Optica Applicata, Vol. LII, No. 2, 2022
DOI: 10.37190/oa220202

Double-image encryption scheme based on the phase-truncated multiple-parameter Fresnel transform

LING ZHOU[1, 2], HANG ZHOU[2], YAN MA[2], NAN-RUN ZHOU[2*]

[1]Department of Energy and Power Engineering, Guangxi Electric Polytechnic Institute, Nanning 530007, China

[2]Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[*]Corresponding author: nrzhou@ncu.edu.cn

A double-image encryption algorithm is proposed with the phase-truncated multiple-parameter Fresnel transform. Firstly, the pixel positions of two plaintext images are scrambled and then the results are merged into one image with the scrambling operation. Subsequently, the resulting image is encrypted by phase truncation and phase reservation in the multiple-parameter Fresnel transform domain. The phase information is scrambled by the affine transform and then recombined with the amplitude information. The final encryption image is obtained with the pixel scrambling and diffusion methods to further enhance the security of the image encryption system, where the scrambling and diffusion operations are based on logistic map, logistic-sine system and 2D logistic -adjusted-sine map. The image encryption scheme is robust against the common attacks due to the nonlinear properties of diffusion and phase truncation. Numerical simulation results verify the performance and the security of the proposed double-image algorithm based on the phase-truncated multiple-parameter Fresnel transform.

Keywords: chaotic system, phase-truncated multiple-parameter Fresnel transform, scrambling and diffusion operations, image encryption.

1. Introduction

During the image transfer and processing, an attacker may acquire the private image information. To avoid information leakage, a number of image encryption algorithms have been proposed. Chaos system has attracted widespread attention in the field of image encryption due to its randomness, ergodicity and sensibility to initial values [1]. A new image encryption algorithm with chaos was demonstrated by a dynamic key selection mechanism to strengthen the ability to resist the chosen-plaintext attack and the known-plaintext attack [1]. For better security, WANG *et al*. proposed a new image encryption scheme by combining Josephus traversing with mixed chaotic map to scramble and diffuse the pixels of images, which could resist common attacks [2].

However, these chaos-based image encryption schemes exhibited some shortcomings. To address these problems, HUA *et al.* constructed a chaotic map with continuous chaotic range [3]. Sun presented an image encryption scheme based on hyper-chaotic system, where the original images were encrypted with pixel-level scrambling and bit-level scrambling, and then the permuted images were further encrypted by DNA encoding and decomposition operation [4]. To solve some security, practicability and feasibility issues, FENG *et al.* proposed an improved image encryption algorithm based on DNA encoding and scrambling [5].

Due to the properties of mathematic transform, the image encryption algorithms in transform domains usually have better anti-interference performance and higher security, and this kind of image encryption algorithms has attracted extensive attention. For example, fractional Fourier transform, discrete cosine transform and fractional Mellin transform have been introduced into image encryption [6, 8]. In addition, the multi-parameter transform may contribute to image encryption with larger key space. A digital image encryption system was constructed with the multiple-parameter discrete fractional random transform to resist statistical analyses effectively [9]. REN *et al.* proposed an image encryption algorithm based on the phase-truncated discrete multiple-parameter fractional Fourier transform, which could enhance the security of the asymmetric cryptosystem and improve the ability to counteract the chosen-plaintext attack [10]. However, the test image with the above-mentioned algorithms is a single gray-scale image. Therefore, a triple color image encryption method was designed to further reduce time complexity and space complexity [11]. GONG *et al.* devised a quaternion discrete fractional Hartley transform to encrypt multiple images with an improved pixel adaptive diffusion to reduce the consumption of keys and increase the encryption capacity [12]. To obtain higher quality of decryption images, a multi-image encryption system was suggested by CHEN *et al.* with compressive sensing and feature fusion, in which the four original images were processed by the optical wavelet transform [13]. MENG *et al.* invented a secret multi-image encryption method with row scanning compressive ghost imaging and phase retrieval in the Fresnel domain to realize secret key data sharing [14]. In 2018, ZHOU *et al.* designed a double-image compression and encryption scheme, where the images were compressed by compressive sensing and then a series of operations were used to re-encrypt the images, which not only could encrypt double images, but also could enhance the security and the robustness of the image encryption algorithm [15].

To improve the ability to resist the chosen-plaintext attack and increase the key space, a double-image encryption algorithm based on phase-truncated multiple-parameter Fresnel transform (PTMPFrT) and chaotic system is proposed. The parameters of the multiple-parameter Fresnel transform and three chaotic systems can be used as keys to enlarge the key space of the double-image encryption scheme. The phase truncation and the XOR operations are adopted to improve the robustness in resisting the chosen -plaintext attack.

2. Fundamental knowledge

2.1. Chaotic system

As a common chaotic system, the logistic map can be expressed as

$$x_{n+1} = \mu x_n (x_n + 1) \tag{1}$$

where μ represents the system parameter in the range of [3.57, 4]. The logistic-sine system (LSS) and the 2D logistic-adjusted-sine map (2D LASM) can be separately described as [16]

$$h_{n+1} = \Big[\omega h_n(1 - h_n) + (4 - \omega)\sin(\pi h_n)\Big] \bmod 1 \tag{2}$$

$$\begin{cases} y_{n+1} = \sin\Big[\pi\beta(z_n + 3)y_n(1 - y_n)\Big] \\ z_{n+1} = \sin\Big[\pi\beta(y_n + 3)z_n(1 - z_n)\Big] \end{cases} \tag{3}$$

where ω and β are the system parameters, and the system will be in a chaotic state if $\alpha, \beta \in [0, 4]$.

