Multimedia Tools and Applications (2023) 82:33465–33497
https://doi.org/10.1007/s11042-023-14573-0

A new image/video encryption scheme based on fractional discrete Tchebichef transform and singular value decomposition

Omar El Ogri[1] · Hicham Karmouni[1] · Mhamed Sayyouri[2] · Hassan Qjidaa[1]

Received: 10 May 2021 / Revised: 22 August 2022 / Accepted: 31 January 2023 /
Published online: 3 March 2023

Abstract
One of the major application areas of the fractional-order discrete transform (FrDTs) is in signal and information security, particularly in signal and image/video encryption. Recently, many researchers proposed techniques that implemented not only the fractional transforms, but also various randomized versions of the FrDTs, which add more security features to signal's encryption. In this paper, we propose a new image/video encryption scheme based on fractional-order discrete Tchebichef transform (FrDTT) using singular value decomposition. The FrDTTs are derived algebraically using the spectral decomposition of discrete Tchebichef polynomials, then the singular value decomposition technique in order to build a basic set of orthonormal eigenvectors which help to develop FrDTTs. Finally, we implement and apply the scheme proposed in this paper for encrypting test images and video sequences. Moreover, we methodically perform the security evaluation in terms of brute force and statistical attacks as well as comparisons with the existing methods in terms of secret key sensitivity and space. The promising experiment results demonstrate the effectiveness and efficiency of our proposed FrDTTs based image encryption techniques.

✉ Omar El Ogri
omar.elogri@usmba.ac.ma

Hicham Karmouni
hicham.karmouni@usmba.ac.ma

Mhamed Sayyouri
mhamed.sayyouri@usmba.ac.ma

Hassan Qjidaa
qjidah@yahoo.fr

[1] CED-ST, STIC, Laboratory of Electronic Signals and Systems of Information LESSI, Dhar El Mahrez Faculty of Science, Sidi Mohamed Ben Abdellah-Fez University, Fez, Morocco

[2] Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, My Abdallah Avenue Km. 5 Imouzzer Road, 72 Fez, BP, Morocco

Keywords Fractional discrete Tchebichef transform · Singular value decomposition · Spectral decomposition · Image encryption · Video encryption

1 Introduction

With the rapid development of network and multimedia technologies, the acquisition and transmission of information has become increasingly fast and convenient. Images and videos are widely distributed on the Internet because of their intuitive and vivid nature and their wealth of information. However, many images do not want to be acquired by illegal users due to multiple privacy and interests. Therefore, how to transmit images and videos safely on the network has become a very important issue. Image and video encryption technology can encrypt before propagation to hide the original information, which is an effective method to solve the image security problem. There are various techniques like Steganography, watermarking, cryptography available for the security of information from the invaders. Among these techniques, Steganography is used to embed the text into another image for the protection of text [4]. In watermarking, the original image is applied as watermarked image on cover image [27]. In cryptography, the whole image is transformed in such a form that is difficult for the interloper to comprehend it, so used for the protection of images [29] and videos [40]. Every security technique has its own significance and applications. But, encryption is one of the best methods used in cryptography for security of images and videos. This method is performed to create confusion and diffusion in the images and videos (or frames of videos). Due to presence of chaos in the ciphered information, hacker will consider information as random noise. The appearance of encrypted form will protect information from getting stolen. Further, encryption can be performed with different algorithms to hide actual data from hackers. The several techniques available for encryption algorithm are chaotic mapping [14], matrix transformation [1], scrambling [46], compressive sensing [60] and encryption using wavelet transform [7] etc. At present, image encryption can be performed in the spatial domain and the transform domain. The spatial domain mainly uses image scrambling, substitution, and diffusion to complete the encryption operation. The initial image scrambling is mostly based on Arnold transform, magic square transform, etc. In recent years, some space-domain image encryption algorithms combined with chaos theory have been proposed [32, 55]. Due to their strong key sensitivity and scrambling characteristics, these similar algorithms have high research value and important research significance. The transform domain encryption algorithm starts from the characteristics of the image transformation matrix and uses the key to generate a new transformation matrix to transform the image, thereby transforming the original clearly identifiable image into random noise information. This encryption method has a higher encryption efficiency. High, anti-interference characteristics, and easy to achieve compression. The characteristics of consideration in any encryption systems are perceptual transparency, capacity, and tamper resistance. Perceptual transparency is the ability to mask the existence of secret data from human visual system [13, 42, 69]. Capacity is the basic concern of any encryption algorithm that allows to increase the amount of secret data hidden into cover video by considering the perceptual transparency. Larger the amount of data hiding capacity, the algorithm is considered better. An encryption method is tampered resistant if the receiver gets the secret data exactly in the same way sent by the sender.

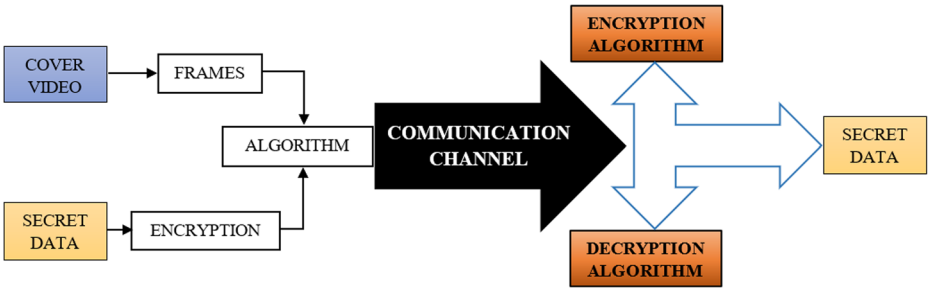


Fig. 1 Layout of steganography

Different components of information security are (Fig. 1):

(i) Cover Video: Envelope video that holds the secret data.
(ii) Secret data: Important information concealed from the intruder.
(iii) Stego Video: Video after encryption data.
(iv) Encryption and Decryption algorithm: Strategy followed to conceal secret data by sender and extracted by the receiver.

Although several techniques are discussed in literature that are used for the security of images and videos, but in most of the techniques in the spatial domain require a large amount of computations, so alternative solution is needed. To fulfill this requirement, two different keys (fractional parameter and random phase code) keys are introduced on each block. By operating in frequency domain, the amount of computation can be reduced, and more efficient processes can be used, for example, digitally encrypted processing in the frequency domain using fractional discrete Tchebichef transform. Secondly, the use of fractional transforms based on Singular Value Decomposition (SVD) has improved the performance of several applications, by providing an extra degree of freedom [22, 36, 37, 66]. It attracts security systems, so many fractional transforms have been implemented for the encryption of images and videos, but still the use of modified fractional transform (like dual parameter based) is required for more improvement. Another motivation is to enhance the performance parameters (like PSNR, MSE etc.) of existing techniques in order to provide better security to the images and videos from hackers. As, discussed in literature the use of fractional transform and random phase keys in combination provides better results. In this paper, we present three contributions in the field of image/video encryption based on FrDTTs. In the first contribution, we develop a new fractional transform for data security based on FrDTTs and the decomposition (SVD) technique in order to build a basic set of orthonormal eigenvectors. In the second contribution, we introduce a new encryption and decryption algorithm for one or various images simultaneously based on proposed FrDTTs, our algorithm has good encryption effect, larger secret key space, and high sensitivity to the secret key. In the third contribution, we propose a novel method for video sequences encryption by introducing a bloc based FrDTTs encryption structure. Finally, we implement and apply the scheme proposed in this work for the encryption of standard test images and video sequences. A methodical security evaluation in terms of brute force and statistical attacks has been followed for each of the proposed scheme. We also verified their resistance against additive noise and transmission errors in the communication channel. The simulation results have demonstrated the considerable contribution of the proposed scheme compared to the existing methods as well as the interest of their uses.

The rest of this paper is structured as follows: Section 2 introduces a related work. Section 3, the definition, and properties of the classical DTTs. Section 4 then provides details of the procedure for deriving FrDTTs. Section 5, an encryption and decryption algorithm for images and video by the proposed FrDTTs. The results of simulations that prove the efficiency of the proposed encryption algorithm based FrDTTs in Section 5. Finally, closing remarks of the paper are available in Section 6.

2 Related work

Information security has become a significant issue for protecting the secret information during transmission in practical applications in the era of information. In recent years, a raft of information security schemes has been used in image encryption, researchers have made some related achievements in the field of image analysis in the encrypted domain. These works can be roughly categorized into two types.

One category focused on the image/video encryption in the space domain. In the literature and in image encryption, several algorithms are developed according to the so-called permutation-diffusion architecture [34, 35, 54]. This architecture includes two important operations, the permutation and the diffusion, the combination between the two is also possible. Algorithms based on the parallel computing system [59] and on piecewise coupled map lattice [53] have shown exceptionally good properties in many aspects regarding security, complexity, speed, computational overhead, etc. Wang et al. [50, 51] suggested an image encryption algorithm based on matrix semi-tensor product theory and the image encryption algorithm based on fractal sorting matrix [64, 65]. The encryption of digital images by using chaotic system is mainly based on the excellent randomness of this system, the chaotic system is usually combined with image encryption methods based on spatial domain. The chaotic system was proposed for data encryption, Fridrich [14] first proposed image encryption scheme based on chaotic system. Wang et al. [52], proposed another image encryption method based on full chaos coupled mapping lattice, then a novel chaotic block image encryption algorithm based on dynamic random growth technique [57]. This encryption algorithm combined the dynamic random growth technique and chaotic system to effectively enhance the key space. Batham, et al. [3], a secure video encryption algorithm which uses an efficient compression technique called as hybrid video codec and encrypts the compressed video frames bitstreams along with motion vectors of each frames using indexed based chaotic sequence. A novel chaotic image encryption scheme using DNA sequence operations was proposed by Xing-Yuan Wang et al. [58].

The other category mainly paid attention to the image/video encryption in the frequency domain. Image encryption algorithm based on frequency domain encrypts the frequency coefficients based on the characteristics of human visual system, it can encrypt important data which is called selective encryption or partial encryption, so that the amount of encryption data is significantly reduced and the encryption efficiency is improved. At present, there are many research on digital image encryption algorithms based on fractional Fourier transform [6, 28, 45, 49]. For example, Unnikrishnan et al. [49] proposed a double random phase encoding scheme, which uses two independent random phase masks to encrypt the image Smooth white noise; Joshi et al. [18] proposed an image encryption algorithm combining Fourier transform and radial Hilbert

transform; Lang et al. [28] proposed image encryption based on multi-parameter discrete fractional storage transform and chaos algorithm. Chen et al. [6], proposed an image encryption algorithm was proposed using singular value decomposition and Arnold transform.

One of the major limitations of these image encryption algorithms is that the encrypted image is a complex-valued image, which also contains amplitude and phase information, which is very unfavorable for transmission and storage. Especially as people have higher and higher requirements for real-time transmission, it is very necessary to propose an image encryption technology that meets real-number transformation, high encryption security, strong noise resistance, and fast calculation speed. The fractional transforms are mostly used for several purposes such as encryption, compression, noise reduction, filtering, watermarking etc. Recently, a number of fractional transforms have been exploited for image and video security in the real domain, such as image encryption based on fractional Fourier transform (FrFT) [28, 31], image/video encryption algorithms based on fractional discrete cosine transform [26, 41, 63], image encryption with fractional sine transform (FrST) [43], image encryption based on fractional discrete Meixner moments (FrDMM) [22], discrete fractional Krawtchouk transform and its application in image encryption and watermarking (FrKT) [36, 37], color image encryption scheme based on fractional Hartley transform (FrHT) [24, 25], fractional Mellin transform (FrMT) [71, 72], encryption of video main frames in the field of DCT transform [2], image and video processing using discrete fractional transforms [17] and secure video steganography using Framelet transform and singular value decomposition [47].

3 Discrete Tchebichef transform

Discrete Tchebichef polynomials were introduced by Pafnuty Chebyshev in [5], and first used in image analysis by Mukundan et al. [39] as a basis function for image moments. The classical Tchebichef orthogonal polynomials of order n are defined from the hypergeometric function ${}_3F_2(\cdot)$ as follows:

$$t_n(x) = \sum_{k=0}^{N-1} a_{k,n} x^k = (1-N)_n \, F_2(-n, -x, 1+n, 1, 1-N, 1) \tag{1}$$

where ${}_3F_2(.)$ is the hypergeometric function, defined as:

$$F_2(a, b, c, d, e, z) = \sum_{k=0}^{n} \frac{(a)_k (b)_k (c)_k}{(d)_k (e)_k} \frac{z^k}{k!} \tag{2}$$

and $(a)_k$is the Pochhammer symbol given by:

$$(a)_k = \frac{\Gamma(a+k)}{\Gamma(a)} = a(a+1)\ldots(a+k-1) \tag{3}$$

The orthogonal Tchebichef polynomial of order n can be written explicitly as follows:

$$t_n(x) = n! \sum_{k=0}^{n} (-1)^{n-k} \binom{N-1-k}{n-k} \binom{n+k}{n} \binom{x}{k} \tag{4}$$

Tchebichef polynomials satisfy the orthogonality condition with norm squared:

$$\rho(n) = (2n)! \binom{N+n}{2n+1}, n = 0, 1, \cdots, N-1, \tag{5}$$

with the binomial coefficient noted $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

For reasons of numerical stability and limited dynamic range, normalized Tchebichef polynomials are introduced by Mukundan [39], as follows:

$$\widetilde{t}_n(x, N) = \frac{t_n(x, N)}{\rho(n)} \tag{6}$$

where $\rho(n)$ is an appropriate constant independent of x that serves as a scaling factor, such that N^n.

