

# Image Encryption Algorithm Based on Compressive Sensing and Fractional DCT via Polynomial Interpolation

Ya-Ru Liang<sup>1</sup>      Zhi-Yong Xiao<sup>2</sup>

<sup>1</sup> School of Engineering, Jiangxi Agricultural University, Nanchang 330045, China

<sup>2</sup> School of Software, Jiangxi Agricultural University, Nanchang 330045, China

**Abstract:** Based on compressive sensing and fractional discrete cosine transform (DCT) via polynomial interpolation (PI-FrDCT), an image encryption algorithm is proposed, in which the compression and encryption of an image are accomplished simultaneously. It can keep information secret more effectively with low data transmission. Three-dimensional piecewise and nonlinear chaotic maps are employed to obtain a generating sequence and the exclusive OR (XOR) matrix, which greatly enlarge the key space of the encryption system. Unlike many other fractional transforms, the output of PI-FrDCT is real, which facilitates the storage, transmission and display of the encrypted image. Due to the introduction of a plain-image-dependent disturbance factor, the initial values and system parameters of the encryption scheme are determined by cipher keys and plain-image. Thus, the proposed encryption scheme is very sensitive to the plain-image, which makes the encryption system more secure. Experimental results demonstrate the validity and the reliability of the proposed encryption algorithm.

**Keywords:** Compressive sensing, fractional discrete cosine transform (DCT) via polynomial interpolation, image encryption, three-dimensional piecewise and nonlinear chaotic maps, real-valued output.

## 1 Introduction

With the rapid development of network communication and multimedia technologies, information can be easy to obtain via the Internet. Correspondingly, however, the insecurity of information arises because of the possibilities of data tampering and theft. In this context the way information is expressed is through text, image, video or speech. An image is amongst the most important means of expressing information due to its comprehensiveness and intuitiveness. Thus, image encryption is necessary so as to resist illegal access to data. Encryption methods based on different transforms and scrambling techniques have been proposed in various literatures. These transforms include Fourier transform<sup>[1, 2]</sup>, fractional Fourier transform (FrFT)<sup>[3, 4]</sup>, gyrator transform<sup>[5]</sup>, Hartley transform<sup>[6]</sup>, Mellin transform<sup>[7]</sup>, random transform<sup>[8]</sup>, etc. For example, Unnikrishnan et al.<sup>[9]</sup> outlined an optical image encryption using FrFT, in which a primary image was encoded to stationary white noise with the fractional orders as the cipher keys. In order to enlarge the key space, an image encryption algorithm based on the multiple-parameter FrFT<sup>[10]</sup> was introduced and showed superior robustness to blind decryption compared with other methods that existed.

The pixel scrambling and diffusion operation, which can change the positions and values of image pixels randomly, is another kind of encryption method<sup>[11–13]</sup>. An encryption algorithm based on hyper-chaos was presented by Gao and Chen<sup>[14]</sup>. It employed a total image shuffling matrix to shuffle image pixels and combined the states of a hyper-chaotic system to change the grey values of the shuffled-image. Another example of an image encryption scheme using reverse 2-dimensional (2D) chaotic maps and dependent diffusion was found in <sup>[15]</sup>, in which the scrambling and diffusion of pixels were achieved simultaneously. In the above mentioned encryption methods, the volume of encrypted image data was equal to or greater than that of the original image.

In many applications, the real-valued data are necessary and can benefit the digital image processing. However, the output of the encrypted images via the conventional encryption methods are usually complex, which increases the burden of storage and transform. In 2004, a method of reality-preserving treatment for a fractional transform was introduced<sup>[16]</sup>. Subsequently, an image encryption based on the reality-preserving multiple-parameter fractional Fourier transform (MPFRFT) was proposed, in which the parameters of the reality-preserving MPFRFT enhanced the space of keys<sup>[17]</sup>. An image encryption algorithm based on the reality-preserving fractional Mellin transform (RpFrMT) was presented in <sup>[18]</sup>, in which the output of the transform was real and the transform was nonlinear. However, the disadvantages were its floating-point output and data expansion with

Research Article

Manuscript received January 27, 2018; accepted September 3, 2018; published online December 4, 2018

Recommended by Associate Editor Zhi-Jie Xu

© Institute of Automation, Chinese Academy of Sciences and Springer-Verlag GmbH Germany, part of Springer Nature 2018

respect to the original image. In addition, the above mentioned reality preserving transform adopted the same way of transforming, i.e., a reality-preserving transform matrix must be constructed and it lost some properties compared with non-reality preserving fractional transform.

Due to the high redundancy of digital images and the limited sensibility of the human eyes to high frequency image information, a certain degree of distortion of image information is allowed. Thus, much of the literature examines lossy image compression. A spectrum cutting is a kind of lossy data compression method. For example, an optical multi-image encryption based on Fourier transform and fractional Fourier transform was proposed in [19]. It performed the operation of Fourier transform to obtain the distributed spectrum, in which most energy in the frequency domain was centralized in the central part of the spectrum. Then, a spectrum cutting was carried out to allow multiple image to be encrypted into a single one. The popularly known Shannon's sampling theory states that the sampling rate must be at least twice the signal bandwidth to avoid the loss of information while sampling a signal. To reduce the encryption and decryption processing time and the cost of storage and transmission of information, a compression method using high speed sampling, and then encryption is often adopted. This method wastes some sampling resources. In 2006, the theory of compressive sensing or compressive sampling (CS) was proposed in [20–22], which achieved the sampling and compression simultaneously. Afterwards, many researchers have focused on CS-based image and signal processing [23–28]. A compression-combined digital image encryption method based on compressive sensing was proposed by Huang and Sakurai [23], in which the block Arnold scrambling was used to permute the positions of measurements, and encryption and compression were accomplished in one step. However, the security of this method was not so high due to the periodicity of Arnold transform. Although Rachlin and Baron [24] proved that the CS-based encryption scheme cannot achieve perfect security, it is still of interest owing to the high computational complexity of breaking through the security. Subsequently, Mayiami et al. [25] proposed a compressed sensing-based encryption which can achieve Shannon's definition of perfect secrecy subject to a restriction on the number of measurements. An image encryption based on compressive sensing and a double random-phase encoding technique was provided in [26], where the image information was encrypted twice with low data transmission and smaller random phase masks so as to effectively improve information security. Generally, an image encryption based on compressive sensing treats the whole measurement matrix as the key. This renders the key too large to distribute and memorize. A novel image coding scheme was investigated by Hu et al. [27], in which the compression and encryption were achieved simultaneously under a parallel compressive sensing framework. And the measurement matrix was constructed by utiliz-

ing a Logistic-Tent system controlled by four keys. This decreased the burden of storage as compared with a key using the whole measurement matrix.

In this paper, an image encryption algorithm based on CS and fractional discrete cosine transform (DCT) via polynomial interpolation (PI-FrDCT) will be proposed, which can keep information secret more effectively with low data transmission. Firstly, the original image is compressed and encrypted by CS. Then the PI-FrDCT is carried out. The PI-FrDCT is a unitary, real and orthogonal transform, in which a specific sequence, called a generating sequence (GS), has resolved the nonuniqueness of a fractional operator. Three-dimensional piecewise and non-linear chaotic maps are employed to generate the random GS, in which the initial values and system parameters are treated as the cipher keys. Lastly, a simple bitwise exclusive OR (XOR) operation is performed to conceal the distribution property of the encrypted image after PI-FrDCT.

The rest of this paper is organized as follows. Section 2 describes some related work. Section 3 introduces the image encryption and decryption process based on CS and PI-FrDCT. Section 4 gives the experimental results and provides analysis. And the conclusions are drawn in Section 5.

## 2 Related work

### 2.1 CS

CS theory points out that if a signal is sparse in one basis then it can be recovered from a small number of projections onto a second basis that is incoherent with the first [20–22]. Usually natural signals in the time domain are non-sparse, but may be sparse in some transform domains, such as discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT) domains. Consider a 1-D discrete signal  $\mathbf{x}$  with length  $N$ , which may be represented in the  $\Psi$  domain:

$$\boldsymbol{\alpha} = \Psi \mathbf{x}. \quad (1)$$

If only  $K$  of the  $N$  coefficients in  $\boldsymbol{\alpha}$  in (1) are non-zeros,  $K \ll N$ ,  $\mathbf{x}$  is termed as  $K$  sparse signal. The linear measurement process is expressed as

$$\mathbf{y} = \Phi \mathbf{x} = \Phi \Psi' \boldsymbol{\alpha} = \Theta \boldsymbol{\alpha} \quad (2)$$

where ' denotes transposition,  $\Phi$  is a measurement matrix with size  $M \times N$  ( $M < N$ ). And the sensor matrix  $\Theta$  is the product of  $\Psi$  and  $\Psi'$ .

In order to perfectly reconstruct the signal from  $\mathbf{y}$ , the sensor matrix  $\Theta$  satisfies the restricted isometry property (RIP) for any  $K$ -sparse vector  $\mathbf{v}$  meeting (3) [29]:

$$1 - \delta_K \leq \frac{\|\Theta \mathbf{v}\|_2^2}{\|\mathbf{v}\|_2^2} \leq 1 + \delta_K \quad (3)$$

where  $\delta_K$  is the smallest number of the isometry constant  $\delta$  of  $\Theta$ ,  $\delta \in (0, 1)$ .

