

Color-image encryption scheme based on channel fusion and spherical diffraction

Jun Wang(王君), Yuan-Xi Zhang(张沅熙), Fan Wang(王凡), Ren-Jie Ni(倪仁杰), and Yu-Heng Hu(胡玉衡)
Citation: Chin. Phys. B, 2022, 31 (**3**): 034205. DOI: 10.1088/1674-1056/ac1b87
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Possibility to break through limitation of measurement range in dual-wavelength digital holography

Tuo Li(李拓), Wen-Xiu Lei(雷文秀), Xin-Kai Sun(孙鑫凯), Jun Dong(董军), Ye Tao(陶冶), and Yi-Shi Shi(史祎诗)
Chin. Phys. B, 2021, 30 (**9**): 094201. DOI: 10.1088/1674-1056/abf348

Impact of the spatial coherence on self-interference digital holography

Xingbing Chao(潮兴兵), Yuan Gao(高源), Jianping Ding(丁剑平), and Hui-Tian Wang(王慧田)
Chin. Phys. B, 2021, 30 (**8**): 084212. DOI: 10.1088/1674-1056/abd766

Single pixel imaging based on semi-continuous wavelet transform

Chao Gao(高超), Xiaoqian Wang(王晓茜), Shuang Wang(王爽), Lidan Gou(苟立丹), Yuling Feng(冯玉玲), Guangyong Jin(金光勇), and Zhihai Yao(姚治海)
Chin. Phys. B, 2021, 30 (**7**): 074201. DOI: 10.1088/1674-1056/abe373

High speed ghost imaging based on a heuristic algorithm and deep learning

Yi-Yi Huang(黄祎祎), Chen Ou-Yang(欧阳琛), Ke Fang(方可), Yu-Feng Dong(董玉峰), Jie Zhang(张杰), Li-Ming Chen(陈黎明), and Ling-An Wu(吴令安)
Chin. Phys. B, 2021, 30 (**6**): 064202. DOI: 10.1088/1674-1056/abea8c

Three-dimensional coherent diffraction imaging of Mie-scatteringspheres by laser single-orientation measurement

Zhang Jian, Fan Jia-Dong, Zhang Jian-Hua, Sun Zhi-Bin, Huang Qing-Jie, Jiang Huai-Dong
Chin. Phys. B, 2015, 24 (**9**): 094201. DOI: 10.1088/1674-1056/24/9/094201

Color-image encryption scheme based on channel fusion and spherical diffraction

Jun Wang(王君)[1,†,‡], Yuan-Xi Zhang(张沅熙)[1,†], Fan Wang(王凡)[1], Ren-Jie Ni(倪仁杰)[1], and Yu-Heng Hu(胡玉衡)[2]

[1] *Sichuan University, School of Electronics and Information Engineering, Chengdu* 610065, *China*
[2] *Department of Electrical and Computer Engineering, University of Wisconsin–Madison, Madison, WI* 53706, *USA*

(Received 16 May 2021; revised manuscript received 1 August 2021; accepted manuscript online 7 August 2021)

A secure encryption scheme for color images based on channel fusion and spherical diffraction is proposed in this paper. In the proposed encryption scheme, a channel fusion technology based on the discrete wavelet transformation is used to transform color images into single-channel grayscale images, firstly. In the process of transformation, the hyperchaotic system is used to permutate and diffuse the information of red–green–blue (RGB) channels to reduce the correlation of channels. Then the fused image is encrypted by spherical diffraction transform. Finally, the complex-valued diffraction result is decomposed into two real parts by the improved equal module decomposition, which are the ciphertext and the private key. Compared with the traditional color image encryption schemes that encrypt RGB channels separately, the proposed scheme is highly secure and robust.

Keywords: channel fusion, hyper-chaotic system, asymmetric encryption, spherical diffraction

PACS: 42.30.–d, 42.30.Va, 42.40.My, 42.40.Kw **DOI:** 10.1088/1674-1056/ac1b87

1. Introduction

In the past few decades, information security has been widely discussed in the military field and civilian field. As one of the most common information carriers, encryption research on the image has always been a concern of scientific researchers. Unlike traditional digital encryption, optical encryption has attracted more and more attention due to its high-speed transmission, parallel processing, and large capacity. The earliest optical encryption system can be traced back to the double random phase encryption scheme proposed by Refregier and Javadi in 1995,[1] which can encrypt the image into stationary white noise in the 4f optical system. However, this symmetry system was later proved to be vulnerable to known-plaintext[2] and chosen-plaintext attacks.[3] To overcome the shortcoming, the fractional Fourier transform,[4,5] fractional Mellin transform,[6,7] phase-shifting interferometry,[8,9] Fresnel transform,[10] ghost image,[11] and cylindrical diffraction[12,13] have been proposed. Moreover, as an important branch of image encryption, a lot of colorful image encryption schemes[14–20] have been proposed based on previous researches.

Nevertheless, most of color image optical encryption schemes at present which convert color plaintext into color ciphertext suffer the problem of information leakage.[21–23] The red–green–blue (RGB) channels of the color image are encrypted independently first in these encryption schemes. Then, encrypted channels are fused into a color image again. In this case, the attacker only needs to know part of the ciphertext and private key to obtain most of the partial information of the plaintext image. There are two feasible schemes to solve this problem. One is to reduce the strong correlation between separate RGB channels and the color image,[24–26] such as changing the pixel values or position of one channel through another channel.[24] However, like the parallel processing scheme, this scheme usually requires optical modulations more than once to obtain the ciphertext. Moreover, since the existing hardware usually discretizes the image, this scheme will lead to more errors in optical encryption and reduce the quality of the decrypted image. Therefore, researchers proposed another scheme[27–29] whose idea is similar to multi-image encryption.[30] Dissimilarly, the second scheme tries to transform a color image into a grayscale image. A common method to transform a color image into a single channel image is to perform the convolution operation on all three channels together.[28,29] Compared with the first scheme, the second scheme is more suitable for optical encryption. However, the second scheme usually requires more private keys to separate the merged images during decryption. And the second scheme does not solve the problem of information leakage well since the attackers can still obtain the complete information about a particular channel if they know the full ciphertext and part of the private keys. Therefore, considering the problems of existing schemes, it is necessary to develop a more secure and efficient color image encryption scheme. The proposed encryption scheme should integrate the advantages of first and second schemes and avoid their disadvantages.