The scaled Discrete Tchebichef polynomials obey a general three-term recursive relation [9]:

$$t_n(x) = \frac{(Ax + B)}{n} t_{n-1}(x) + \frac{C}{n} t_{n-2}(x) \tag{7}$$

with

$$\begin{aligned} A &= \frac{2}{n}\sqrt{\frac{4n^2-1}{N^2-n^2}}, B = \frac{1-N}{n}\sqrt{\frac{4n^2-1}{N^2-n^2}}, \\ C &= \frac{1-n}{n}\sqrt{\frac{2n+1}{2n-3}}\sqrt{\frac{N^2-(n-1)^2}{N^2-n^2}} \end{aligned} \tag{8}$$

$$t_0(x) = \frac{1}{\sqrt{N}}, t_1(x) = \frac{2x + 1 - N}{N}\sqrt{\frac{3}{N(N^2-1)}} \tag{9}$$

where $n, x = 2, 3, \ldots, N - 1$,

For a digital image $f(x, y)$ its DTT can be defined as

$$T_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} t_n(x) t_m(y) f(x, y) n, m = 0, 1, \ldots . N-1 \tag{10}$$

The corresponding discrete Tchebichef transform (iDTTs, inverse DTTs) is

$$f(x, y) = \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} t_n(x) t_m(y) T_{nm} \tag{11}$$

In practical applications, the DTTs of an image can be expressed as a matrix:

$$\mathrm{T} = \mathrm{C}^T \mathrm{fC} \tag{12}$$

where $\mathrm{T} = \{T_{nm}\}_{n=0,m=0}^{n=N-1,m=N-1}$, $\mathrm{C} = \{t_n(x)\}_{n=0,x=0}^{n=N-1,x=N-1}$ and $\mathrm{f} = \{f(x, y)\}_{x,y=0}^{x,y=N-1}$.

Similarly, the inverse moment transform can be represented using the matrix as follows [10]:

$$\mathrm{f} = \mathrm{CTC}^{T} \tag{13}$$

The DTTs introduced into the literature are calculated for integer orders. In the following sections, we propose the calculation of the DTTs for fractional order (real) in order to generalize their calculation and to benefit other properties for non-integer orders.

4 Proposed fractional-order discrete Tchebichef transform

In this section, we provide a framework for deriving FrDTTs by the decomposition the properties of the eigenvalues and eigenvectors of the DTTs matrix which help to develop the new fractional discrete Tchebichef polynomials. In the following subsections, analysis regarding the decomposition of the polynomial's matrices and important properties of FrDTTs are provided.

4.1 Eigenvalues and eigenvectors of the discrete Tchebichef polynomials

For a DTTs matrix $\mathrm{C} = \{t_n(x)\}_{n,x=0}^{n,x=N-1}$ of the order N will be noted C in the following. The matrix C checks the following properties [8]:

Property (i): It is real matrix.
Property (ii): It is unitary, i.e., $\mathrm{C}^{H}\mathrm{C} = \mathrm{C}\mathrm{C}^{H} = \mathrm{I}$, where C^{H} is the transposed matrix of C and I is the identity matrix.
Property (iii): It is orthogonal,
Property (iv): It is symmetrical, so $\mathrm{C} = \mathrm{C}^{T}$.
Property (v): It has the following two eigenvalues: $\lambda_k = (-1)^k k = 0, 1$.
The proof of property (v) is given in Appendix A.

The characteristic of the unitary matrix makes the eigenvalues of C, λ_k distributed on the unit circle, that is, $\lambda_k = e^{j\varphi_k}$ (φ_k is a real number). Perform eigenvalue decomposition on the DTT matrix to obtain the corresponding eigenvalue matrix D and eigenvector matrix V, satisfying

$$\mathrm{C} = \mathrm{VDV}^{H} = \sum_{n=1}^{N} \mathrm{U}_n e^{-j\varphi_n} = \sum_{n=1}^{N} \mathrm{U}_n \lambda_n \tag{14}$$

where, V is the unitary matrix, which is composed of N eigenvectors nu of C, V^{H} is the conjugate transpose matrix of V, satisfying $\mathrm{U}_n \triangleq u_n u_n^{H}$, D is the diagonal matrix whose diagonal is the eigenvalue λ_k.

According to the above properties of C, the eigenvalue multiplicities of the matrix C can be given by the following Table 1:

Table 1 Multiplicities of the eigenvalues for matrix C

N	$2N_0$ (*Even*)	$2N_0+1$ (*Odd*)
Multiplicity of λ_0	$\frac{N}{2}$	$\frac{N+1}{2}$
Multiplicity of λ_1	$\frac{N}{2}$	$\frac{N-1}{2}$

where N is the size of Discrete Tchebichef polynomial matrix.

According to the spectral theorem [61]:

$$\mathrm{C} = \sum_{k=0}^{1} \lambda_k \mathrm{P}_k = \lambda_0 \mathrm{P}_0 + \lambda_1 \mathrm{P}_1 \tag{15}$$

where P_k denotes the spectral projector for Cassociated with the eigenvalueλ_k. Also, for any integer$m$, has the following spectral decomposition [61]:

$$\mathrm{C}^m = \lambda_0^m \mathrm{P}_0 + \lambda_1^m \mathrm{P}_1 \tag{16}$$

we write the equation above for $m = 0, 1$ on the matrix form, to obtain the two matrices P_0 and P_1.

$$\begin{pmatrix} \mathrm{I} \\ \mathrm{C} \end{pmatrix} = \sum_{k=0}^{1} \lambda_k^m \begin{pmatrix} \mathrm{P}_0 \\ \mathrm{P}_1 \end{pmatrix} = \mathrm{H} \begin{pmatrix} \mathrm{P}_0 \\ \mathrm{P}_1 \end{pmatrix} \text{ with } \mathrm{H} = \begin{pmatrix} \mathrm{I} & \mathrm{I} \\ \lambda_0 \mathrm{I} & \lambda_1 \mathrm{I} \end{pmatrix} \tag{17}$$

Using the Eq. (17), the expression $\mathrm{HH}^H = 2\mathrm{I}$, to prove the relation between the inverse of H and transpose of H we find $\mathrm{H}^{-1} = 0.5\mathrm{H}^T$.

By multiplying the $\mathrm{H}^{-1} = 0.5\mathrm{H}^T$ relation of the two left sides of Eq. (17), we obtain the following expressions for the projection matrices P_0 and P_1:

$$\mathrm{P}_0 = 0.5(\mathrm{I} + \mathrm{C}) \textbf{ and } \mathrm{P}_1 = 0.5(\mathrm{I} - \mathrm{C}) \tag{18}$$

In the following, we will study the eigenvalues and the eigenvectors of the two spectral projector matrices P_0 and P_1., then we will present their properties.

From Eq. (18), we can get some properties of P_0 and P_1:

Property (a): $\mathrm{P}_\mathrm{i}^T = \mathrm{P}_\mathrm{i}$ ***and*** $\mathrm{P}_\mathrm{i}^2 = \mathrm{P}_\mathrm{i}, i = \boldsymbol{0}, \boldsymbol{1}$.
Property (b): $\mathrm{P}_0\mathrm{P}_1 = 0$, where 0 denotes the zero matrix.
Property (c): The eigenvalues of a projection matrix P_0 and P_1 are only 0 and 1 [44].
The multiplicity of eigenvalue 1 for P_0 is equal to the multiplicity of eigenvalue 1 of C.
The multiplicity of eigenvalue 1 for P_1 is equal to the multiplicity of eigenvalue −1 of C.

The proof of properties (a)-(b) and (c) is given in Appendix B.

Lemma 1 The eigenvectors of P_0 are orthogonal to those of P_1, for the non-zero eigenvalues.

Lemma 2 For the non-zero eigenvalues: the eigenvectors of P_0 and P_1 are the eigenvectors of C, corresponding to eigenvalues $\lambda_0 = 1$, $\lambda_1 = -1$ of C, respectively.

The proofs of both Lemmas 1 and 2 are given in Appendix C.

In the following, by performing the SVD decomposition of P_0 and P_1, we have derive a set of orthonormal eigenvectors of C by using the decomposition SVD of its orthogonal projection matrices on its eigenspaces [16, 44].

SVD of its orthogonal projection matrices on its eigenspaces [16, 44].

The SVD decomposition of P_0 and P_1, are given as:

$$\mathrm{P}_0 = \mathrm{U}_0\mathrm{S}_0\mathrm{V}_0^T \textbf{ and } \mathrm{P}_1 = \mathrm{U}_1\mathrm{S}_1\mathrm{V}_1^T \tag{19}$$

where U_i ***and*** V_i, $(i = 1, 2)$ are unitary matrices and S_i a diagonal matrix with real and positive coefficient. Since the singular values of P_0 and P_1 are square root of non-negative eigenvalues

Table 2 Multiplicities of the non-zero eigenvalues for P_0 and P_1

N	P_0	P_1
$2N_0$ (***Even***)	$\frac{N}{2}$	$\frac{N}{2}$
$2N_0+1$ (*Odd*)	$\frac{N+1}{2}$	$\frac{N-1}{2}$

of $P_0P_0^T$ and $P_1P_1^T$, respectively, using properties (a), (b) and (c), we can easily rewrite the Eqs. (19) as follows:

$$P_0 = P_0^T P_0 = V_0 S_0 V_0^T; P_1 = P_1^T P_1 = V_1 S_1 V_1^T \tag{20}$$

It can be observed from Eqs. (20) that:

$$P_0 V_0 = V_0 S_0; P_1 V_1 = V_1 S_1 \tag{21}$$

The above equation shows that V_0 and V_1 are a set of orthonormal eigenvectors of P_0 and P_1, respectively.

According to Table 1 and *propriety (c)*, the multiplicities of the non-zero eigenvalues for P_0 and P_1 are summarized for an $N \times N$ transform as follows:

According to the Table 2 and *Lemma 2*, we are now ready to derive a set of orthonormal eigenvectors of C.

Taking u_i and v_j be the ith and jth column of V_0 and V_1,respectively, a set of orthonormal eigenvectors V of C can be written as follows:

$$V = \begin{cases} \left[u_1, u_2, \ldots., u_{\frac{N}{2}}, v_1, v_2, \ldots., v_{\frac{N}{2}}\right], & \text{if Nis even} \\ \left[u_1, u_2, \ldots., u_{\frac{N-1}{2}}, u_{\frac{N+1}{2}}, v_1, v_2, \ldots., v_{\frac{N-1}{2}}\right], & \text{if Nisodd} \end{cases} \tag{22}$$

4.2 Definition of fractional-order discrete Tchebichef polynomials

In this section, traditional DTTs are extended to FrDTTs in order to effectively improve their performance in image reconstruction. Such extension mainly involves the modification of Fractional-order Discrete Tchebichef Polynomials (FrDTPs) matrix that also satisfies the properties of the polynomial matrices in the DTTs, these polynomials replace the eigenvalues

Table 3 Main mathematical properties of FrDTPs

For $\alpha=0$	It is obvious C^0 reduces to the identity matrix $C^0=VD^0V^H=VV^H=I$.
For $\alpha=1$	It is obvious then the FrDTPs is reduced to the traditional discrete Tchebichef polynomials $C^1=VD^1V^H=C$. where C is the classical DTTs matrix
Additivity property	$C^\alpha C^\beta=(VD^\alpha V^H)(VD^\beta V^H)=VD^{\alpha+\beta}V^H=C^{\alpha+\beta}$
Unitary property of FrDTPs	$C^\alpha C^{-\alpha}=(VD^\alpha V^T)(VD^{-\alpha}V^T)=VD^{(\alpha-\alpha)}V^T=I$

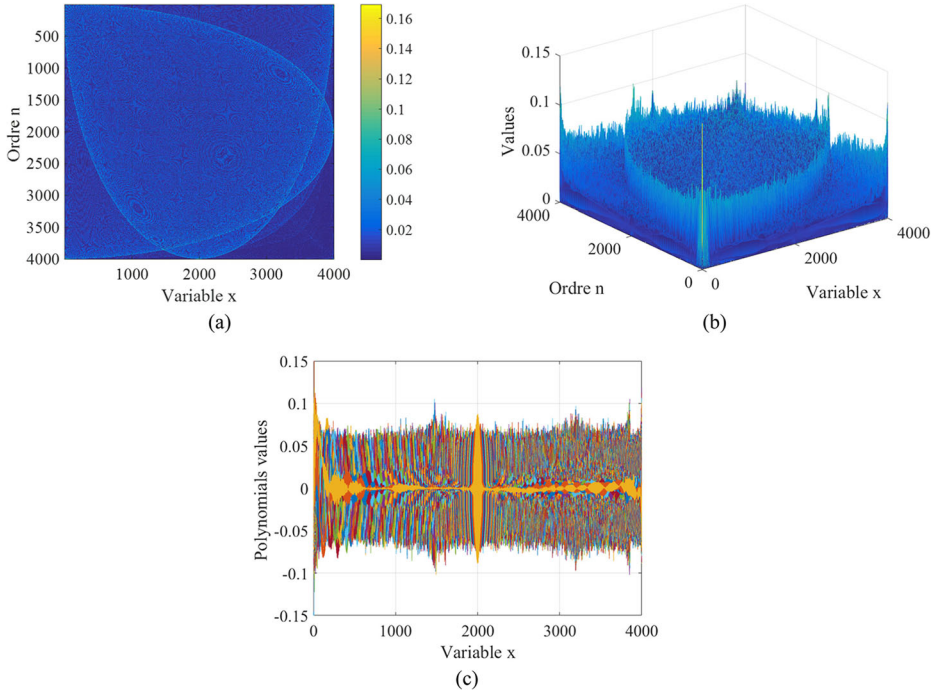


Fig. 2 **a** 2D plot of FrDTPs, **b** 3D plot of FrDTPs and **c** all polynomial curves of FrDTPs using algorithm 1 with $\alpha = 1$

$\lambda_k = e^{j\varphi_k}$ with its α^{th} power $\alpha\Re$ on the basis of matrix eigen-decomposition, that is The diagonal matrix D is replaced by its power of α, so that the definition of FrDTPs matrix C^{α} is:

$$C^{\alpha} = VD^{\alpha}V^{H} = \sum_{k=0}^{N-1} \lambda_k^{\alpha} v_k v_k^{H}, k = 0, \cdots, N-1 \tag{23}$$

where $V = [v_0, v_1, \ldots\ldots\ldots, v_{N-1}]$ with v_k $(k = 0, 1, \ldots\ldots\ldots, N-1)$ is the C eigenvector obtained from (Eq. 15), and D^{α} is defined as:

$$D^{\alpha} = \boldsymbol{Diag}\left\{\boldsymbol{1}, e^{-j\alpha}, e^{-j\boldsymbol{2}\alpha}, \ldots\ldots\ldots, e^{-j(N-\boldsymbol{1})\alpha}\right\} \tag{24}$$

The main mathematical properties of FrDTPs are shown in Table 3 [22, 36, 38]. In addition, we will show in detail the steps of this proposed algorithm to calculate the coefficients of the matrix of fractional discrete Tchebichef polynomials. Algorithm 1 summarizes the steps for calculating the FrDTPs matrix.