RIP ensures that  $\Theta$  will not map two different  $K$ -sparse signals into the same set, i.e., the formed matrix by each  $M$  column vector extracted from  $\Theta$  is non-singular.

Meanwhile, the measurement data length  $M$  is restricted by the inequation:

$$M \geq cK \log\left(\frac{N}{K}\right) \quad (4)$$

where  $c$  is a small constant,  $K$  is the sparsity degree.

Since  $\mathbf{x}$  is  $K$ -sparse,  $\mathbf{x}$  can be rebuilt from  $\mathbf{y}$  by solving the optimal problem below:

$$\min \|\alpha\|_0 \text{ subject to } \mathbf{y} = \Theta\alpha. \quad (5)$$

The above problem is optimal in theory. But, it is not feasible numerically because it is an NP-hard problem<sup>[30]</sup>. To overcome this difficulty, some relaxing reconstruction algorithms, such as basis pursuit (BP)<sup>[31]</sup>, total variation (TV)<sup>[32]</sup>, matching pursuit (MP)<sup>[33]</sup>, orthogonal matching pursuit (OMP)<sup>[34]</sup>, smooth  $l_0$  algorithm (SL<sub>0</sub>)<sup>[35]</sup>, have been developed. Since SL<sub>0</sub> not only solves the problem of an intractable computational load of the minimal  $l_0$  search, it also results in an algorithm which is much faster than those algorithms based on minimizing the  $l_1$  norm<sup>[35]</sup>. Thus, SL<sub>0</sub> is adopted in the proposed algorithm.

## 2.2 PI-FrDCT

For a signal of length  $N$ , its fractional DCT (FrDCT) matrix  $\mathbf{C}_\alpha$  is defined as<sup>[36–39]</sup>

$$\begin{aligned} \mathbf{C}_\alpha = 2\text{Re} \left[ \sum_{n=1}^{\frac{N}{2}} \mathbf{U}_n \lambda_n^\alpha \right] &= 2\text{Re} \left[ \sum_{n=1}^{\frac{N}{2}} \mathbf{U}_n e^{j(\varphi_n + 2\pi q_n)\alpha} \right] = \\ &= \sum_{n=1}^{\frac{N}{2}} (\mathbf{A}_n \cos \omega_n \alpha + \mathbf{B}_n \sin \omega_n \alpha) \end{aligned} \quad (6)$$

where  $\alpha$  is the fractional order,  $N$  is an integer multiple of 4,  $\mathbf{U}_n = \mathbf{u}_n \mathbf{u}_n^*$  is a unitary matrix,  $\mathbf{u}_n$  is the  $n$ -th eigenvector of the  $N \times N$  DCT matrix,  $\mathbf{A}_n = 2\text{Re}[\mathbf{U}_n]$ ,  $\mathbf{B}_n = 2\text{Im}[\mathbf{U}_n]$ ,  $\omega_n = \varphi_n + 2\pi q_n$ ,  $0 < \varphi_n < \pi$ ,  $n = 1, 2, \dots, \frac{N}{2}$ ,  $N$  is an integer multiple of 4,  $q_n$  is an arbitrary integer.  $\mathbf{q} = (q_1, q_2, \dots, q_{\frac{N}{2}})$  resolves the nonuniqueness of a fractional operator and is called “the generating sequence” of the FrDCT. The detailed derivation of  $\mathbf{C}_\alpha$  can be found in [36, 38]. The FrDCT inherits all features of DCT, such as having a unique orthonormal basis, the reality preservation, index additivity, and non-periodicity.

To compute  $\mathbf{C}_\alpha$ , one can write an interpolation formula for (6) that allows the construction of  $\mathbf{C}_\alpha$ . The FrDCT matrix via polynomial interpolation is expressed as

$$\mathbf{C}_\alpha = \sum_{r=0}^{N-1} \mathbf{C}_{\alpha_r} l_r(\alpha) \quad (7)$$

where  $\alpha_r$  is considered as the  $r$ -th “fraction”, and  $l_r(\alpha) = \sum_{n=1}^{\frac{N}{2}} (d_{2n-1,r} \cos \omega_n \alpha + d_{2n,r} \sin \omega_n \alpha)$ ,  $\mathbf{D} = \|\mathbf{d}_{nr}\| = \mathbf{H}^{-1}$ ,  $\mathbf{H} = \|\mathbf{h}_{rn}\|$  with  $h_{r,2n-1} = \cos \omega_n \alpha_r$ ,  $h_{r,2n} = \sin \omega_n \alpha_r$ ,  $r = 0, 1, \dots, N-1$ ,  $n = 1, 2, \dots, \frac{N}{2}$ . The detailed derivation of the interpolation formula of  $\mathbf{C}_\alpha$  is demonstrated in [36, 39].

Equation (7) is the general interpolation formula, which gives the FrDCT matrix as a weighted combination of its values at the  $N$  different fractions  $\alpha_r$ .

From (7), the FrDCT via polynomial interpolation (PI-FrDCT)  $\mathbf{S}_\alpha$  of a given sequence  $\mathbf{s}$  can be obtained by

$$\mathbf{S}_\alpha = \sum_{r=0}^{N-1} \mathbf{S}_{\alpha_r} l_r(\alpha). \quad (8)$$

Thus,  $\mathbf{S}_\alpha$  can be obtained by merely evaluating the FrDCTs  $\mathbf{S}_{\alpha_r}$  of  $\mathbf{s}$  for  $N$  different fractions  $\alpha_r$ . The inverse PI-FrDCT of  $\mathbf{S}_\alpha$  can be expressed as

$$\mathbf{s} = \mathbf{C}_{-\alpha} \mathbf{S}_\alpha = \sum_{r=0}^{N-1} \mathbf{C}_{\alpha_r} \mathbf{S}_{\alpha_r} l_r(-\alpha). \quad (9)$$

For simplicity,  $\alpha_r = nr$ ,  $r = 0, 1, \dots, N-1$  and  $n = 1, 2, 3, \dots$  is chosen.

In this paper, the condition number of matrix  $\mathbf{H}$  is calculated for different  $n$  when  $\alpha_r = nr$ . When  $\alpha_r = 5r$ ,  $r = 0, 1, \dots, N-1$ , the coefficient matrix  $\mathbf{H}$  is found not singular and the equation set (7) is well-conditioned. Of course,  $n$  can be set to any other values satisfying (7). Choosing  $\alpha_r = 5r$ ,  $r = 0, 1, \dots, N-1$ , yields

$$\mathbf{C}_\alpha = \sum_{r=0}^{N-1} \mathbf{C}_{5r} l_r(\alpha). \quad (10)$$

At last, The PI-FrDCT of a given sequence  $\mathbf{s}$  can be expressed as

$$\mathbf{S}_\alpha = l_0(\alpha) \mathbf{s} + l_1(\alpha) \mathbf{s}^5 + l_2(\alpha) \mathbf{s}^{10} + \dots + l_{N-1}(\alpha) \mathbf{s}^{5(N-1)} \quad (11)$$

where  $\mathbf{s}$  is the original sequence,  $\mathbf{s}^5$  is the 5th DCT of  $\mathbf{s}$ ,  $\mathbf{s}^{10}$  is the 5th DCT of  $\mathbf{s}^5$ , etc.

From (11), the PI-FrDCT can be completed by merely calculating the multiple DCT of the signal and  $l_r$  with the arguments  $\varphi_n$  of the eigenvalues and the generating sequence  $\mathbf{q} = (q_1, q_2, \dots, q_{\frac{N}{2}})$  due to  $\omega_n = \varphi_n + 2\pi q_n$ . It does not require the calculation of the orthonormal set  $\mathbf{u}_{\pm n}$  of eigenvectors compared with (7), and allows fast computation.

For any fraction  $\alpha$ , one can iterate the DCT algorithm by  $5(N-1)$  times. Since fast algorithms are

available for the DCT, with a computational complexity of  $N \log_2 N$  operations<sup>[33]</sup>, the calculation of  $K$  distinct PI-FrDCTs using (11) has complexity of  $5(N-1) \log_2 N + KN$  operations, instead of the  $KN^2$  operations required for direct calculation. Hence, with the approach of (11), an improvement can be obtained for  $K > 5 \log_2 N$ .