2.2. Multiple-parameter Fresnel transform

The two-dimensional multiple-parameter Fresnel transform (2D MPFrT) on $f(x, y)$ with a free space propagation distance z is defined as

$$\mathrm{MPFrT}_{z,\lambda,\alpha}\{f(x, y)\} = \frac{\exp(\mathrm{i}kz)}{\mathrm{i}\lambda z}\exp\left[\frac{\mathrm{i}\pi}{\lambda z}(x^2 + y^2)\right] \times \mathrm{F}^{\alpha}\left\{f(x, y)\exp\left[\frac{\mathrm{i}\pi}{\lambda z}(x_0^2 + y_0^2)\right]\right\} \tag{4}$$

where $\mathrm{F}^{\alpha}\{\cdot\}$ denotes the fractional Fourier transform of order α, λ is the wavelength of a parallel beam. (x, y) and (x_0, y_0) are the coordinates of input plane and output plane, respectively.

2.3. Phase truncation operation based on the multiple-parameter Fresnel transform

Phase truncation (PT) and phase reservation (PR) operations on signal $f(x, y)$ in the MPFrT domain can be constructed as

$$\mathrm{G}(u, v) = \mathrm{PT}\left\{\mathrm{MPFrT}_{z1}^{\lambda}\Big[f(x, y) \cdot \mathrm{PRM}_1\Big]\right\} \tag{5}$$

$$\mathrm{P}_1(u, v) = \mathrm{PR}\left\{\mathrm{MPFrT}_{z1}^{\lambda}\left[f(x, y) \cdot \mathrm{PRM}_1\right]\right\} \tag{6}$$

where PRM_1 is a random phase mask. Then $\mathrm{G}(u, v)$ is modulated by the second random phase mask PRM_2, while $\mathrm{P}_1(u, v)$ is confused to obtain the second random phase mask PRM_2 by the affine transform [17].

$$\mathrm{PRM}_2 = \mathrm{AT}\left[\mathrm{P}_1(u, v)\right] \tag{7}$$

$$\mathrm{E}(\xi, \eta) = \mathrm{PT}\left\{\mathrm{MPFrT}_{z2}^{\lambda}\left[\mathrm{G}(u, v) \cdot \mathrm{PRM}_2\right]\right\} \tag{8}$$

$$\mathrm{P}_2(\xi, \eta) = \mathrm{PR}\left\{\mathrm{MPFrT}_{z2}^{\lambda}\left[\mathrm{G}(u, v) \cdot \mathrm{PRM}_2\right]\right\} \tag{9}$$

The image decryption process is the inverse one of image encryption.

3. Double-image encryption algorithm based on the PTMPFrT

The block diagrams of double-image encryption process and decryption process are illustrated in Figs. 1 and 2, respectively. The double-image encryption process is detailed as follows, where A and B are two plaintext images, while C is the ciphertext image.

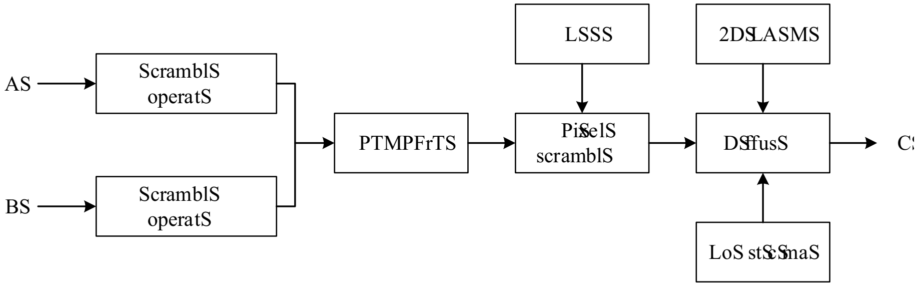

Fig. 1. Double-image encryption process.

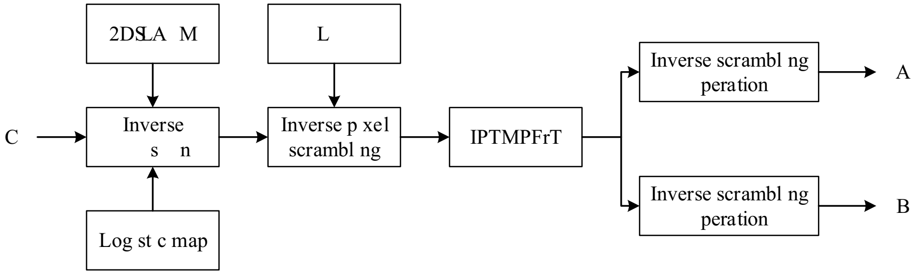

Fig. 2. Double-image decryption process.

Step 1: The pixel positions of the two original images of size $N \times N$ are shuffled by the scrambling operation and then a composite image F(x, y) of size $N \times N$ is produced.