In this paper, a color-image encryption scheme based on

[†]These authors contributed equally to this work.
[‡]Corresponding author. E-mail: jwang@scu.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

channel fusion and spherical diffraction is proposed. In this scheme, a color image is first transformed into a grayscale image by channel fusion technology based on a hyperchaotic system and discrete wavelet transform (DWT). Here, the hyperchaotic system is to reduce the correlation between the RGB channels and colorful original image, and the DWT is to transform the color image into a grayscale image. Then, the grayscale image is modulated by a mask generated by the hyperchaotic system. The modulation result is input into an asymmetric spherical diffraction system which is more secure than the symmetric system. Finally, the improved equal module decomposition (IEMD) is used to hide the complex-valued result of diffraction into two real-values masks which are more valuable for the actual data transmission. The proposed scheme can solve the problem of information leakage well in optical encryption. The simulation results and safety analysis prove the effectiveness of our scheme.

2. Principle of encryption and decryption

Here in this section, some basic principles related to our proposed scheme are introduced.

2.1. Encryption in spherical diffraction domain

Owing to the asymmetric property of spherical diffraction, the shortcomings of symmetry of the plane diffraction encryption schemes can be overcome. Therefore, it can resist ciphertext attack, plaintext attack, and phase-retrieval attack. Meanwhile, the diffraction parameter can also be used as a private key to improve the security of the encryption scheme.

According to spherical holographic theory,[31–35] the object surface and observation surface of spherical diffraction are the surfaces of concentric spheres with radii of r and R. Hence, there are two propagation models which are inside-to-outside propagation (IOP) model and outside-to-inside propagation (OIP) model as shown in Figs. 1(a) and 1(b).

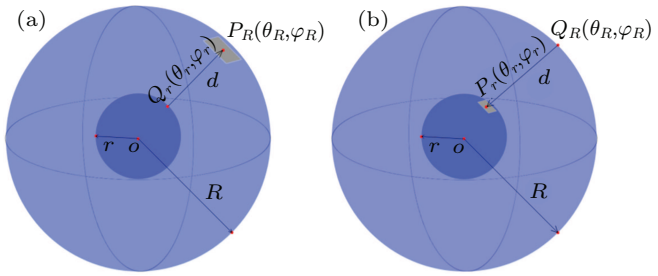


Fig. 1. Spherical diffraction of (a) inside-to-outside propagation model and (b) outside-to-inside propagation model.

For the IOP model, $Q_r(\theta_r, \varphi_r)$ and $P_R(\theta_R, \varphi_R)$ represent the object point and observation point in the spherical coordinate, respectively. For the OIP model, $Q_R(\theta_R, \varphi_R)$ and $P_r(\theta_r, \varphi_r)$ denote the object point and observation point in the spherical coordinate, respectively. The θ_r and θ_R are in a range from $-\pi$ to π, and φ_R and φ_r are in a range from $-\pi/2$ to $\pi/2$. If we denote the diffraction distributions on inner surfaces and outer surfaces as $u_r(\theta_r, \varphi_r)$ and $u_R(\theta_R, \varphi_R)$, the diffraction integral equations based on the Rayleigh–Sommerfeld integral equation of the two models can be written as

$$\begin{cases} u_R(\theta_R,\phi_R) = C\iint_s u_r(\theta_r,\phi_r)\cos\alpha\dfrac{\exp(\mathrm{i}kd_{O_rP_R})}{d_{O_rP_R}}\,\mathrm{d}\theta_r\,\mathrm{d}\phi_r = \mathrm{Sp}D_R(u_R(\theta_R,\phi_R)),\ldots,\mathrm{IOP}, \\ u_r(\theta_r,\phi_r) = C\iint_s u_R(\theta_R,\phi_R)\cos\alpha\dfrac{\exp(\mathrm{i}kd_{O_RP_r})}{d_{O_RP_r}}\,\mathrm{d}\theta_R\,\mathrm{d}\phi_R = \mathrm{Sp}D_r(u_r(\theta_r,\phi_r)),\ldots,\mathrm{OIP}, \end{cases} \tag{1}$$

$$\cos\alpha = \frac{r - R\cos(\theta_R-\theta_r)\cos(\phi_R-\phi_r)}{d_{O_RP_r}}, \tag{2}$$

$$\begin{aligned} d &= d_{O_RP_r} = d_{O_rP_R} \\ &= \sqrt{r^2+R^2-2Rr\cos(\theta_R-\theta_r)\cos(\phi_R-\phi_r)}, \end{aligned} \tag{3}$$

where C is a constant and k denotes the wavenumber of the incident light, d represents the distance between the observation point P and the object point Q, and s refers to the object surface.

2.2. Improved equal module decomposition

In conventional equal module decomposition (EMD),[36] a complex amplitude U can be represented by two equal module masks P_1 and P_2. The new distribution of complex amplitude can be rewritten as

$$U = A\cdot\exp(\mathrm{i}\beta) = P_1 + P_2, \tag{4}$$

where A is the amplitude of U, and β is the phase of U. If a random phase mask (RPM) (in the following text, RPM is denoted by R) distributed uniformly in the interval $[0, 2\pi]$, R_2 is expressed as

$$R_2 = 2\pi\cdot\mathrm{rand}(M\cdot N), \tag{5}$$

where rand $(M\times N)$ means a random number matrix of M rows and N columns, and the value range of element is [0, 1]. Here, P_1 will be gained by A, and P_2 by β and R_2.

However, P_1 and P_2 are expressed as two complex-valued masks and they are not convenient to transmit. Therefore, an IEMD scheme is used[37] to solve the problem. Here in the IEMD the output of P_1 and P_2 are replaced by C and PK which are both real valued. Under the IEMD, the decomposition equation of complex amplitude U is as follows:

$$U = C\cdot[\exp(\mathrm{i}R_2) + \exp(\mathrm{i}PK)],$$

$$C = 0.5A \cdot [\cos(\beta - R_2)]^{-1}, \quad PK = 2\beta - R_2 = \arg(P_2), \tag{6}$$

where C is ciphertext, and PK is the private key. In our scheme, R_2 is generated from the hyperchaotic system controlled by private key. Therefore, it is not necessary to transmit R_2. Hence, U is hidden into two real-valued masks [C, PK] successfully.

