical diagram; (b) Image encryption; (c) Decryption image of (b).

sending end displays, encrypts and transmits the plain, while the receiving end stores, decrypts and displays the received cipher image. The experimental results are shown in Fig. 4. The experiment simulates the general correspondence environment with an optical network, so the scheme proposed in this paper will be widely applicable in the future.

#### A. Histogram Analysis

Histogram contains a large number of image information, we usually study the histogram information to obtain the image

tone distribution. Fig. 5(a)–(d) show the image and its histogram before and after encryption, respectively. We can see that the original image has a good statistical characteristics, and the image after encryption by this algorithm presents a noise-like distribution in the histogram statistical characteristics. Fig. 5(e)–(p) show the image and its histogram distribution before and after the original image is separated from RGB three channels. It can be found that the encryption effect of the original image under a single channel still presents a noise-like distribution, which proves that the image encrypted by this algorithm can well hide the image gray value information and improve the ability of the encrypted image to resist statistical characteristic analysis attacks.

#### B. Chaos Sequences

The quality of chaotic sequences is directly related to the effect of image encryption. A good chaotic sequence should have various characteristics such as sensitivity to initial values and uncertainty. As shown in Fig. 6(a)–(d), the chaotic sequence diagrams of four dimensions, respectively. It can be found that the hyperchaotic system used in this paper presents irregular characteristics and long-term unpredictability on  $x - t$  axis,  $y - t$  axis,  $z - t$  axis and  $w - t$  axis, which can be judged that it has a good performance.

#### C. Correlation Analysis of Adjacent Pixels

Strong correlation between adjacent pixels is a basic characteristic of natural images. The correlation of adjacent pixels reflects the degree of correlation of pixel values in adjacent positions of the image. A good image encryption algorithm should be able to reduce the correlation between neighboring pixels and try to achieve zero correlation. Generally, the horizontal, vertical, and diagonal pixels of the image are analyzed, as shown in Fig. 7. The ideal encryption algorithm should make the pixel correlation between images low enough to make it resistible for statistical attacks and ensure the security of encryption. The related calculation formula is as follows:

$$\begin{cases} Cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \\ E(x) = \frac{1}{N} \sum_{i=1}^N x_i \\ r_{xy} = \frac{Cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{cases} \quad (15)$$

where  $Cov(x, y)$  is the covariance between pixel values  $x$  and  $y$ ,  $N$  is the number of adjacent pixel pairs of the image to be analyzed,  $E(x)$  and  $D(x)$  are respectively the expected and mean square error of pixel value  $x$ .  $r_{xy}$  is the correlation coefficient of pixel value  $x$  and  $y$ .  $D(y)$  is the mean square error of the pixel value  $y$ .

Correlation is a statistical characteristic, which is the statistics of a specific situation of an image that is narrowed down to a chart. By comparing the correlation between plain and cipher to analyze whether the encrypted image is a chaotic, irregular

