Optica Applicata, Vol. LII, No. 4, 2022
DOI: 10.37190/oa220415

Double-image encryption algorithm based on discrete fractional angular transform and fractional Fourier transform

Tian Qiu[1,2], Wei-Hua Dai[3], Su-Hua Chen[2,*], Hang Zhou[2], Li-Hua Gong[2]

[1]Department of Mathematics, Nanchang University, Nanchang 330031, China

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

[3]School of Computer Science and Engineering, Northeastern University, Shenyang, 110169, China

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

By combining fractional Fourier transform with discrete fractional angular transform, a double-image encryption algorithm is designed. The discrete cosine transform is performed on two grayscale images to generate a spectrum image, and then the generated spectrum image is compressed into an image with Zigzag scanning. The compressed image is processed with the discrete fractional angular transform, and then fractional Fourier transform and double random phase coding are executed on the image. The DNA operation controlled by chaotic system is introduced to change the pixel values. Finally, the ciphertext image is obtained through bit-level permutation and pixel adaptive diffusion. The statistical information of the plaintext images is employed as the input of the SHA-256 to calculate the initial conditions of the chaotic map. Simulation experiments demonstrate that the double-image encryption algorithm can effectively reduce the correlation among adjacent pixels of the plaintext images.

Keywords: chaotic system, fractional transform, discrete fractional angular transform, double-image encryption.

1. Introduction

Under the environment of big data, the security of the image data transmission has become an important topic. Gao *et al*. proposed a new nonlinear chaotic encryption algorithm to solve the problem of relatively small key space in the 1D chaotic image encryption algorithm [1]. Zhu *et al*. realized the bit-level permutation of images with Logistic map, where the bit-level permutation operation could change the pixel posi-

tions of images and the pixel values [2]. Combining the improved Logistic map with the butterfly structure, HANIS *et al*. designed an image encryption algorithm to enhance the security of the cryptographic system [3]. ZHOU *et al*. proposed an image encryption scheme based on a simple and effective cascaded chaotic map and obtained excellent encryption performance [4]. To improve the encryption speed, TALHAOUI *et al*. designed an encryption scheme utilizing a novel 1D chaotic map [5]. It was found that low-dimensional chaotic systems are vulnerable to attacks because of small key space [6]. Compared with low-dimensional chaotic systems, high-dimensional ones possess multiple variables and parameters, which own a more complex chaotic behavior and larger chaotic space.

For larger key space, GAO *et al*. presented an image encryption algorithm with a combination of hyperchaotic maps to change the pixel values [7]. Relying on the high-dimensional Lorenz chaotic system and the perceptron model, WANG *et al*. proposed an image encryption scheme to effectively solve the periodic state problem caused by a discrete chaotic system [8]. However, it is reported that some image encryption schemes based on single high-dimensional chaotic systems also face security risks. DNA computing with high storage density, strong parallelism and low power consumption [9] can enhance the security of image encryption together with the chaotic system. WEI *et al*. combined DNA sequence addition with Chen's chaotic system to realize image encryption and achieved good security [10]. Based on DNA encoding, SUN designed an image encryption algorithm with strong security [11]. HU *et al*. proposed an image encryption scheme based on high-dimensional chaotic system and DNA sequence loop operation [12]. YU *et al*. described a double-image encryption algorithm under the spatiotemporal chaos and DNA operation techniques to accelerate the encryption efficiency [13]. The image encryption scheme utilizing memristive hyperchaotic system, cellular automata and DNA sequence operations showed good encryption performance [14].

Image encryption algorithms in the transform domain usually have better anti-interference performance and higher security. LIU *et al*. devised an image encryption scheme with fractional Fourier transform and pixel scrambling operation based on double random phase encoding [15]. JI *et al*. investigated an image encryption algorithm with discrete cosine transform and related scrambling diffusion [16]. With the increase of the image transmission data, usually the single image encryption algorithms are of low efficiency to meet the real-life applications. Naturally, double-image and multi-image encryption methods have emerged [17, 18]. A double-image encryption algorithm was devised with the chaotic pixel scrambling technology in the discrete multi-parameter fractional transform domain [19]. Based on DNA encoding and chaotic systems, ZHANG *et al*. described a multi-image encryption scheme to improve the encryption efficiency [20]. ZHOU *et al*. designed a double-image compression encryption scheme, which effectively encrypt two images with high security and robustness [21]. SUI *et al*. presented a nonlinear double-image encryption algorithm based on the Logistic map, which effectively resists the chosen-plaintext attack [22]. When to encrypt multiple images, compression is usually necessary to reduce the transmission burden, which

may result in a loss of partial image information and reduce the quality of the decryption image. To solve this problem, CHEN *et al*. designed an image encryption algorithm by combining wavelet transform, feature fusion techniques with phase truncation and phase retention in the Fresnel domain [23]. ZHANG *et al*. presented a double-image encryption method by constructing a new discrete fraction random transform based on 2D Logistic map and Chirikov standard map [24].

Based on the above discussions, it can be found that it is necessary to develop a fast and secure image encryption algorithm with large key space, which can effectively avoid the fragility of linear encryption methods. Therefore, a double color images encryption algorithm based on discrete fractional angular transform and discrete Fourier transform is designed. Image compression is achieved through discrete cosine transform, and the nonlinear DNA technology accelerates the encryption speed and further enhances the security of the cryptographic system.

The rest of this paper is organized as follows. Section 2 introduces the relevant knowledge. In Section 3, the proposed image encryption algorithm is described in detail. Simulation results and security analyses are presented in Section 4. Finally, a conclusion is reached in Section 5.

2. Preliminary knowledge

2.1. Chaotic systems

The Logistic map is a very common 1D chaotic system,

$$x_{n+1} = \mu x_n(x_n + 1), \qquad x_0 \in (0, 1) \tag{1}$$

where μ is the system parameter of the chaotic map, $\mu \in [3.57, 4]$.

