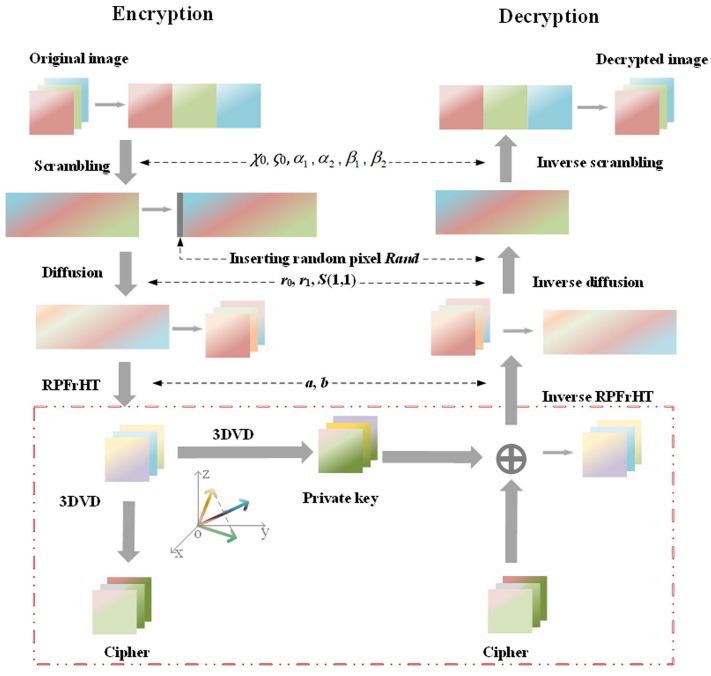
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

A Novel 3D Vector Decomposition for Color-Image Encryption

Volume 12, Number 2, April 2020

Zheng Zhu
Chao Wu
Jun Wang, *Senior Member, IEEE*
Keya Hu
Xu-dong Chen



DOI: 10.1109/JPHOT.2020.2981494

A Novel 3D Vector Decomposition for Color-Image Encryption

Zheng Zhu, Chao Wu, Jun Wang, *Senior Member, IEEE*, Keya Hu, and Xu-dong Chen

School of Electronics & Information Engineering, Sichuan University, Chengdu 610065, China

DOI:10.1109/JPHOT.2020.2981494

Manuscript received February 18, 2020; revised March 4, 2020; accepted March 14, 2020. Date of publication March 17, 2020; date of current version April 16, 2020. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant U1933132 and in part by the Sichuan Science and Technology Program under Grant 2018GZ0533. Corresponding author: Jun Wang (e-mail: jwang@scu.edu.cn).

Abstract: In this paper, a novel 3D vector decomposition is proposed for color-image encryption, in which a 3D vector is decomposed into two 3D vectors with random size in a random plane for providing a reliable security constraint. The technique of 3D vector decomposition, as far as we know, firstly offers a three-component encryption with one action, which fits well color-image encryption, and outputs a real ciphertext, which is convenient for recording and transmission. Furthermore, we employ an 1D chaos, which has strong chaotic properties, and reality-preserving fractional Hartley transform to cooperate 3D vector decomposition for constructing a color-image cryptosystem. Therefore, the proposed cryptosystem accomplishes improved security by reducing the single-channel attack risk in individual color-image encryption and avoiding the vulnerable channel in sequential color-image encryption as well as reduced the amount of data of transform-based cryptosystem by avoiding the complex output. Also, it has the advantages of strong chaotic performances, large key space and high key sensitivity, which is highly robust against various attacks. Experimental results show the effectiveness and superiority of the proposed cryptosystem.

Index Terms: 3D vector decomposition, 1D chaos, reality-preserving fractional Hartley transform, color-image encryption.

1. Introduction

With the advent of cloud computing and big data, more and more attention has been paid to information security. Images often provide a wealth of information, so image encryption has become a crucial issue and has attracted more and more concern. Image encryption techniques can be divided into two categories, one is chaos-based encryption [1]–[9], the other is transform-based encryption [10]–[15]. They each have their own advantages. Chaotic system is widely used in image encryption because of their good random behavior, ergodicity, and sensitivity to initial values. Among them, the 1D chaotic system [16]–[18] has attracted the attention of researchers because it has simpler structure and is easier to implement than multidimensional chaotic system, such as Logistic map [19] and Tent map [20]. However, its chaotic trajectory is simple and easy to predict, its chaotic range is narrow, which is vulnerable to attack. Therefore, a chaotic system with a simple structure but strong chaotic properties is urgently needed.