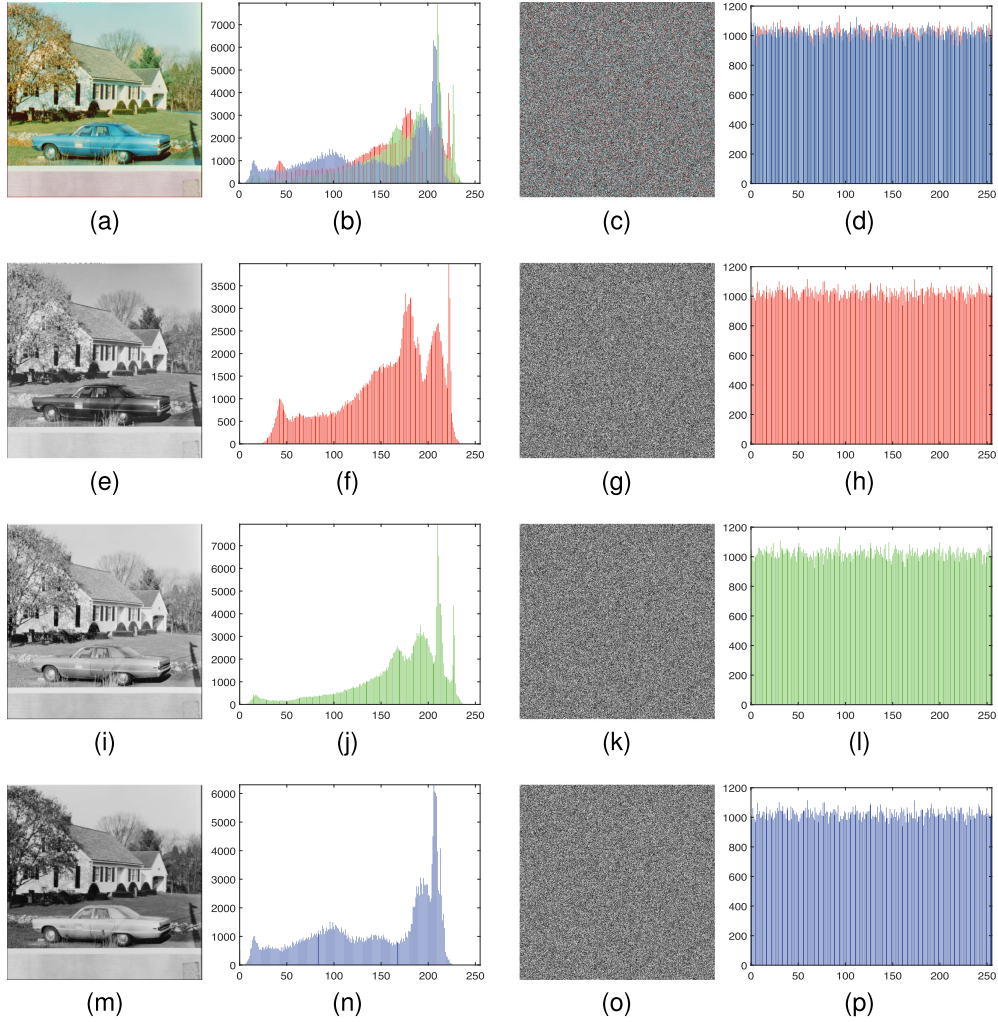


Fig. 5. The histogram of images before and after encryption: (a) Plain image of House; (b) Histogram of (a); (c) Cipher image of (a); (d) Histogram of (c); (e) R channel image of (a); (f) Histogram of (e); (g) Cipher image of (e); (h) Histogram of (g); (i) G channel image of (a); (j) Histogram of (i); (k) Cipher image of (i); (l) Histogram of (i); (m) B channel image of (a); (n) Histogram of (m); (o) Cipher image of (m); (p) Histogram of (o).

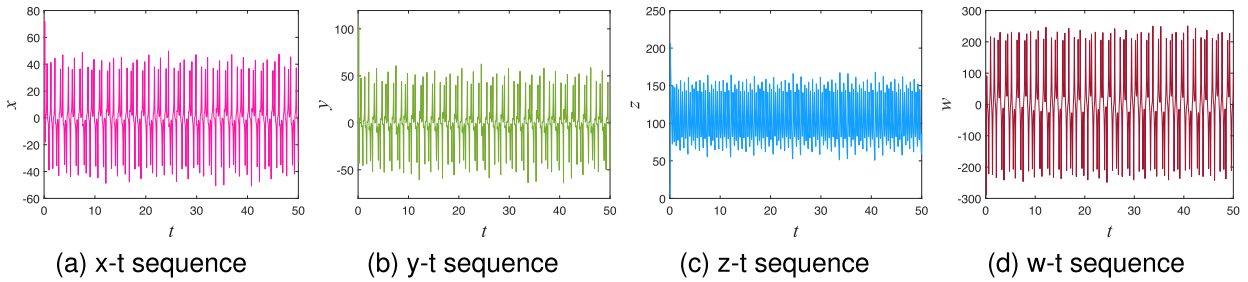


Fig. 6. Timing waveform diagram of memristive hyperchaos.

image. Here, we select five images for the correlation analysis of pixels before and after encryption. The experimental data is shown in Table I. It can be found that each group of images before encryption has a strong correlation in the horizontal, vertical and diagonal directions. After encryption, the calculation values of each group of images tend to be zero, indicating that there is no correlation, which proves that the image after encryption

by the algorithm designed in this paper has a good encryption effect.