3. Proposed scheme

3.1. Encryption process

Step 1 First, we need to generate several sequences or masks. In this step, Chen *et al.*'s four-dimensional (4D) hyperchaotic system[38] is used to generate the sequences and masks for subsequent encryption. The hyperchaotic system is as follows:

$$\begin{cases} \dot{x} = a(y - x - w) + byz, \\ \dot{y} = c(4x + y) - xz, \\ \dot{z} = dx - ez + xy, \\ \dot{w} = rx + f(3yz + y^2). \end{cases} \tag{7}$$

Here, the parameters of the system are set to be $a = 80$, $b = 45$, $c = 22$, $d = 5$, $e = 21$, $f = 8$, and $r = 78$, and they are broadcasted as public keys.

The initial conditions used as private keys are determined by different plaintexts. The initial value of x, y, z, and w are determined by variance and mean of the color plaintext, respectively. The generated four sequences are used as key1, key2, R_1, and R_2 for subsequent encryption. The key1 and key2 are used in the channel fusion process. R_1 is a random phase mask which forms a complex amplitude with the fused image in spherical diffraction. R_2 is the random mask in IEMD.

In the actual transmission, the only private keys we need to transmit are the initial values of the hyperchaotic system.

Step 2 In this step, the color plaintext is processed by channel fusion based on DWT and the keys generated by the hyperchaotic system. The channel fusion will change the distribution and values of the plaintext pixels through key1 and key2 and finally resulting in a grayscale image.

Firstly, the RGB channels of colorful image are separated, and they are processed by as follows:

$$S = FL[I_{\mathrm{R}}(x,y)] \circ FL[I_{\mathrm{G}}(x,y)] \circ FL[I_{\mathrm{B}}(x,y)], \tag{8}$$

where I_{R}, I_{G}, and I_{B} represent the corresponding RGB channels of the original image, $FL[\cdot]$ denotes the progress of transforming a two-dimensional (2D) image matrix into a one-dimensional (1D) pixel sequence, $\circ$ refers to the matrix splicing operation, and S is the spliced sequence.

Secondly, the sequence S is diffused and permuted by key1 and key2 which are obtained in step 1, and expressed as

$$S_1 = \mathrm{Per}(S \oplus \mathrm{key1}, \mathrm{key2}), \tag{9}$$

where Per(a, b) denotes using b to permute a, and $\oplus$ is the operation of XOR.

After that, S_1 is reshaped from a sequence to three matrices. Each of the three matrices contains part of the information about the three RGB channels, which means that the strong correlation between the RGB channels is weakened. In this way, the corresponding color plaintext cannot be recovered well while missing any matrix. After reshaping the fusion sequence back to three gray-scale images, they will perform inverse DWT[39] together with the interfering image to finally get a grayscale image

$$f(x,y) = \mathrm{IDWT}[\mathrm{Re}(S_1) \circ I_t], \tag{10}$$

where IDWT[$\cdot$] is the inverse discrete wavelet transform, Re($\cdot$) is the operator of reshaping. I_t is the interfering image, and $f(x, y)$ is the grayscale image after fusion. The process of channel fusion is shown in Fig. 2, and the intermediate and the final results of channel fusion are shown in Fig. 3. The size of final fused image is four times that of the original image.

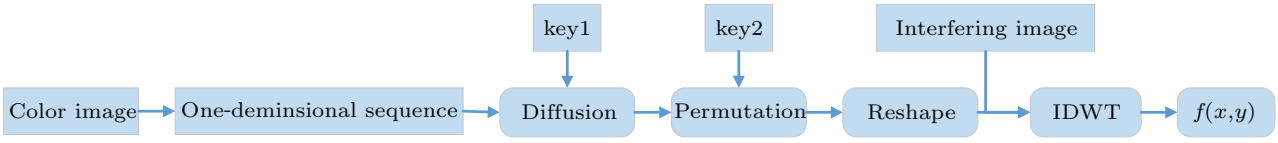


Fig. 2. Channel fusion process.

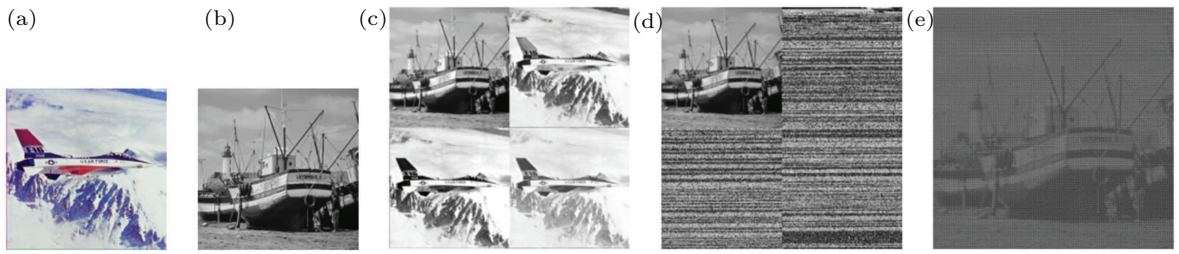


Fig. 3. Channel fusion results, showing (a) original image, (b) interfering image, IDWT without (c) and with (d) permutation and diffusion, and (e) fusion image.

Step 3 After the channels are fused, the phase mask $\mathrm{RPM}(x,y)=\exp(\mathrm{j}R_1)$ generated by the hyperchaotic system and $f(x,y)$ together form the complex amplitude distribution to be diffracted.

According to the theory of Eq. (1), the result of diffraction in IOP mode is expressed as a complex distribution

$$U(x,y)=\mathrm{Sp}D_{\mathrm{R}}\left[(f(x,y)\cdot\mathrm{RPM}(x,y)\right]. \tag{11}$$

Step 4 Owing to the fact that the result of spherical diffraction is a complex distribution, it is necessary to make it more convenient to the actual data transmission. Compared with the traditional EMD, the IEMD can hide complex amplitude into two real-value masks while improving security. According to Eq. (6), the result of spherical diffraction can be rewritten as

$$\begin{aligned} &U=C\cdot[\exp(\mathrm{i}R_2)+\exp(\mathrm{i}PK)],\\ &C=0.5A\cdot[\cos(\beta-R_2)]^{-1},\quad PK=2\beta-R_2. \end{aligned} \tag{12}$$

The whole encryption progress is shown in Fig. 4.