The transform-based encryption techniques can change the domain. For example, Refregier and Javidi first proposed double random phase encoding (DRPE) in 1995 [21], which realized the conversion between the spatial domain and Fourier transform domain. Compared with this, the fractional transformation has better performance and increased number of parameters, which contributes to higher security performance of image encryption. Hence, Unnikrishnan [22] introduced DRPE to fractional Fourier transform for the first time, and then, modifications, such as fractional cosine transform [23], fractional Fresnel transform [24], and fractional Hartley transform [25] are derived based on DRPE. However, the output of all fractional transformations is complex, which is hard to transmit and record. Therefore, how a transformation can have better performance without increasing the burden of data has always been researchers' unremitting pursuit.

Chaos and fractional transform can provide important parameters, while one-time pad tend to provide stronger security constraints than important parameters. Cai *et al.* have proposed a cryptosystem based on equal-mode decomposition (EMD) [27], which decomposed a 2D vector into two 2D vectors, one of which is ciphertext and the other is a private key as a security constraint. This technique provided a reliable one-way function of trapdoor [28], and was widely used in image encryption, such as Fresnel-based cryptosystem [29], cascaded EMD cryptosystem [30], etc. However, the output of the conventional EMD is complex and only applicable to grayscale images. A color-image contains richer information than the grayscale image, so color-image encryption [31]–[34] has always been an important issue. However, color-image is individually encrypted with the same algorithm for each channel [35], [36], which leads to data volume surge, inefficient recording or transmission and is weak in single-channel attacks, or is encrypted each channel sequentially [37]–[39], which makes the last encrypted channel less secure. Besides, the transform-based color-image encryption generally outputs complex ciphertext, which is hard to record and transmit. Therefore, realizing three-component encryption with one action for color-image which strengthens the channels security, while maintaining small amount of data is an attractive research issue.

In this paper, we construct a novel 3D vector decomposition (3DVD) for color-image encryption. In the spatial coordinate system, the proposed 3DVD decomposes a 3D vector into two 3D vectors with equal modulus. The decomposition plane and size are random, which disturbs the information. This technique, as far as we know, firstly realizes three-component encryption with one action and gives real outputs, which reduces the amount of data and facilitates recording and transmission. Additionally, we apply a 1D chaos [40] with large chaotic range and excellent chaotic performances, as well as reality-preserving fractional Hartley transform (RPFrHT) [41] to offer a real input for 3DVD in order to construct a color-image cryptosystem. Moreover, the proposed cryptosystem reduces the single-channel attack risks in color-image individual encryption, avoids the vulnerable channel in sequential image encryption and has large key space as well as high key sensitivity. Experimental results show that the scheme is safe and reliable, and has strong robustness to various attacks.

2. Related Work

This section mainly introduces the technology proposed in this paper, including the Logistic-Tent system (LTS) and the Reality-Preserving Fractional Hartley transform (RPFrHT).

2.1 Logistic-Tent system (LTS)

The logistic map is a classic 1D chaos with simple dynamic equation and complex chaotic behavior, and the mathematical definition is given by:

$$X_{n+1} = \mu X_n(1 - X_n), \tag{1}$$

where μ is a parameter with range of (0, 4].

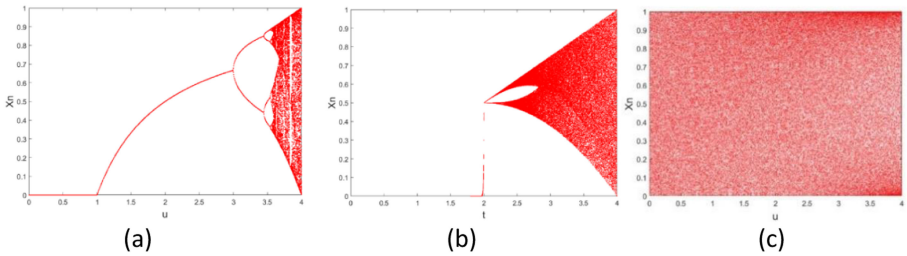


Fig. 1. The bifurcation of (a) Logistic map, (b) Tent map, and (c) LTS.