*D. Encryption Quality Analysis*

The signal-to-noise ratio is a parameter commonly used in the engineering field, and it is also one of the important indicators used to detect image encryption quality. This paper introduces



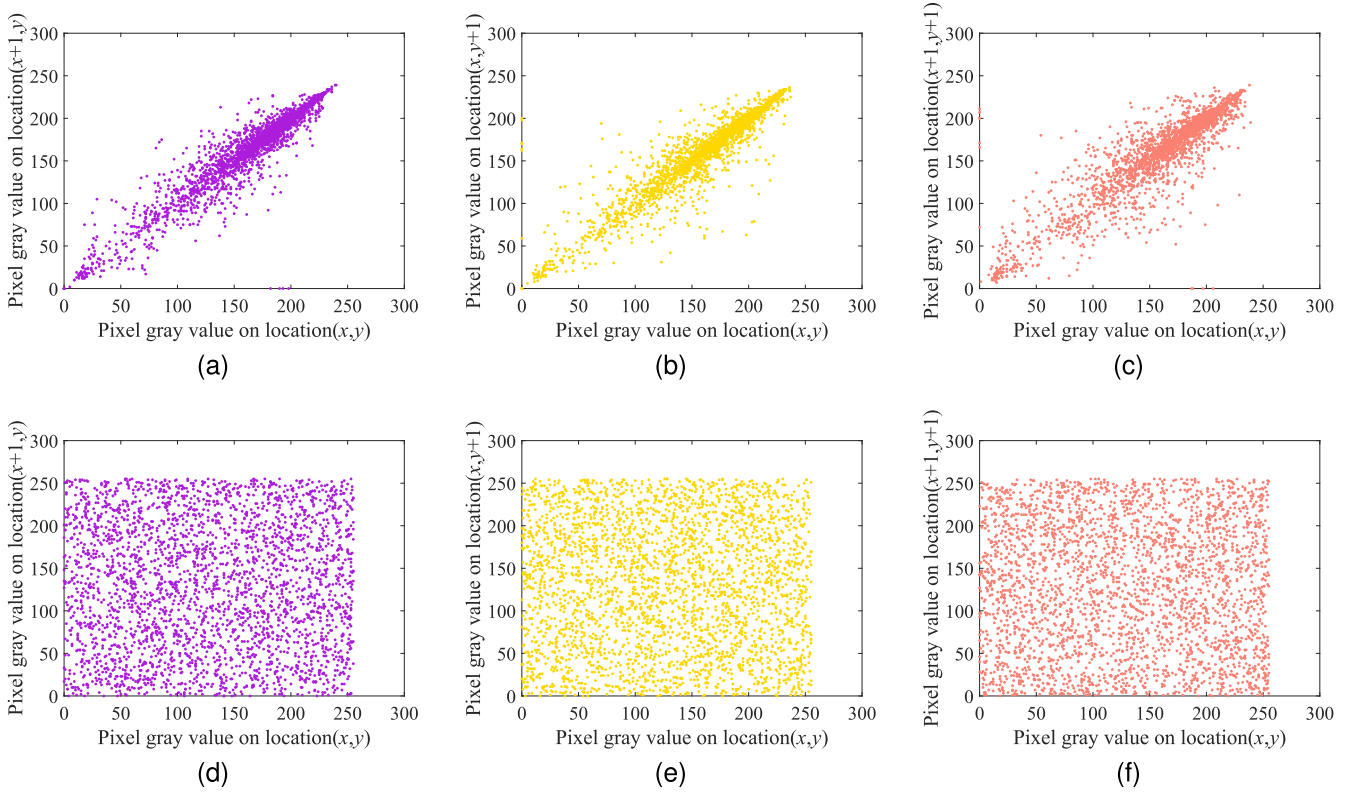


Fig. 7. The correlation characteristic: (a) Horizontal direction of plain; (b) Vertical direction of plain; (c) Diagonal direction of plain; (d) Horizontal direction of cipher; (e) Vertical direction of cipher; (f) Diagonal direction of cipher.