Step 2: Matrix F(x, y) is modulated by the first random phase mask $\mathrm{R}_1(x, y)$ and encrypted in the MPFrT domain with z_1.

$$\mathrm{F}_1(x, y) = \mathrm{MPFrT}_{z1}^{\lambda}\left\{\mathrm{F}(x, y) \cdot \exp\left[\mathrm{i}2\pi\mathrm{R}_1(x, y)\right]\right\} \tag{10}$$

Step 3: The phase truncation operation is executed on $\mathrm{F}_1(x, y)$, the amplitude of the spectrum G(u, v) is retained, while the phase part $\mathrm{P}_1(u, v)$ is truncated.

$$\mathrm{G}(u, v) = \mathrm{PT}\left\{\mathrm{MPFrT}_{z1}^{\lambda}\left[\mathrm{F}_1(x, y)\right]\right\} \tag{11}$$

$$\mathrm{P}_1(u, v) = \mathrm{PR}\left\{\mathrm{MPFrT}_{z1}^{\lambda}\left[\mathrm{F}_1(x, y)\right]\right\} \tag{12}$$

Step 4: E(ξ, η) is obtained by performing the MPFrT with z_2 after being modulated by the second random phase mask $\mathrm{R}_2(x, y)$.

$$\mathrm{R}_2(x, y) = \mathrm{AT}\left[\mathrm{R}_1(x, y)\right] \tag{13}$$

$$\mathrm{E}(\xi, \eta) = \mathrm{PT}\left\{\mathrm{MPFrT}_{z2}^{\lambda}\left\{\mathrm{G}(u, v) \cdot \exp\left[\mathrm{i}2\pi\mathrm{R}_2(x, y)\right]\right\}\right\} \tag{14}$$

$$\mathrm{P}_2(\xi, \eta) = \mathrm{PT}\left\{\mathrm{MPFrT}_{z2}^{\lambda}\left\{\mathrm{G}(u, v) \cdot \exp\left[\mathrm{i}2\pi\mathrm{R}_2(x, y)\right]\right\}\right\} \tag{15}$$

Step 5: The chaotic sequence is produced by the logistic-sine system with initial condition h_0 as the initial input of logistic map, and then the generated sequence is divided into $S = \{S_1, S_2, \mathrm{K}, S_{N^2}\}$ and $Q = \{Q_1, Q_2, \mathrm{K}, Q_{N^2}\}$ of length N^2. The random sequences S and Q are sorted to obtain the index sequences G_1 and G_2. The white noise-like image E can be scrambled as

$$E(i, j) = K\left[G_1(i), G_2(j)\right] \tag{16}$$

$G_1(i)$ represents the i-th element in index sequence G_1, while $G_2(j)$ is the j-th element in index sequence G_2. They constitute the horizontal and the vertical coordinates of the scrambled image K.

Step 6: The 2D logistic-adjusted-sine map with two initial values y_0 and z_0 is iterated to generate two random sequences O and P. Another random sequence T is obtained by logistic map with initial value x_0. The scrambled image K is converted into a sequence U. The elements of the above sequences are mapped into the range [0, 255]. XOR operation is performed on the three sequences, *i.e.*,

$$V = U \oplus O \oplus P \oplus T \tag{17}$$

The parameters of the chaotic system based on the plaintext image can be calculated as: $x_0 = \psi + \mathrm{Rs}$, $y_0 = v + \mathrm{Rs}$, $z_0 = o + \mathrm{Rs}$, $h_0 = \theta + \mathrm{Rs}$, where

$$\mathrm{Rs} = \frac{1}{1000 \times M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[f_1(i,j) + f_2(i,j) \right]$$

and $f_1(i,j)$ and $f_2(i,j)$ are the pixel values of the original images and $M \times N$ is the image size.

4. Simulation results and analysis

A series of experiments are carried out on Matlab (R2016a) to analyze the performance of the proposed double-image encryption scheme based on the PTMPFrT, including histograms analysis, correlation analysis, key space analysis and so on.

4.1. Encryption results and decryption results

Two original images *Baboon* and *Peppers* with pixels shown in Figs. 3**a** and 3**b** serve as the test images. The simulation parameters of the logistic map and the logistic-sine system are computed as $x_0 = 0.4269$, $\mu = 3.98$, $h_0 = 0.5269$, and $\omega = 3.99$. The parameters of 2D LASM are calculated as $y_0 = 0.2269$, $z_0 = 0.3269$, and $\beta = 3.99$. The four parameters of the 2D MPFrT are set as $z_1 = 0.5$ m, $z_2 = 0.6$ m, $\lambda = 632.8$ nm, and $\alpha = 0.2$. The encryption image is shown in Fig. 3**c**, and the corresponding correct decryption images are given in Figs. 3**d** and 3**e**, respectively. Compared with the two original images, the decryption images are still visually discernible. A similar conclusion can be obtained by testing the two images *Couple* and *Man*. In addition, the proposed image encryption algorithm can also be used to encrypt color image. Firstly, the color image is decomposed into R, G, B components, which can be treated as three images. Then the R, G, B components are scrambled and the results are merged into one image with the scrambling operation. Finally, the color ciphertext image can be obtained with our proposed algorithm. Image *Girl* of size 256 × 256 is chosen as the test image. In the scrambling operation, the information selected from the three images is scrambled into one image, in which a small part of information is lost and a distorted image with low resolution would be generated. Therefore, the phase truncation operation based on the multi-parameter Fresnel transform is first carried out for the three components respectively, and then the scrambling operation is performed to obtain the ciphertext image. The experimental results are shown in Fig. 3. The decryption result is acceptable.