It should be noted that the eigenvalue decomposition of the Tchebichef transformation matrix will be used to define the discrete FrDTPs. The eigenvalues and vectors of FrDTPs are derived and some properties of FrDTPs are also studied. However, the proposed algorithm satisfies exactly the property of orthogonality up to the last order of FrDTPs ($n = 4000$) which shows the numerical stability of the values of FrDTPs calculated by the algorithm proposed. Therefore, the orthogonality of the FrDTPs polynomial matrix can be destroyed due to a numerical approximation in the calculation process. Indeed, the following Fig. 2 shows the distribution of the polynomial coefficients of the FrDTPs up to the order $n = 4000$. We can see

that the FrDTPs values are well calculated, stable and verified all properties ((iii) end (iv)) of orthogonality and symmetry. It is important to also note that the proposed stability condition can be easily adapted for the stabilization of computation of other types of discrete orthogonal polynomials of high orders.

Algorithm 1 Computation of the Fractional Discrete Tchebichef Polynomials with respect to the order n

Inputs: N : The maximum value of the variable x , $N_{\max}$: polynomial order, α : Fractional parameter ***Output:*** Coefficient matrix of Fractional Discrete Tchebichef Polynomials *FrDTPs*	

Step 1	***for*** $n \leftarrow 0$ *to* N-1 ***do***
	for $x \leftarrow 0$ *to* N-1 ***do***
	Compute the values of $t_0(x)$ *and* $t_1(x)$ *using Eq. (9)*
	end
	end

Step 2	***for*** $n \leftarrow 2$ *to* N-1 ***do***
	for $x \leftarrow 0$ *to* N-1 ***do***
	Compute the values of A, B *and* C *using Eq. (8).*
	Compute the values of $\boldsymbol{C} = \{t_n(x)\}_{n=0,x=0}^{n=N-1,x=N-1}$ *using Eq. (7).*
	end
	end

Step 3	*Compute the projection matrices* $\boldsymbol{P}_0$ *and* $\boldsymbol{P}_1$ *using Eq. (18) are the eigenvectors of* $\boldsymbol{C}$ *,* *corresponding to eigenvalues* $\lambda_0 = 1$, $\lambda_1 = -1$ *of* $\boldsymbol{C}$ *, respectively*
Step 4	*Compute the values of* $\boldsymbol{U}, \boldsymbol{S}$ *and* $\boldsymbol{V}$ *using Eq. (19) for derive a set of orthonormal eigenvectors of* $\boldsymbol{C}$ *by using the SVD decomposition of* P_0 *and* P_1 $[U_0, S_0, V_0] = SVD(\boldsymbol{P}_0)$; $[U_1, S_1, V_1] = SVD(\boldsymbol{P}_1)$;
Step 5	***for*** $k \leftarrow 0$ *to* N-1 ***do*** *Compute the values of* $FrDTPs = \boldsymbol{C}^{\alpha}$ *using Eq. (23)* ***end*** $FrDTPs = \boldsymbol{C}^{\alpha}$

It is worth mentioning that when α is an unnatural number, $(\pm 1)^{\alpha} = e^{\pm j2\pi\alpha}$ is a complex number, so the matrix C^{α} is also a complex matrix. In order to obtain a FrDTTs matrix that always satisfies the real matrix, the eigenvalues of the matrix should not include ±1. Compared with DCTs, when the signal length N of the matrix dimension is a multiple of 4, it does not contain the eigenvalue ±1. DTTs has certain advantages. It satisfies that when the matrix dimension is even, that is, $N = 2N_0$ does not contain the eigenvalue ±1. It is more flexible and convenient in practical applications [11, 12, 21].

4.3 Proposed fractional-order discrete Tchebichef transform

The generalized FrDTTs are obtained from the FrDTPs. It can be seen from Eq. (23) that the inverse matrix of C^{α} can be obtained by its negative order matrix $C^{-\alpha}$. The FrDTTs are obtained from the FrDTPs presented in the previous subsection. Thus, the 1D forward FrDTTs of signal $f(x)$ of length N with fractional order α can be defined as follows:

$$\mathrm{F}^{\alpha} = \mathrm{C}^{\alpha} f \tag{25}$$

The reconstruction of the signal $f(x)$can be found from its transform by using the following expression:

$$f = \mathrm{F}^{\alpha}\mathrm{C}^{-\alpha} \tag{26}$$

In 2D case, the FrDTTs in terms of polynomials matrices C^{α} with fractional order $(\alpha,\ \beta)$, for an image with intensity function $f(x,\ y)$, can be defined as follows:

$$\mathrm{F}^{\alpha,\beta} = \mathrm{C}^{\alpha}\mathrm{f}\mathrm{C}^{\beta} \tag{27}$$

The Eq. (27) leads to the following inverse reconstruction procedure:

$$\mathrm{f} = \mathrm{C}^{-\alpha}\mathrm{F}^{\alpha,\beta}\mathrm{C}^{-\beta} \tag{28}$$

5 Proposed image/video encryption scheme using FrDTTs

In the several applications of image/video processing like business conferencing, military communication, secure transfer of images, Medical imaging, Road safety, Electronic signature, Remote monitoring [15, 30] etc., the content of image/video is required to be preserved. So, for the preservation of image/video information security techniques are required. To meet this requirement several techniques had been invented. Recently, a number of fractional transform based image/video encryption methods have been widely studied in recent years [19, 20, 22, 62, 67, 73]. In this section, an FrDTTs based image/video encryption and decryption scheme is proposed. Offering good security quality, resistance against image processing and large key space and high robustness against various kinds of attacks. The proposed scheme is a real-value-toreal-value mapping in encryption and decryption processes. In summary, different fractional orders will generate different FrDTTs matrices. Such characteristics can be well applied to image/video encryption. This section introduces a new image/video encryption method based on FrDTTs and gives detailed steps of the encryption and decryption process. Figure 3 illustrates the flowchart of the image/video encryption and decryption processes, and details are given in the following.

5.1 Encryption process

As mentioned above, different fractional orders $(\alpha_k,\ \beta_k)$ result in different C^{α_k} and C^{β_k}. This property can be used for image encryption efficiently. Let a sequence of video frames have R frames of size $N\times M$, which we note I_r, $r = 1,2, \cdots, R$. Each frame I_r is divided at the beginning into K blocks B_k, $k = 1,2, \cdots, K \in \mathbb{N}*$ of width n and length m. Thus, each B_k block is encrypted separately as shown in Fig. 4. Let $\mathrm{C}^{\alpha_{x_k}}$, $\mathrm{C}^{\alpha_{y_k}}$, $\mathrm{C}^{\beta_{x_k}}$ and $\mathrm{C}^{\beta_{y_k}}$ be real FrDTTs matrices of size $n\times m$ constructed according to Eq. (27) with $\alpha_{x_k}, \alpha_{y_k}, \beta_{x_k}$ and β_{y_k} being fractional orders. Thus, for each value of $k = 1, 2, \cdots, K$, the block B_k is encrypted in the following steps:

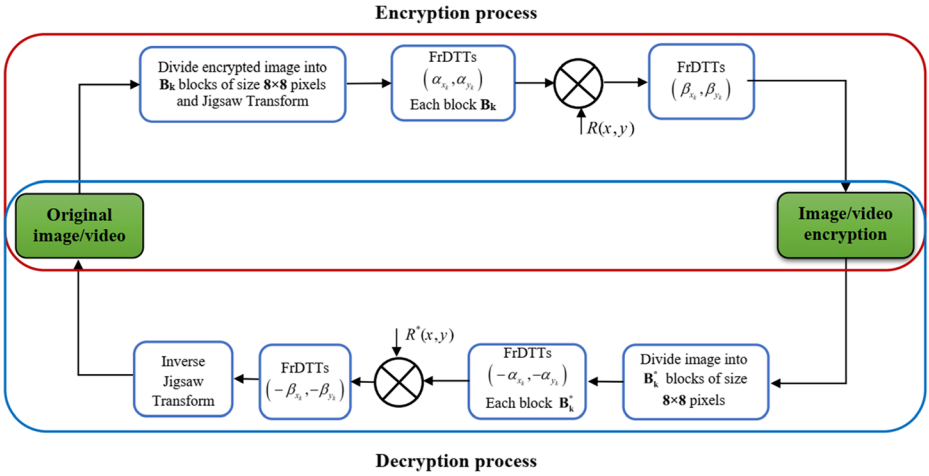


Fig. 3 The flowchart of the proposed scheme

Step 1. This step alters the image in the transverse direction, the original image I_r divided into sub-blocks B_k of size 8 × 8 pixels. Then each of these image blocks B_k undergoes a Jigsaw Transform (JT) [22]: $B_k = \{b_k(i, j),\ 0 \le i, j < 7\}$ $(k = 1, 2, \ldots, N^2/64)$.

Step 2. The two-dimensional FrDTTs of the fractional order $\alpha_{x_k}, \alpha_{y_k}$ are computed for each block B_k by using the following equation: $F_{B_k}^{\alpha_{x_k},\alpha_{y_k}} = C^{\alpha_{x_k}} B_k C^{\alpha_{y_k}}$. The transform matrix of one block is denoted by $F_{B_k}^{\alpha_{x_k},\alpha_{y_k}}$. with $C^{\alpha_{x_k}}$ and $C^{\alpha_{y_k}}$ the matrix generated from the fractional discrete Tchebichef matrix defined in Eq. (27).

Step 3. To ensure the security of each block $B_k$we secretly select the blocks (8 × 8) in image $f(x, y)$. The secret key FrDTTs (Key1) of fractional order $\alpha_{x_k}, \alpha_{y_k}$ corresponds to the position of the selected blocks.

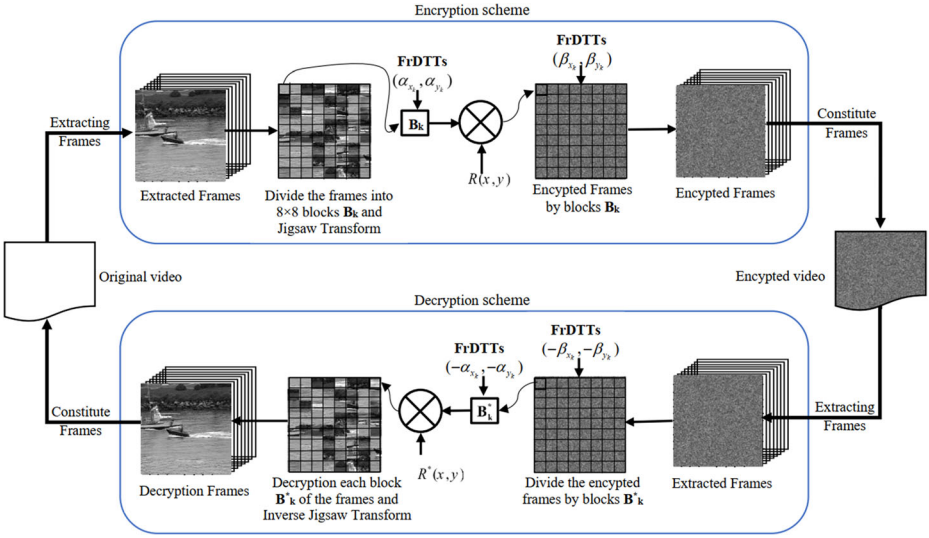


Fig. 4 Scheme of the encryption and decryption system based on FrDTTs

Step 4. Perform data masking on each block of the original image, then the pixels of the output of each block are multiplied by a random phase code $R(x, y)$ (Key2). With $R(x, y)$is chosen to be a phase function $e^{i\varphi(x, y)}$, where $\varphi(x, y)$ is a random function uniformly distributed over $[0, 2\pi]$.

Step 5. For the last step of the encryption procedure, introduces the last security key FrDTTs (Key3) of fractional order β_{x_k}, β_{y_k} into the $f(x, y)$ image to produce the encrypted final image I_r.

5.2 Decryption process

The decryption process is the inverse transformation of the encryption process. Based on FrDTTs satisfying exponential additivity, the fractional orders $\alpha_{x_k}, \alpha_{y_k}, \beta_{x_k}$ and β_{y_k} can be selected. Figure 4 shows the main steps of decryption procedure which can be described in the following:

Step 1. The first step of the decryption procedure, an inverse FrDTTs of order $-\beta_{x_k}, -\beta_{y_k}$ is performed on the encrypted image I_r then divide the image into small non-overlapping blocks $(B_k)^*$ of size 8 × 8 pixels. $(B_k)^* = \{b_k^*(i,j), 0 \le i, j < 7\}(k = 1, 2, \ldots, N^2/64)$.