TABLE I  
CORRELATION COEFFICIENTS OF THE ORIGINAL AND ENCRYPTED IMAGES

Images	Original image			Encrypted image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
5.1.09.tiff	0.9394	0.9044	0.9135	0.0453	0.0309	0.0308
5.1.10.tiff	0.8561	0.9011	0.8205	0.0361	-0.0144	-0.0349
5.1.12.tiff	0.9734	0.9579	0.9309	0.0069	0.0305	0.0021
5.1.13.tiff	0.8765	0.8626	0.7901	-0.0075	0.0181	-0.0195
5.3.01.tiff	0.9805	0.9761	0.9740	0.0008	-0.0107	-0.0376

Peak Signal to Noise Ratio (PSNR) to analyze the image encryption quality. The relevant calculation formula is as follows:

$$\begin{cases} \text{PSNR} = 10 - \log_{10} \frac{255^2}{\text{MSE}} \\ \text{MSE} = \frac{1}{H \times W \times 3} \sum_{i=1}^H \sum_{j=1}^W \sum_{k=1}^3 (P(i, j, k) - C(i, j, k))^2 \end{cases} \quad (16)$$

The smaller the value of PSNR, the greater the difference between the encrypted image and the original image. It can be seen that there is distortion before and after encryption, which can better hide the original information. Table II shows the encryption quality of this scheme, we can see that the PSNR value of this algorithm is smaller than other algorithms.

### E. Differential Analysis

In image encryption algorithms, the measurement of plain sensitivity usually uses the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). Among of these parameters, NPCR mainly compare the values of the pixels at the corresponding positions in two images, and record the proportion of the number of different pixels in all pixels, UACI mainly measures the average difference of pixels at corresponding positions in the two while. The calculation formula is as follows:

$$\begin{cases} \text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\% \\ \text{UACI} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \left[ \frac{x(i, j) - \hat{x}(i, j)}{255} \right] \times 100\% \end{cases} \quad (17)$$

where  $M \times N$  is the size of the matrix  $x$  and  $\hat{x}$  are the cipher before and after the plain changes by one pixel.  $D(i, j)$  is define as:

$$D(i, j) = \begin{cases} 0, & x(i, j) = \hat{x}(i, j) \\ 1, & x(i, j) \neq \hat{x}(i, j) \end{cases} \quad (18)$$

For two random images, the theoretical value of NPCR is 99.6094 and the theoretical value of UACI is 33.4635. These two theoretical values are used as standards to evaluate whether the NPCR and UACI of the algorithm meet the expectations. It can be seen from Table III and Table IV that the NPCR and



TABLE II  
THE PSNR OF THE CIPHER IMAGES WITH DIFFERENT CRYPTOSYSTEMS

Images	This paper	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [45]	Ref. [43]
5.1.09.tiff	27.4401	27.4404	27.4256	27.4457	27.4983	27.5133
5.1.10.tiff	27.1044	27.0146	27.0155	27.0001	27.0895	27.0887
5.1.12.tiff	25.4032	25.7063	25.7078	25.6952	25.6984	25.6897
5.1.13.tiff	23.3489	24.7913	24.7972	24.7988	24.7865	24.8125
5.3.01.tiff	29.7645	29.1231	29.1189	29.1302	29.1557	29.1115

TABLE III  
NPCR VALUES UNDER DIFFERENT ALGORITHMS

Images	This paper	Ref. [43]	Ref. [44]	Ref. [41]	Ref. [40]	Ref. [42]	Ref. [46]
5.1.09.tiff	99.6113	99.6142	99.6033	99.5789	99.6017	99.6188	99.6019
5.1.10.tiff	99.6262	99.6163	99.6323	99.6017	99.6338	99.6289	99.6354
5.1.12.tiff	99.5956	99.6445	99.5789	99.6126	99.6013	99.6132	99.6853
5.1.13.tiff	99.6172	99.6185	99.6017	99.5911	99.5682	99.6254	99.6516
5.3.01.tiff	99.6123	99.6092	99.6126	99.4726	99.5733	99.5998	99.6541