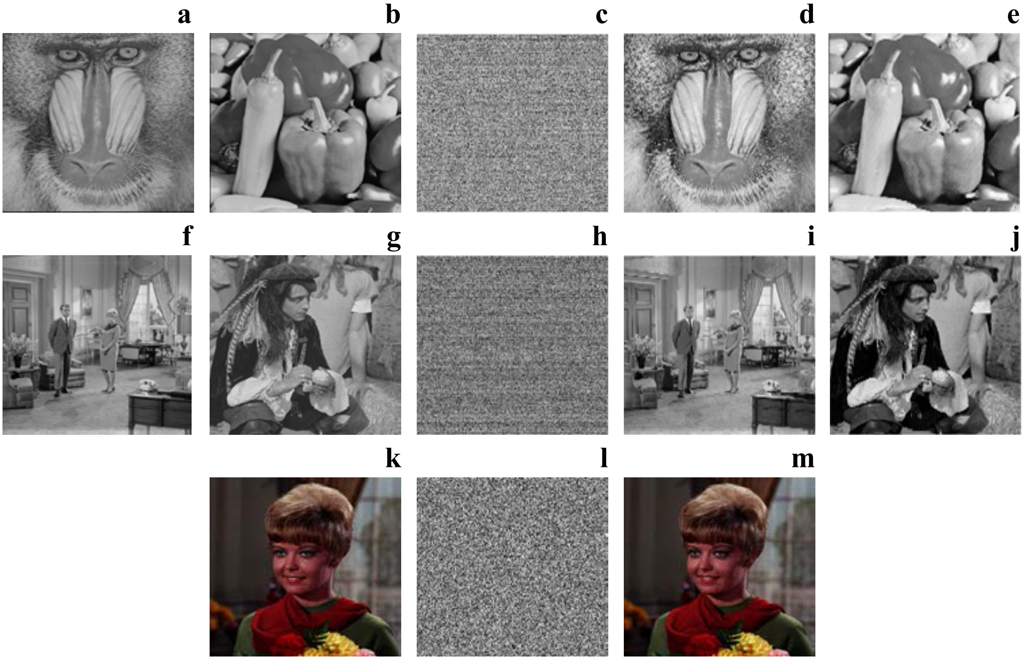

Fig. 3. Encryption and decryption results: (**a**) original *Baboon*, (**b**) original *Peppers*, (**c**) encryption image; (**d**) decryption *Baboon*, (**e**) decryption *Peppers*, (**f**) original *Couple*; (**g**) original *Man*, (**h**) encryption image, (**i**) decryption *Couple*, (**j**) decryption *Man*, (**k**) original *Girl*, (**l**) encryption image, (**m**) decryption *Girl*.

Table 1. SSIM values for different test images.

Image	*Baboon*	*Peppers*	*Couple*	*Man*
SSIM value	0.9895	0.9846	0.9699	0.9806

The structural similarity index measure (SSIM) is employed to evaluate the degree of similarity between original image f and decryption one $f^{\%}$ [18].

$$\mathrm{SSIM}(f,\ f^{\%}) = \frac{(2\mu_f\,\mu_{f^{\%}} + c_1)(2\sigma_{ff^{\%}} + c_2)}{(\mu_f^2 + \mu_{f^{\%}}^2 + c_1)(\sigma_f^2 + \sigma_{f^{\%}}^2 + c_2)} \tag{18}$$

The SSIM value close to 1 indicates the high degree of similarity between the original image and the decryption one. The SSIM values for different test images are arranged in Table 1, which reveals the high-quality reconstruction for original images.

4.2. Histogram analysis

The histograms of the test images *Baboon* and *Peppers* are respectively exhibited in Figs. 4**a** and 4**b**, while the histogram of the corresponding encryption image is illus-