The Tent map is another classic 1D chaos, which is famous for its tent-like shape features, and its mathematical definition is given by:

$$X_{n+1} = \begin{cases} tX_n/2 & X_i < 0.5 \\ t(1-X_n)/2 & X_i \geq 0.5 \end{cases}, \tag{2}$$

where t is a parameter with range of (0, 4].

Zhou [40] proposed a nonlinear chaotic system by employing Logistic map and Tent map as seed maps, which names Logistic-Tent system (LTS). The LTS has better characteristics, whose mathematical expression is given by:

$$X_{n+1} = LTS(\mu, X_n) = \begin{cases} (\mu X_n(1-X_n) + (4-\mu)X_n/2) \bmod 1 & X_i < 0.5 \\ (\mu X_n(1-X_n) + (4-\mu)(1-X_n)/2) \bmod 1 & X_i \geq 0.5 \end{cases}, \tag{3}$$

where μ belongs to (0, 4].

Fig. 1(a)–(c) represent the bifurcation diagram of Logistic map, Tent map and LTS, respectively. The output sequences of LTS uniformly distribute within [0, 1]. Compared with the ouput of Logistic map and Tent map, LTS has better chaotics performance.

2.2 Reality-Preserving Fractional Hartley Transform (RPFrHT)

The eign-decomposition of the Hartley transformation matrix at N points can be given by [42]:

$$H = \sum_{k=0}^{N-1} \exp[-j\pi k] u_k u_k^T, \tag{4}$$

where u_k is an eigenvector corresponding to eigencalue exp $(-j\pi k]$, which can be obtained from the eigenvector of real-valued symmetric matrix W. $(\omega = 2\pi/N)$.

$$W = \begin{bmatrix} 2 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 2\cos(\omega) & 1 & \cdots & 0 & 0 \\ 2 & 1 & 2\cos(2\omega) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2\cos[(N-2)\omega] & 1 \\ 1 & 0 & 0 & \cdots & 1 & 2\cos[(N-1)\omega] \end{bmatrix}, \tag{5}$$

The fractional Hartley transform is defined as:

$$H^a = UD^aU^T = \sum_{k=0}^{N-1} \exp[-j\pi ak] u_k u_k^T, \tag{6}$$

where $U = [u_0 | u_1 | \cdots | u_{N-1}]$. It can be seen that when $a = 1$, H degenerates into a Hartley matrix. Suppose signal be x, then its FrHT is expressed as:

$$y_a = H^a x, \tag{7}$$

However, the output of FrHT is still complex, and the next step is to make the output of FrHT real. The paper [33] proposed a Reality-Preserving FrHT (RPFrHT). The steps are as follows:

①: Set $x = \{x_1, x_2, \ldots, x_N\}^T$ be a real-valued signal of length N, where N is an even number, and H^a is a matrix for FrHT with a siz of $N/2$. Convert x into a complex signal of length $N/2$, which is defined as:

$$\widehat{x} = \{x_1 + j \cdot x_{N/2+1}, x_2 + j \cdot x_{N/2+2}, \ldots, x_{N/2} + j \cdot x_N\}^T, \tag{8}$$

②: $\widehat{y} = H^a \widehat{x}$. Reconstruct $y = \{\mathrm{Re}(\widehat{y}), \mathrm{Im}(\widehat{y})\}^T$ as the output of RPFrHT, which is expressed as:

$$\begin{aligned} \widehat{y} = H^a x &= \{\mathrm{Re}(H^a) + j \cdot \mathrm{Im}(H^a)\} \cdot \{\mathrm{Re}(\widehat{x}) + j \cdot \mathrm{Im}(\widehat{x})\} \\ &= \{\mathrm{Re}(H^a)\mathrm{Re}(\widehat{x}) - \mathrm{Im}(H^a)\mathrm{Im}(\widehat{x})\} + j \cdot \{\mathrm{Im}(H^a)\mathrm{Re}(\widehat{x}) + \mathrm{Re}(H^a)\mathrm{Im}(\widehat{x})\}, \end{aligned} \tag{9}$$