TABLE IV  
UACI VALUES UNDER DIFFERENT ALGORITHMS

Images	This paper	Ref. [43]	Ref. [44]	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [45]	Ref. [46]
5.1.09.tiff	26.2421	26.2053	26.2205	35.3193	33.4512	36.4351	34.1524	33.8954
5.1.10.tiff	28.5411	28.4539	28.6369	36.7742	34.7713	37.3387	35.5412	34.5142
5.1.12.tiff	35.2363	35.3191	35.3353	37.8812	35.3200	37.3500	36.1388	33.5698
5.1.13.tiff	48.8296	48.8632	48.8713	33.4423	36.6237	34.4791	35.6894	35.1895
5.3.01.tiff	32.5115	32.4841	32.4824	30.2433	35.1334	39.1443	36.4215	34.9581

TABLE V  
THE ENTROPY OF THE CIPHER IMAGES WITH DIFFERENT CRYPTOSYSTEMS

Image	This paper	Original image	Ref. [43]	Ref. [44]	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [45]	Ref. [46]
5.1.09.tif	7.9900	6.7093	7.9971	7.9974	7.9974	7.9969	7.9971	7.9983	7.9972
5.1.10.tif	7.9969	7.3118	7.9973	7.9971	7.9967	7.9975	7.9973	7.9972	7.9973
5.1.12.tif	7.9972	6.7057	7.9972	7.9973	7.9975	7.9971	7.9973	7.9984	7.9976
5.1.13.tif	7.9974	1.5483	7.9973	7.9973	7.9975	7.9972	7.9976	7.9993	7.9979
5.3.01.tif	7.9998	7.5237	7.9998	7.9998	7.9998	7.9998	7.9998	7.9992	7.9969

UACI values of the algorithm in this paper are close to the theoretical values and equivalent to those in other literature. The experimental results show that the cipher image encrypted by this algorithm can effectively resist the attacks of special plain.

#### F. Information Entropy

Information entropy is used as a measure of image uncertainty. For an encryption system, the greater the entropy of the cipher image is, the better the encryption performance is. Theoretically, when the pixel value distribution of cipher is more chaotic, the pixel value distribution is more uniform, and the calculated value is closer to the theoretical value of 8. The formula of information entropy is with 8-bit grayscale. The formula for calculating the information entropy of an image with a gray value of 256 is as follows:

$$H = - \sum_{i=1}^L p(i) \log_2 p(i) \quad (19)$$

where  $p(i)$  is the probability that the gray value  $i$  appears.  $L$  is the number of gray levels of the image.

The experimental results are shown in Table V. After it is encrypted by the algorithm in this paper, the algorithm information entropy proposed in this paper is close to the theoretical value 8, indicating that the cipher pixel value is evenly distributed and the encryption quality is great.

#### G. Key Space

Due to the high sensitivity of memristor chaos to the initial value, the initial value can be selected as part of the key. The diffraction distance and wavelength involved in the DRPE process can also be used as a key to expand the key space. Key space is divided into static key and dynamic key. The static key  $\text{KEY} = \{x(0), y(0), z(0), w(0), \lambda_R, \lambda_G, \lambda_B, D_q (q = 1, 2)\}$ . Where  $\{x(0), y(0), z(0), w(0)\}$  is the initial condition of

memristor chaotic system. Dynamic key determined by SHA-256. Assuming that the initial parameters of chaotic system are double data with accuracy of  $10^{-16}$ , the key space of this part is  $10^{64}$ . If other static keys are used as key parameters, the key space of this part is  $(10^4)^3$ . And the key space of dynamic key is  $10^{34}$ . Based on the above, the key space of the algorithm is  $10^{110} \approx 2^{365}$ , that is, 365 b key length. Therefore, in current computing capacity conditions, enough to resist violent attacks.

## V. CONCLUSION

In this paper, a digital encryption scheme for optical color images based on a mixture of frequency and spatial domains is proposed. A double random transform method in optical theory is utilized, a memristive hyperchaotic system is introduced to enhance the security of the encryption scheme as well. The overall conclusions regarding this encryption scheme are mainly as follows.

1) The key space is effectively expanded by using the double random phase transformation method in optical theory, while the method based on frequency domain processing and encryption can further improve the security.