The PI-FrDCT of an image  $F$  can be calculated as follows:

Let  $T \in \mathbf{R}^{M \times N}$  be an intermediate matrix, and be denoted by  $(t_{ij})_{M \times N}$ . The matrices  $G$  and  $F$  are denoted by  $(g_{ij})_{M \times N}$  and  $(f_{ij})_{M \times N}$ , respectively. If they are supposed to be images transformed and to be transformed, respectively, then

$$\begin{cases} t_{i,:} = l_0(\alpha) f_{i,:} + l_1(\alpha) f_{i,:}^5 + l_2(\alpha) f_{i,:}^{10} + \cdots + l_{N-1}(\alpha) f_{i,:}^{5(N-1)}, \\ \quad i = 0, 1, \dots, M-1 \\ g_{:,j} = l_0(\beta) t_{:,j} + l_1(\beta) t_{:,j}^5 + l_2(\beta) t_{:,j}^{10} + \cdots + l_{M-1}(\beta) t_{:,j}^{5(M-1)}, \\ \quad j = 0, 1, \dots, N-1 \end{cases} \quad (12)$$

where  $\alpha$  and  $\beta$  are the fractional orders of row and column, respectively,  $M$  and  $N$  are integer multiples of 4,  $t_{i,:}$  and  $g_{:,j}$  are the  $i$ -th row of the matrix  $T$  and the  $j$ -th column of the matrix  $G$ , respectively, and

$$\begin{aligned} l_r(\alpha) &= \sum_{n=1}^{\frac{N}{2}} (d_{2n-1,r} \cos(\varphi_n + 2\pi p_n) \alpha + d_{2n,r} \sin(\varphi_n + 2\pi p_n) \alpha) \\ l_r(\beta) &= \sum_{n=1}^{\frac{M}{2}} (d_{2n-1,r} \cos(\varphi_n + 2\pi q_n) \beta + d_{2n,r} \sin(\varphi_n + 2\pi q_n) \beta) \end{aligned} \quad (13)$$

where  $p = (p_1, p_2, \dots, p_{\frac{N}{2}})$  and  $q = (q_1, q_2, \dots, q_{\frac{M}{2}})$  are respectively generating sequences of the rows and the columns of PI-FrDCT.

The inverse PI-FrDCT is simply given by

$$\begin{cases} t_{:,i} = l_0(-\beta) g_{:,i} + l_1(-\beta) g_{:,i}^5 + l_2(-\beta) g_{:,i}^{10} + \cdots + \\ \quad l_{M-1}(-\beta) g_{:,i}^{5(M-1)}, \quad i = 0, 1, \dots, N-1 \\ f_{j,:} = l_0(-\alpha) t_{j,:} + l_1(-\alpha) t_{j,:}^5 + l_2(-\alpha) t_{j,:}^{10} + \cdots + \\ \quad l_{N-1}(-\alpha) t_{j,:}^{5(N-1)}, \quad j = 0, 1, \dots, M-1. \end{cases} \quad (14)$$

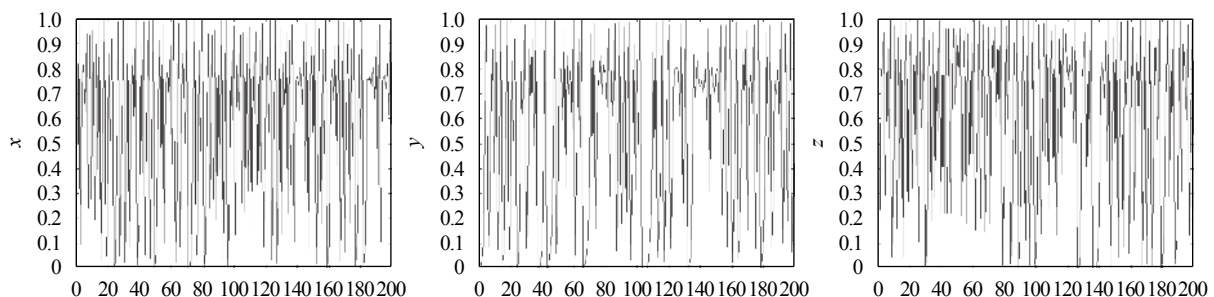


Fig. 1 From left to right are chaotic behaviors of  $x$ ,  $y$ ,  $z$  ( $x_0=0.8232$ ,  $y_0=0.235$ ,  $z_0=0.8654$ ,  $b_1=1.5$ ,  $b_2=0.892$ ,  $b_3=3.256$ ,  $b_4=1.2389$ )

## 2.3 Three-dimensional piecewise and nonlinear chaotic maps

Three-dimensional (3D) piecewise and nonlinear chaotic maps<sup>[40]</sup> are employed to generate the GS, since they have more initial and system parameters than in one-dimensional case:

$$\begin{cases} x_{n+1} = \frac{4b_1b_3x_n(1-x_n)}{1+4(b_1b_3-1)x_n(1-x_n)} \\ y_{n+1} = \frac{4b_1^2y_n(1-y_n)}{1+4(b_1^2-1)y_n(1-y_n)} \\ z_{n+1} = \frac{4b_3^2z_n(1-z_n)}{1+4(b_3^2-1)z_n(1-z_n)} \\ x_n \in \left[0, \frac{1}{2}\right] \\ x_{n+1} = \frac{4b_2b_4x_n(1-x_n)}{1+4(b_2b_4-1)x_n(1-x_n)} \\ y_{n+1} = \frac{4b_2^2y_n(1-y_n)}{1+4(b_2^2-1)y_n(1-y_n)} \\ z_{n+1} = \frac{4b_4^2z_n(1-z_n)}{1+4(b_4^2-1)z_n(1-z_n)} \\ x_n \in \left[\frac{1}{2}, 1\right] \end{cases} \quad (15)$$

where  $x_n, y_n \in (0, 1)$ ,  $n = 0, 1, 2, \dots$ , and  $x_0, y_0$  are the initial values. If  $0.52 < b_1b_3, b_2b_4, b_1, b_2, b_3, b_4 \leq 6$ , the 3D piecewise and nonlinear chaotic maps will exhibit chaotic behavior. Fig. 1 exhibits the chaotic nature of  $x, y, z$  in (15) and Fig. 2 shows the bifurcation behavior of  $x$ .

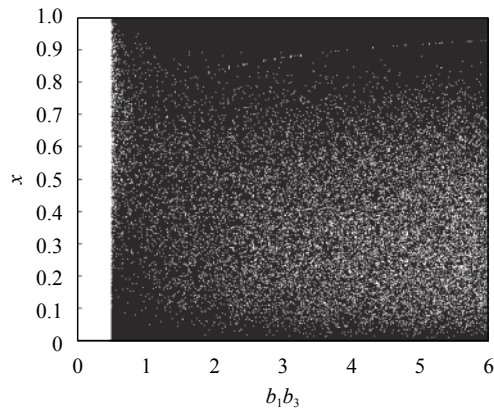
## 2.4 Generation of variable initial values and system parameters

In this paper, a disturbance factor  $\Delta$  associated with the plain-image is introduced and generated by<sup>[38]</sup>

$$\Delta = \frac{\sum_{i,j} f(i,j)}{255 \times M \times N} \quad (16)$$

where  $f(i,j)$  indicates the pixel value of plain-image at  $(i,j)$  and  $M \times N$  is the size of image.

With the disturbance factor, the actual initial values

Fig. 2 Bifurcation behavior of  $x$  ( $x_0=0.011$ )

and system parameters can be modified such that:

$$z' = z + \Delta \quad (17)$$

where  $z$  represents given initial values and system parameters.  $z'$  represents the actual ones. If there is even a one bit difference between two plain images, the actual initial values and system parameters will be completely different due to the introduction of  $\Delta$ .

### 3 Image encryption and decryption process on CS and PI-FrDCT

The encryption and decryption process of the proposed method is shown in Fig. 3 and the image encryption steps are as follows.

**Step 1.** Construct measurement matrix  $\Phi$  with size  $M \times N$  [41]:

Generate a sequence with length  $N + m_1$  by a logistic map, i.e.,  $x'_{n+1} = \mu x'_n(1 - x'_n)$  with an initial value  $x'_0$  and a system parameter  $\mu$ , discard previous  $m_1$  entries for enhancing randomness and confusion to obtain the sequence  $\eta = [\eta_1, \eta_2, \dots, \eta_N]$  and mark  $\varepsilon = [\varepsilon_1, \varepsilon_2, \dots, \varepsilon_N]$

as the result of index sequence of sorting  $\eta$  in descending order.

Sort the natural sequence  $n = [1, 2, \dots, N]$  according to the index sequence  $\varepsilon$ , mark  $pp = [pp_1, pp_2, \dots, pp_N]$  as the result of sorting  $n$ .

Generate the Hadamard matrix  $J$  of order  $N$ , choose the row vectors,  $J(pp_1, :)$ ,  $J(pp_2, :)$ ,  $\dots$ ,  $J(pp_M, :)$  and then form the measurement matrix  $\Phi$ , i.e.,

$$\Phi = \begin{bmatrix} J(pp_1, :) \\ J(pp_2, :) \\ \vdots \\ J(pp_M, :) \end{bmatrix}.$$

**Step 2.** Obtain  $I_2$  with size  $M \times M$  by one-time measuring or two-time measuring  $I_1$  using  $\Phi$ .

a) For one-time measuring, apply CS to  $I_1$  and mark  $I_{1'}$  with size  $M \times N$  as the result of the measurement, and then  $I_2$  is taken column-wise from  $I_{1'}$ .

b) For two-time measuring, obtain  $I_2$  in accordance with

$$I_2 = \Phi \Psi (\Phi \Psi I_1)' \quad (18)$$

where  $\Psi$  is the discrete wavelet transform matrix and  $I_1$  is the original image.