Hence

$$y = \begin{bmatrix} \mathrm{Re}(H^a) & -\mathrm{Im}(H^a) \\ \mathrm{Im}(H^a) & \mathrm{Re}(H^a) \end{bmatrix} \begin{bmatrix} \mathrm{Re}(\widehat{x}) \\ \mathrm{Im}(\widehat{x}) \end{bmatrix} = R_H^a x, \tag{10}$$

Where

$$R_H^a = \begin{bmatrix} \mathrm{Re}(H^a) & -\mathrm{Im}(H^a) \\ \mathrm{Im}(H^a) & \mathrm{Re}(H^a) \end{bmatrix}, \tag{11}$$

For 2D signal X, its RPFrHT is:

$$Y = R_H^a \cdot X \cdot R_H^b, \tag{12}$$

3. Proposed 3D Vector Decomposition (3DVD)

LTS and RPFrHT can provide important parameters for the cryptosystem. However, a private key is far stronger than the constraint of important parameters, from which we focus on protecting the cryptosystem with the private key to enhance the security of the cryptosystem. Compared with 2D Equal Modulus Decomposition (EMD) [27], 3DVD is a new technology to decompose a space vector into two space vectors with random size in random plane, which is applicable for color image. Because it can realize three-component encryption with one action, which can help cryptosystem for avoiding the vulnerable channel in sequential image encryption. The two vectors after decomposition are used as ciphertext and private key (PK), respectively, which can provide a superior, effective and valid security constraint. More importantly, this technique gives real outputs in the encryption process, which is convenient for recording and transmission.

In the space coordinate system, a space vector can be decomposed into two 3D vectors with equal modulus. A color image I (x, y, z) is regarded as a 3D vector, and it is decomposed into two vectors with equal modulus P_1 and P_2, where the angle between P_1/P_2 and I is ξ, the normal vector of the P_1oP_2 plane is k (A, B, C), the angle between the projection of the vector I on the xoy plane and the y axis is ω, and the angle between the vector I and the z-axis is $\pi/2-\delta$. The vector decomposition diagram is shown in Fig. 2 step (a). Where:

$$\tan(\omega) = x/y, \sin(\delta) = z/\sqrt{x^2 + y^2 + z^2}. \tag{13}$$

First, the vector I and plane P_1oP_2 are rotated ω degrees around the z-axis to the zoy plane and then rotated $\pi/2 - \delta$ degrees around the x-axis, at this point, the vector I' overlaps with the z-axis, $P_1'oP_2'$ plane after rotation P_1oP_2 plane perpendicular to the plane xoy, in which the rotated nomal

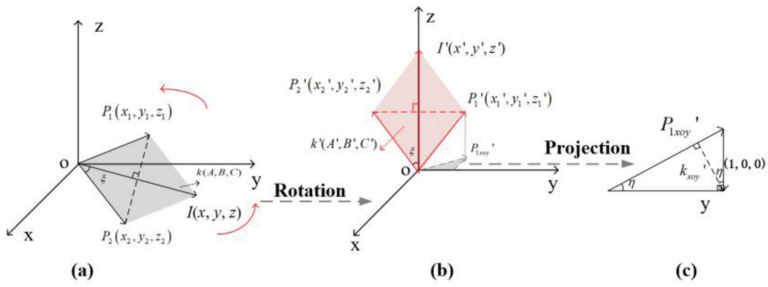


Fig. 2. The vector decomposition diagram.

vector is k' (A', B', C'), the rotated P_1 and P_2 are P' (x'_1, y'_1, z'_1) and P'_2 (x'_2, y'_2, z'_2), respectively. The rotated vector decomposition diagram is shown in Fig. 2 step (b).

Suppose the projection of P' on the *xoy* plane is P'_{1xoy}, and the projection of k' on the *xoy* plane is k'_{xoy}, the angle between k'_{xoy} and the vector (1, 0, 0) is η. The projection diagram is shown in Fig. 2 step (c).