2) The significant nonlinear characteristics possessed by the memristor hyperchaotic system effectively enhance the random characteristics of the encryption sequence and ensure the encryption quality.

3) Based on the double random transform and the memristor hyperchaotic system, as well as the introduction of the plain correlation mechanism of cryptanalysis, the optical digital image encryption scheme has the characteristics of large key space, excellent comprehensive performance, and the ability to resist common attacks.

4) The verification of the results based on the experimental platform of embedded optical communication network corroborates the hardware feasibility and easy implementation of the proposed algorithm.

Therefore, the proposed scheme in this paper is a preferred optical digital image secure communication technology scheme with good application prospects.

## ACKNOWLEDGMENT

There is not any conflict of interest to declare by the authors.

## REFERENCES

- [1] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Opt. Lasers Eng.*, vol. 128, 2020, Art. no. 105995.
- [2] N. Zhou, Y. Wang, L. Gong, H. He, and J. Wu, "Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform," *Opt. Commun.*, vol. 284, pp. 2789–2796, 2011.
- [3] K. Zhai et al., "Data fragmentation multipath secure coherent optical communication system based on electrical signal processing," *IEEE Photon. J.*, vol. 14, no. 4, pp. 1–6, Aug. 2022.
- [4] Y. Peng, S. He, and K. Sun, "Chaos in the discrete memristor-based system with fractional-order difference," *Results Phys.*, vol. 24, 2021, Art. no. 104106.
- [5] H. Wen and S. Yu, "Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 134, no. 7, pp. 1–16, 2019.
- [6] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, 2020, Art. no. 107684.
- [7] Q. Chen et al., "Secure spread spectrum communication using super-orthogonal optical chaos signals," *IEEE Photon. J.*, vol. 14, no. 4, pp. 1–6, Aug. 2022.
- [8] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, 2019, Art. no. 102361.
- [9] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, 2020, Art. no. 102566.
- [10] H. Wen, S. Yu, and J. Lv, "Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 21, no. 3, 2019, Art. no. 246.
- [11] M. Chen et al., "Multistability induced by two symmetric stable node-foci in modified canonical Chua's circuit," *Nonlinear Dyn.*, vol. 82, no. 2, pp. 789–802, 2017.
- [12] Y. Bai et al., "Highly secure and reliable 7-core fiber optical OFDM access system based on chaos encryption inside polar code," *IEEE Photon. J.*, vol. 14, no. 1, pp. 1–6, Feb. 2022.
- [13] H. Wen, C. Zhang, L. Huang, J. Ke, and D. Xiong, "Security analysis of a color image encryption algorithm using a fractional-order chaos," *Entropy*, vol. 23, 2021, Art. no. 258.
- [14] X. Wang et al., "Security enhancement of image encryption method based on fresnel diffraction with chaotic phase," *Opt. Commun.*, vol. 506, 2022, Art. no. 127544.
- [15] H. Wen et al., "A quantum chaotic image cryptosystem and its application in IoT secure communication," *IEEE Access*, vol. 9, pp. 20481–20492, 2021.
- [16] Y. Zhang et al., "An efficient multi-level encryption scheme for stereoscopic medical images based on coupled chaotic system and Otsu threshold segmentation," *Comput. Biol. Med.*, vol. 146, 2022, Art. no. 105542.
- [17] M. Chen et al., "Dynamics of self-excited attractors and hidden attractors in generalized memristor-based Chua's circuit," *Nonlinear Dyn.*, vol. 81, no. 1, pp. 215–226, 2015.
- [18] H. Wen et al., "High-quality restoration image encryption using DCT frequency-domain compression coding and chaos," *Sci. Rep.*, vol. 12, no. 1, pp. 1–16, 2022.
- [19] D. Yan, L. Wang, S. Duan, J. Chen, and J. Chen, "Chaotic attractors generated by a memristor-based chaotic system and Julia fractal," *Chaos Solitons*, vol. 146, 2021, Art. no. 110773.
- [20] H. Wen, Z. Liu, and H. Lai, "Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key," *Mathematics*, vol. 10, no. 17, 2022, Art. no. 3180.
- [21] C. Li, K. Tan, B. Feng, and J. Lü, "The graph structure of the generalized discrete Arnold cat map," *IEEE Trans. Comput.*, vol. 71, no. 2, pp. 364–377, Feb. 2022.
- [22] H. Wen et al., "A security-enhanced image communication scheme using cellular neural network," *Entropy*, vol. 23, no. 8, 2021, Art. no. 1000.
- [23] H. Wen et al., "Design and embedded implementation of secure image encryption scheme using DWT and 2D-LASM," *Entropy*, vol. 24, no. 10, 2022, Art. no. 1332.
- [24] B. Bao et al., "Third-order RLCM-four-elements-based chaotic circuit and its coexisting bubbles," *AEU-International J. Electron. Commun.*, vol. 94, pp. 26–35, 2018.
- [25] S. Liansheng, D. Cong, Z. Xiao, T. Ailing, and A. Anand, "Double-image encryption based on interference and logistic map under the framework of double random phase encoding," *Opt. Lasers Eng.*, vol. 122, pp. 113–122, 2019.
- [26] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography," *Laser Technol.*, vol. 127, 2020, Art. no. 106171.
- [27] X. Jiang et al., "Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding," *Opt. Commun.*, vol. 484, 2021, Art. no. 126683.
- [28] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons Fractals*, vol. 152, 2021, Art. no. 111318.
- [29] L. Wang, T. Dong, and M.-F. Ge, "Finite-time synchronization of memristor chaotic systems and its application in image encryption," *Appl. Math. Comput.*, vol. 347, pp. 293–305, 2019.
- [30] M. Yildirim, "DNA encoding for RGB image encryption with memristor based neuron model and chaos phenomenon," *Microelectron. J.*, vol. 104, 2020, Art. no. 104878.