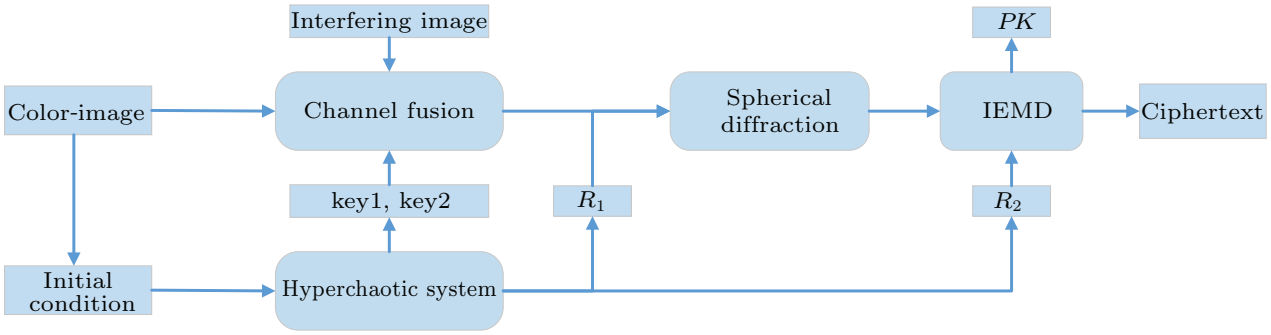


Fig. 4. Encryption process.

3.2. Decryption progress

Step 1 Firstly, according to Eq. (12), we can obtain the complex amplitude U. The U is modulated by RPM^* after spherical diffraction. The fused image $f(x,y)$ can be obtained from

$$f(x,y)=\mathrm{ISp}D_{\mathrm{R}}\left[U(x,y)\right]\cdot\mathrm{RPM}^*(x,y), \tag{13}$$

where $\mathrm{ISp}D_{\mathrm{R}}[\cdot]$ is the inverse process of the spherical diffraction, and $\mathrm{RPM}^*(x,y)$ is the conjugate of $\mathrm{RPM}(x,y)$.

Step 2 Secondly, $f(x,y)$ is processed by the DWT. Three high-frequency sub-bands LH, HL, HH will be flattened into 1D at sequence and then be spliced together as follows:

$$(\mathrm{LL},\mathrm{LH},\mathrm{HL},\mathrm{HH})=\mathrm{DWT}\left[f(x,y)\right], \tag{14}$$

$$S_2=FL[\mathrm{LH}]\circ FL[\mathrm{HL}]\circ FL[\mathrm{HH}], \tag{15}$$

where LH corresponds to the red channel, HL denotes the green channel, and HH refers to the blue channel. The correspondence between subbands and channels will be determined by the encryption process.

Step 3 Then, S_2 is inversely permuted and inversely diffused to restore S. According to Eqs. (8) and (15), the one-dimensional sequence S with complete RGB three-channel information is then reshaped into three two-dimensional matrices corresponding to RGB. Finally, the RGB channels are merged and the colorful plaintext is restored as shown below:

$$S=(\mathrm{Per}(S_2,\mathrm{key2})^{-1})\oplus\mathrm{key1}, \tag{16}$$

$$\begin{aligned} I(x,y)=\mathrm{merge}\{&\mathrm{Re}\left[I_{\mathrm{R}}(x,y)\right],\\ &\mathrm{Re}\left[I_{\mathrm{G}}(x,y)\right],\quad \mathrm{Re}\left[I_{\mathrm{B}}(x,y)\right]\}, \end{aligned} \tag{17}$$

where $\mathrm{Per}(a,b)^{-1}$ is the inverse process of $\mathrm{Per}(a,b)$, and $\mathrm{merge}\{\cdot\}$ means RGB channels' mergence.

4. Simulation results

4.1. Encryption and decryption result

The simulation is performed with Python 3.8.2 to analyze the performance of the proposed scheme on a 64-bit computer. In the simulation, the radius of the outer sphere R, the radius of the inner sphere r, and the wavelength λ are set to be 500 mm, 50 mm, and 0.25 mm. According to the spherical holographic sampling theory,[34,35] the above parameters require that the number of sampling points in the horizontal and vertical directions of the image should be at least 2513 pixels and 1257 pixels. However, if we select only 1/5 of the sphere surface, the minimum number of sampling points required will be 503 pixels and 252 pixels in the corresponding direction. To achieve this goal, the size of the original image is select as $256\times256\times3$, and the corresponding size of the ciphertext is 512×512. Figure 5 shows the result of encryption and decryption with plaintext 'baboon'. The parameters related to spherical diffraction and the hyperchaotic system are listed in Table 1.

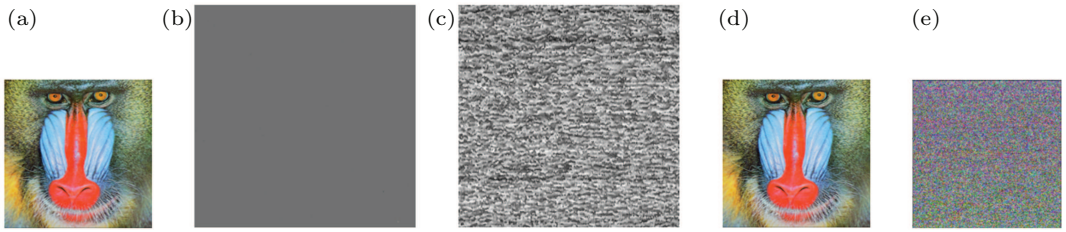


Fig. 5. Encryption and decryption results, showing (a) original image, (b) cipher-text, (c) private key *PK*, (d) decryption result with correct *PK*, and (e) decryption result with the wrong *PK*.

Table 1. Parameters of spherical diffraction and Chen's 4D hyperchaotic system.

R (mm)	r (mm)	λ (mm)	x	y	z	w
500	50	0.25	0.1136	0.5286	0.4371	0.5872

To better evaluate the quality of encryption and decryption, we introduce PSNR and SSIM as reference indexes. The corresponding equation is as follows:

$$\mathrm{PSNR}(I_\mathrm{o}, I_\mathrm{d}) = 10\log_{10}\left[\frac{M\cdot N\cdot 255^2}{\sum\limits_{\forall x,y}\left[I_\mathrm{o}(x,y)-I_\mathrm{d}(x,y)\right]^2}\right], \quad (18)$$

where M and N represent the sizes of the evaluated images, I_o and I_d denote the original image and the decrypted image, respectively.

$$\mathrm{SSIM}(I_\mathrm{o}, I_\mathrm{d}) = \frac{(2\mu_{I_\mathrm{o}}\mu_{I_\mathrm{d}}+c_1)(2\sigma_{I_\mathrm{o}I_\mathrm{d}}c_2)}{(\mu_{I_\mathrm{o}}^2+\mu_{I_\mathrm{d}}^2+c_1)(\sigma_{I_\mathrm{o}}^2+\sigma_{I_\mathrm{d}}^2+c_2)},$$

$$c_1 = (k_1 L)^2, \quad c_2 = (k_2 L)^2, \quad (19)$$

where μ_{I_o} and μ_{I_d} represent the mean values of the original image and the decryption result image respectively; σ_{I_o}, σ_{I_d}, $\sigma_{I_\mathrm{o}I_\mathrm{d}}$ represent the variance of the original image and the decrypted image and the co-variance between them, respectively; c_1 and c_2 are constants to avoid division by 0; L denotes the dynamic range of pixel values. Usually, $k_1 = 0.01$ and $k_2 = 0.03$.