With two Logistic maps, a 2D Logistic map can be formed, whose chaos behavior is more complicated than Logistic map.

$$\begin{cases} W_{n+1} = \lambda_1 W_n(1 - W_n) + \gamma_1 W_n^2 \\ U_{n+1} = \lambda_2 U_n(1 - U_n) + \gamma_2(W_n + W_n U_n) \end{cases} \tag{2}$$

If the initial values W_0 and U_0 are in the range of (0, 1), the control parameters are $2.75 < \lambda_1 < 3.4$, and $2.7 < \lambda_2 < 3.45$, and $0.15 < \gamma_1 < 0.21$, and $0.13 < \gamma_2 < 0.15$, then the system will be in a chaotic state.

2.2. Discrete cosine transform

The discrete cosine transform of a 2D image $f(m', n')$ of size $M \times N$ is defined as [16]:

$$F(\delta, \sigma) = \frac{1}{\sqrt{MN}} C(\delta)C(\sigma) \sum_{m'=0}^{M-1} \sum_{n'=0}^{N-1} f(m', n') \cos\frac{(2m'+1)\pi\delta}{2M} \cos\frac{(2n'+1)\pi\sigma}{2N} \tag{3}$$

where:

$m', \delta = 0, 1, ..., M-1$

$n', \sigma = 0, 1, ..., N-1$

$$C(\delta) = \begin{cases} 1/\sqrt{2}, & \delta = 0 \\ 1, & \delta \neq 0 \end{cases}$$

Its inverse transform is

$$f(m', n') = \frac{1}{\sqrt{MN}} \sum_{\delta=0}^{M-1} \sum_{\sigma=0}^{N-1} C(\delta) C(\sigma) F(\delta, \sigma) \cos\frac{(2m'+1)\pi\delta}{2M} \cos\frac{(2n'+1)\pi\sigma}{2N} \tag{4}$$

2.3. Discrete fractional angular transform

Discrete fractional angular transform (DFrAT) is defined by the recursive process of two angles, which can quickly process a signal,

$$\mathbf{L}_N^{\alpha,\beta} = \mathbf{K}_N^{\beta} \mathbf{D}_N^{\alpha} (\mathbf{K}_N^{\beta})^{\mathrm{T}} \tag{5}$$

where T is the transposition operation, $\mathbf{D}_N^{\alpha} = \mathrm{diag}\{\lambda_k^{\alpha}\}_{k=0, 1, ..., N-1}$ is the diagonal matrix and $\lambda_k^{\alpha} = \exp(-jk\alpha)$ is the eigenvalue of the DFrAT. $\mathbf{K}_N^{\beta}$ is composed of eigenvectors and angles of the DFrAT.

2.4. Fractional Fourier transform

The definition of fractional Fourier transform (FrFT) of order p is

$$\mathrm{FrFT}_p\{f(x)\} = \int_{-\infty}^{+\infty} K_p(x, u) f(x)\,\mathrm{d}x \tag{6}$$

$$K_p(x, u) = \begin{cases} \sqrt{\dfrac{1 - j\cot\alpha}{2\pi}} \exp\left(j\dfrac{x^2+u^2}{2}\cot\alpha - j\dfrac{xu}{\sin\alpha}\right), & \alpha \neq k\pi \\ \delta(u-x), & \alpha = 2k\pi \\ \delta(u+x), & \alpha = (2k+1)\pi \end{cases} \tag{7}$$

where $K_p(x, u)$ is the kernel function of the fractional Fourier transform of order p, while FrFT_p represents the fractional Fourier transform of order p. Its inverse transform is

$$f(x) = \int_{-\infty}^{+\infty} \mathrm{FrFT}_p\{f(x)\} K_{-p}(x, u)\,\mathrm{d}u \tag{8}$$

3. Double-image encryption algorithm

The encryption process of the proposed double-image encryption algorithm is shown in Fig. 1. The specific image encryption steps are listed as follows.

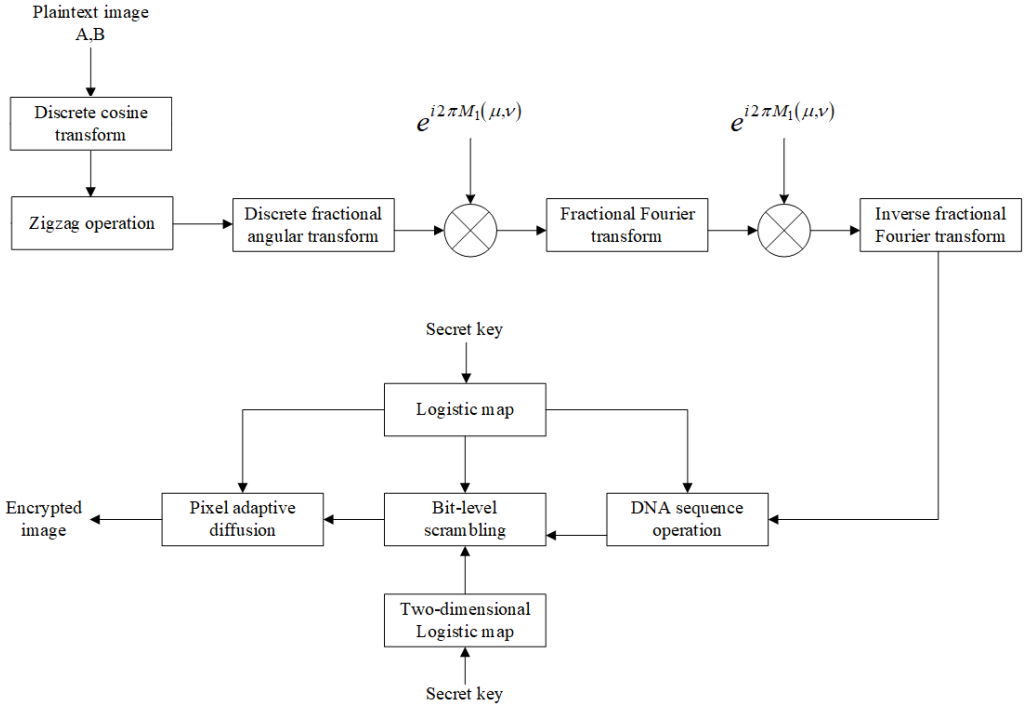


Fig. 1. Double-image encryption algorithm based on chaotic system and FrFT.