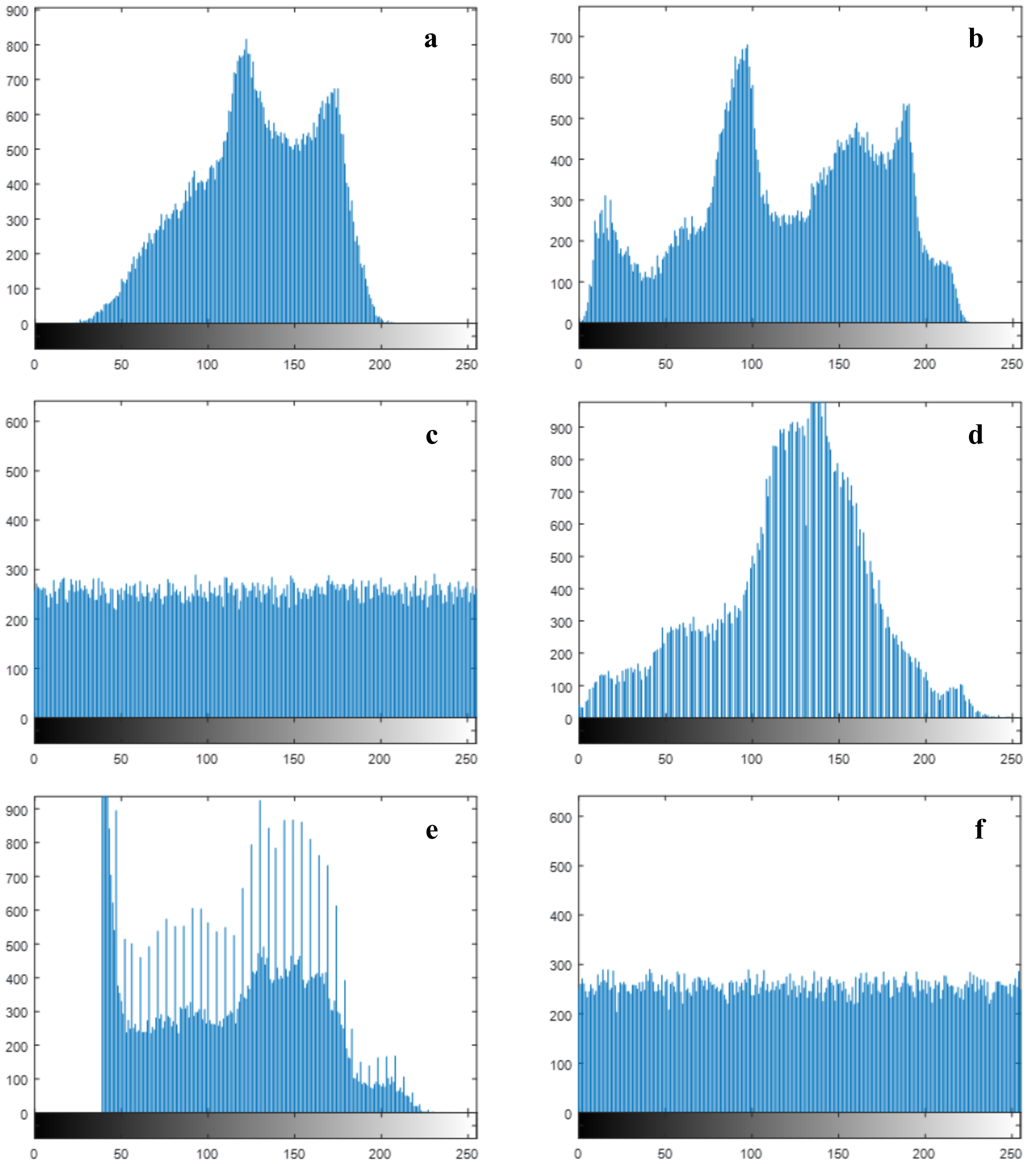

Fig. 4. Histograms: (**a**) *Baboon*, (**b**) *Peppers*, (**c**) encryption image, (**d**) *Couple*, (**e**) *Man*, and (**f**) encryption image.

trated in Fig. 4**c**. Figures 4**d**–4**f** are another set of examples. The histograms of encryption images show a similar distribution even if the histogram of each original image is distributed differently. To further verify the uniformity of the histogram of the encryption image, Kolmogorov–Smirnov test (K-S test) is taken to verify the assumption that the distribution of the encryption image obeys a theoretical uniform distribution.

$$D = \max\left|f(x) - g(x)\right| \tag{19}$$

where x is a pixel value, $f(x)$ and $g(x)$ are the cumulative probability functions of two distributions. When the size of a sample is 256 × 256, the critical values for the significance levels of 0.05 and 0.01 are 0.005 and 0.006, respectively. K-S test results for different encryption images are collected in Table 2. Evidently, the values of D for different encryption images are smaller than the critical values, thus the hypothesis is confirmed. Consequently, the proposed double-image encryption algorithm is immune to the statistical attack.

Table 2. K-S test results for different encryption images.

Image	*Baboon–Peppers*	*Couple–Man*
D-value	0.0032	0.0047
P-value	0.8957	0.4675
Decision	Accepted	Accepted

4.3. Correlation analysis

The correlation coefficient C of an image can be obtained as

$$C = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{20}$$

where $\bar{x} = \sum_{i=1}^{N} x_i$ and $\bar{y} = \sum_{i=1}^{N} y_i$. The pixel diffusion and scrambling operations can reduce the correlation among adjacent pixels by altering the pixel values and changing the pixel positions. Table 3 lists the correlation coefficients of the proposed algorithm and those in [12, 15, 17]. It is obvious that the correlation coefficient among adjacent pixels in the original images is large, while that in the encryption images is small and even tends to 0. The correlation distributions in the horizontal direction are shown in Fig. 5. The adjacent pixels in the original images are tightly correlated while

Table 3. Correlation coefficients of adjacent pixels.

Algorithm	Image	Horizontal direction	Vertical direction	Diagonal direction
	Baboon	0.9519	0.9246	0.8980
	Peppers	0.9491	0.9517	0.9155
Proposed algorithm	Encryption image	0.0171	–0.0106	–0.0016
Ref. [12]	Encryption image	0.0142	–0.0092	0.0157
Ref. [15]	Encryption image	0.0098	0.0582	0.0042
Ref. [17]	Encryption image	0.0120	0.0917	0.1019