4.2. Histogram

The histogram shows the effectiveness and security of the encryption scheme. The histograms of ciphertext and plaintext should be completely different in the ideal encryption scheme. Figure 6 shows the histograms corresponding to RGB channels of color images 'airplane' and 'baboon', and their respective ciphertext histograms, which shows that the histogram of the ciphertext is different from that of any channel.

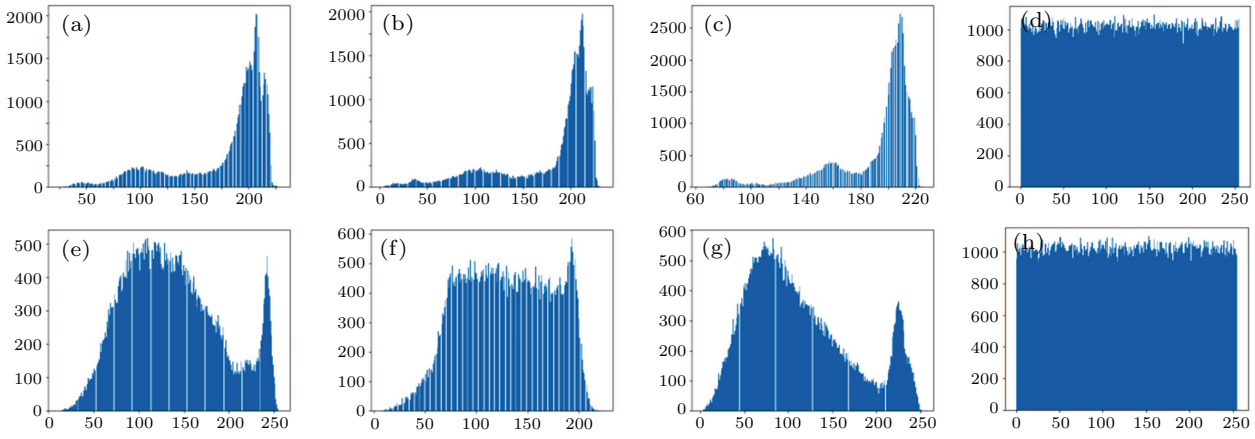


Fig. 6. (a)–(c) RGB channels' histograms of 'airplane', (d) ciphertext histogram of 'airplane', (e)–(g) RGB channels' histograms of 'baboon', and (h) ciphertext histogram of 'baboon'.

4.3. Key sensitivity and key space analysis

Key sensitivity is usually used to test the reliability of an encryption scheme. Figures 7(a) and 7(b) show the sensitivity sensitivities of spherical diffraction parameters and initial values of hyperchaotic systems, respectively. Here, 'baboon' is selected as the plaintext.

The dependence of SSIM on the change of r, R, λ are shown in Fig. 7(a). When r, R, and λ change 1% , 1%, 3%, the SSIM value would change dramatically.

The initial condition of the chaotic sequence is also used as a private key. Figure 7(b) shows the decryption effects of changes in initial conditions, indicating that the initial condition changing by 0.25% will have a significant influence on the decryption result when the initial condition is 4 decimal places. With the increase of the decimal places of the initial condition, the spatial sensitivity of the initial condition becomes stronger.

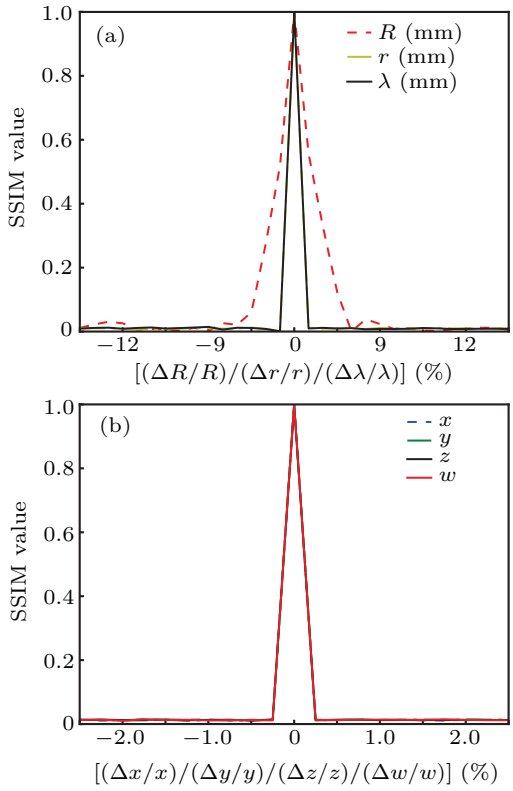


Fig. 7. (a) Key sensitivity of spherical diffraction, and (b) key sensitivity of initial conditions of 4D hyperchaotic system.

4.4. Noise and occlusion attacks

Usually, the ciphertext may be polluted during transmission. Therefore, it is very important to ensure that the encryption scheme is robust to noise attack. In this part, multiplicative Gaussian noise is used to test the anti-noise performance of the image. The additive Gaussian noise model is as follows:

$$P' = P \cdot (1 + kG), \tag{20}$$

where P and P' represent ciphertext and ciphertext with noise, respectively, G denotes the Gaussian noise with a mean value of 0 and a standard deviation of 0.01, and k refers to the signal-to-noise ratio. Figures 8(a)–8(d) show the decryption results of the plaintext 'baboon' under different strengths of multiplicative Gaussian noise attack. The strengths of the four images are $k = 0.01$, 0.05, 0.1, and 0.5, and the corresponding PSNR values are 28.16 dB, 21.58 dB, 18.51 dB, and 11.45 dB, respectively.