Step 1: The maximal and the minimal pixel gray values of two plaintext images and the frequency of each gray value are concatenated into a string. And then a binary sequence of length 256 is obtained by the SHA-256 with the string. The sequence is divided into binary sequences h_1, h_2, h_3, ..., h_{32} of length 8. And the initial values of the chaotic system can be obtained as follows:

$$h = h_1, h_2, h_3, ..., h_{32} \tag{9}$$

$$W_0 = \zeta_0 + \frac{h_1 \oplus h_2 \oplus h_3 \oplus ... \oplus h_{11}}{256} \tag{10}$$

$$U_0 = \zeta_1 + \frac{h_{12} \oplus h_{13} \oplus h_{14} \oplus ... \oplus h_{22}}{256} \tag{11}$$

$$x_0 = \zeta_2 + \frac{h_{23} \oplus h_{24} \oplus h_{25} \oplus ... \oplus h_{32}}{256} \tag{12}$$

Step 2: Zigzag operation is performed on two plaintext images of size $N \times N$.

1) Discrete cosine transform is conducted on the two plaintext images to obtain the spectrum image.

2) Zigzag scanning is performed on each spectrum to obtain two 1D matrices, and they are compressed proportionally and recombined into a 2D matrix of size $N \times N$.

Step 3: The DFrAT is performed on matrix **I** to obtain $f(x, y)$.

Step 4: In the FrFT domain, double random phase encoding operation is executed on $f(x, y)$.

1) $h(x, y) = f(x, y)\exp\{j2\pi\mathbf{M}_1(x, y)\}$ can be obtained by multiplying $f(x, y)$ and the first random phase mask $\exp\{j2\pi\mathbf{M}_1(x, y)\}$, and then the FrFT is performed on $h(x, y)$ to produce $H(u, v)$.

2) $G(u, v) = H(u, v)\exp\{j2\pi\mathbf{M}_2(x, y)\}$ can be acquired by multiplying $H(u, v)$ and the second random phase mask $\exp\{j2\pi\mathbf{M}_2(x, y)\}$, and then the inverse FrFT is performed on $G(u, v)$ to generate the complex-valued image *P*. Among them, two phase masks can be generated by the 2D Logistic map. Two chaotic sequences $X = = \{X_1, X_2, ..., X_{N \times N + L}\}$ and $Y = \{Y_1, Y_2, ..., Y_{N \times N + L}\}$ of length $N \times N + L$ can be generated by the 2D Logistic map with initial conditions of W_0 and U_0. Discarding the first L elements, a new sequence $X' = \{X'_1, X'_2, ..., X'_{N \times N}\}$ can be obtained. Then sequence X' is converted into a 2D matrix $\mathbf{M}_1(x, y)$. 2D matrix $\mathbf{M}_2(x, y)$ can be obtained with similar operation on sequence *Y*.

Step 5: The DNA sequence encryption is operated on the complex-valued image with the chaotic sequence.

1) The chaotic sequences *X*, *Y*, *Z*, *K* of length $3N$ can be produced by setting x_0, y_0, z_0, k_0 as the initial values and the iterations of Logistic map. To avoid the transient effect, the first N elements of each sequence will be deleted, and then four chaotic sequences of length $2N$ are converted into eight sub-chaotic sequences x_1, x_2, y_1, y_2, z_1, z_2, k_1, k_2, of length N. Then they are respectively transformed into integer sequences with the following equations:

$$\eta' = \text{round}(10^{14}\eta)\bmod 256, \quad \eta \in \{x_1, x_2, y_1, y_2, z_1, z_2\} \tag{13}$$

$$g' = \text{round}(10^{14}g)\bmod 3, \quad g \in \{k_1, k_2\} \tag{14}$$

To obtain two new chaotic sequences W_1 and W_2 the q-th of the sequence k_1 is utilized to determine q-th of W_1 extracted from the sequences x_1, y_1, z_1. Similarly, sequence W_2 is generated.

$$W_l(i) = \begin{cases} x'_l(i), & k'_l = 0 \\ y'_l(i), & k'_l = 1 \\ z'_l(i), & k'_l = 2 \end{cases} \tag{15}$$

where $i = 1, 2, ..., N$, and $l = 1, 2$.

Each element of the generated chaotic sequences W_1 and W_2 is represented by an 8-bit binary, and it is converted to a string type. Then W_1 and W_2 are converted into the DNA sequences W_1' and W_2' with the DNA encoding rule 2, respectively.

2) Each element in the complex-valued image P represented by an 8-bit binary is then converted into the corresponding DNA sequence $P'(i,j)$ with the DNA encoding rule 1. The DNA complementary operations are performed on $P'(i,j)$ and W_1' to generate a new DNA sequence $e_1(i,j)$.

$$e_1(i,j) = \begin{cases} \text{ComR6}(P'(i,j)), & W_1' = \text{A} \\ \text{ComR2}(P'(i,j)), & W_1' = \text{C} \\ \text{ComR1}(P'(i,j)), & W_1' = \text{G} \\ \text{ComR4}(P'(i,j)), & W_1' = \text{T} \end{cases} \tag{16}$$

where $i, j = 1, 2, ..., N$, and ComRn represent the n-th complementary rule.

3) DNA addition operation is performed on the DNA sequences $e_1(i)$ and W_2' by the DNA encoding rule 2.

$$b(i) = e_1(i) + W_2'(i) \tag{17}$$

4) The DNA sequence $b(i)$ is decoded by the DNA encoding rule 5.

Step 6: The images are scrambled with the bit-level permutation method.