Step 2. The FrDTTs matrix $\left(F_{B_k}^{\alpha_{x_k}, \alpha_{y_k}}\right)^*$ is computed for each decryption block $(B_k)^*$ by $\left(F_{B_k}^{\alpha_{x_k}, \alpha_{y_k}}\right)^* = C^{-\alpha_{x_k}}(B_k)^* C^{-\alpha_{y_k}}$.

Step 3. Perform the inverse FrDTTs on each block, for one block coefficients $(B_k)^*$ multiplied with the conjugate of the random phase mask $R^*(x, y)$.

Step 4. For the last step of the decryption procedure, introduce the inverse FrDTTs of fractional order $-\alpha_{x_k}, -\alpha_{y_k}$ in each frame blocks, then we undergo an inverse Jigsaw transformation (IJT) to produce the final decrypted frame I_r.

The main advantage of the proposed method is that for a single frame I_r we use 4× fractional orders $\alpha_{x_k}, \alpha_{y_k}, \beta_{x_k}$ and β_{y_k} instead of 4 fractional orders in the method FrDTTs, which significantly improves the secret key space. In addition, the use of the real FrDTTs transform and block random phase makes the proposed video image sequence encryption algorithm more efficient in terms of transmission rate and computational complexity. The process can be

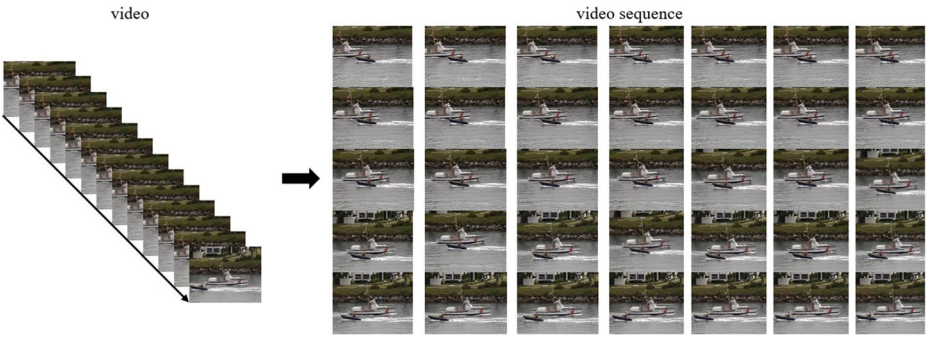


Fig. 5 Picture of a video sequence

defined as a sequence of images presented at a certain rate expressed in the number of frames per second (FPS) (Fig. 5).

6 Simulation results

In this section, we first analyze the fractional-order transformation performance of various encryption methods from the perspective of sensitivity analysis, key space analysis and robustness to the noise attack. In the experiments, we use "Lena" and "Peppers" images of different sizes. Then, we present simulation results of applying the proposed block-based encryption method on a few test video image sequences [48, 68] of standard CIF (352 × 288) and gray level (8bits) format.

6.1 Histogram analysis

The histogram is a very important analysis method used to describe the number of pixels in the image with different gray levels and their frequency of occurrence. The histograms of the original images usually are different, while those of encrypted images obey a uniform distribution, by which the attackers cannot obtain useful information. Mathematically, the variances of histograms are calculated by [70]:

$$Var(Y) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2} \left(Y_i - Y_j\right)^2 \tag{29}$$

where Y is the vector of the histogram values and $Y = \{Y_1, Y_2, \ldots, Y_{256}\}$, Y_i and Y_j are the numbers of pixels which gray values are equal to i and j respectively.

The variance of the histogram reflects the histogram uniform distribution for the encrypted video sequence, where both are inversely proportional. Low variance means a uniform histogram. Table 4 shows the variances of histograms for the test video sequence. The variances of the encrypted video sequence are smaller than the variances of the original video sequence. Figure 6a, b, c and d shows the histograms and pixel distributions of the original images Lena and Peppers. Although the histograms and pixel distributions of the two original images are different from each other, the histograms of encrypted images are almost the same, following a nearly uniform distribution. Thus, one believes that the attackers cannot obtain any useful information by histogram analysis.

To evaluate the security of the proposed method against statistical histogram analysis. Let a sequence of video images in CIF format composed of 100 frames and Q a secret key which is

Table 4 Variances of histograms for both Original and encrypted video sequence

Video		Variances of histograms				Average value
		Frame 1	Frame 2	Frame 3	Frame 4	
Original video sequence	Tennis	1.17×10^5	2.13×10^5	1.02×10^5	5.01×10^5	$\mathbf{2.33 \times 10^5}$
	CoastGuard	7.9×10^5	8.62×10^5	6.3×10^5	9.01×10^5	$\mathbf{7.95 \times 10^5}$
Encryption video sequence	Tennis	248.471	257.1392	262.943	249.451	**254.50**
	CoastGuard	291.918	287.439	294.632	296.158	**292.54**

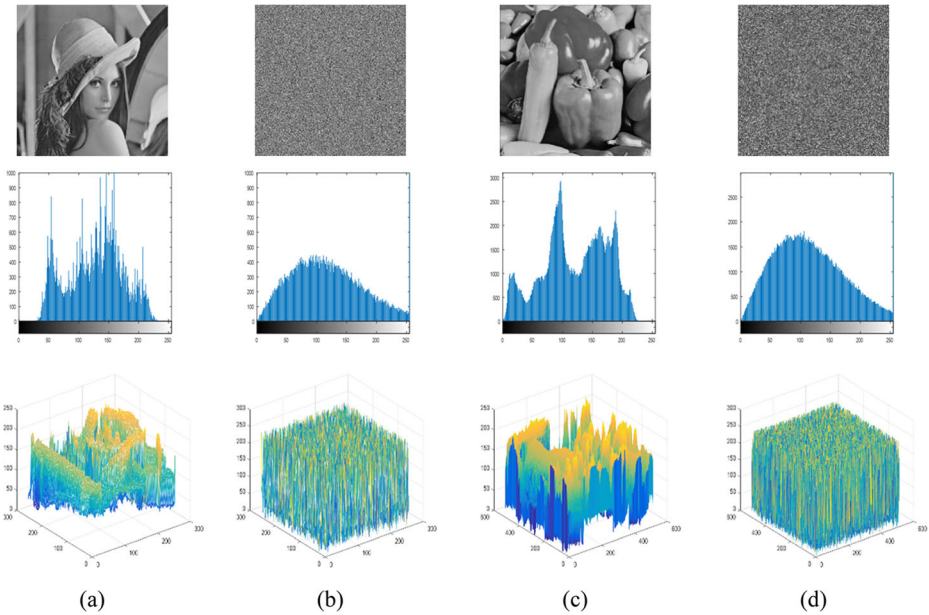


Fig. 6 Histograms and pixel distributions before and after image encryption

defined by: fractional orders $\left(\alpha_{x_k}, \alpha_{y_k}, \beta_{x_k}, \beta_{y_k}\right)$ and the width n and length m of the block. Suppose we have four frames randomly drawn from a sequence of Tennis video images.

Figure 7 shows the encryption of these frames using the proposed method with the secret key Q defined earlier. We notice that the histograms of the encrypted frames are entirely different from those of the original frames, and they are generally identical regardless of the original frame. This reduces the risk of statistical attacks based on collecting information about the original frames by analyzing the histograms of the encrypted frames. Figure 7a, b show different frames from the Tennis video sequence along with their corresponding histograms, and then Fig. 7e, f shows the histograms and pixel distributions of corresponding encrypted frames. Consequently, the proposed method is robust against statistical analysis by histogram.

6.2 Correlation of adjacent pixels

The correlation coefficient is another useful indicator to evaluate the performance of image/video encryption and decryption scheme. To test the correlation of the encrypted image/video obtained by the FrDTTs based method proposed in this paper, 1000 pairs of neighboring pixels are randomly selected as samples from the horizontal, vertical, and diagonal directions of the original image and the encrypted image and calculate the correlation coefficient for the three directions. The correlation coefficient, $R_{x,\,y}$, can be obtained using the following equation [23].

$$R_{x,y} = \frac{E[(x - E(x))(y - E(y))]}{\sqrt{D(x) \times D(y)}} \tag{30}$$

where

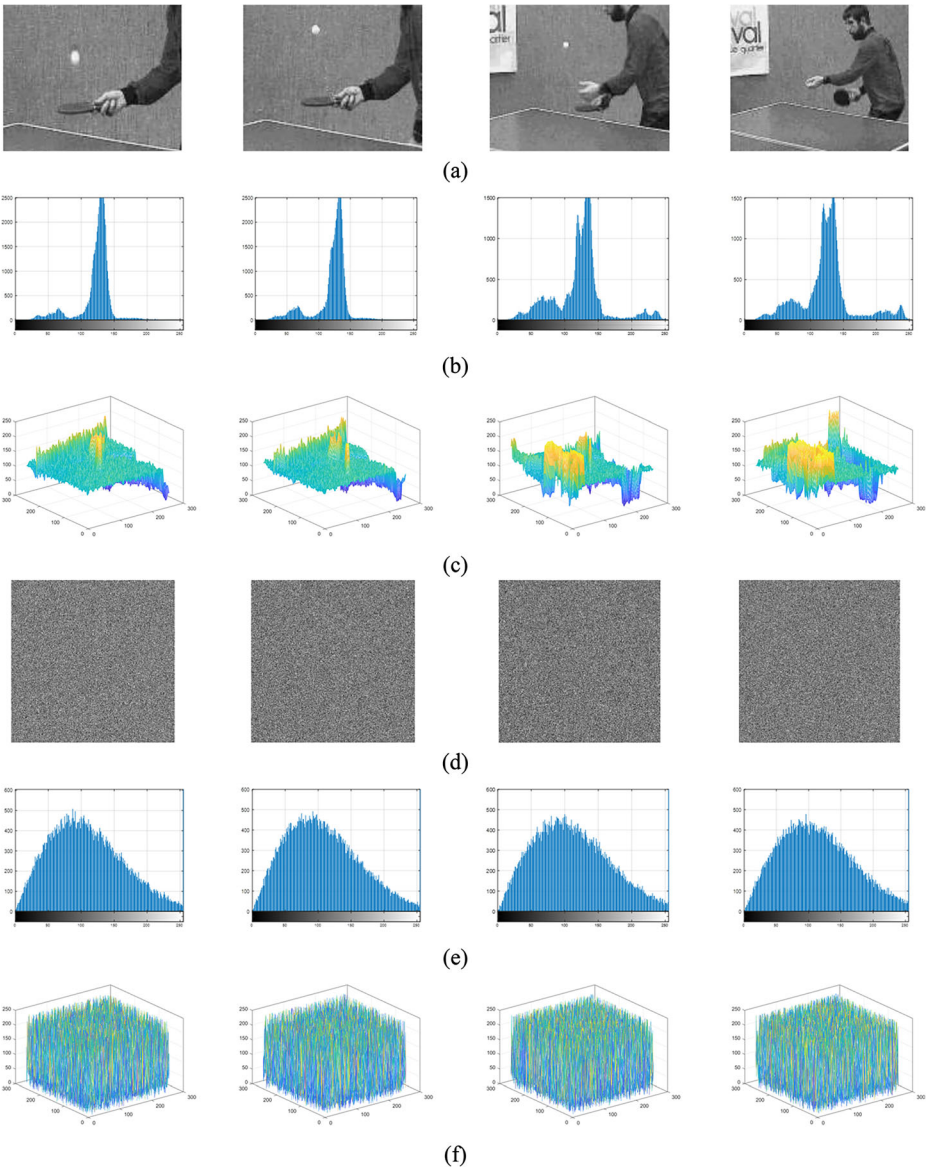


Fig. 7 Histograms and pixel distributions of some frames of the Tennis video sequence (**a**) original frames, (**b**) histograms of original frames, (**c**) pixel distributions of original frames, (**d**) encrypted frames, (**e**) histograms of encrypted frames and (**f**) pixel distributions of encrypted frames

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{31}$$

x and y are gray-scale values of the adjacent pixels in the image. Figure 8 shows the correlation analysis between the pixels of "Lena" images before and after the encryption in three directions (horizontal, vertical and diagonal) to evaluate the performance of the proposed scheme, and the results are listed in Table 5 with a comparison with recent

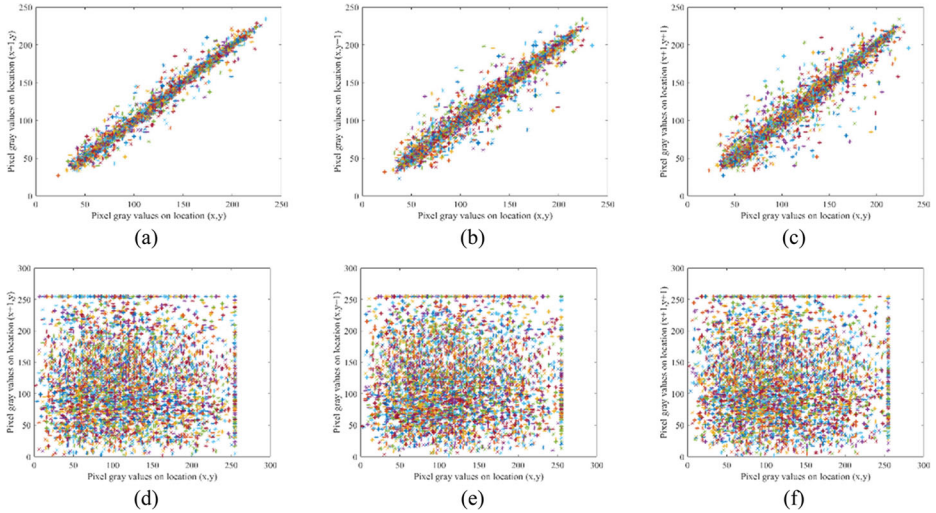


Fig. 8 The correlation plots of the Lena image and the corresponding encrypted image of Lena (**a**) horizontal; (**b**) vertical; (**c**) diagonal; (**d**) horizontal of the encrypted image; (**e**) vertical of the encrypted image; (**f**) diagonal of the encrypted image

published results. The Table 5, we can see that the correlation coefficients of adjacent pixels in the three directions of the original image are close to 1, while the correlation coefficients of the encrypted image are close to 0. This shows that the proposed encryption algorithm can reduce the correlation between pixels very well and can resist the attack using image correlation.