**Step 3.** Perform the PI-FrDCT for  $I_2$  in accordance with (12), and mark  $I_3$  as the result of PI-FrDCT.

For an image  $I_2$  of size  $M \times M$ , two generating sequences of length  $\frac{M}{2}$  are necessary for PI-FrDCT. First, a chaotic sequence of length  $m + M + M^2$  is generated by iterating (15); and the previous  $m$  entries are discarded to obtain the sequences  $x = [x_0, x_1, \dots, x_{\frac{M}{2}-1}]$ ,  $y = [y_0, y_1, \dots, y_{\frac{M}{2}-1}]$  and  $z = [z_0, z_1, \dots, z_{M^2-1}]$ .  $m$  entries are discarded to further confirm the randomness of the sequences. Since the GS takes integer values,  $p$  and  $q$  are uniformly quantized to map intervals  $(0, 0.25]$ ,  $(0.25, 0.5]$ ,

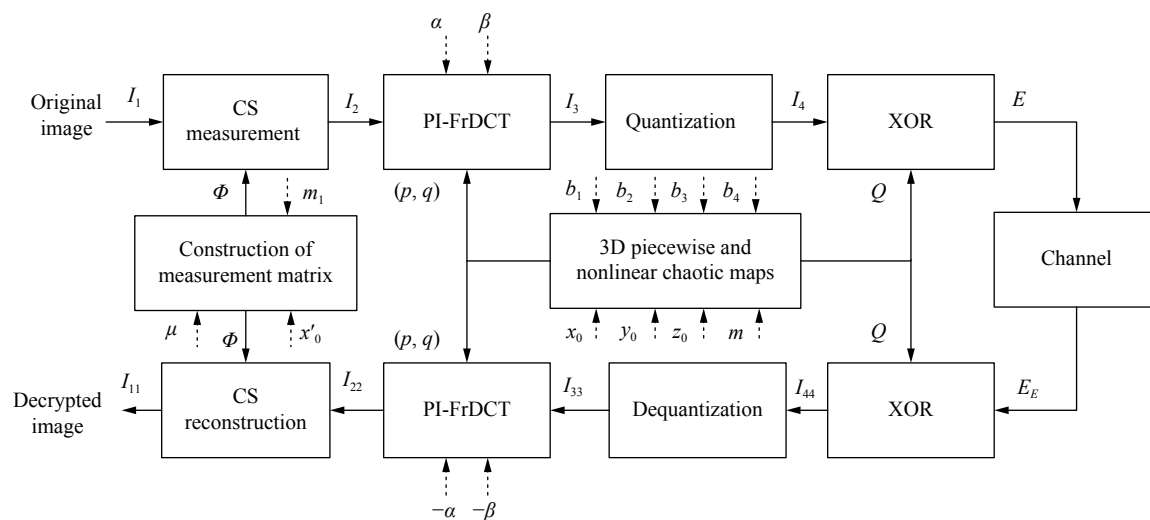


Fig. 3 Flowchart of the encryption and decryption process



$(0.5, 0.75]$ ,  $(0.75, 1)$  into integers 0, 1, 2, 3, respectively. The matrix  $\mathbf{Q}$  of size  $M \times M$ , which serves as a diffusion matrix for the XOR operation, is taken column-wise from  $\mathbf{zz} = [zz_0 \ zz_1 \ \cdots \ zz_{M^2-1}]$  with

$$zz_i = (z_i \times 10^9) \bmod 256, \ i = 0, 1, \dots, M^2 - 1. \quad (19)$$

**Step 4.** Non-uniformly quantize  $\mathbf{I}_3$  with 8bits in accordance with (20) to obtain  $\mathbf{I}_4$ :

$$\mathbf{I}_4 = \text{round}(128 \times \tan(\frac{\mathbf{I}_3}{1000}) + 128). \quad (20)$$

**Step 5.** Carry out bitwise XOR to conceal the distribution property of  $\mathbf{I}_4$  and make the energy uniformly distributed over the entire image  $\mathbf{E}$ .

$$\mathbf{E} = \mathbf{I}_4 \oplus \mathbf{Q} \quad (21)$$

where  $\oplus$  denotes the bitwise XOR operation.

The decryption process is the XOR followed by the dequantization, the inverse operation of PI-FrDCT and the reconstruction operation with the  $\text{SL}_0$  algorithm. All the cipher keys do not change except for the fractional orders, which are  $-\alpha$  and  $-\beta$ , respectively.

Instead of minimizing the  $l_1$  norm using linear programming (LP), the  $\text{SL}_0$  algorithm directly minimizes the  $l_0$  norm and is about two to three orders of magnitude faster than the interior-point LP solvers, while keeping the same accuracy. The detailed description of the  $\text{SL}_0$  algorithm can be found in [35].

## 4 Experimental results and analyses

The proposed algorithm is tested using two images, Lena and Peppers, both with size  $512 \times 512$  (Figs. 4(a) and 4(d)). An average value should be subtracted to remove the direct current (DC) component, so that the quantiza-

tion error can be as small as possible in the quantization process after PI-FrDCT. 128 is selected as an approximation of the DC value for convenience.  $\alpha$ ,  $\beta$ ,  $x'_0$ ,  $\mu$ ,  $m_1$ ,  $b_1$ ,  $b_2$ ,  $b_3$ ,  $b_4$ ,  $x_0$ ,  $y_0$ ,  $z_0$ ,  $m$  and  $\Delta$  serve as the cipher keys. Since the sensitivity of the fractional orders  $\alpha$  and  $\beta$  to the decrypted image quality is not high, they serve as auxiliary keys. According to Section 2.3,  $x'_0$ ,  $\mu$ ,  $m_1$ ,  $b_1$ ,  $b_2$ ,  $b_3$ ,  $b_4$ ,  $x_0$ ,  $y_0$ ,  $z_0$  and  $m$  are randomly chosen within the specified intervals. In our experiment,  $\alpha$  and  $\beta$  are set to be 0.7689 and 0.4578, a disturbance factor  $\Delta$  associated with the plain-image is produced in the encryption process according to (16). The common initial value and parameter  $x'_0$ ,  $\mu$ ,  $m_1$ ,  $b_1$ ,  $b_2$ ,  $b_3$ ,  $b_4$ ,  $x_0$ ,  $y_0$ ,  $z_0$  and  $m$  are set to be 0.1105, 3.9924, 1000, 3.2569, 0.89254, 2.5672, 1.862, 0.2345, 0.56897, 0.9875, 2000, respectively. These parameters can of course be set to be any other values satisfying the conditions. The actual cipher keys of  $x'_0$ ,  $\mu$ ,  $m_1$ ,  $b_1$ ,  $b_2$ ,  $b_3$ ,  $b_4$ ,  $x_0$ ,  $y_0$  and  $z_0$  are obtained by (17). The encryption and decryption results are shown in Fig. 4. Here, the compression ratio is 1.78, i.e., the size of the encrypted image is  $384 \times 384$ . As can be seen, the decrypted images contain the main information in spite of some distortion. To evaluate the security and effectiveness of the proposed algorithm, statistical analysis, key space analysis and robustness analysis are carried out.

In addition, the encryption algorithm performing one-time measuring in the CS stage is called Algorithm 1, and the encryption algorithm using the two-time measuring in the process of the encryption is called Algorithm 2. The experiments are performed in order to analyze the difference between Algorithms 1 and 2 with the same compression ratio.

### 4.1 Statistical analysis

#### 4.1.1 Histogram

Histograms of both original test and encrypted images are shown in Fig. 5. From Figs. 5(b) and 5(d), it can be found that histograms of the encrypted images exhibit a uniform distribution and are different from those of the original images. None of the useful information is leaked to the adversary. The introduction of PI-FrDCT and XOR operations makes the encrypted scheme more secure. Hence, the proposed algorithm is secure enough to resist statistical analysis attacks by histogram analysis.

#### 4.1.2 Information entropy

The information entropy is expressed as

$$H(m) = - \sum_{i=0}^{L-1} P(m_i) \log_2 P(m_i) \quad (22)$$

where  $m_i$  is the  $i$ -th gray value for an  $L$ -gray level image and  $P(m_i)$  is its normalized occurrence frequency. A larger entropy usually means a more uncertain distribution. The maximum entropy for an image with 256 gray levels is 8 when all gray levels are equally distributed, indicating the largest randomness. As shown in Table 1, the values of information entropy for different

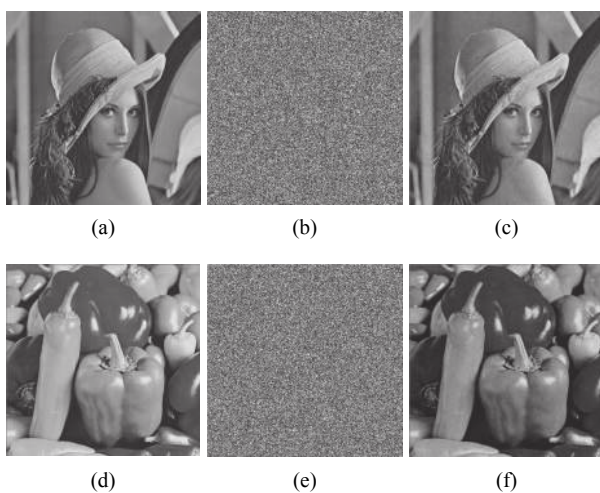


Fig. 4 Test image and results: (a) Original Lena, (b) Encrypted image of (a), (c) Decrypted image of (b), (d) Original Peppers, (e) Encrypted image of (d), and (f) Decrypted image of (e)