1) Chaotic sequences $G = \{G_1, G_2, ..., G_{N\times N+L}\}$ and $H = \{H_1, H_2, ..., H_{N\times N+L}\}$ of length $N \times N + L$ can be obtained by iterating the 2D Logistic map with initial values of q_0 and w_0. By discarding the first L values of each sequence, a new sequence $G' = \{G_1', G_2', ..., G_{N\times N}'\}$ can be obtained and then it is converted into an integer sequence with Eq. (13).

2) Each element of image O of size $N \times N$ is represented by an 8-bit binary to generate a matrix $\mathbf{O}'$ of size $(N \times N) \times 8$. The cyclic shift operation is taken for the matrix $\mathbf{O}'$.

$$\mathbf{B} = \text{cirshift}(\mathbf{A}, \kappa, m) \tag{18}$$

where $\mathbf{B}$ represents the matrix after the cyclic shift operation, $\mathbf{A}$ represents the matrix to be shifted, κ represents the number of shifts. m taking 1 represents a column shift, while m taking 2 represents a row shift. A negative number m indicates the inverse operation.

The row elements of matrix $\mathbf{O}'$ are scrambled, and matrix $\mathbf{G}'$ is applied to control the bit number of the moved elements.

$$\mathbf{O}''(k,:) = \text{cirshift}(\mathbf{O}'(k,:), \mathbf{G}'(k), 2) \tag{19}$$

where $k = 1, 2, ..., N \times N$, and $\mathbf{O}''(k,:)$ and $\mathbf{O}'(k,:)$ are the row elements of the matrices after shifting and before shifting, respectively, and $\mathbf{G}'(k)$ is the bit number of the moved elements.

Similarly, the elements in the j-th column of matrix $\mathbf{O}''$ are scrambled, and the bit number of the shifted column is controlled by matrix $\mathbf{H}'(j)$.

$$\mathbf{O}''(:, j) = \text{cirshift}(\mathbf{O}'(:, j), \mathbf{H}'(j), 1) \tag{20}$$

Step 7: The images are diffused by the pixel adaptive diffusion method.
The modular operation of pixel adaptive diffusion is defined as:

$$C(i,j) = \begin{cases} (\mathbf{O}''(i,j) + \mathbf{O}''(N,N) + T(i,j)) \bmod 256, & i = 1,\ j = 1 \\ (\mathbf{O}''(i,j) + C(N, j-1) + T(i,j)) \bmod 256, & i = 1,\ j \neq 1 \\ (\mathbf{O}''(i,j) + C(i-1, j) + T(i,j)) \bmod 256, & i \neq 1 \end{cases} \tag{21}$$

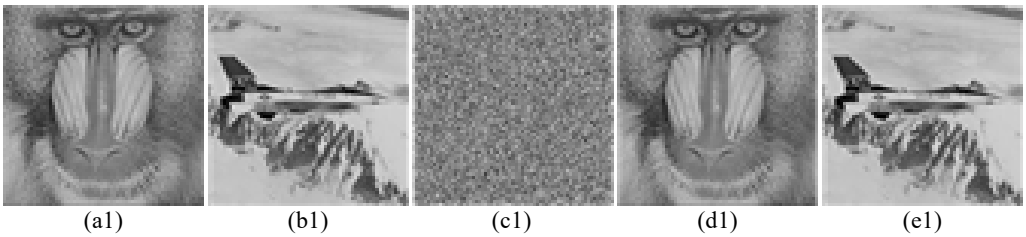
where $T(i, j)$ is the chaotic sequence generated by the Logistic map, $\mathbf{O}''(i, j)$ is the image obtained after bit-level permutation, and $C(i, j)$ is the encryption image.

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

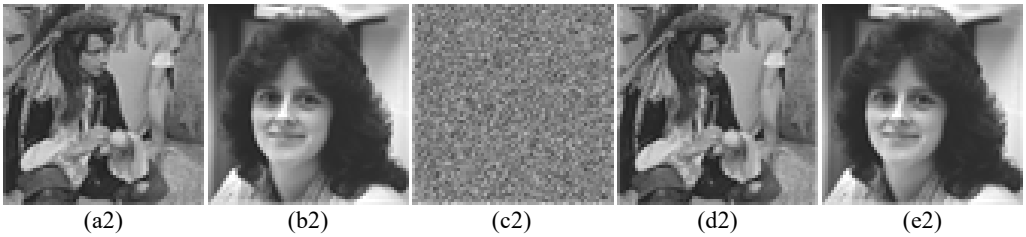
4. Simulation results and performance analyses

4.1. Encryption and decryption results

A series of experiments are carried out on MATLAB 2019(a) software to verify the feasibility of the algorithm. The grayscale images *Baboon* and *Plane* of size 256 × 256 are chosen as the test images, as shown in Fig. 2(a1) and (b1). The images *Man* and *Woman* are the other test images. The parameters W_0, U_0, λ_1, λ_2, γ_1 and γ_2 of the 2D Logistic map are 0.2212, 0.3212, 2.99, 3.39, 0.19, 0.14, respectively, while the pa-



(a1) (b1) (c1) (d1) (e1)



(a2) (b2) (c2) (d2) (e2)

Fig. 2. (a1) Original image *Baboon*. (b1) Original image *Plane*. (c1) Encryption image for (a1) and (b1). (d1) Decryption image *Baboon*. (e1) Decryption image *Plane*. (a2) Original image *Man*. (b2) Original image *Woman*. (c2) Encryption image for (a2) and (b2). (d2) Decryption image *Man*. (e2) Decryption image *Woman*.

rameters x_0 and μ of the Logistic map are 0.412 and 3.97, respectively. a and p take 0.2 and 0.3, respectively. As shown in Fig. 2, it is easy to know that the proposed image encryption algorithm is feasible.