Thus, the results are expressed as:

$$\cos(\eta) = A'/\sqrt{A'^2 + B'^2 + C'^2},\ r = \sqrt{x^2 + y^2 + z^2}, \tag{14}$$

$$\begin{cases} x'_1 = r/2 \cdot \tan(\xi) \cdot \sin(\eta) \\ y'_1 = r/2 \cdot \tan(\xi) \cdot \cos(\eta) \\ z'_1 = r/2 \end{cases}, \quad \begin{cases} x'_2 = -x'_1 \\ y'_2 = -y'_1 \\ z'_2 = r/2 \end{cases}, \tag{15}$$

The P'_1 and P'_2 are reversely rotated according to the mentioned steps, that is, multiplying by two rotation matrices to obtain P_1 and P_2, which is defined as:

$$P_1 = P'_1(x'_1, y'_1, z'_1) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & \sin(\delta) & -\cos(\delta) \\ 0 & \cos(\delta) & \sin(\delta) \end{bmatrix} \cdot \begin{bmatrix} \cos(\omega) & -\sin(\omega) & 0 \\ \sin(\omega) & \cos(\omega) & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{16}$$

$$P_2 = P'_2(x'_2, y'_2, z'_2) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & \sin(\delta) & -\cos(\delta) \\ 0 & \cos(\delta) & \sin(\delta) \end{bmatrix} \cdot \begin{bmatrix} \cos(\omega) & -\sin(\omega) & 0 \\ \sin(\omega) & \cos(\omega) & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{17}$$

The inverse process is:

$$I = P_1 + P_2, \tag{18}$$

For convenience, this paper takes the above rotation method as an example.

4. Color-Image Encryption Scheme

The We proposed a real-valued, effective cryptosystem with high security performance by applying the above technology to color-image encryption. This section details the encryption and decryption process of the cryptosystem.

4.1 Process of Encryption

I. Given six initial values $\chi 0$, $\varsigma 0$, $\alpha 1$, $\beta 1$, $\alpha 2$ and $\beta 2$, two random sequences of size M $\times$ 3N/2 are generated by the following two equations [43]:

$$\chi_{n+1} = \alpha_1 \chi_n (1 - \chi_n) + \beta_1 \varsigma^2, \tag{19}$$

$$\varsigma_{n+1} = \alpha_2 \varsigma_n (1 - \varsigma_n) + \beta_2 (\chi_n^2 + \chi_n \varsigma_n), \tag{20}$$

By combining the two sequences together and arranging them in uniform ascending order, an address sequence d with a size of $M \times 3N$ is obtained.

II. The R, G and B channels of the original color image are arranged into a picture with a size of $M \times 3N$, and the address sequence d is scrambled it to obtain result C. This step not only achieves single-channel scrambling, but also realizes channel-to-channel scrambling.

III. Insert a column of random numbers in front of the C matrix to get $R_i(j)$, that is:

$$R_i(j) = \begin{cases} \text{Rand}(i) & \text{if } j = 1 \\ C(i, j-1) & \text{otherwise} \end{cases}, \tag{21}$$

Employ $R_i(j)$ and LTS to diffuse the image according to the following equation to get $B_i(j)$:

$$B_i(j) = \begin{cases} R_i(j) & \text{if } j = 1 \\ B_i(j-1) \oplus R_i(j) \oplus (\left\lfloor S(i, j) \cdot 10^{10} \right\rfloor \bmod 256) & \text{otherwise} \end{cases}, \tag{22}$$

where $\oplus$ denotes the bit-wise XOR operation, $\lfloor \cdot \rfloor$ is the floor function, S is the random sequence generated by LTS, whose expression is:

$$S(i, j) = \begin{cases} S(1, 1) & \text{for } i = 1, j = 1 \\ LTS(r_0, S(i-1, 1)) & \text{for } i > 1, j = 1 \\ LTS(r_1, S(i, j-1)) & \text{for } i > 1, j > 1 \end{cases}, \tag{23}$$

where r_0, r_1, $S(1,1)$ are initial paremeters defined by users. Fig. 4 is the process of inserting random pixel and diffusion.

IV. Remove the fist column of $B_i(j)$, reshape it to X of size $M \times N \times 3$, and perform RPFrHT on each channel of X to get y:

$$Y_i = R_H^a \cdot X_i \cdot R_H^b, \tag{24}$$

where $i =$ (R,G,B) denotes the i channel.

V. Take y as the input of 3DVD, and output the ciphertext and PK.

$$[\text{cipher}, \text{PK}] = 3dVD(Y), \tag{25}$$

where 3DVD represents the 3DVD.