In the process of transmission, the occlusion of ciphertext is also one of the possible pollutions. Figure 9 shows the decryption effects under different occlusion ratios: 50×50 pixels (1%), 100×100 pixels (4%), 150×150 pixels (8%), and 200×200 pixels (15%), respectively. The corresponding PSNR values are 17.79 dB, 14.68 dB, 12.81 dB, and 11.61 dB, respectively. Table 2 shows the decryption quality of the proposed scheme and Ref. [36] under the same clipping ratio. It shows that the proposed scheme is more resistant to ciphertext occlusion than the counterpart in Ref. [36].

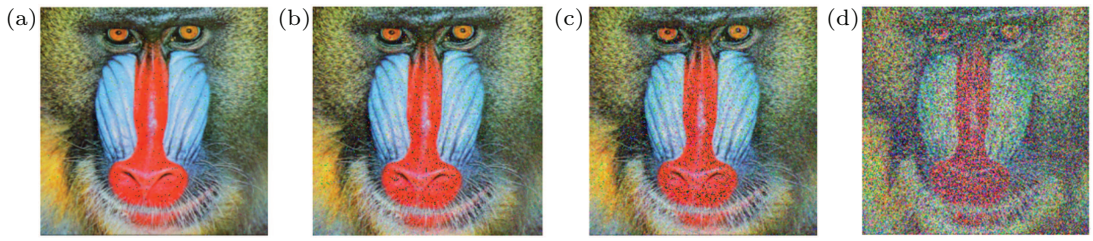


Fig. 8. Decryption results of encryption image with noise strengths: $k = 0.01$ (a), 0.05 (b), 0.1 (c), and 0.5 (d).

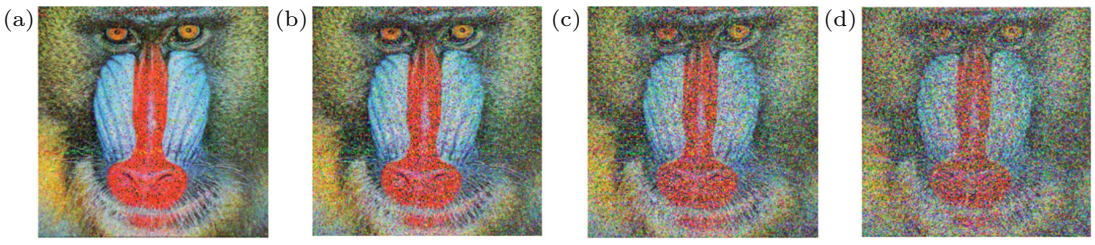


Fig. 9. Decryption results of encryption image with occlusion of (a) 50×50 pixels (1%), (b) 100×100 pixels (4%), (c) 150×150 pixels (8%), and (d) 200×200 pixels (15%).

Table 2. Comparison of t ability to resistocclusion between Ref. [36] and proposed scheme, with 'baboon' chosen as plaintext.

	SSIM			MSE		
Occlusion radio	1%	2%	3%	1%	2%	3%
Proposed	0.53	0.46	0.42	4.8×10^2	6.3×10^2	7.7×10^2
Ref. [36]	0.21	0.18	0.13	5.8×10^4	6.2×10^4	9.1×10^4

4.5. Error analysis of spatial light modulator

Since spatial light modulator carries out the numerical quantization of the image on the target plane, quantization errors are regarded as a main error in optical encryption. To simulate an actual optical decryption, we will test this error to approach to the simulation results of real optical experiments.[40]

Figures 10(a)–10(d) show the decryption effects of the images at different quantization levels: 2^2 levels, 2^4 levels, 2^8 levels, 2^{16} levels, and the corresponding PSNR values are 10.25 dB, 15.28 dB, 26.34 dB, and 29.02 dB, respectively. Under the introduction of this error, the proposed scheme is better than Ref. [21]. Figure 11 shows the difference between the two schemes. The corresponding PSNR values are 11.54 dB and 27.63 dB, and SSIM values are 0.69 and 0.79, respectively.

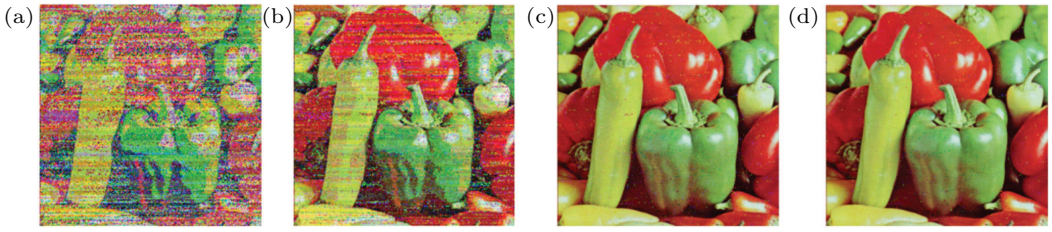


Fig. 10. Decryption results at (a) 2^2, (b) 2^4, (c) 2^8, and (d) 2^{16} quantization levels.

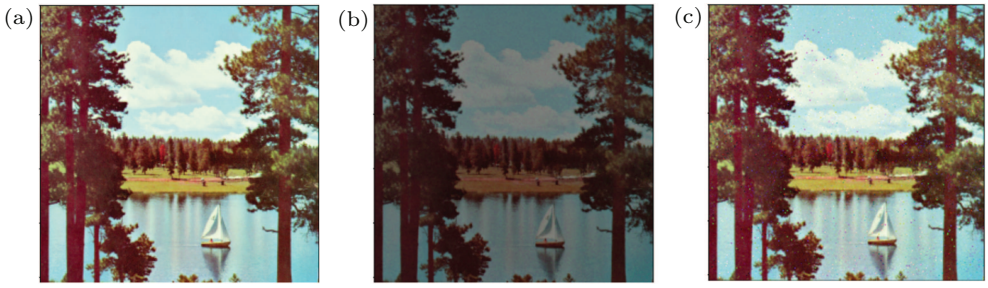


Fig. 11. Decryption results with quantization level 2^8, showing (a) original image, (b) decryption result of Ref. [21], and (c) decryption result of the proposed scheme.

4.6. Resisting information leakage

The current partial color image encryption adopts three channels parallel processing method,[21–23] which has the risk of information leakage in the process of transmission. Unlike these schemes, the single-channel grayscale ciphertext and the low correlation among the three channels in our scheme can significantly reduce the possibility of information leakage during transmission. To test the ability to resist information leakage, we assume that the information leakage has occurred. That is, the attacker has obtained the information about one of the three RGB channels, which means that for our scheme, the attacker has obtained a subband completely. Meanwhile, we assume that the attacker knows all the private keys and the encryption scheme.