Figure 9 shows the correlation analysis between the pixels of some CoastGuard frames of the video sequence before and after encryption in three directions (horizontal, vertical and diagonal) in order to evaluate the performance of the proposed scheme, Table 6 shows the

Table 5 Correlation coefficients of different images using the proposed method and other similar methods

Method	Image	Testing direction			Average value
		Vertical	Horizontal	Diagonal	
	Original Lena (512×512)	0.9513	0.9607	0.9347	**0.9489**
Proposed method	Encryption « Lena »	0.0112	– 0.0201	– 0.0131	**0.0148**
FrDCT [62]	Encryption « Lena »	0.0593	– 0.0504	– 0.0493	**0.0530**
FrDFT [31]	Encryption « Lena »	– 0.0575	0.0671	– 0.0716	**0.0654**
FrMT [73]	Encryption « Lena »	0.0753	0.0613	– 0.0405	**0.0590**
DFrST [43]	Encryption « Lena »	0.0540	0.4834	0.6274	**0.3883**
DFrKT [37]	Encryption « Lena »	0.0213	– 0.0379	– 0.0192	**0.0213**
FrHT [24]	Encryption « Lena »	0.0301	– 0.0921	– 0.0461	**0.0301**
	Original Peppers (1024×1024)	0.9638	0.9467	0.9785	**0.9630**
Proposed method	Encryption « Peppers »	0.0092	– 0.0121	– 0.0160	**0.0124**
FrDCT [62]	Encryption « Peppers »	0.0464	– 0.0492	– 0.0506	**0.0487**
FrDFT [31]	Encryption « Peppers »	– 0.0656	0.0808	– 0.0737	**0.0734**
FrMT [73]	Encryption « Peppers »	0.0532	0.0402	– 0.0653	**0.0529**
DFrST [43]	Encryption « Peppers »	0.0602	0.5322	0.5923	**0.3949**
DFrKT [37]	Encryption « Peppers »	0.0301	– 0.0293	– 0.0278	**0.0301**
FrHT [24]	Encryption « Peppers »	0.0219	– 0.0726	– 0.0537	**0.0219**

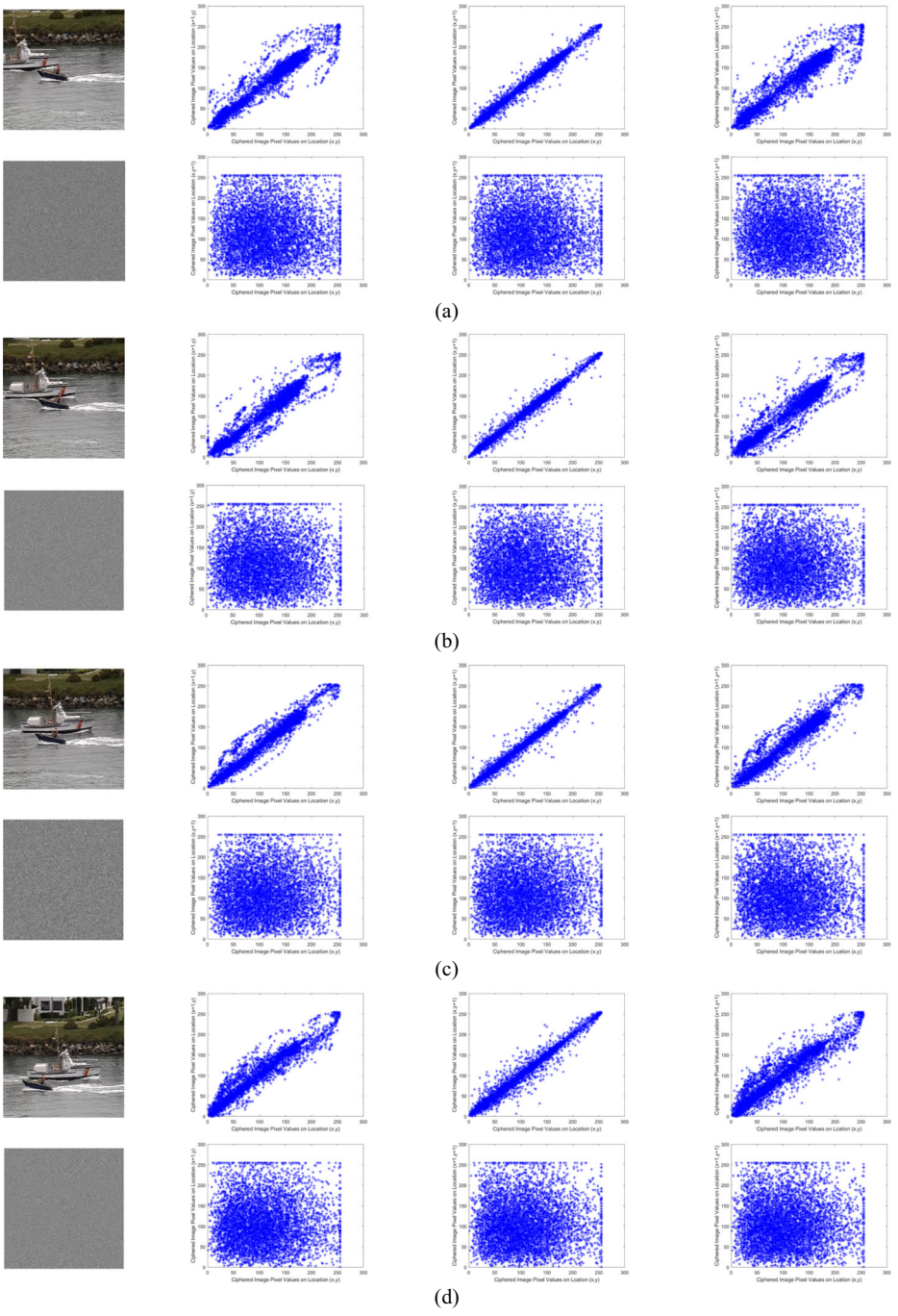


Fig. 9 Correlation distributions of two adjacent pixels in original and encrypted video sequence. **a** Correlation of two adjacent pixels in frame 1 of the video sequence **b** Correlation of two adjacent pixels in frame 2 of the video sequence **c** Correlation of two adjacent pixels in frame 3 of the video sequence **d** Correlation of two adjacent pixels in frame 1 of the video sequence

correlation coefficients of the Tennis frames of the video sequence in the horizontal, vertical and diagonal directions respectively. From these results, we can see that there are strong neighborhood correlations between the adjacent pixels of each frame of the original video sequence, while those of the encrypted video sequence. Consequently, the proposed algorithm can effectively realize the confusion and diffusion of image information, which shows a capability against the correlation analysis attack.

6.3 Robustness differential attack

In this attack, the attacker encrypts the plain image with the proposed method. Then, the attackers penetrate the cryptosystem by tracing the difference between two encrypted images. The number of pixels change rate (NPCR) and the unified averaged changed intensity (UACI) are commonly used to evaluate the strength of any encryption process. The NPCR is the change rate of the number of pixels of the cipher-image when only one pixel of the plain image is modified. The UACI calculate the average intensity of differences between the plain and the encrypted images. They are calculated as follows [33].

$$\boldsymbol{NPCR} = \frac{\boldsymbol{1}}{N \times M}\left(\sum_{i=1}^{N}\sum_{j=1}^{M} D(i,j)\right) \times \boldsymbol{100\%} \tag{32}$$

$$\boldsymbol{UACI} = \frac{\boldsymbol{1}}{N \times M}\left[\sum_{i=1}^{N}\sum_{j=1}^{M} \frac{|C_2(i,j) - C_1(i,j)|}{\boldsymbol{255}}\right] \times \boldsymbol{100\%} \tag{33}$$

where $D(i,j) = \begin{cases} 1, \text{if} C_1(i,j) \neq C_2(i,j) \\ 0, \text{if} C_1(i,j) = C_2(i,j) \end{cases}$ and N, M is the image dimensions, L = 255 for image intensity. To get the best encryption strength against the diferential attack, NPCR and

Table 6 Correlation coefficients of tennis video sequence using the proposed method and other similar methods

Method	video	Directions	Correlation coefficients				Average value
			Frame 1	Frame 2	Frame 3	Frame 4	
Proposed method	Encryption Tennis video sequence	Horizontal	0.0037	0.0094	0.0094	0.0065	**0.0073**
		Vertical	0.0039	0.0042	0.0042	0.0085	**0.0052**
		Diagonal	0.0139	0.0017	0.0017	0.0081	**0.0064**
FrDFT [17]	Encryption Tennis video sequence	Horizontal	– 0.0120	0.0230	– 0.0423	– 0.0301	**0.0230**
		Vertical	– 0.0142	0.0103	– 0.0237	– 0.0415	**0.0103**
		Diagonal	– 0.0630	0.0460	– 0.0335	– 0.0526	**0.0460**
DFrST [43]	Encryption Tennis video sequence	Horizontal	– 0.0432	0.0452	0.0137	– 0.0524	**0.0295**
		Vertical	– 0.0554	0.0642	– 0.0689	– 0.0621	**0.0642**
		Diagonal	– 0.0232	– 0.0536	0.0127	– 0.0349	**0.0127**
DFrKT [37]	Encryption Tennis video sequence	Horizontal	– 0.0726	– 0.0279	0.0230	– 0.0786	**0.0230**
		Vertical	0.0456	0.0236	– 0.0047	0.0443	**0.0378**
		Diagonal	0.0467	– 0.0032	0.0336	0.0498	**0.0434**
FrHT [24]	Encryption Tennis video sequence	Horizontal	0.0324	– 0.0654	– 0.0435	0.0459	**0.0392**
		Vertical	0.0257	– 0.0549	– 0.0248	0.0168	**0.0213**
		Diagonal	0.0278	– 0.0351	– 0.0532	0.0327	**0.0303**

Table 7 The comparison results of average NPCR and UACI in proposed method and similar method

Method	Test image	Average (NPCR) (%)	Average (UACI) (%)
Proposed method	Lena (512×512)	99.99%	33.54%
	Peppers (1024×1024)	99.98%	33.59%
FrDCT [62]	Lena (512×512)	98.21%	29.44%
FrDFT [31]	Lena (512×512)	98.81%	31.46%
FrMT [73]	Lena (512×512)	98.61%	30.45%
DFrST [43]	Lena (512×512)	99.61%	33.45%
DFrKT [37]	Lena (512×512)	99.14%	32.95%
FrHT [24]	Lena (512×512)	99.56%	32.44%

UACI must be higher and in the range of >99% and >33%, respectively. Tables 7 and 8 shows the results according to the proposed method of NPCR and UACI and compares the NPCR and UACI average of different encryption method for Lena image and tennis video sequence. From this table, we know that the proposed method has a larger NPCR average compared with other method, which show that the proposed method has excellent robustness against differential attack than the other method.

6.4 Sensitivity analysis to keys

The analysis of key space is required to calculate the space of key that is used for the encryption process. It should be as large as possible for good encryption technique. The fractional parameters of Tchebichef are involved in the proposed encryption algorithm, namely are served as the private keys for the cryptosystem. We analyze the influence of the number of erroneous fractional orders for image/video encryption. Next, we will check the sensitivity of our algorithm to the keys. To further validate the sensitivity of the key, this paper quantifies the mean square error (MSE) between the decrypted image and the original image by computing the MSE as follows:

$$MSE = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} |I_O(i,j) - I_D(i,j)|^2 \tag{34}$$

Table 8 The comparison results of average NPCR and UACI in proposed method and similar method

Method	Average NPCR and UACI	Test tennis video sequence				Average value
		Frame 1	Frame 2	Frame 3	Frame 4	
Proposed method	(NPCR) (%)	99.99%	99.98%	99.97%	99.98%	**99.98%**
	(UACI) (%)	33.74%	33.87%	33.66%	33.94%	**33.80%**
FrDFT [17]	(NPCR) (%)	97.92%	98.78%	97.89%	98.67%	**98.32%**
	(UACI) (%)	30.47%	31.14%	31.57%	31.24%	**31.11%**
DFrST [43]	(NPCR) (%)	98.96%	99.28%	98.54%	98.94%	**98.93%**
	(UACI) (%)	32.35%	33.29%	32.47%	33.53%	**32.91%**
DFrKT [37]	(NPCR) (%)	99.39%	98.79%	99.39%	98.47%	**99.01%**
	(UACI) (%)	33.16%	32.96%	33.19%	33.89%	**33.30%**
FrHT [24]	(NPCR) (%)	98.23%	98.98%	98.92%	99.11%	**98.81%**
	(UACI) (%)	32.64%	32.92%	32.48%	32.95%	**32.75%**

The *PSNR* is defined by:

$$\boldsymbol{PSNR} = \boldsymbol{10} \times log_{\boldsymbol{10}}\left(\frac{\boldsymbol{255^2}}{\boldsymbol{MSE}}\right)(db) \tag{35}$$

where $I_O(i, j)$ denotes the original image pixel, $I_D(i, j)$ is the pixel of the decrypted image, $N \times M$ are the size of original and decrypted images.