4.2. Histogram

Figures 3(a1) and (b1) ((a2) and (b2)) show the histograms of plaintext images *Baboon* and *Plane* (*Man* and *Woman*). Figures 3(c1) and (c2) are the histograms of their corresponding encryption images. The DNA sequence operation, bit-level permutation and pixel adaptive diffusion operations have fully changed the pixel values of the encryption images, making them almost evenly distributed within the range of 0...255. As shown in Fig. 3 which exhibits no similarity in appearance with that of the original images. To further analyze the histogram uniformity, a chi-square test is introduced.

$$\chi^2 = \sum_{L=0}^{255} \frac{(v_L - E)^2}{E} \tag{22}$$

where v_L is the number of pixel values as pixel gray value L observed in the encryption images, and E is the expected number of pixel values. Table 1 records the chi-square

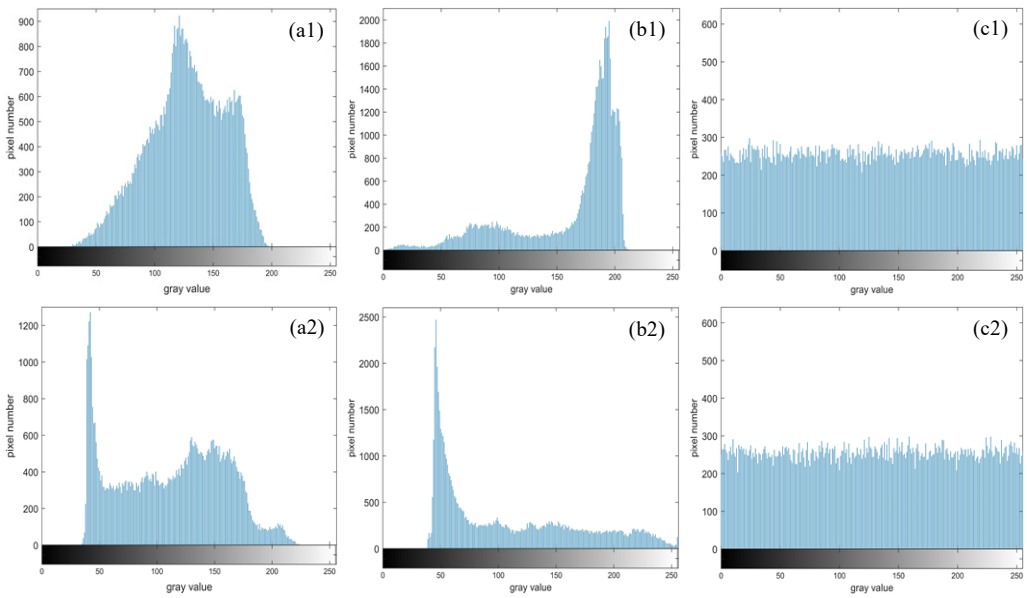


Fig. 3. Histogram of (a1) image *Baboon*, (b1) image *Plane*, (c1) ciphertext image *Baboon–Plane*; and histogram of (a2) image *Man*, (b2) image *Woman*, (c2) ciphertext image *Man–Woman*.

T a b l e 1. Results of chi-square test.

Ciphertext image	χ^2-value	P-value	Results
Baboon–Plane	264.6953	0.3251	Accepted
Man–Woman	236.3281	0.7934	Accepted

T a b l e 2. Correlation coefficient between the adjacent pixels of images.

Algorithm	Image	Horizontal	Vertical	Diagonal
	Baboon	0.8688	0.8996	0.8191
	Plane	0.9187	0.9142	0.8526
Proposed algorithm	Ciphertext image	–0.0073	0.0063	–0.0080
[20]	Ciphertext image	–0.0324	0.0124	0.0215
[24]	Ciphertext image	0.0301	–0.0221	–0.0339
	Man	0.9569	0.9358	0.9096
	Woman	0.9921	0.9913	0.9862
Proposed algorithm	Ciphertext image	–0.0018	0.0146	–0.0079
[20]	Ciphertext image	0.0221	0.0188	0.0284
[24]	Ciphertext image	0.0114	0.0126	–0.0021