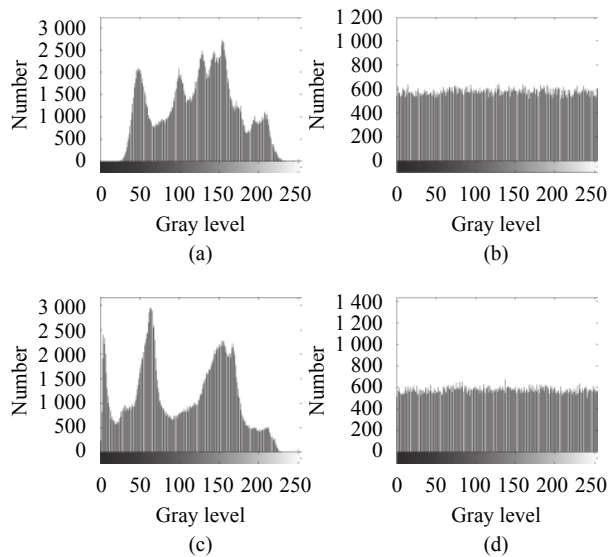


Fig. 5 Histograms: (a) Original Lena, (b) Encrypted Lena, (c) Original Peppers, and (d) Encrypted Peppers

Table 1 Information entropy of original and encrypted images

	Original image	Algorithm 1	Algorithm 2
Lena	7.4455	7.9984	7.9985
Peppers	7.5715	7.9986	7.9984
Barbara	7.4664	7.9987	7.9987
Boat	7.1238	7.9986	7.9988
Plane	6.7054	7.9986	7.9984
Camera	7.0480	7.9983	7.9984

encrypted images using Algorithms 1 and 2 are larger than those for different original images, and are very close to 8. It indicates that the distribution of the image grey value is completely random and possesses an ability to resist entropy based attacks. Thus, it can be concluded that the proposed algorithm can effectively resist entropy based attacks.

#### 4.1.3 Correlation of adjacent pixels

Correlation analysis is considered here. Pairs of all adjacent pixels in the horizontal, vertical or diagonal directions from both the original image and encrypted image are selected and then the correlation coefficients of adjacent pixels for each direction are calculated as

$$r_{xy} = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2 \sum_{i=1}^N (y_i - \bar{y})^2}} \quad (23)$$

where  $\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i$  and  $\bar{y} = \frac{1}{N} \sum_{i=1}^N y_i$ ,  $x_i$  and  $y_i$  are gray values of two adjacent pixels in an image,  $N$  represents the number of pairs of adjacent pixels in the same image.

The values of the correlation coefficients of adjacent pixels in the encrypted image are reduced compared with those in the corresponding encrypted image and the original image, as shown in Table 2. The correlation coefficients of the proposed Algorithm 2 are relatively smaller than those of Algorithm 1 in Table 2. The results show the coefficients of the proposed Algorithm 2 are all sufficiently low, which indicates a satisfactory confusion effect.

As an example, the experimental results of the Lena image are exhibited in Fig. 6. From Figs. 6(a)–6(c), it can be seen that the joint distribution of gray values of adjacent pixels of the original image in three directions distributes near the diagonal of the coordinate plane. This demonstrates a strong correlation in the original image. And from Figs. 6(d)–6(f), the joint distribution of gray values of adjacent pixels of the encrypted images in three directions exhibit relatively uniform. Therefore, we can conclude that the statistical analysis attack on our scheme is infeasible.

In conclusion, the results in Fig. 6 and Table 2 demonstrate that the correlation between adjacent pixels in the encrypted image is greatly reduced.

#### 4.1.4 Differential attack analysis

To evaluate the ability to resist differential attacks, two criteria are defined: the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). The NPCR and UACI are defined as [38, 42]

$$\text{NPCR} = \frac{\sum_{i,j} C(i,j)}{M \times N} \times 100\% \quad (24)$$

$$C(i,j) = \begin{cases} 0, & T_1(i,j) = T_2(i,j) \\ 1, & T_1(i,j) \neq T_2(i,j) \end{cases} \quad (25)$$

where  $M \times N$  is the size of images  $T_1$  and  $T_2$ .  $T_1(i,j)$  and  $T_2(i,j)$  indicate the pixel values of two cipher-images at  $(i,j)$ , corresponding to two plain-images that are different by one pixel.

$$\text{UACI} = \frac{\sum_{i,j} |T_1(i,j) - T_2(i,j)|}{255 \times M \times N} \times 100\%. \quad (26)$$

For an image with 8bits for each pixel, the expected values of NPCR and UACI are respectively 99.61% and 33.46% [43]. As shown in Table 3, the NPCRs are all above 99.60% and the UACIs of the encrypted image are all over 33.20%, which indicates that the values of each pixel pair at the same location in two encrypted images are substantially different. Thus, the encryption scheme is very sensitive with respect to a small change in the plain-images even by as little as one pixel difference. The scheme is even more secure due to combining CS, PI-FrDCT and XOR operations. In conclusion, the results in Table 3 demonstrate that the proposed encrypted algorithm has an ability to resist a differential attack.

Table 2 Correlation coefficients of adjacent pixels

Algorithm	Image	Horizontal	Vertical	Diagonal
Algorithm 1	Original Lena	0.952 976	0.984 795	0.948 743
	Encrypted Lena	0.005 358	0.019 380	0.003 486
Algorithm 2	Encrypted Lena	0.000 536	-0.000 220	0.000 684
	Original Peppers	0.977 372	0.980 018	0.970 839
Algorithm 1	Encrypted Peppers	0.031 067	-0.004 843	0.005 990
	Encrypted Peppers	-0.002 496	-0.002 326	0.000 855
Algorithm 1	Original Barbara	0.919 631	0.968 776	0.914 610
	Encrypted Barbara	-0.001 703	-0.005 070	-0.017 998
Algorithm 2	Encrypted Barbara	0.006 552	-0.004 922	-0.001 693
	Original Boat	0.957 812	0.957 637	0.941 071
Algorithm 1	Encrypted Boat	0.006 925	-0.027 532	-0.006 066
	Encrypted Boat	0.001 010	0.001 783	-0.001 020
Algorithm 1	Original Plane	0.962 652	0.960 947	0.925 657
	Encrypted Plane	0.068 614	0.085 247	0.004 917
Algorithm 2	Encrypted Plane	-0.014 870	0.014 370	0.006 899
Algorithm 1	Original Camera	0.986 567	0.990 648	0.985 069
	Encrypted Camera	0.112 101	0.164 102	0.010 177
Algorithm 2	Encrypted Camera	-0.001 703	0.002 353	0.001 361

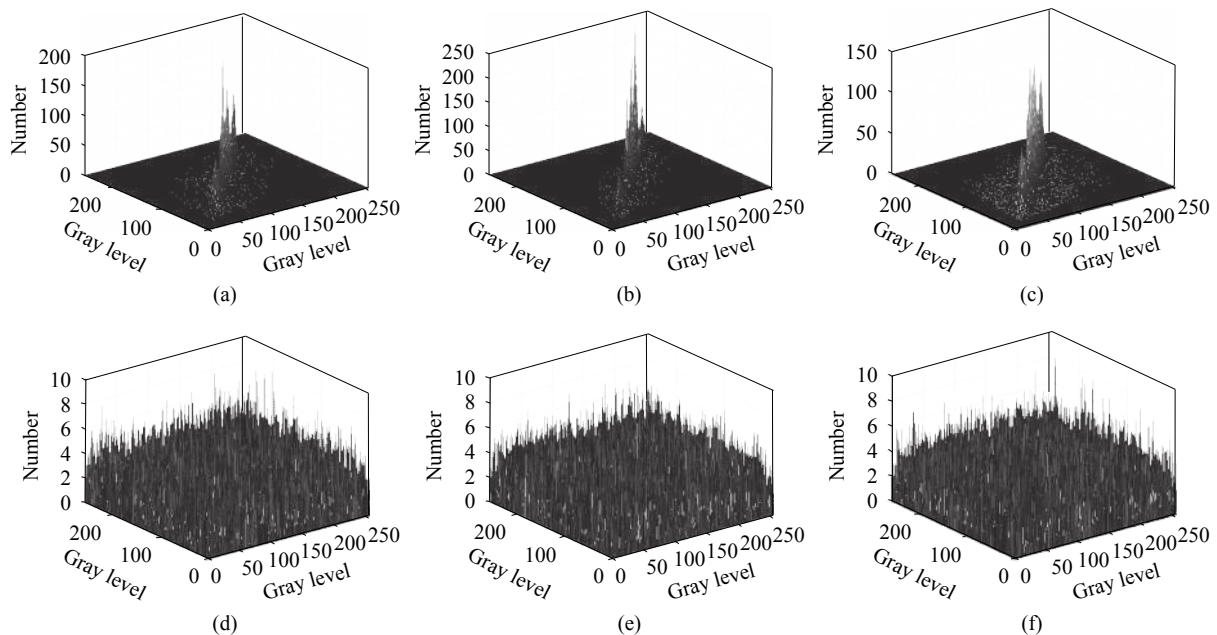


Fig. 6 Joint distribution of gray values of adjacent pixels of the original Lena and encrypted Lena: (a), (b) and (c) are the horizontal, vertical and diagonal correlations of the original Lena, respectively. (d), (e) and (f) are the horizontal, vertical and diagonal correlations of the encrypted image, respectively.