Figures 10 and 11 show that even if the deviation of the correct keys and fractional-orders parameters are adjusted down to (δ_x, δ_y), no useful information can still be obtained from the decrypted image/video. We assume that incorrect keys locate in the vicinity of the correct key values, and then the relations between the keys used for decryption and encryption are $\alpha_x^{'} = \alpha_x + \delta_x, \alpha_y^{'} = \alpha_y + \delta_y$.

Figure 12a and 13a display the MSE with changes of fractional orders. The x-axis δ represents the deviation distance (in the interval $[-0.05,\ 0.05]$ with step size 0,002) to the correct fractional orders. From the simulation results, we learn that the decrypted image/video has very distinct difference even if a very small deviation occurs in the fractional orders. When the deviation is up to 0.0003, the decrypted image/video is fuzzy and when the deviation is larger than 0.0003, one has difficulty in recovering the original image/video from the encrypted one.

Figures 12b and 13b compares the security between the fractional transform of different encryption algorithms FrDTT, FrDCTs [62] , FrDFTs [31], FrMTs [73], DFrST [43], DFrKT [37] and FrHT [24], from the results of the MSE for grayscale image. The x-axis δ represents the deviation distance (in the interval $[-0.1,\ 0.1]$ with step size 0,002) to the correct transform order parameters. This result demonstrates the effectiveness and performances of the proposed scheme in terms of its ability to secure image/video and sensitivity to Keys. It should be noted that when the keys are all correct, the original image/video can be completely decrypted with MSE = 0 for all compared algorithms.

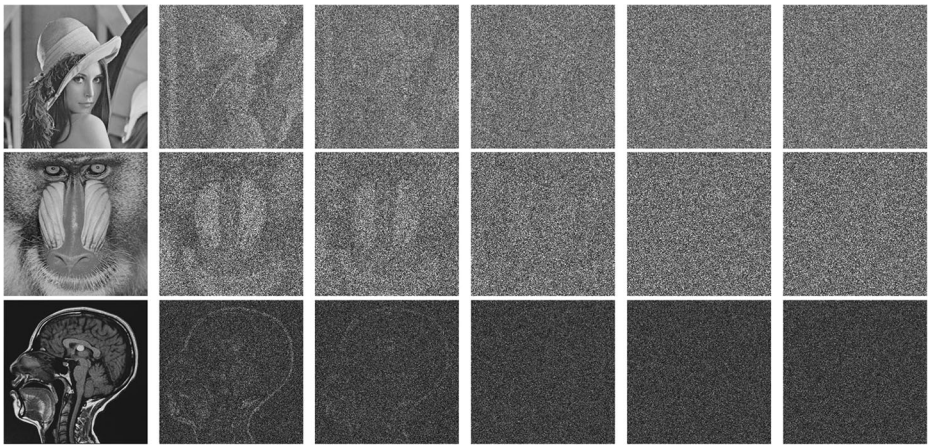


Fig. 10 Decrypted images with different fractional order deviations: (**a**) Original image (**b**) $\delta = 0.0005$, (**c**) $\delta = 0.0003$, (**d**) $\delta = 0.0025$, (**e**) $\delta = 0.001$ and (**f**) $\delta = 0.01$

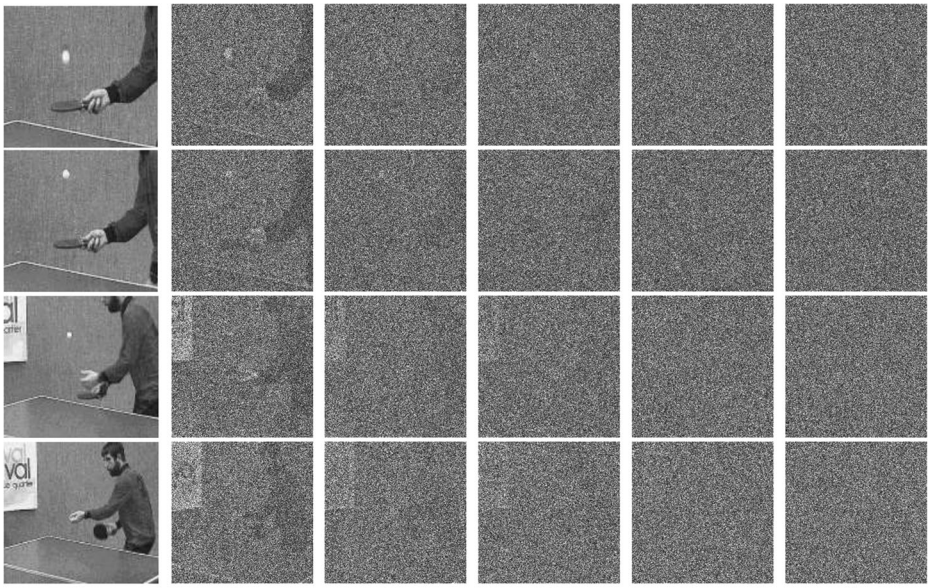
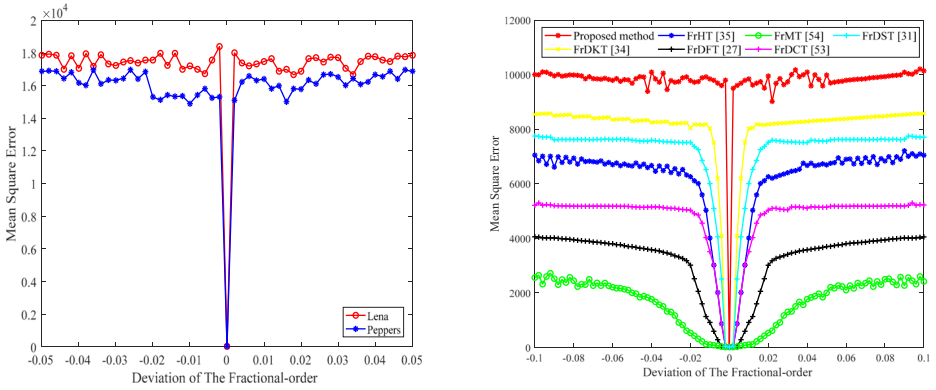


Fig. 11 Decrypted Tennis video sequence with different fractional order deviations: (**a**) Original video sequence (**b**) $\delta = 0.0005$, (**c**) $\delta = 0.0003$, (**d**) $\delta = 0.0025$, (**e**) $\delta = 0.001$ and (**f**) $\delta = 0.01$

6.5 Robustness detection

6.5.1 Robustness to the noise attack

Since the encrypted image/video are easily affected by noise and data loss during transmission and processing, it is necessary to measure the robustness of the proposed image/video encryption algorithm. Therefore, it is necessary to measure the quality of an image/video encryption method to verify its anti-noise ability. In this paper, the Gaussian white noise with



(a) (b)

Fig. 12 The MSE between the plain and encrypted image with the variation of deviation distance $\delta = \delta_x = \delta_y$. **a** the images Lena and Peppers **b** comparison of MSEs of cryptosystems based on proposed method, FrDCTs [62] , FrDFTs [31], FrMTs [73], DFrST [43], DFrKT [37] and FrHT [24]

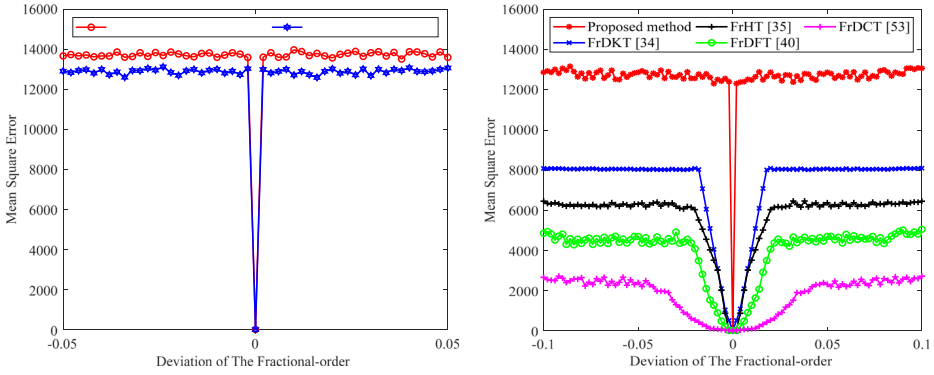


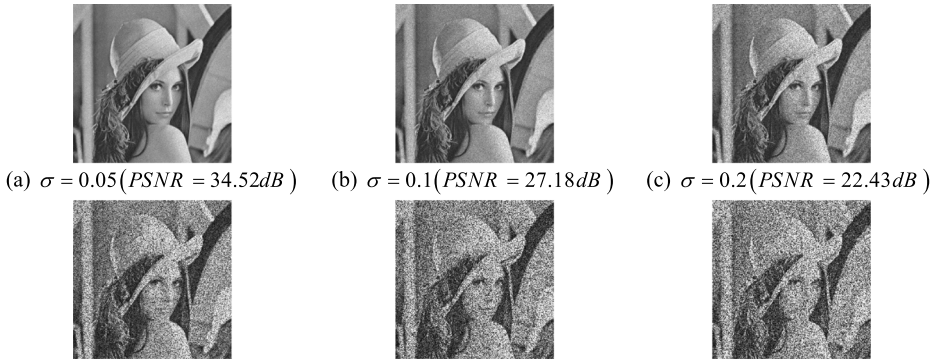
Fig. 13 The MSE between the plain and encrypted video sequence with the variation of deviation distance $\delta = \delta_x = \delta_y$. **a** The CoastGuard and Tennis video sequence. **b** Comparison of MSEs of cryptosystems based on proposed method, FrDCTs [62] , FrDFT [17], DFrKT [37] and FrHT [24]

the mean value of 0 and variance of 1 is added to the encrypted image/video of "Lena" and tennis video sequence by Eq. (36) for noise interference.

$$E' = E(1 + \sigma G) \tag{36}$$

where $E$and E' represent of the ideal encrypted image and the noise-affected encrypted image, respectively. Parameter σ is a coefficient on noise strength or intensity, and G represents Gaussian random data with zero-mean and identity standard deviation.

To see the resistance of the proposed method against noise, Fig. 15 shows four frames of a tennis video sequence along with their PSNRs when decrypted with an additive white Gaussian noise of variable power coefficient σ we notice that the frames remain identifiable despite the presence of noise. In the same way, Fig. 14 shows the encrypted images of the proposed method in this paper at Gaussian noise intensity σ correctly decrypted image at 0.05, 0.10, 0.20, 0.50, 0.80, 1.00.



(a) $\sigma = 0.05\left(PSNR = 34.52dB\right)$ (b) $\sigma = 0.1\left(PSNR = 27.18dB\right)$ (c) $\sigma = 0.2\left(PSNR = 22.43dB\right)$

(d) $\sigma = 0.5\left(PSNR = 16.13dB\right)$ (e) $\sigma = 0.8\left(PSNR = 11.04dB\right)$ (f) $\sigma = 1\left(PSNR = 10.71dB\right)$

Fig. 14 Decrypted image with different Gaussian noise intensities

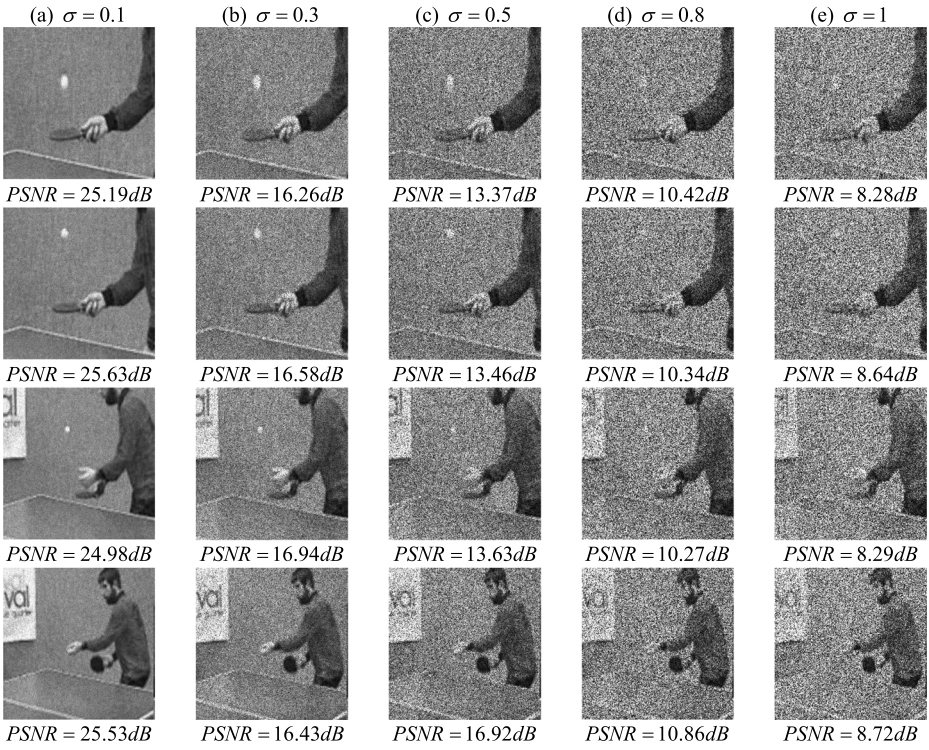


Fig. 15 Decrypted tennis video sequence with different Gaussian noise intensities σ

As can be seen in Figs. 14 and 15, although the quality of the decrypted image/video gradually increases as the intensity of the Gaussian noise added to the decryption increases, the image/video quality after decryption is also decreasing. The noise intensity drops, but at 0.10 the image/video is clearly visible, and even when the intensity is increased to 1.00, the image is still visible. The original image/video information is vaguely recognizable, thus it can be seen that the encryption method proposed in this paper has good anti-noise performance. In order to deepen the comparison with current classical methods of image encryption, experiments were carried out to calculate the PSNR values of the decrypted images of proposed method, FrDCTs [62] , FrDFTs [31], FrMTs [73], DFrST [43], DFrKT [37] and FrHT [24]. From Table 9, we

Table 9 The PSNR values of the decrypted images "Lena" after different intensities of Gaussian noise interference using the proposed method and other similar methods

Noise Intensity σ	Decrypted image quality (PSNR)						
	Proposed method	FrDCTs [62]	FrDFTs [31]	FrMTs [73]	DFrST [43]	DFrKT [37]	FrHT [24]
0.05	**34.52**	32.85	33.29	31.23	31.54	33.29	31.73
0.10	**27.18**	25.92	26.23	24.83	24.26	25.99	25.19
0.20	**22.43**	20.64	21.56	19.39	21.41	21.39	20.33
0.50	**16.13**	12.83	14.03	13.61	11.38	14.92	11.87
0.80	**11.04**	8.54	10.84	9.47	9.23	10.84	9.35
1.00	**10.71**	6.87	9.79	7.19	7.79	9.88	7.65

can see that, although the PSNR values of images decrypted by FrDFTs under different noise intensities of 0.80 and 1.00.