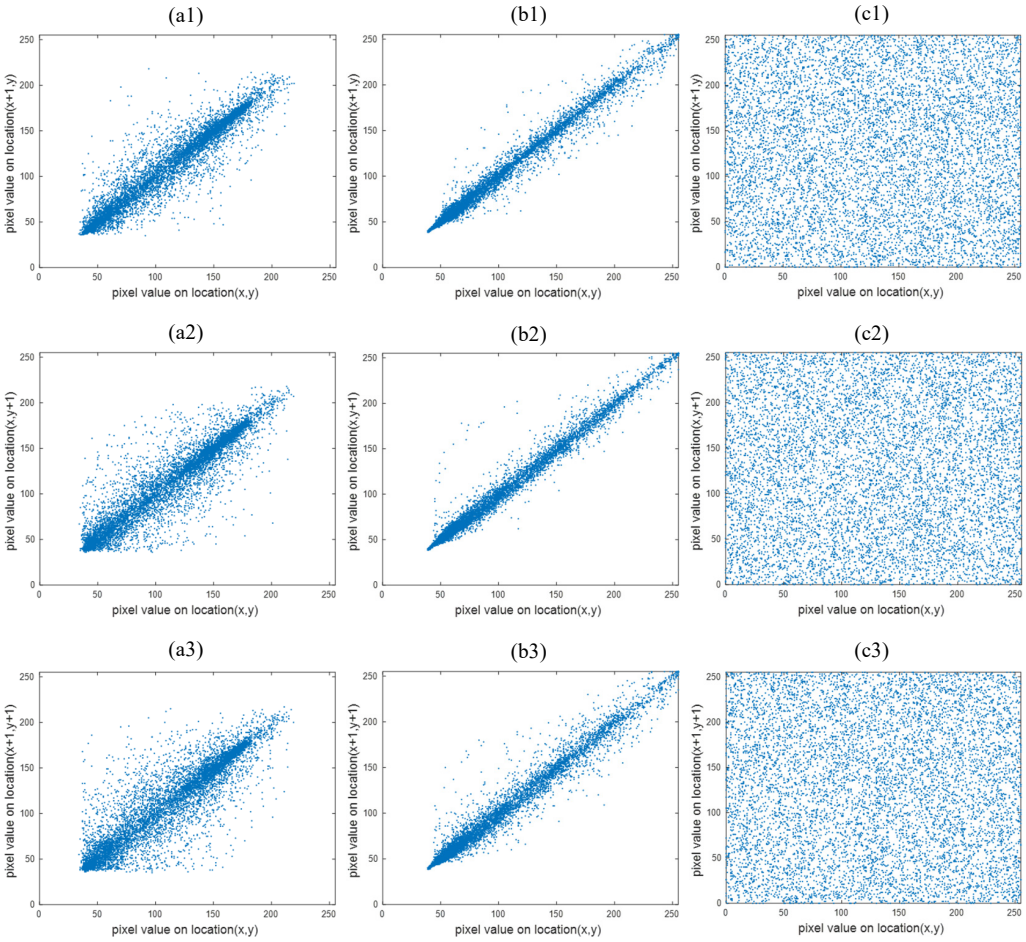


Fig. 4. Correlation distribution of different images.

values of the two sets of ciphertext images, which are all lower than the critical value of 293.247.

4.3. Pixel correlation

Table 2 shows the correlation coefficients between adjacent pixels in horizontal, vertical and diagonal directions for plaintext image and ciphertext one. Figures 4(a1)–(a3) ((b1)–(b3)) are the adjacent pixel distributions of the plaintext image *Man* (*Woman*) in three directions. Apparently, the correlation coefficient between adjacent pixels of the ciphertext image is greatly reduced compared with that of the plaintext image, and the performance of the proposed scheme is better than that of other schemes.

4.4. Information entropy

Table 3 lists the entropy values of two sets of test images after encryption. From Table 3, it can be seen that the entropy values of the encryption images are close to the ideal value of 8 bits, and its local Shannon entropy meets the critical values.

4.5. Differential attack

Differential attack is considered to be the most common way to destroy many image encryption algorithms. The NPCR and the UACI values, respectively shown in Tables 4 and 5, are within the ideal range.

T a b l e 3. The results of Shannon entropy and local Shannon entropy (bit).

Test images	Information entropy	Local entropy	Critical value of local Shannon entropy		
			$h_{\text{left}}^{1*0.05} = 7.9019$	$h_{\text{left}}^{1*0.01} = 7.9017$	$h_{\text{left}}^{1*0.001} = 7.9015$
			$h_{\text{right}}^{1*0.05} = 7.9030$	$h_{\text{right}}^{1*0.01} = 7.9032$	$h_{\text{right}}^{1*0.001} = 7.9034$
Boat–Lax	7.9970	7.9027	Pass	Pass	Pass
Baboon–Plane	7.9971	7.9019	Pass	Pass	Pass

T a b l e 4. NPCR values of the ciphertext images.

Ciphertext images	NPCR [%]	Critical values of NPCR		
		$N_{0.05}^{*} = 99.5693\%$	$N_{0.01}^{*} = 99.5527\%$	$N_{0.001}^{*} = 99.5341\%$
Man–Woman	99.65	Pass	Pass	Pass
Baboon–Plane	99.66	Pass	Pass	Pass

T a b l e 5. UACI values of the ciphertext images.

Ciphertext images	UACI [%]	Critical values of UACI		
		$U_{0.05}^{*-} = 33.2824\%$	$U_{0.01}^{*-} = 33.2255\%$	$U_{0.001}^{*-} = 33.1594\%$
		$U_{0.05}^{*+} = 33.6447\%$	$U_{0.01}^{*+} = 33.7016\%$	$U_{0.001}^{*+} = 33.7677\%$
Man–Woman	33.55	Pass	Pass	Pass
Baboon–Plane	33.58	Pass	Pass	Pass

$$\mathrm{NPCR}(C_1, C_2) = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} D(i, j) \times 100\% \tag{23}$$

$$\mathrm{UACI}(C_1, C_2) = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} \frac{\left| C_1(i, j) - C_2(i, j) \right|}{255} \times 100\% \tag{24}$$

$$D(i, j) = \begin{cases} 0, & C_1(i, j) = C_2(i, j) \\ 1, & C_1(i, j) \neq C_2(i, j) \end{cases} \tag{25}$$

where $C_1(i, j)$ and $C_2(i, j)$ are ciphertext images before and after changing the pixel value at location (i, j) in the plaintext image.

4.6. Key sensitivity

The main keys in the algorithm are W_0, U_0, x_0, the initial values of the chaotic system, and the order p of the FrFT. Figures 5(a1) and (b1) ((c1) and (d1); (a2) and (b2); (c2) and (d2)) are the decryption images when the key $W_0(U_0; x_0; p)$ is changed from 0.2212 to $0.2212 + 10^{-15}$ (0.3212 to $0.3212 + 10^{-15}$; 0.4212 to $0.4212 + 10^{-15}$; 0.3 to $0.3 + 10^{-3}$) with other keys unchanged. It is shown that any slight change in the secret key will fail the decryption. Thus the proposed scheme is sensitive to the secret key.