Figure 12 shows the comparison of the decryption effect between the two schemes under the condition of only knowing channel B information, taking the result in Ref. [23] as the comparison. The corresponding SSIM values of Figs. 10(c), 10(g), 10(d), and 10(h) are 0.99, 0.99, 0.09, and 0.09, respectively, showing that the ciphertext security of our scheme is much higher than the parallel processing scheme.

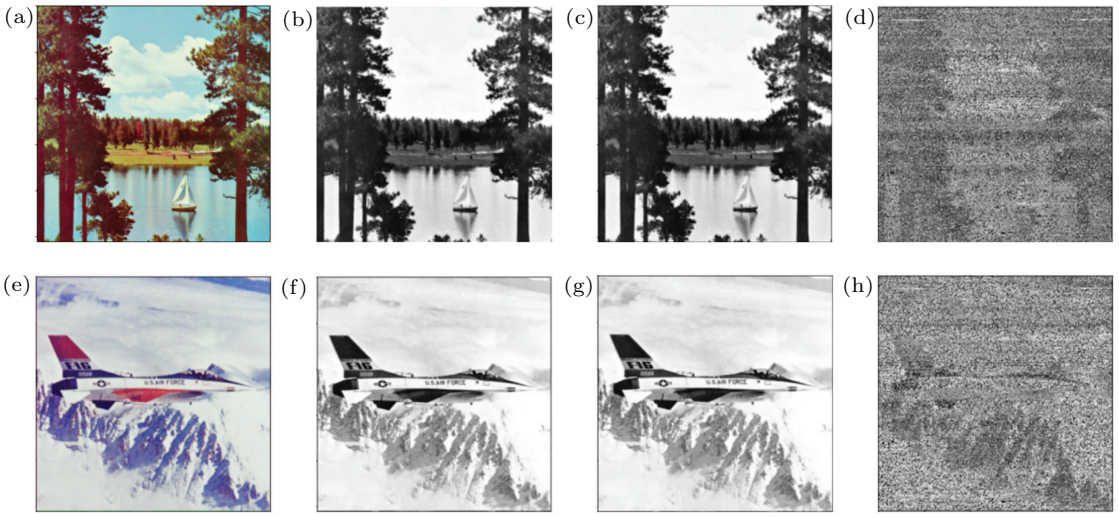


Fig. 12. Comparison of anti-information leakage ability between the literature and the proposed scheme, with channel B taken for example, displaying ((a), (e)) plaintext, ((b), (f)) B channel of plaintext, ((c), (g)) decryption result of Ref. [23], ((d), (h)) decryption of the proposed scheme.

4.7. Potential attack analysis

Phase iterative attack is a common way to attack optical encryption.[41] Here, we compare the resistance to phase iterative attack between Ref. [23] and our scheme. To compare the result better, the black edge is padded around the image. Figure 13 shows the phase recovery of the image after 500 iterations, and figure 14 shows the relation between the number of iterations and the SSIM of the recovered image.

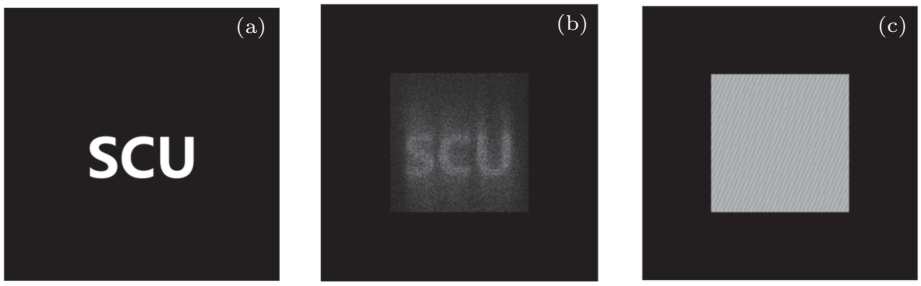


Fig. 13. Result of phase iterative attack: (a) plaintext, (b) result of Ref. [23], (c) result of the proposed scheme.

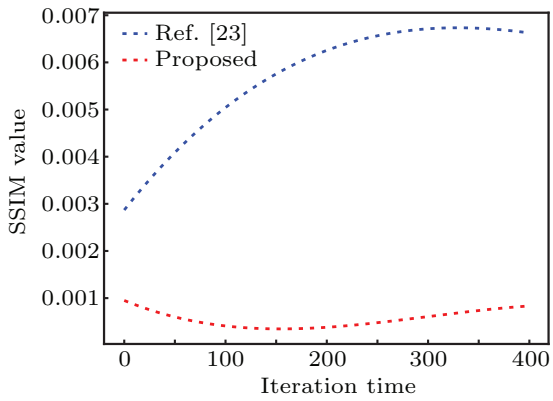


Fig. 14. Comparison of phase attack results between Ref. [23] and the proposed scheme.

Compared with linear optical system, nonlinear optical system has better resistance to phase attack. And since spherical diffraction is just one kind of nonlinear optical system, our scheme has a better performance against phase attack.

An encryption system with high security should be able to resist differential attacks. In general, the number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used to evaluate the ability to resist differential attacks, and defined as

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{21}$$

$$D(i,j) = \begin{cases} 1, & E(i,j) \neq E'(i,j), \\ 0, & E(i,j) = E'(i,j), \end{cases} \tag{22}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|E(i,j) - E'(i,j)|}{255} \times 100\%, \tag{23}$$

where E and E' represent the ciphertext and the ciphertext with only one pixel changed, respectively.

The corresponding NPCR and UACI values under different plaintexts are shown in Table 3 as compared with those in Refs. [24,42–44]. The result from the characteristics of chaotic systems shows that the difference in result caused by small changes in initial values is widely divergent. And since the initial value is determined by the colorful plaintext, a small change in the plaintext will make the key completely different. Therefore it has a strong ability to resist differential attacks.

Table 3. Values of NPCR and UACI of different schemes.