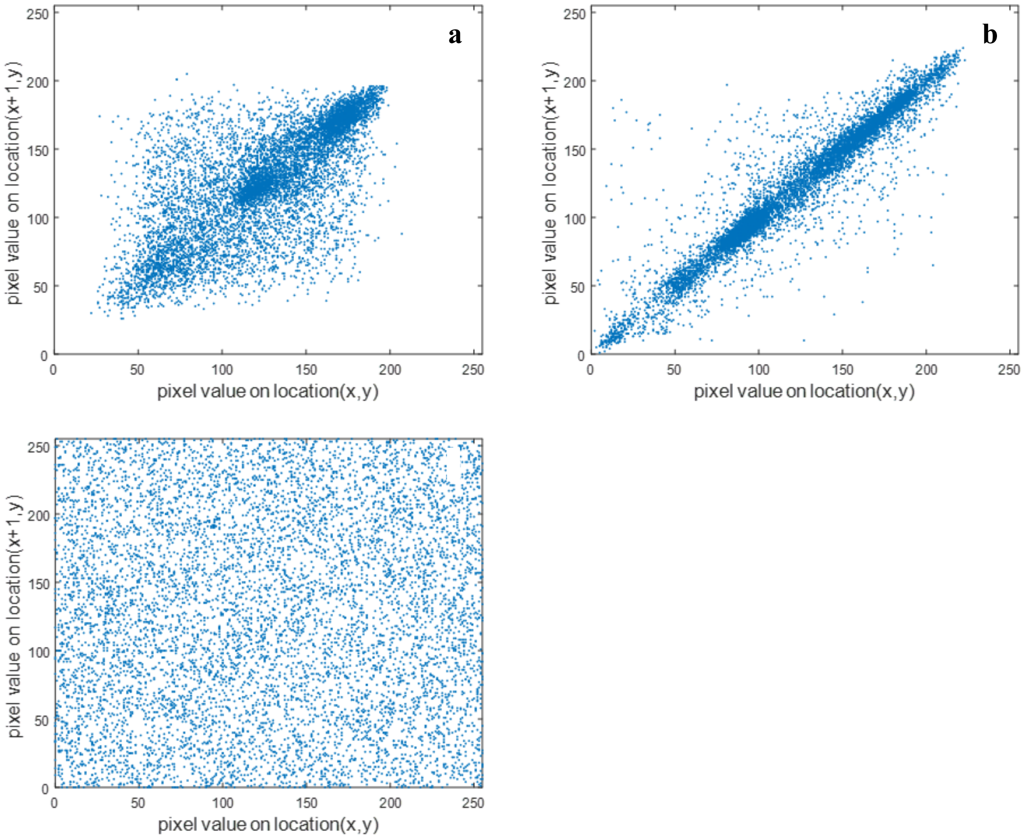

Fig. 5. Correlation distributions in the horizontal direction: (**a**) *Baboon*, (**b**) *Peppers*, (**c**) encryption image.

the correlations of the encryption results are feeble. Thus, this double-image encryption algorithm can resist the differential attack to some extent.

4.4. Information entropy analysis

The Shannon entropy of a random variable is

$$H(x) = -\sum_{i=1}^{N} p(x_i) \log_2 p(x_i) \tag{21}$$

where $p(x_i)$ is the probability of the occurrence of x_i. To reflect the randomness of the encryption image more truly, local Shannon entropy [19] was introduced to make up for the lack of accuracy and efficiency of Shannon entropy. The entropy values in different encryption schemes are listed in Table 4. As observed, the information entropy values of encryption images are close to 8 bits and the local Shannon entropy values are within the optimal value range. It means that the proposed image encryption algorithm has high randomness.

T a b l e 4. Information entropy of different images (bit).

Image	Global Shannon entropy	Local Shannon entropy	Critical local entropy		
			$h_{\text{left}}^{1*0.05} = 7.9019$ $h_{\text{right}}^{1*0.05} = 7.9030$	$h_{\text{left}}^{1*0.01} = 7.9017$ $h_{\text{right}}^{1*0.01} = 7.9032$	$h_{\text{left}}^{1*0.001} = 7.9015$ $h_{\text{right}}^{1*0.001} = 7.9034$
Baboon–Peppers	7.9973	7.9028	Pass	Pass	Pass
Couple–Man	7.9975	7.9027	Pass	Pass	Pass
Ref. [15]	7.9977	7.9034	Pass	Pass	Pass
Ref. [17]	7.9972	7.9024	Pass	Pass	Pass

4.5. Key space analysis

Parameter λ is considered as a supplementary key since it is not sensitive enough. Initial conditions x_0, y_0, z_0, h_0 and fractional order α are the main keys in this proposed algorithm. The precision of each initial value of chaotic system is approximate 10^{-15}, and the deviation of α is 10^{-3}. The total key space of the proposed algorithm is about 2^{189} at least and greater than that in [13]. Therefore, the proposed image encryption algorithm has good performance in resisting the statistical analysis attack.

4.6. Noise attack and occlusion attack

The encryption image is supposed to be contaminated by noise as

$$C' = C + kG \tag{22}$$

where C' and C are the noisy encryption image and the correct encryption one, respectively, k is a coefficient reflecting the noise strength, and G represents the Gaussian