Figure 16 shows the computed MSE between a decrypted tennis video sequence and the corresponding original video sequence as a function of the variable power coefficient σ. In this experiment, the MSE curves between the original video sequence and decrypted one with different σ of FrDCTs [62] , FrDFTs [17], DFrKT [37] and the proposed method are shown in Fig. 16a. This Figure shows the decrypted video performance of FrDCTs [62] , FrDFT [17], DFrKT [37] encrypted Tennis frame and the proposed method after Gaussian noise interference of different intensity. However, the FrDTTs based video sequence encryption method proposed in this article is better than the other in most cases has a better robustness.

6.5.2 Classical types of attacks

The proposed scheme for the image/video encryption is robust; it protects image/video from several attacks that are applied by the intruder, for the data extraction from encrypted image/video. There are four classical types of attacks [56]:

(i) ciphertext only attack (COA): the intruder doesn't have any idea about the key used for encryption. Attacker tries to calculate the key to hack information. The encrypted image/video in proposed scheme is free from COA because of the use of fractional parameter keys, so attacker won't be able to calculate it, without the presence of original fractional parameter. It is also called as replacement attacks.

(ii) known plaintext attack (KPA): the attacker has some plaintexts and their corresponding ciphertext also, with use of them unauthorized person tries to calculate the relation between original and encrypted information. In proposed scheme fractional parameter and random phase code two asymmetric keys are applied alternatively on each frame of video. So, even if the hacker gets the information about public key, he won't be able to extract original information, without the presence of private key. In this way proposed scheme is free from KPA attacks.

(iii) chosen ciphertext attack (CCA): only ciphertext or encrypted data is used to hack the information, by doing little change in encrypted information and observing variation

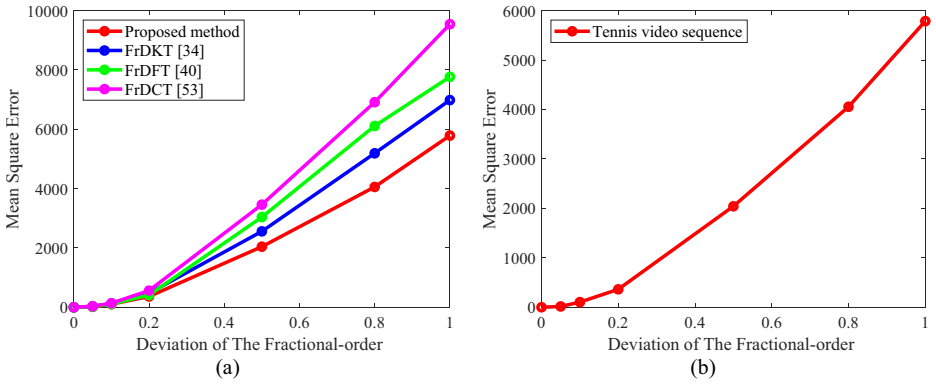


Fig. 16 **a** Robustness performance decrypted tennis video sequence of FrDCTs [62] , FrDFT [17], DFrKT [37] and proposed method after different intensity Gaussian noise interference. **b** Robustness performance of the proposed method against noise perturbation with different σ

from image/video. Due to use of two different keys (fractional parameter and random phase code) for different image/video, the observation between two ciphered image/video will not facilitate hacker to deduce relation between them. So, the image/video is secured from chosen ciphertext attacks.

(iv) chosen plaintext attack (CPA): the opponent has obtained temporary access to the encryption machinery. Hence, he can choose a plaintext string, and construct the corresponding ciphertext string.

In this way due to use of two different keys (fractional parameter and random phase code) for the encryption of image/video, the information is highly secure from the invaders. So, the proposed scheme can resist the chosen plaintext/ciphertext attack.

6.6 Computational complexity analysis

The complexity of the proposed algorithm is the sum of the complexities needed to implement the proposed algorithm. We count the main operations used in each step, and the total number represents the cipher's complexity. Step 1 is to compute the 8×8 FrDTTs of a frame block using the matrix given by Eq. (27). The video sequence encryption process with secret keys is mainly implemented by times two-dimensional FrDTTs for each block of the frame. So the time complexity in Step 1 is $(n_f \times M \times N)$, with n_f the number of frames. The time complexity in Step 2 is $(n_f \times M \times N)$ since the time-consuming part is the number of the FrDTTs for each block. Therefore, considering that a block of an $M \times N$ frame

has to be transformed at most 8 times. Similar to Step 2, the mathematical complexity for the random phase mask can also be computed along similar lines for each block. The complexity of the random phase block in Step 3 is also $(8 \times n_f \times M \times N)$. In the last stage, four key streams with size of $M \times N$ are used to modify the image pixels. Therefore, the total time complexity of the presented encryption scheme is $(8 \times n_f \times M \times N)$

. This will increase the security of the encryption process by many orders of magnitude in addition to the security provided by the FrDTTs and the random phase codes. However, our proposed algorithm can be executed in a parallel mode, which can accelerate the operation speed.

6.7 NIST statistical tests

NIST tests were performed on 100 encrypted Lena 256×256 Gy-scale images, each encrypted with hundred different keys. Table 10 below shows the obtained results of NIST tests. As it can be observed, all the tests were passed with a minimum passing rate of 98%.

7 Conclusion

In this paper, we have proposed an efficient method for the encryption of video image sequences. This method makes it possible to individually encrypt each frame of a video sequence using fractional-order discrete Tchebichef transform, which is advantageous in terms of transmission rate and in complexity of calculations. In addition, a block encryption scheme has been adopted and introduced in order to improve the sensitivity and space of the key. The method proposed in this paper extends the fractional-order discrete Tchebichef transform to the

Table 10 NIST Results for 100 Encrypted Lena 256 × 256 Images

NIST test	P value	Result of tests
Frequency	0.54524	Pass
Block Frequency	0.54420	Pass
Cumulative Sums	0.79747	Pass
Runs	0.85283	Pass
Longest Runs	0.94638	Pass
Rank	0.43538	Pass
FFT	0.65793	Pass
Non-overlapping Templates	0.87692	Pass
Overlapping Templates	0.86537	Pass
Universal	0.44986	Pass
Approximate Entropy	0.79918	Pass
Random Excursions	0.86579	Pass
Random Excursions Variant	0.97160	Pass
Serial	0.86537	Pass
Linear Complexity	0.96495	Pass

fractional-order vector in the real domain. Moreover, the use of fractional-orders parameters settings increases the key space for image/video encryption and has high key sensitivity. In addition, the encrypted image/video is a real-value image/video, and its size is the same as the original image/video size, which is convenient for display, transmission, and storage. Finally, the simulation results clearly show the feasibility of the proposed method as well as its resistance against statistical, brute force and noise attacks. Therefore, the image/video encryption method proposed in this paper can have a good application scenario in the field of image/video encryption communication.

Appendix A

Proof of **property** *(v)* Let λ be an eigenvalue of Tchebichef polynomial matrix and u the corresponding eigenvector, then $Cu = \lambda u$, using the *properties (iii)* and *(iv),* we have:

$$u = CCu = \lambda Cu = \lambda^2 u \tag{A1}$$

thus. {Key1, Key2}

$$\left(\lambda^2 - 1\right)u = 0 \tag{A2}$$

The matrix C has only two eigenvalues $\{1, -1\}$, The proof of Eq. (19) has been completed

Appendix B

Proof of properties (a)-(b) Let $C \in \mathbb{C}^{N \times N}$ be Tchebichef polynomial matrix, with their eigenvalues on the diagonal of a diagonal matrix $\Lambda = diag\ (\lambda_1, \ldots\ldots\lambda_N) \in \mathbb{C}^{N \times N}$ and the corresponding eigenvectors forming the columns of a matrix $V = [u_1, \ldots\ldots, u_N] \in \mathbb{C}^{N \times N}$, we have:

$$C = V\Lambda V^{-1} \tag{B.1}$$

where, the orthonormal vectors u_1, ……u_N are eigenvectors of C, corresponding to eigenvalues λ_1, ……λ_N.

$$\mathrm{C} = [u_1 \cdots\cdots u_N] \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix} \begin{bmatrix} u_1^T \\ \vdots \\ u_N^T \end{bmatrix} = [\lambda_1 u_1 \cdots\cdots \lambda_N u_N] \begin{bmatrix} u_1^T \\ \vdots \\ u_N^T \end{bmatrix} \tag{B.2}$$

$$\mathrm{C} = \lambda_1 u_1 u_1^T \cdots\cdots \lambda_N u_N u_N^T \tag{B.3}$$

Notice that the matrices

$$\mathrm{P}_j := u_j u_j^T \in \mathbb{C}^{N \times N} \tag{B.4}$$

are orthogonal projectors, since $\mathrm{P}_j^T = \mathrm{P}_j$ and $\mathrm{P}_j^2 := u_j \left(u_j^T u_j \right) u_j^T = u_j u_j^T = \mathrm{P}_j$

$$\mathrm{C} = \sum_{j=1}^{N} \lambda_j \mathrm{P}_j \tag{B.5}$$

if $j \neq k$, then the orthogonality of the eigenvectors implies

$$\mathrm{P}_j \mathrm{P}_k = u_j u_j^T u_k u_k^T = 0 \tag{B.6}$$

The proof of *properties (a)* and *(b)* has been completed.

Proof of propriety (c) Let γ, η and λ be respectively the eigenvalues of the matrices P_0,P_1 and C of size $N \times N$, using Eq. (18), we have:

$$\begin{aligned} |\gamma I - \mathrm{P}_0| &= |\gamma I - 0.5(\mathrm{C} + I)| = |(\gamma - 0.5) I - 0.5\mathrm{C}| \\ &= |(\gamma - 0.5) I - 0.5\mathrm{C}| = 0.5^N |(2\gamma - 1) I - \mathrm{C}| \\ &= 0 \end{aligned} \tag{B.7}$$

Similarly, we have

$$|\eta I - \mathrm{P}_1| = 0.5^N |(2\eta - 1) I - \mathrm{C}| = 0, \textbf{\textit{and}}\ |\lambda I - \mathrm{C}| = \boldsymbol{0} \tag{B.8}$$

From (B.7) and (B.8), we have

$$2\gamma - 1 = \lambda, \textbf{\textit{and}} - (\boldsymbol{2\eta - 1}) = \lambda \tag{B.9}$$

Hence, if $\lambda = 1$, there is $\gamma = 1$, $\eta = 0$, and if $\lambda = -1$, then $\gamma = 0$, $\eta = 1$.

The proof of *propriety (c)* has been completed.

Appendix C

Let P_0 and P_1 the spectral projection matrices of Tchebichef polynomial matrix $\mathrm{C} \in \mathbb{C}^{N \times N}$, and u,v be their eigenvectors corresponding to $\lambda = 1$, respectively.

Proof of Lemma 1 From Table 1 and *Property (c)*, we have:

$$\mathrm{P}_0 u = u, \textbf{\textit{and}}\ \mathrm{P}_{\boldsymbol{1}} v = v \tag{C.1}$$

using (C.1) and *Property (b)*, we have:

$$u^T v = (\mathrm{P}_0 u)^T (\mathrm{P}_1 v) = u^T {\mathrm{P}_0}^T \mathrm{P}_1 v = 0 \tag{C.2}$$

The proof of *Lemma 1* has been completed.