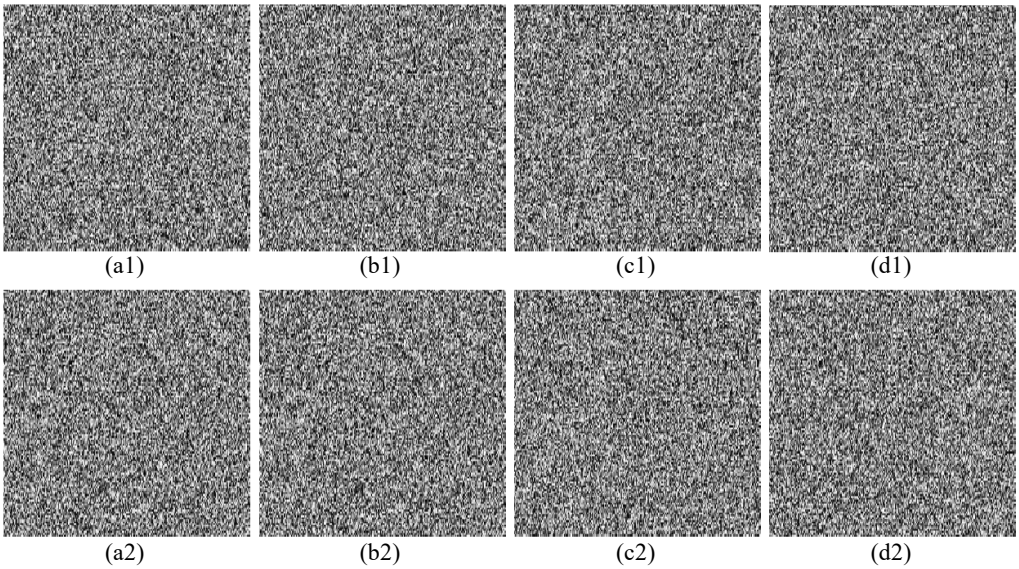


Fig. 5. Decryption images *Boat* and *Lax* with wrong keys: (a1, b1) $W_0 = 0.2212 + 10^{-15}$, (c1, d1) $U_0 = = 0.3212 + 10^{-15}$, (a2, b2) $x_0 = 0.4212 + 10^{-15}$, (c2, d2) $p = 0.3 + 10^{-3}$.

The calculation accuracy of the initial values of the chaotic system is 10^{-15}, while that of the fractional order p is 10^{-3}. Therefore, the total key space of the algorithm is about 2^{154}, which cannot be cracked by the brute-force attack.

4.7. Noise attack

Gaussian noises of different intensities are added to the ciphertext image, and then the correct keys are utilized for decryption. When the noise intensity coefficient is 1 (5;

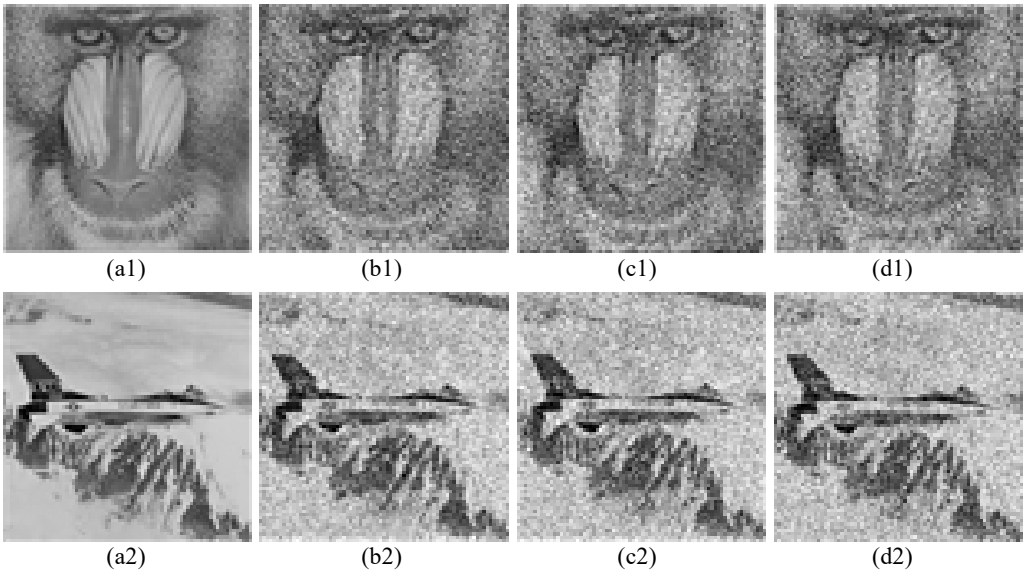


Fig. 6. Decryption images *Baboon* and *Plane* with different noise intensity coefficients: (a1, a2) $k = 1$, (b1, b2) $k = 5$, (c1, c2) $k = 10$, (d1, d2) $k = 15$.

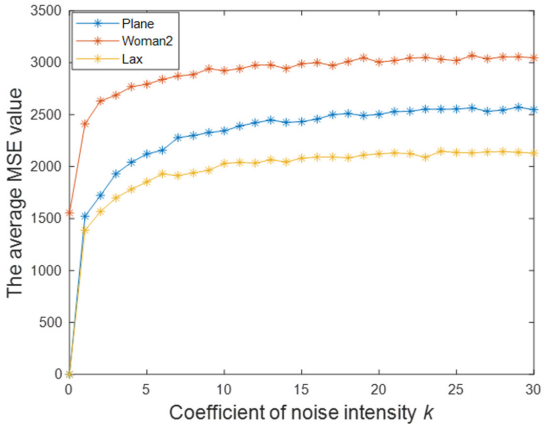


Fig. 7. MSE curves *versus* noise level k.

10; 15), Figs. 6(a1) and (a2) ((b1) and (b2); (c1) and (c2); (d1) and (d2)) are the corresponding decryption images of *Cameraman* and *Lake*, respectively. Figure 7 shows the MSE curve *versus* the intensity of noise.

$$\mathrm{MSE} = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} \left[P(i,j) - Q(i,j) \right]^2 \tag{26}$$

where $P(i, j)$ (or $Q(i, j)$) is the value of the pixel (i, j) in the original (encryption) image, respectively. The quality of decryption image decreases with the increase of noise intensity, however the basic information of the decryption image can still be distinguished. In summary, the proposed double-image encryption algorithm has good robustness against noise attack.

5. Conclusions

By integrating discrete fractional angular transform, fractional Fourier transform, chaotic system, bit-level permutation and pixel adaptive diffusion operation, a double-image encryption scheme is designed. Discrete cosine transform and Zigzag operation are utilized to compress two plaintext images, and then the discrete fractional angular transform is adopted to encrypt the compressed images. The images are further encrypted in the fractional Fourier transform domain with double random phase encoding technology. The DNA sequence operation controlled by the chaotic system changes the pixel values of the images. Bit-level permutation and pixel adaptive diffusion reduce the correlation between image pixels. The key obtained with SHA-256 makes the double-image encryption scheme more secure. The nonlinear DNA sequence operations improve the security to resist the chosen-plaintext attack. Experimental simulation results show that the double-image encryption scheme can effectively encrypt two images simultaneously.