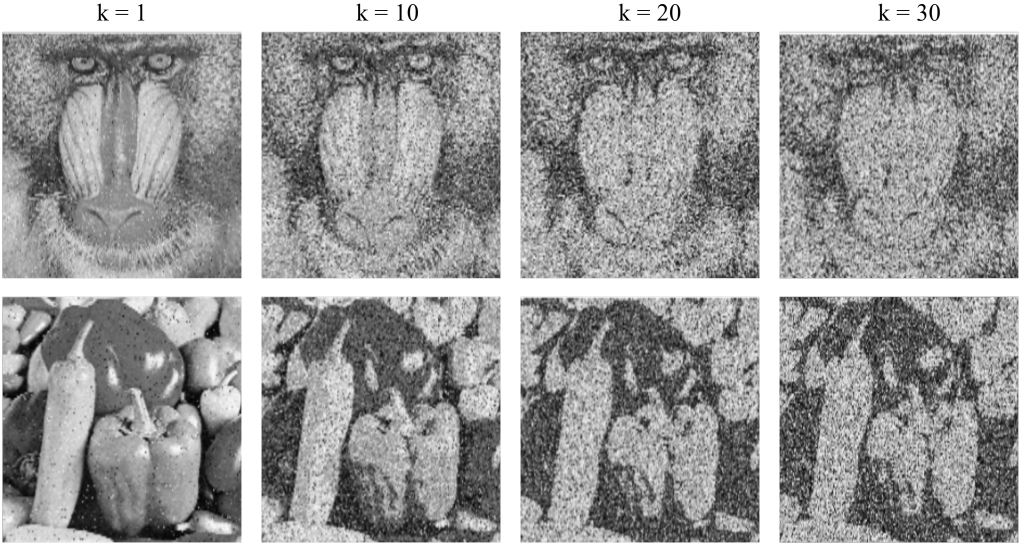

Fig. 6. Decryption images *Baboon* and *Peppers* with different noise intensities.

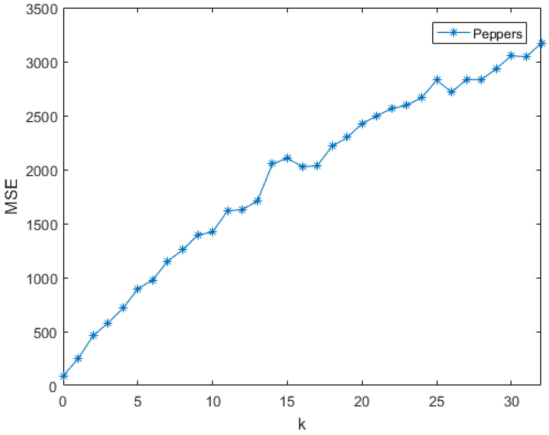

Fig. 7. MSE curve *versus* *k*.

Table 5. SSIM values for different test images with different noise intensities.

Noise intensity *k*	Image	SSIM	Image	SSIM
1	*Baboon*	0.9426	*Peppers*	0.9525
10	*Baboon*	0.6911	*Peppers*	0.7644
20	*Baboon*	0.5630	*Peppers*	0.6164
30	*Baboon*	0.4822	*Peppers*	0.5291

noise with zero-mean and normal distribution. Figure 6 gives the results with different noise intensities 1, 10, 20 and 30, respectively. The MSE curve is shown in Fig. 7. The SSIM values for different test images with different noise intensities are compiled in Table 5. With the increase of noise intensity, the reconstruction quality of the de-

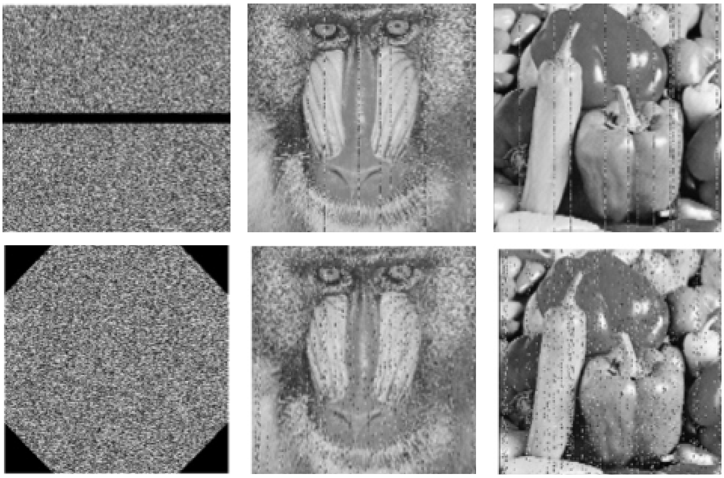

Fig. 8. Results of occlusion attack.

cryption images deteriorates continuously, while the characteristics of the original images are still retained visually. Thus, the proposed double-image encryption scheme can resist noise attack to a certain degree. To analyze the robustness of the proposed algorithm, the encryption images are cropped with 5% and 10%, respectively. The corresponding decryption results are shown in Fig. 8. The main information of the original images can still be obtained from the decryption images. Therefore, the proposed double-image encryption scheme can defend the cropping attack to some degree.

4.7. Chosen-plaintext attack

In the proposed double-image encryption algorithm, the keys used are associated with the plaintext information, therefore different plaintext images could produce completely different keys. In addition, the phase truncation and the XOR operations are nonlinear. That is to say, it is more difficult for an attacker to obtain the correct keys. Hence, the proposed double-image encryption algorithm could also resist the chosen-plaintext attack.

5. Conclusion

A double-image encryption scheme based on the phase-truncated multiple-parameter Fresnel transform is presented. Two original images are firstly encrypted by the scrambling operation, where the pixel positions of the original images are changed and then the two scrambled images are combined into one image. The intermediate image is encrypted by phase truncation and phase reservation in the multiple-parameter Fresnel transform domain, then the phase information is scrambled by the affine transform. Further, the resulting image is scrambled and diffused with different chaotic systems with their initial conditions related to the plaintext image. The proposed scheme can encrypt two images once, which is expedient for image transmission. Due to the introduction of the phase truncation and the XOR operations, the proposed algorithm is robust to resist the chosen-plaintext attack. Moreover, the security of the presented double-image encryption algorithm is acceptable for its large key space.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Grant no. 61861029), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant no. 20162BCB22011), the Cultivation Plan of Applied Research of Jiangxi Province (Grant no. 20181BBE58022).