## 4.2 Key space

In the proposed algorithm, the cipher keys are  $\alpha$ ,  $\beta$ ,  $x'_0$ ,  $\mu$ ,  $m_1$ ,  $b_1$ ,  $b_2$ ,  $b_3$ ,  $b_4$ ,  $x_0$ ,  $y_0$ ,  $z_0$ ,  $m$  and  $\Delta$ . The fractional orders  $\alpha$  and  $\beta$  serve as auxiliary keys. Fig. 7 illustrates the decrypted images of Lena with just one wrong key during decryption. Intuitively, the decrypted images

are completely disordered, as shown in Fig. 7. The results show that any slight mismatch in the cipher key will lead to an incorrect decoding. If the error is up to  $10^{-15}$ , the key space size is  $10^{135}$  if  $x'_0$ ,  $\mu$ ,  $b_1$ ,  $b_2$ ,  $b_3$ ,  $b_4$ ,  $x_0$ ,  $y_0$  and  $z_0$  are used as cipher keys. In addition, the choice of  $\alpha$ ,  $\beta$ ,  $m_1$  and  $m$  makes the actual key space even larger. The introduction of PI-FrDCT and 3D piecewise and nonlin-



Table 3 NPCRs and UACIs for different encrypted images

	Algorithm	NPCR (%)	UACI (%)
Lena	Algorithm 1	99.6189	33.3335
	Algorithm 2	99.6216	33.3009
Peppers	Algorithm 1	99.6297	33.2017
	Algorithm 2	99.6345	33.2193
Barbara	Algorithm 1	99.6107	33.2178
	Algorithm 2	99.6053	33.2416
Boat	Algorithm 1	99.6114	33.2241
	Algorithm 2	99.6134	33.2226
Plane	Algorithm 1	99.6101	33.3330
	Algorithm 2	99.6053	33.3427
Camera	Algorithm 1	99.6250	33.2841
	Algorithm 2	99.6250	33.259 8

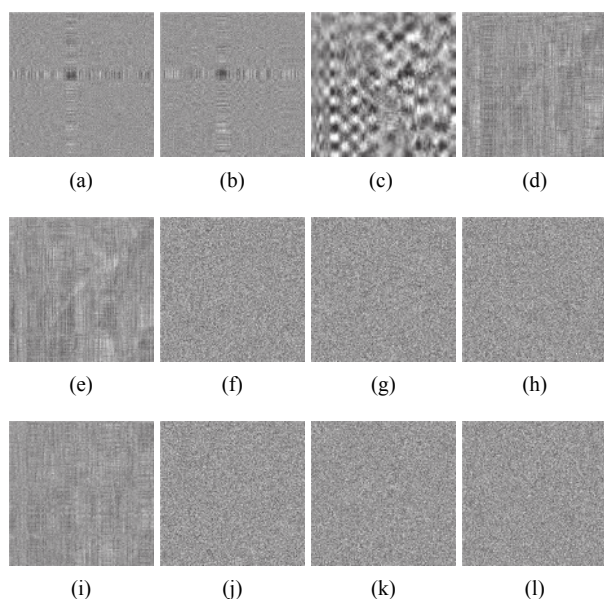


Fig. 7 Decrypted images with only one wrong key. The deviations are respectively: (a)  $\Delta x'_0 = 10^{-15}$ , (b)  $\Delta \mu = 10^{-15}$ , (c)  $\Delta m_1 = 1$ , (d)  $\Delta b_1 = 10^{-15}$ , (e)  $\Delta b_2 = 10^{-15}$ , (f)  $\Delta b_3 = 10^{-15}$ , (g)  $\Delta b_4 = 10^{-15}$ , (h)  $\Delta x_0 = 10^{-15}$ , (i)  $\Delta y_0 = 10^{-15}$ , (j)  $\Delta z_0 = 10^{-15}$ , (k)  $\Delta m = 1$ , (l) use  $\Delta$  of Peppers.

ear chaotic maps enlarges the key space and enhances the security of the encryption scheme. Therefore, the key space is large enough to resist brute-force attacks.

### 4.3 Robustness analysis

For a noise attack, the Gaussian noises are added into the encrypted image<sup>[38]</sup>:

$$E_N = E(1 + kG) \quad (27)$$

where  $E_N$  and  $E$  are the noise-affected and noiseless encrypted images, respectively.  $k$  represents the intensity

level of the added noise.  $G$  is the Gaussian noise with zero-mean and unit standard deviation. When  $k$  is respectively set to 0.01, 0.05, 0.1 and 0.5, the corresponding decrypted images of Lena and Peppers are exhibited in Fig. 8. As shown in Figs. 8(a)–8(h), the quality of the decrypted images decreases with the increase of added noise intensity. The content of decrypted image can still be identified despite the interference of noise to some extent. Figs. 9(a)–9(c) respectively show the encrypted images with an occlusion of  $\frac{1}{64}$ ,  $\frac{1}{16}$  and  $\frac{1}{4}$ . Figs. 9(d)–9(i)

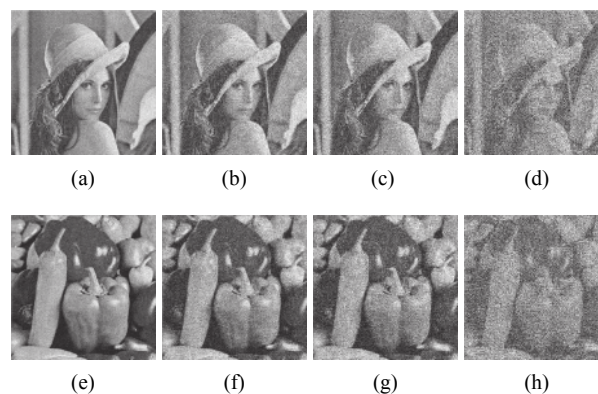


Fig. 8 Decrypted images with Gaussian noise intensity levels of: (a), (e)  $k=0.01$ ; (b), (f)  $k=0.05$ , (c), (g)  $k=0.1$  and (d), (h)  $k=0.5$

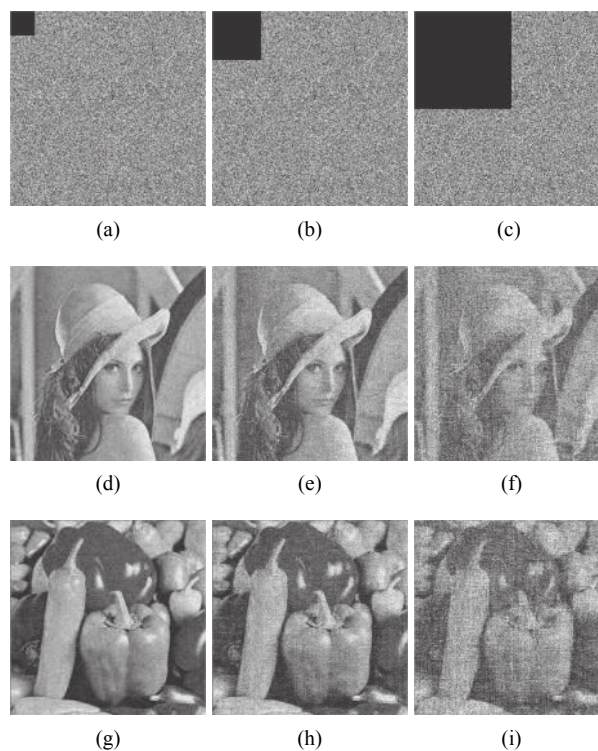


Fig. 9 Results of anti-occlusion attacks: the encrypted images for Lena with an occlusion of (a)  $\frac{1}{64}$ , (b)  $\frac{1}{16}$ , (c)  $\frac{1}{4}$ ; (d), (e) and (f) are decrypted images from (a), (b), (c), respectively; (g), (h), (i) are decrypted images for Peppers under the same occlusions as in (a), (b), (c), respectively.

show the corresponding decrypted images for Lena and Peppers. The quality of the decrypted images decreases as the occlusion size increases. Although the encrypted image is partly occluded, the main content of the original images can be still recognized from the decrypted image, as shown in Figs.9(d)–9(i). Hence, the proposed encryption scheme has a certain robustness against noise and occlusion attacks.

#### 4.4 Compression performance











To measure the similarity of original and decrypted images for different compression ratios, the peak signal-to-noise ratio (PSNR)<sup>[31]</sup> is adopted.

$$\text{PSNR} = 10\log_{10} \frac{255^2 \times M \times N}{\sum_{i=1}^M \sum_{j=1}^N [\mathbf{O}(i,j) - \mathbf{I}(i,j)]^2} \quad (\text{dB}) \quad (28)$$

where  $M \times N$  is the size of image,  $\mathbf{I}(i,j)$  and  $\mathbf{O}(i,j)$  are the pixel values of the original and reconstructed images at  $(i,j)$ , respectively.