	NPCR (%)					UACI (%)				
Plaintext	Proposed	Ref. [24]	Ref. [42]	Ref. [43]	Ref. [44]	Proposed	Ref. [24]	Ref. [42]	Ref. [43]	Ref. [44]
Baboon	99.9834	99.7973	99.8183	99.6094	0.002	33.51	33.72	33.43	33.46	6×10^{-4}
Airplane	99.9971	99.5130	99.6098	99.6078	0.002	33.89	33.62	33.51	33.45	6×10^{-4}
Girl	99.9962	99.6859	99.6259	99.6089	0.002	33.43	34.58	33.46	33.45	6×10^{-4}
Peppers	99.9929	99.6142	99.6324	99.6088	0.002	33.29	33.46	34.18	33.44	6×10^{-4}

5. Conclusions

In this paper, an efficient and secure color image encryption scheme based on channel fusion and spherical diffraction is proposed. Especially, channel fusion technology can effectively solve the problem of information leakage in color image encryption and reduce the loss of encryption. Compared with the symmetric system, the asymmetric spherical diffraction system used in this paper can significantly improve the anti-attack ability and security of the scheme. Besides, the IEMD also solves the problem that the diffraction result is complex-valued. The simulation results and the comparison show the high security and robustness of the proposed scheme. Therefore, the proposed scheme may be used as a reference to resist-

ing the risk of information leakage in color image encryption.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. U1933132) and the Chengdu Science and Technology Program, Sichuan Province, China (Grant No. 2019-GH02-00070-HZ).

References

[1] Refregier P and Javidi P 1995 *Opt. Lett.* **20** 767
[2] Li T and Shi Y S 2016 *Chin. Phys. Lett.* **33** 014206
[3] Carnicer A, Montes-Usategui M, Arcos S and Juvells I 2005 *Opt. Lett.* **30** 1644
[4] Tao R, Lang J and Wang Y 2008 *Opt. Lett.* **33** 581
[5] Farah M A B, Guesmi R, Kachouri A and Samet M 2020 *Opt. Laser Technol.* **121** 105777
[6] Zhou N R, Wang Y X and Wu J H 2011 *Opt. Commun.* **284** 5588
[7] Zhou N R, Liu X B, Zhang Y and Yang Y X 2013 *Opt. Laser Technol.* **47** 341
[8] Hua L L Xu N and Yang G 2014 *Chin. Phys. B* **23** 064201
[9] Zhang X, Meng X F, Wang Y R, Yang X L and Yin Y K 2018 *Chin. Phys. B* **27** 074205
[10] Dou S F, Shen X J, Zhou B, Wang L and Lin C 2019 *Opt. Laser Technol.* **112** 56
[11] Zhang Y D and Zhao S M 2017 *Chin. Phys. B* **26** 054205
[12] Wang J, Wang Q H and Hu Y H 2018 *IEEE Photon. J.* **10** 7801014
[13] Wang J, Li X W, Hu Y H and Wang Q H 2018 *Opt. Commun.* **410** 468
[14] Wang Y, Liu Q, Wang J and Wang Q H 2018 *Chin. Phys. B* **27** 034202
[15] Yao L L, Yuan C J, Qiang J J, Feng S T and Nie S P 2017 *Opt. Laser Eng.* **89** 72
[16] Su Y G, Xu W J, Li T L, Zhao J and Liu S Q 2021 *Opt. Laser Eng.* **140** 106550
[17] Zhou N R, Wang Y X, Gong L H, Chen X B and Yang Y X 2012 *Opt. Laser Technol.* **44** 2270
[18] Zhang L M, Sun K H, Liu W H and He S B 2017 *Chin. Phys. B* **26** 100504
[19] Wu X J, Wang D W, Kurths J and Kan H 2016 *Information Sciences* **349–350** 137
[20] Qu G, Meng X F, Yin Y K, Wu H Z, Yang X L, Peng X and He W Q 2020 *Opt. Laser Eng.* **137** 106392
[21] Chen H, Tanougast C, Liu Z J and Sieler L 2017 *Opt. Laser Eng.* **93** 1
[22] Kumari E, Mukherjee S, Singh P and Kumar R 2020 *Results in Optics* **1** 100005
[23] S.Faragallah O, S.El-sayed H, Afifi A and El-Shafai W 2021 *Opt. Laser Eng.* **137** 106333
[24] Yildirim M 2021 *Optik* **237** 166728
[25] Huang L Q, Cai S T, Xiong X M and Xiao M Q 2018 *Opt. Laser Eng.* **115** 7
[26] Wang Y, Quan C and Tay C.J 2015 *Opt. Commun.* **344** 147
[27] Deng X P and Zhao D M 2012 *Opt. Laser Technol.* **44** 136
[28] Sui L S, Xin M T, Tian A L and Jin H Y 2013 *Opt. Laser Eng.* **51** 1297
[29] Abuturab M R 2014 *Opt. Laser Eng.* **58** 39
[30] Chen X D, Liu Q, Wang J and Wang Q H 2018 *Opt. Laser Technol.* **107** 302
[31] Li B Y, Wang J, Chen C, Li Y J, Yang R X and Chen N 2020 *Opt. Express* **28** 31373
[32] Jackin B J and Yatagai T 2013 *Opt. Express* **21** 935
[33] Li G, Phan A H, Kim N and Park J H 2013 *Appl. Opt.* **52** 3567
[34] Tachiki M L, Sando Y, Itoh M, Yatagai T 2006 *Appl. Opt.* **45** 3527
[35] Li G, Hong K, Yeom J, Chen N, Park J H, Kim N and Lee B 2014 *Chin. Opt. Lett.* **12** 060016
[36] Zhu Z, Chen X D, Wu C, Wang J and Wang W 2020 *Opt. Laser Technol.* **126** 106106
[37] Wang J, Chen X D, Zeng J Q, Wang Q H and Hu Y H 2019 *IEEE Access.* **7** 66234
[38] Chen L J, Tang S, Li Q D and Zhong S M 2018 *Mathematics and Computers in Simulation* **146** 44
[39] Wu C, Hu K Y, Wang Y, Wang J and Wang Q H 2019 *Opt. Commun.* **448** 26
[40] He Z H, Sui X M, Jin G F, Chu D P and Cao L C 2021 *Opt. Express* **29** 119
[41] Kong D Z, Shen X J, Cao L C and Jin G F 2018 *Appl. Opt.* **56** 3449
[42] Xian Y J, Wang X Y, Yan X P, Li Q and Wang X Y 2020 *Opt. Laser Eng.* **134** 106202
[43] Huang L Q, Cai S T, Xiong X M and Xiao M Q 2018 *Opt. Laser Eng.* **115** 7
[44] Gao T G and Chen Z Q 2008 *Phys. Lett. A* **372** 394