References

[1] Xiuli Chai, Kang Yang, Zhihua Gan, *A new chaos-based image encryption algorithm with dynamic key selection mechanisms*, Multimedia Tools and Applications **76**(7), 2017, pp. 9907–9927, DOI: 10.1007/s11042-016-3585-x.

[2] Xingyuan Wang, Xiaoqiang Zhu, Yingqian Zhang, *An image encryption algorithm based on Josephus traversing and mixed chaotic map*, IEEE Access **6**, 2018, pp. 23733–23746, DOI: 10.1109/ACCESS.2018.2805847.

[3] Zhongyun Hua, Zhihua Zhu, Shuang Yi, Zheng Zhang, Hejiao Huang, *Cross-plane colour image encryption using a two-dimensional logistic tent modular map*, Information Sciences **546**, 2021, pp. 1063–1083, DOI: 10.1016/j.ins.2020.09.032.

[4] Shuliang Sun, *A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling*, IEEE Photonics Journal **10**(2), 2018, article 7201714, DOI: 10.1109/JPHOT.2018.2817550.

[5] Wei Feng, Yi-Gang He, *Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling*, IEEE Photonics Journal **10**(6), 2018, article 7909215, DOI: 10.1109/JPHOT.2018.2880590.

[6] Miao Zhang, Xiao-Jun Tong, Jie Liu, Zhu Wang, Jinlong Liu, Baolong Liu, Jing Ma, *Image compression and encryption scheme based on compressive sensing and Fourier transform*, IEEE Access **8**, 2020, pp. 40838–40849, DOI: 10.1109/ACCESS.2020.2976798.

[7] Xiaoyong Ji, Sen Bai, Guibin Zhu, Bing Yan, *Image encryption and compression based on the generalized knight's tour, discrete cosine transform and chaotic maps*, Multimedia Tools and Applications **76**(10), 2017, pp. 12965–12979, DOI: 10.1007/s11042-016-3684-8.

[8] Mengmeng Wang, Pousset Y., Carré P., Perrine C., Nanrun Zhou, Jianhua Wu, *Optical image encryption scheme based on apertured fractional Mellin transform*, Optics and Laser Technology **124**, 2020, article 106001, DOI: 10.1016/j.optlastec.2019.106001.

[9] Nanrun Zhou, Taiji Dong, Jianhua Wu, *Novel image encryption algorithm based on multiple-parameter discrete fractional random transform*, Optics Communications **283**(15), 2010, pp. 3037–3042, DOI: 10.1016/j.optcom.2010.03.064.

[10] Guanghui Ren, Jianan Han, Jiahui Fu, Mingguang Shan, *Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional Fourier transform*, Optical Review **25**(6), 2018, pp. 701–707, DOI: 10.1007/s10043-018-0464-x.

[11] Joshi A.B., Kumar D., Gaffar A., Mishra D.C., *Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform*, Optics and Lasers in Engineering **133**, 2020, article 106139, DOI: 10.1016/j.optlaseng.2020.106139.

[12] Huo-Sheng Ye, Nan-Run Zhou, Li-Hua Gong, *Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion*, Signal Processing **175**, 2020, 107652, DOI: 10.1016/j.sigpro.2020.107652.

[13] Xu-Dong Chen, Qi Liu, Jun Wang, Qiong-Hua Wang, *Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction*, Optics and Laser Technology **107**, 2018, pp. 302–312, DOI: 10.1016/j.optlastec.2018.06.016.

[14] Xianye Li, Xiangfeng Meng, Yurong Wang, Xiulun Yang, Yongkai Yin, Xiang Peng, Wenqi He, Guoyan Dong, Hongyi Chen, *Secret shared multiple -image encryption based on row scanning compressive ghost imaging and phase retrieval in the Fresnel domain*, Optics and Lasers in Engineering **96**, 2017, pp. 7–16, DOI: 10.1016/j.optlaseng.2017.04.005.

[15] Nanrun Zhou, Hao Jiang, Lihua Gong, Xinwen Xie, *Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging*, Optics and Lasers in Engineering **110**, 2018, pp. 72–79, DOI: 10.1016/j.optlaseng.2018.05.014.

[16] Kunshu Wang, Xiaojun Wu, Baoqiang Liu, *Double color images encryption based on DNA sequences and block permutation*, [In] *Proceedings of the 2017 2nd International Conference on Machinery, Electronics and Control Simulation* (*MECS 2017*), 2017, pp. 695–703, DOI: 10.2991/mecs-17.2017.129.

[17] Aimin Yan, Jiabin Dong, Yongfang Li, *A novel nonlinear double image encryption based on affine transform and gyrator transform*, Journal of Optics **20**(11), 2018, article 115702, DOI: 10.1088/2040-8986/aae31d.

[18] Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P., *Image quality assessment: from error visibility to structural similarity*, IEEE Transactions on Image Processing **13**(4), 2004, pp. 600–612, DOI: 10.1109/TIP.2003.819861.

[19] Yue Wu, Yicong Zhou, Saveriades G., Agaian S., Noonan J.P., Natarajan P., *Local Shannon entropy measure with statistical tests for image randomness*, Information Sciences **222**, 2013, pp. 323–342, DOI: 10.1016/j.ins.2012.07.049.

[20] Yue Wu, Noonan J.P., Agaian S., *NPCR and UACI randomness tests for image encryption*, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications **1**(2), 2011, pp. 31–38.

Received December 31, 2020
in revised form March 29, 2021