In order to obtain the same compression ratio, the number of rows of the sensor matrix in Algorithm 1 is smaller than that in Algorithm 2. As shown in Tables 4 and 5, the quality of the reconstructed images decreases as the compression ratio increases. From Table 4, the quality of the reconstructed image using Algorithm 1 is

Table 4 Reconstructed image for different compression ratios of Lena

Compression ratio	Decrypted images		Size of encrypted image
	Algorithm 1	Algorithm 2	
1.306:1			448×448
1.78:1			384×384
2.56:1			320×320
4:1			256×256
7.11:1			192×192

visually inferior to that using Algorithm 2 when the compression ratio is 4:1. For instance, Lena's mouth and eyebrows become blurred. In particular, from the reconstructed images in Tables 4 and 5 and PSNR in Tables 6 and 7, more information is lost when adopting Algorithm 1 than adopting Algorithm 2, when the compression ratio is 7.11:1. Even though the PSNR of the proposed algorithm is relatively small when the compression ratio is up to 7.11:1, the main content of the reconstructed images can be obtained. Tables 6 and 7 list the PSNR of the proposed algorithm and the algorithm in [19]. Compressive sensing is a signal processing tool to efficiently acquire and reconstruct a signal. Its principle is based on optimization and sparsity. The signal can be sampled at a frequency smaller than that required by the Nyquist theory. Although the PSNRs of proposed algorithm are not superior to those in [19], both of [19] and ours are of significance and we need not focus on their PSNRs too much.

Table 5 Reconstructed image for different compression ratios of Peppers











Compression ratio	Decrypted images		Size of encrypted image
	Algorithm 1	Algorithm 2	
1.306:1			448×448
1.78:1			384×384
2.56:1			320×320
4:1			256×256
7.11:1			192×192

Table 6 PSNR for different compression ratios of Lena

Compression ratio	PSNR (dB)		
	Reference [19]	Algorithm 1	Algorithm 2
1.306:1	43.7162	39.5420	36.3516
1.78:1	40.3293	34.9400	32.2785
2.56:1	37.8124	30.6873	28.5479
4:1	35.3508	26.3369	26.1006
7.11:1	32.6772	19.8274	23.4567

Table 7 PSNR for different compression ratios of Peppers

Compression ratio	PSNR (dB)		
	Reference [19]	Algorithm 1	Algorithm 2
1.306:1	39.3963	38.2418	35.9605
1.78:1	35.9300	34.3119	32.7708
2.56:1	34.0884	29.5596	28.9986
4:1	32.4140	24.0902	25.7883
7.11:1	30.7389	16.9537	22.4488

#### 4.5 Known-plaintext and chosen-plaintext attacks analysis

It is clear that in the proposed scheme, the initial values and system parameters of the encryption scheme are determined by cipher keys and plain-image due to introduction of a disturbance factor. The actual initial values and system parameters are different for different plain-images. A disturbance factor makes the encryption system more effective in resisting the known-plaintext and chose-plaintext attacks. In addition, GSs used in the PI-FrDCT and the matrix  $Q$  used in the XOR operation are generated by 3D piecewise and nonlinear chaotic maps and are also different for different plain-images. Hence, the correct decrypted results cannot be obtained when a disturbance factor for another image is adopted, as shown in Fig. 7 (l). Thus, the proposed algorithm can resist the known-plaintext and chosen-plaintext attacks.

#### 5 Conclusions

In this paper, we proposed an encryption scheme based on CS and PI-FrDCT, in which the compression and encryption are achieved simultaneously. In the encryption phase, we utilized the CS theory to encrypt and compress the original image. To enhance the security of the encrypted image, the resulting image after CS is re-encrypted by PI-FrDCT. The real-valued output is quantized with 8 bits for a coefficient, which makes the encrypted results convenient for storage, display and transmission. Meanwhile, GSs and the XOR matrix are generated by 3D piecewise and nonlinear chaotic maps, which further strengthen the security of the encryption scheme. The sensitivity of cipher keys is high due to employing the 3D piecewise and nonlinear chaotic maps. Experimental results show the effectiveness and high security of the proposed scheme. For example, it has a high sensitivity, a sufficiently large key space, a robustness against noise and occlusion attacks and an ability to resist common attacks.

#### Acknowledgements

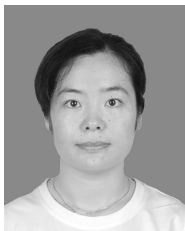
This work was supported by National Natural Science Foundation of China (Nos. 61662047 and 61462061).

#### References

- [1] G. H. Situ, J. J. Zhang. A cascaded iterative Fourier transform algorithm for optical security applications. *Optik – International Journal for Light and Electron Optics*, vol. 114, no. 10, pp. 473–477, 2003. DOI: [10.1078/0030-4026-00291](https://doi.org/10.1078/0030-4026-00291).
- [2] X. G. Wang, D. M. Zhao. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain. *Optics Communications*, vol. 284, no. 1, pp. 148–152, 2011. DOI: [10.1016/j.optcom.2010.09.034](https://doi.org/10.1016/j.optcom.2010.09.034).
- [3] M. H. Annaby, M. A. Rushdi, E. A. Nehary. Image encryption via discrete fractional Fourier-type transforms generated by random matrices. *Signal Processing: Image Communication*, vol. 49, pp. 25–46, 2016. DOI: [10.1016/j.image.2016.09.006](https://doi.org/10.1016/j.image.2016.09.006).
- [4] L. S. Sui, K. K. Duan, J. L. Liang, Z. Q. Zhang, H. N. Meng. Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. *Optics and Lasers in Engineering*, vol. 62, pp. 139–152, 2014. DOI: [10.1016/j.optlaseng.2014.06.003](https://doi.org/10.1016/j.optlaseng.2014.06.003).
- [5] L. S. Sui, M. J. Xu, A. L. Tian. Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain. *Optics and Lasers in Engineering*, vol. 91, pp. 106–114, 2017. DOI: [10.1016/j.optlaseng.2016.11.017](https://doi.org/10.1016/j.optlaseng.2016.11.017).
- [6] Z. J. Liu, M. A. Ahmad, S. T. Liu. Image encryption based on double random amplitude coding in random Hartley transform domain. *Optik – International Journal for Light and Electron Optics*, vol. 121, no. 11, pp. 959–964, 2010. DOI: [10.1016/j.ijleo.2008.12.006](https://doi.org/10.1016/j.ijleo.2008.12.006).
- [7] S. M. Pan, R. H. Wen, Z. H. Zhou, N. R. Zhou. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 2933–2953, 2017. DOI: [10.1007/s11042-015-3209-x](https://doi.org/10.1007/s11042-015-3209-x).
- [8] N. R. Zhou, J. P. Yang, C. F. Tan, S. M. Pan, Z. H. Zhou. Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform. *Optics Communications*, vol. 354, pp. 112–121, 2015. DOI: [10.1016/j.optcom.2015.05.043](https://doi.org/10.1016/j.optcom.2015.05.043).
- [9] G. Unnikrishnan, J. Joseph, K. Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Optics Letters*, vol. 25, no. 12, pp. 887–889, 2000. DOI: [10.1364/OL.25.000887](https://doi.org/10.1364/OL.25.000887).
- [10] R. Tao, J. Lang, Y. Wang. Optical image encryption based on the multiple-parameter fractional Fourier transform. *Optics Letters*, vol. 33, no. 6, pp. 581–583, 2008. DOI: [10.1364/OL.33.000581](https://doi.org/10.1364/OL.33.000581).
- [11] Y. P. Li, C. H. Wang, H. Chen. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017. DOI: [10.1016/j.optlaseng.2016.10.020](https://doi.org/10.1016/j.optlaseng.2016.10.020).
- [12] Z. Parvin, H. Seyedarabi, M. Shamsi. A new secure and sensitive image encryption scheme based on new substitution with chaotic function. *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10631–10648, 2016. DOI: [10.1007/s11042-014-2115-y](https://doi.org/10.1007/s11042-014-2115-y).
- [13] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, M. Lee. Image encryption using a synchronous permutation-diffusion technique. *Optics and Laser Technology*, vol. 90, pp. 146–154, 2017. DOI: [10.1016/j.optlaseng.2016.10.006](https://doi.org/10.1016/j.optlaseng.2016.10.006).
- [14] T. G. Gao, Z. Q. Chen. A new image encryption algorithm based on hyper-chaos. *Physics Letters A*, vol. 372, no. 4,