- [31] Z. Yang, D. Liang, D. Ding, and Y. Hu, "Dynamic behavior of fractional-order memristive time-delay system and image encryption application," *Modern Phys. Lett. B*, vol. 35, 2021, Art. no. 2150271.
- [32] Q. Lai, Z. Wan, L. K. Kengne, P. D. K. Kuate, and C. Chen, "Two-memristor-based chaotic system with infinite coexisting attractors," *IEEE Trans. Circuits Syst. II-Express Briefs*, vol. 68, no. 6, pp. 2197–2201, Jun. 2021.
- [33] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator," *Optik*, vol. 217, 2020, Art. no. 164653.
- [34] T. Logeswaran, S. Kalaivani, S. Karunakaran, L. V. Anand, and K. V. Kumar, "The generalized non-linear fresnel transform and its application to image encryption," *Mater. Today: Proc.*, 2020.
- [35] C. Wu, J. Chang, C. Quan, X. Zhang, and Y. Zhang, "The optical image compression and encryption method based on fresnel diffraction and discrete wavelet transform," *Results Opt.*, vol. 1, 2020, Art. no. 100021.
- [36] B. Wang, F. Zou, and J. Cheng, "A memristor-based chaotic system and its application in image encryption," *Optik*, vol. 154, pp. 538–544, 2018.
- [37] H. Hu, Y. Cao, J. Xu, C. Ma, and H. Yan, "An image compression and encryption algorithm based on the fractional-order simplest chaotic circuit," *IEEE Access*, vol. 9, pp. 22141–22155, 2021.
- [38] "The USC-SIPI image database." [Online]. Available: <http://sipi.usc.edu/database>
- [39] "The ground truth database." [Online]. Available: <http://www.cs.washington.edu/research/imagedatabase>
- [40] M. Essaid, I. Akharraz, A. Saaidi, and E. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–87, 2019.
- [41] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, pp. 6954–68, 2015.
- [42] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, pp. 331–340, 2018.
- [43] Q. Yin and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *Int. J. Bifurc. Chaos*, vol. 28, pp. 1850047:1–1850047:13, 2018.
- [44] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, 2016.
- [45] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, 2019, doi: [10.1007/s11042-018-6739-1](https://doi.org/10.1007/s11042-018-6739-1).
- [46] X. Huang, T. Sun, Y. Li., and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic system," *Entropy*, vol. 17, no. 1, pp. 28–38, 2014, doi: [10.3390/e17010028](https://doi.org/10.3390/e17010028).