Proof of Lemma 2 From Eq. (15), *Lemma 1* and *property (b)* we have:

$$\begin{aligned} \mathrm{C}u &= (\lambda_0 \mathrm{P}_0 + \lambda_1 \mathrm{P}_1)u = \lambda_0 \mathrm{P}_0 u + \lambda_1 \mathrm{P}_1 u \\ &= \lambda_0 \mathrm{P}_0 u + \lambda_1 \mathrm{P}_1 \mathrm{P}_0 u = \lambda_0 \mathrm{P}_0 u + \lambda_1 \mathrm{P}_1^T \mathrm{P}_0 u \\ &= \lambda_0 \mathrm{P}_0 u = \lambda_0 u \end{aligned} \tag{C.3}$$

$$\begin{aligned} \mathrm{C}v &= (\lambda_0 \mathrm{P}_0 + \lambda_1 \mathrm{P}_1)v = \lambda_0 \mathrm{P}_0 v + \lambda_1 \mathrm{P}_1 v \\ &= \lambda_0 \mathrm{P}_0 \mathrm{P}_1 v + \lambda_1 \mathrm{P}_1 v = \lambda_1 \mathrm{P}_1 v = \lambda_1 v \end{aligned} \tag{C.4}$$

The proof of *Lemma 2* has been completed.**Abbreviations** *FrDTs,* Fractional-order Discrete Transform.; *FrDTTs,* Fractional-order Discrete Tchebichef Transform.; *FrDTPs,* Fractional-order Discrete Tchebichef Polynomials.; *DTTs,* Discrete Tchebichef Transform.; *SVD,* Singular Value Decomposition.; *FrDFTs,* Fractional Discrete Fourier Transform.; *DFrSTs,* Discrete Fractional Sine Transform.; *FrDMMs,* Fractional discrete Meixner moments.; *DFrKTs,* Discrete Fractional Krawtchouk Transform.; *FrHTs,* Fractional Hartley Transform.; *FrMTs,* Fractional Mellin Transform.; *DCTs,* Discrete Cosine Transform.; *FrDCTs,* Fractional Discrete Cosine Transform.; *NPCR,* Number of Pixels Change Rate.; *UACI,* Unified Averaged Changed Intensity.; *MSE,* Mean Square Error.; *NIST,* National Institute of Standards and Technology; *PSNR,* Peak Signal to Noise Ratio

Acknowledgements The authors would like to thank the anonymous referees for their valuable comments and suggestions.

Funding No funding has been granted for this work.

Data availability The datasets generated in our experiments are available from CVG - UGR - Image database, URL link: http://decsai.ugr.es/cvg/dbimagenes/. (2017). Accessed 12 February 2020.

The datasets used or analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Acharya B, Patra SK, Panda G (2008) "Image encryption by novel cryptosystem using matrix transformation," in 2008 First International Conference on Emerging Trends in Engineering and Technology, pp. 77–81
2. Bahrami S, Naderi M (2014) Encryption of video main frames in the field of DCT transform using A5/1 and W7 stream encryption algorithms. Arab J Sci Eng 39(5):4077–4088
3. Batham S, Acharya AK, Yadav VK, Paulo R (2013) A new video encryption algorithm based on indexed based chaotic sequence. In: Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, pp 139–143. https://doi.org/10.1049/cp.2013.2307

4. Bhatnagar G, Wu QJ (2014) Biometric inspired multimedia encryption based on dual parameter fractional fourier transform. IEEE Trans Syst Man Cybern Syst 44(9):1234–1247
5. Chebyshev PL (1853) Théorie Des Mécanismes Connus Sous Le Nom De Parallélogrammes. St.-Pétersbourg: Imprimerie de l'Académie impériale des sciences
6. Chen L, Zhao D, Ge F (2013) Image encryption based on singular value decomposition and Arnold transform in fractional domain. Opt Commun 291:98–103. https://doi.org/10.1016/j.optcom.2012.10.080
7. Cheng H, Li X (2000) Partial encryption of compressed images and videos. IEEE Trans Signal Process 48(8):2439–2451
8. Chihara TS (2011) An introduction to orthogonal polynomials. In: Dover Books on Mathematics. Dover Publications, New York
9. Daoui A, Karmouni H, Azzayani A, Sayyouri M, Qjidaa H (2020) "Large Size 1D Signal Analysis by Hybrid Tchebichef-Charlier Moments," in 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), pp. 1–6
10. El Ogri O, Karmouni H, Sayyouri M, Qjidaa H (2021) 3D image recognition using new set of fractional-order Legendre moments and deep neural networks. Signal Process Image Commun 98:116410. https://doi.org/10.1016/j.image.2021.116410
11. El Ogri O et al (2021) Novel fractional-order Jacobi moments and invariant moments for pattern recognition applications. Neural Comput & Applic 33(20):13539–13565
12. El Ogri O, Daoui A, Yamni M, Karmouni H, Sayyouri M, Qjidaa H (2020) New set of fractional-order generalized Laguerre moment invariants for pattern recognition. Multimed Tools Appl 79:23261–23294. https://doi.org/10.1007/s11042-020-09084-1
13. Fatnassi A, Gharsellaoui H, Bouamama S (2020) New hybrid proposed solution for video steganography based on clustering algorithm. Int J Secur Priv Pervasive Comput IJSPPC 12(2):30–43
14. Fridrich J (1997) Image encryption based on chaotic maps, in 1997 IEEE international conference on systems, man, and cybernetics. Comput Cybern Simul 2:1105–1110
15. Guizani S, Nasser N (2012) "An audio/video crypto—Adaptive optical steganography technique," in 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1057–1062
16. Hanna MT, Seif NPA, Ahmed WAEM (2004) Hermite-Gaussian-like eigenvectors of the discrete Fourier transform matrix based on the singular-value decomposition of its orthogonal projection matrices. IEEE Trans Circuits Syst Regul Pap 51(11):2245–2254
17. Jindal N, Singh K (2014) Image and video processing using discrete fractional transforms. Signal Image Vid Process 8(8):1543–1553
18. Joshi M, Shakher C, Singh K (2010) Fractional Fourier plane image encryption technique using radial hilbert-, and jigsaw transform. Opt Lasers Eng 48(7–8):754–759
19. Kang X, Tao R (2019) Color image encryption using pixel scrambling operator and reality-preserving MPFRHT. IEEE Trans Circuits Syst Vid Technol 29(7):1919–1932. https://doi.org/10.1109/TCSVT.2018.2859253
20. Kang X, Ming A, Tao R (2019) Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption. IEEE Trans Circuits Syst Vid Technol 29(6):1595–1607. https://doi.org/10.1109/TCSVT.2018.2851983
21. Karmouni H, Yamni M, Daoui A, Sayyouri M, Qjidaa H (2021) A new fast algorithm to compute moment 3D invariants of generalized Laguerre modified by fractional-order for pattern recognition. Multidim Syst Sign Process 32(2):431–464
22. Karmouni H, Sayyouri M, Qjidaa H A novel image encryption method based on fractional discrete Meixner moments. Opt Lasers Eng 137:106346
23. Karuna Y, Reddy GR (2020) Broadband subspace decomposition of convoluted speech data using polynomial EVD algorithms. Multimed Tools Appl 79(7):5281–5299
24. Kaur G, Agarwal R, Patidar V (2021) "Color image encryption scheme based on fractional Hartley transform and chaotic substitution–permutation," Vis Comput, https://doi.org/10.1007/s00371-021-02066-w
25. Kaur G, Agarwal R, Patidar V (2021) "Color image encryption system using combination of robust chaos and chaotic order fractional Hartley transformation," J King Saud Univ Comput Inf Sci, https://doi.org/10.1016/j.jksuci.2021.03.007.
26. Kumar S, Panna B, Jha RK (2019) Medical image encryption using fractional discrete cosine transform with chaotic function. Med Biol Eng Comput 57(11):2517–2533
27. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
28. Lang J, Tao R, Wang Y (2010) Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function. Opt Commun 283(10):2092–2096
29. Li S, Zheng X (2002) "Cryptanalysis of a chaotic image encryption method," in 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353), vol. 2, p. II–II

30. Lian S (2008) Multimedia content encryption: techniques and applications (1st ed.). Auerbach Publications. https://doi.org/10.1201/9781420065282
31. Lima JB, Novaes LFG (2014) Image encryption based on the fractional Fourier transform over finite fields. Signal Process 94:521–530
32. Liu X (2015) Analysis and improvement for image encryption algorithm based on multiple chaotic mapping. Open Autom Control Syst J 7(1):1560–1565
33. Liu L, Miao S (2017) An image encryption algorithm based on baker map with varying parameter. Multimed Tools Appl 76(15):16511–16527
34. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16):3895–3903. https://doi.org/10.1016/j.optcom.2011.04.001
35. Liu H, Wang X, Kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–1466. https://doi.org/10.1016/j.asoc.2012.01.016
36. Liu X, Han G, Wu J, Shao Z, Coatrieux G, Shu H (2017) Fractional Krawtchouk transform with an application to image watermarking. IEEE Trans Signal Process 65(7):1894–1908
37. Liu X, Wu Y, Zhang H, Wu J, Zhang L (2021) Quaternion discrete fractional Krawtchouk transform and its application in color image encryption and watermarking. Signal Process 189:108275
38. McBride AC, Kerr FH (1987) On Namias's fractional Fourier transforms. IMA J Appl Math 39(2):159–175
39. Mukundan R, Ong SH, Lee PA (2001) Image analysis by Tchebichef moments. IEEE Trans Image Process 10(9):1357–1364
40. Oliveira PA, Cintra RJ, Bayer FM, Kulasekera S, Madanayake A (2016) Low-complexity image and video coding based on an approximate discrete Tchebichef transform. IEEE Trans Circuits Syst Vid Technol 27(5):1066–1076
41. Rajesh GR, Nargunam AS (2013) "Steganography algorithm based on discrete cosine transform for data embedding into raw video streams," in IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), pp. 554–558
42. Ramalingam M, Isa NAM, Puviarasi R (2020) A secured data hiding using affine transformation in video steganography. Procedia Comput Sci 171:1147–1156
43. Salunke S, Venkatadri M, Hashmi MF, Ahuja B (2021) Novel beta function-based image encryption with fractional sine transform. Mater. Today Proc 47:6991–699
44. Stewart GW (1973) Introduction to matrix computations. Elsevier
45. Sui L, Lu H, Ning X, Wang Y (2014) Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain. Opt Eng 53(2):026108
46. Sun Q, Guan P, Qiu Y, Xue Y (2012) "A novel digital image encryption method based on one-dimensional random scrambling," in 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, pp. 1669–1672
47. Suresh M, Sam IS (2021) "A Secure Video Steganography Using Framelet Transform and Singular Value Decomposition," in Data Intelligence and Cognitive Informatics, Springer, pp. 781–790
48. "Test Sequences." (2021) https://pi4.informatik.uni-mannheim.de/~kiess/test_sequences/download/ (accessed Dec. 12, 2021)
49. Unnikrishnan G, Joseph J, Singh K (2000) Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt Lett 25(12):887–889
50. Wang X, Gao S (2020) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci 539:195–214. https://doi.org/10.1016/j.ins.2020.06.030
51. Wang X, Gao S (2020) Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Inf Sci 507:16–36. https://doi.org/10.1016/j.ins.2019.08.041
52. Wang X, Liu P (2021) A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Trans Circuits Syst Regul Pap 69(3):1291–1301
53. Wang X, Yang J (2021) A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient. Inf Sci 569:217–240. https://doi.org/10.1016/j.ins.2021.04.013
54. Wang X, Zhang M (2021) An image encryption algorithm based on new chaos and diffusion values of a truth table. Inf Sci 579:128–149. https://doi.org/10.1016/j.ins.2021.07.096
55. Wang Y, Wong K-W, Liao X, Chen G (2011) A new chaos-based fast image encryption algorithm. Appl Soft Comput 11(1):514–522
56. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108. https://doi.org/10.1016/j.sigpro.2011.10.023
57. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18. https://doi.org/10.1016/j.optlaseng.2014.08.005
58. Wang X-Y, Zhang Y-Q, Bao X-M (2015) A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 73:53–61. https://doi.org/10.1016/j.optlaseng.2015.03.022

59. Wang X, Feng L, Zhao H (2019) Fast image encryption algorithm based on parallel computing system. Inf Sci 486:340–358
60. Wang X, Liu C, Jiang D (2021) A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inf Sci 574:505–527
61. Watkins DS (2007) The matrix eigenvalue problem. Society for Industrial and Applied Mathematics. https://doi.org/10.1137/1.9780898717808
62. Wu J, Guo F, Zeng P, Zhou N (2013) Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence. J Mod Opt 60(20):1760–1771
63. Wu J, Zhang M, Zhou N (2017) Image encryption scheme based on random fractional discrete cosine transform and dependent scrambling and diffusion. J Mod Opt 64(4):334–346
64. Xian Y, Wang X (2021) Fractal sorting matrix and its application on chaotic image encryption. Inf Sci 547: 1154–1169. https://doi.org/10.1016/j.ins.2020.09.055
65. Xian Y, Wang X, Teng L (2021) Double parameters fractal sorting matrix and its application in image encryption. IEEE Trans Circuits Syst Video Technol 32(6):4028–4037. https://doi.org/10.1109/TCSVT.2021.3108767
66. Yamni M, Daoui A, Karmouni H, Sayyouri M, Qjidaa H, Flusser J (2020) Fractional Charlier moments for image reconstruction and image watermarking. Signal Process 171:107509
67. Yang T, Ma J, Wang Q, Miao Y, Wang X, Meng Q (2018) Image feature extraction in encrypted domain with privacy-preserving Hahn moments. IEEE Access 6:47521–47534. https://doi.org/10.1109/ACCESS.2018.2866861
68. "YUV Sequences." (2021) http://trace.eas.asu.edu/yuv/index.html (accessed Dec. 12, 2021).
69. Zhang L, Chen D (2020) The large capacity embedding algorithm for H. 264/AVC intra-prediction mode video steganography based on linear block code over Z4. Multimed Tools Appl 79:1–19
70. Zhang Y-Q, Wang X-Y (2015) A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 26:10–20. https://doi.org/10.1016/j.asoc.2014.09.039
71. Zhou N, Wang Y, Wu J (2011) Image encryption algorithm based on the multi-order discrete fractional Mellin transform. Opt Commun 284(24):5588–5597
72. Zhou N, Wang Y, Gong L, Chen X, Yang Y (2012) Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. Opt Laser Technol 44(7):2270–2281
73. Zhou N, Liu X, Zhang Y, Yang Y (2013) Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain. Opt Laser Technol 47:341–346. https://doi.org/10.1016/j.optlastec.2012.08.033