Acknowledgment
This work is supported by the National Natural Science Foundation of China (Grant No. 61861029).

References

[1] GAO H.J., ZHANG Y.S., LIANG S.Y., LI D.Q., *A new chaotic algorithm for image encryption*, Chaos, Solitons and Fractals **29**(2), 2006, pp. 393–399, DOI: 10.1016/j.chaos.2005.08.110.

[2] ZHU Z.L., ZHANG W., WONG K.W., YU H., *A chaos-based symmetric image encryption scheme using a bit-level permutation*, Information Sciences **181**(6), 2011, pp. 1171–1186, DOI: 10.1016/j.ins.2010.11.009.

[3] HANIS S., AMUTHA R., *A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure*, Nonlinear Dynamics **95**(1), 2019, pp. 421–432, DOI: 10.1007/s11071-018-4573-7.

[4] ZHOU Y.C., BAO L., CHEN C.L.P., *A new 1D chaotic system for image encryption*, Signal Processing **97**, 2014, pp. 172–182, DOI: 10.1016/j.sigpro.2013.10.034.

[5] TALHAOUI M.Z., WANG X.Y., *A new fractional one dimensional chaotic map and its application in high-speed image encryption*, Information Sciences **550**, 2021, pp. 13–26, DOI: 10.1016/j.ins.2020.10.048.

[6] PONOMARENKO V.I., PROKHOROV M.D., *Extracting information masked by the chaotic signal of a time -delay system*, Physical Review E **66**(2), 2002, article no. 026215, DOI: 10.1103/PhysRevE.66.026215.

[7] GAO T.G., CHEN Z.Q., *A new image encryption algorithm based on hyper-chaos*, Physics Letters A **372**(4), 2008, pp. 394–400, DOI: 10.1016/j.physleta.2007.07.040.

[8] WANG X.Y., YANG L., LIU R., KADIR A., *A chaotic image encryption algorithm based on perceptron model*, Nonlinear Dynamics **62**(3), 2010, pp. 615–621, DOI: 10.1007/s11071-010-9749-8.

[9] WANG X.Y., LI P., ZHANG Y.Q., LIU L.Y., ZHANG H.Z., WANG X.K., *A novel color image encryption scheme using DNA permutation based on the Lorenz system*, Multimedia Tools and Applications **77**(5), 2018, pp. 6243–6265, DOI: 10.1007/s11042-017-4534-z.

[10] WEI X.P., GUO L., ZHANG Q., ZHANG J.X., LIAN S.G., *A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system*, Journal of Systems and Software **85**(2), 2012, pp. 290–299, DOI: 10.1016/j.jss.2011.08.017.

[11] SUN S.L., *A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling*, IEEE Photonics Journal **10**(2), 2018, article no. 7201714, DOI: 10.1109/JPHOT.2018.2817550.

[12] HU T., LIU Y., GONG L.H., OUYANG C.J., *An image encryption scheme combining chaos with cycle operation for DNA sequences*, Nonlinear Dynamics **87**(1), 2017, pp. 51–66, DOI: 10.1007/s11071-016-3024-6.

[13] YU W., LIU Y., GONG L., TIAN M., TU L., *Double-image encryption based on spatiotemporal chaos and DNA operations*, Multimedia Tools and Applications **78**(14), 2019, pp. 20037–20064, DOI: 10.1007/s11042-018-7110-2.

[14] CHAI X.L., GAN Z., YANG K., CHEN Y.R., LIU X.X., *An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations*, Signal Processing: Image Communication **52**, 2017, pp. 6–19, DOI: 10.1016/j.image.2016.12.007.

[15] LIU Z.J., LI S., LIU W., WANG Y.H., LIU S.T., *Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding*, Optics and Lasers in Engineering **51**(1), 2013, pp. 8–14, DOI: 10.1016/j.optlaseng.2012.08.004.

[16] JI X.Y., BAI S., ZHU G.B., YAN B., *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.

[17] SINGH H., *Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain*, Optica Applicata **47**(4), 2017, pp. 557–578.

[18] YANG Y.G., GUAN B.W., ZHOU Y.H., SHI W.M., *Double image compression-encryption algorithm based on fractional order hyper chaotic system and DNA approach*, Multimedia Tools and Applications **80**(1), 2021, pp. 691–710, DOI: 10.1007/s11042-020-09779-5.

[19] SHAN M.G., CHANG J., ZHONG Z., HAO B.G., *Double image encryption based on discrete multiple -parameter fractional Fourier transform and chaotic maps*, Optics Communications **285**(21–22), 2012, pp. 4227–4234, DOI: 10.1016/j.optcom.2012.06.023.

[20] ZHANG Q., LIU L.L., WEI X.P., *Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps*, AEU - International Journal of Electronics and Communications **68**(3), 2014, pp. 186–192, DOI: 10.1016/j.aeue.2013.08.007.

[21] ZHOU N.R., JIANG H., GONG L.H., XIE X.W., *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.

[22] SUI L.S., DU C., ZHANG X., TIAN A., ASUNDI A., *Double-image encryption based on interference and logistic map under the framework of double random phase encoding*, Optics and Lasers in Engineering **122**, 2019, pp. 113–122, DOI: 10.1016/j.optlaseng.2019.06.005.

[23] CHEN X.D., LIU Q., WANG J., WANG Q.H., *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.

[24] ZHANG Y.S., XIAO D., *Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform*, Optics and Lasers in Engineering **51**(4), 2013, pp. 472–480, DOI: 10.1016/j.optlaseng.2012.11.001.

Received April 22, 2022
in revised form June 4, 2022