- pp. 394–400, 2008. DOI: [10.1016/j.physleta.2007.07.040](https://doi.org/10.1016/j.physleta.2007.07.040).
- [15] W. Zhang, K. W. Wong, H. Yu, Z. L. Zhu. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 8, pp. 2066–2080, 2013. DOI: [10.1016/j.cnsns.2012.12.012](https://doi.org/10.1016/j.cnsns.2012.12.012).
- [16] I. Venturini, P. Duhamel. Reality preserving fractional transforms. In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Montreal, Canada, vol. 5, pp. 205–208, 2004.
- [17] J. Lang. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform. *Optics Communications*, vol. 285, no. 10–11, pp. 2584–2590, 2012. DOI: [10.1016/j.optcom.2012.01.085](https://doi.org/10.1016/j.optcom.2012.01.085).
- [18] N. R. Zhou, Y. X. Wang, L. H. Gong, X. B. Chen, Y. X. Yang. Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. *Optics & Laser Technology*, vol. 44, no. 7, pp. 2270–2281, 2012. DOI: [10.1016/j.optlastec.2012.02.027](https://doi.org/10.1016/j.optlastec.2012.02.027).
- [19] Z. J. Liu, Y. Zhang, H. F. Zhao, M. A. Ahmad, S. T. Liu. Optical multi-image encryption based on frequency shift. *Optik-International Journal for Light and Electron Optics*, vol. 122, no. 11, pp. 1010–1013, 2011. DOI: [10.1016/j.ijleo.2010.06.039](https://doi.org/10.1016/j.ijleo.2010.06.039).
- [20] E. J. Candès. Compressive sampling. In *Proceedings of the International Congress of Mathematics*, Madrid, Spain, pp. 1433–1452, 2006.
- [21] E. J. Candès, J. Romberg, T. Tao. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006. DOI: [10.1109/TIT.2005.862083](https://doi.org/10.1109/TIT.2005.862083).
- [22] D. L. Donoho. Compressed sensing. *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006. DOI: [10.1109/TIT.2006.871582](https://doi.org/10.1109/TIT.2006.871582).
- [23] R. Huang, K. Sakurai. A robust and compression-combined digital image encryption method based on compressive sensing. In *Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Dalian, China, pp. 105–108, 2011. DOI: [10.1109/IIHMSP.2011.53](https://doi.org/10.1109/IIHMSP.2011.53).
- [24] Y. Rachlin, D. Baron. The secrecy of compressed sensing measurements. In *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, Urbana, USA, pp. 813–817, 2008. DOI: [10.1109/ALLERTON.2008.4797641](https://doi.org/10.1109/ALLERTON.2008.4797641).
- [25] M. R. Mayiami, B. Seyfe, H. G. Bafghi. Perfect secrecy via compressed sensing. In *Proceedings of Iran Workshop on Communication and Information Theory*, Tehran, Iran, pp. 1–5, 2013. DOI: [10.1109/IWCIT.2013.6555751](https://doi.org/10.1109/IWCIT.2013.6555751).
- [26] P. Lu, Z. Y. Xu, X. Lu, X. Y. Liu. Digital image information encryption based on compressive sensing and double random-phase encoding technique. *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 16, pp. 2514–2518, 2013. DOI: [10.1016/j.ijleo.2012.08.017](https://doi.org/10.1016/j.ijleo.2012.08.017).
- [27] G. Q. Hu, D. Xiao, Y. Wang, T. Xiang. An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *Journal of Visual Communication and Image Representation*, vol. 44, pp. 116–127, 2017. DOI: [10.1016/j.jvcir.2017.01.022](https://doi.org/10.1016/j.jvcir.2017.01.022).
- [28] C. Feng, L. Xiao, Z. H. Wei. Compressive sensing inverse synthetic aperture radar imaging based on gini index regularization. *International Journal of Automation and Computing*, vol. 11, no. 4, pp. 441–448, 2014. DOI: [10.1007/s11633-014-0811-8](https://doi.org/10.1007/s11633-014-0811-8).
- [29] E. J. Candès. The restricted isometry property and its implications for compressed sensing. *Comptes Rendus Mathématique*, vol. 346, no. 9–10, pp. 589–592, 2008. DOI: [10.1016/j.crma.2008.03.014](https://doi.org/10.1016/j.crma.2008.03.014).
- [30] B. K. Natarajan. Sparse approximate solutions to linear systems. *SIAM Journal on Computing*, vol. 24, no. 2, pp. 227–234, 1995. DOI: [10.1137/S0097539792240406](https://doi.org/10.1137/S0097539792240406).
- [31] S. S. Chen, D. L. Donoho, M. A. Saunders. Atomic decomposition by basis pursuit. *SIAM Journal on Scientific Computing*, vol. 20, no. 1, pp. 33–61, 1998. DOI: [10.1137/S1064827596304010](https://doi.org/10.1137/S1064827596304010).
- [32] Y. Zhang, Y. Y. Wang, C. Zhang. Total variation based gradient descent algorithm for sparse-view photoacoustic image reconstruction. *Ultrasonics*, vol. 52, no. 8, pp. 1046–1055, 2012. DOI: [10.1016/j.ultras.2012.08.012](https://doi.org/10.1016/j.ultras.2012.08.012).
- [33] S. G. Mallat, Z. F. Zhang. Matching pursuits with time-frequency dictionaries. *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3397–3415, 1993. DOI: [10.1109/78.258082](https://doi.org/10.1109/78.258082).
- [34] E. T. Liu, V. N. Temlyakov. The orthogonal super greedy algorithm and applications in compressed sensing. *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2040–2047, 2012. DOI: [10.1109/TIT.2011.2177632](https://doi.org/10.1109/TIT.2011.2177632).
- [35] H. Mohimani, M. Babaie-Zadeh, C. Jutten. A fast approach for overcomplete sparse decomposition based on smoothed  $l^0$  norm. *IEEE Transactions on Signal Processing*, vol. 57, no. 1, pp. 289–301, 2009. DOI: [10.1109/TSP.2008.2007606](https://doi.org/10.1109/TSP.2008.2007606).
- [36] G. Cariolaro, T. Erseghe, P. Kraniuskauskas. The fractional discrete cosine transform. *IEEE Transactions on Signal Processing*, vol. 50, no. 4, pp. 902–911, 2002. DOI: [10.1109/78.992138](https://doi.org/10.1109/78.992138).
- [37] J. H. Wu, F. F. Guo, P. P. Zeng, N. R. Zhou. Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence. *Journal of Modern Optics*, vol. 60, no. 20, pp. 1760–1771, 2013. DOI: [10.1080/09500340.2013.858189](https://doi.org/10.1080/09500340.2013.858189).
- [38] Y. R. Liang, G. P. Liu, N. R. Zhou, J. H. Wu. Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion. *Journal of Modern Optics*, vol. 62, no. 4, pp. 251–264, 2014. DOI: [10.1080/09500340.2014.964342](https://doi.org/10.1080/09500340.2014.964342).
- [39] Y. R. Liang, J. H. Wu. New image encryption combining fractional DCT via polynomial interpolation with dependent scrambling and diffusion. *Journal of China Universities of Posts and Telecommunications*, vol. 22, no. 5, pp. 1–9, 2015. DOI: [10.1016/S1005-8885\(15\)60673-2](https://doi.org/10.1016/S1005-8885(15)60673-2).
- [40] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, Z. Hassan. A novel scheme for image encryption based on 2D piecewise chaotic maps. *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, 2010. DOI: [10.1016/j.optcom.2010.04.056](https://doi.org/10.1016/j.optcom.2010.04.056).
- [41] N. R. Zhou, A. D. Zhang, J. H. Wu, D. J. Pei, Y. X. Yang. Novel hybrid image compression-encryption algorithm based on compressive sensing. *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 18, pp. 5075–5080, 2014. DOI: [10.1016/j.ijleo.2014.06.054](https://doi.org/10.1016/j.ijleo.2014.06.054).
- [42] A. S. Arumugam, D. N. Krishnan. Biometric encryption and bio-fusion authentication using combined Arnold transition and permutation matrices. *International Journal of Engineering Science and Technology*, vol. 2, no. 10, pp. 5357–5369, 2010.
- [43] V. Patidar, N. K. Pareek, G. K. Purohit, K. K. Sud. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011. DOI: [10.1016/j.optcom.2011.05.028](https://doi.org/10.1016/j.optcom.2011.05.028).



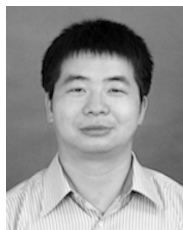
**Ya-Ru Liang** received the B.Sc. degree in automation from Heilongjiang Institute of Technology, China in 2002, the M.Sc. degree in power electronics and power drives from Shenyang University of Technology, China in 2008, and the Ph.D. degree in mechanical engineering from Nanchang University, China in 2016. Currently, she

is a lecturer in Department of Electronic Information Engineering, Jiangxi Agricultural University, China.

Her research interests include image processing, image encryption and information security.

E-mail: liangyaru@jxau.edu.cn

ORCID iD: 0000-0002-2716-0704



**Zhi-Yong Xiao** received the B.Sc. degree in electronic information engineering from Nanchang Hangkong University, China in 2001, and the M.Sc. degree in control theory and engineering from East China University of Technology, China in 2008. He is a Ph.D. degree candidate in mechanical engineering at School of Mechatronic Engineering, Nanchang University, China.

His research interests include image processing, computer vision and pattern recognition.

E-mail: zhyxiao@jxau.edu.cn (Corresponding author)

ORCID iD: 0000-0003-0773-3461