4.2 Process of Decryption

I. Add ciphertext and PK to get Dy:

$$D_y = \text{cipher} + PK, \tag{26}$$

II. Perform inverse RPFrHT on D_y to get D_x:

$$D_x = R_H^{-a} \cdot D_y \cdot R_H^{-b}, \tag{27}$$

III. Reshape D_x for size $M \times 3N$, insert the random sequence of encryption III in front of D_x to get D_B, and perform inverse diffusion operation on it. The inverse diffusion is given by:

$$D_R(i, j) = D_B(i, j-1) \oplus D_B(i, j) \oplus (\left\lfloor S(i, j) \cdot 10^{10} \right\rfloor \bmod 256), \tag{28}$$

Remove the first column of D_R, then it is scrambled in reverse. Reshape the product to $M \times N \times 3$ to get the decrypted image D_{img}.

The flow chart of encryption and decryption is shown in Fig. 3.

5. Encryption and Decryption Results

In order to verify the validity and feasibility of the proposed technology, this paper uses MATLAB for numerical research. The initial values of parameters are shown in Table 1. This work was done

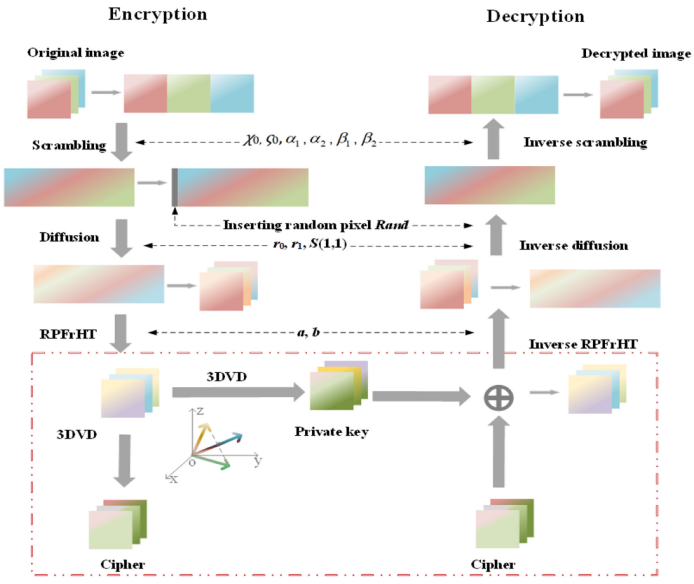


Fig. 3. Flow chart of encryption and decryption, and 3DVD is denoted by dotted box.

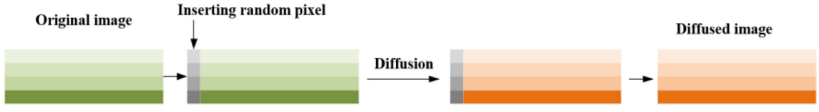


Fig. 4. The process of inserting random pixels and diffusion.

TABLE 1
The Parameters of Each Process

	RPFrHT	Diffusion	Scrambling
Value	a=0.2, b=0.7	r_0=3.997, r_1=3.99, $S(1,1)$=0.6	α_1=2.9748, α_2=3.1756, β_1=0.2149, β_2=0.1429, χ_0=255W/(M×N×3), $\varsigma_0 = e^{-x_0}$

on a laptop with Processor Intel (R) Core (TM) i5-4590 @ 3.30 GHz, Memory 4096 MB RAM, and 64-bit OS Win10.

The decryption performance and decryption quality are determined by calculating the correlation coefficient (CC) and peak signal-to-noise ratio (PSNR) between the input and decrypted images. The CC can be given by:

$$CC = \frac{E\{[I_o - E[I_o]][I_d - E[I_d]]\}}{\sqrt{E\{[I_o - E[I_o]]^2\}}\sqrt{E\{[I_d - E[I_d]]^2\}}}, \tag{29}$$

where I_o and I_d are the original and decrypted images, respectively. $E[\cdot]$ denotes the expected value of function, $M \times N$ is the size of images.

Fig. 5(a)–(d) and Fig. 5(e)–(h) are the original image, ciphertext, PK and decrypted image, respectively. The CC values and PSNR values are 1 and inf, respectively. It can be seen that the cryptosystem is lossless.

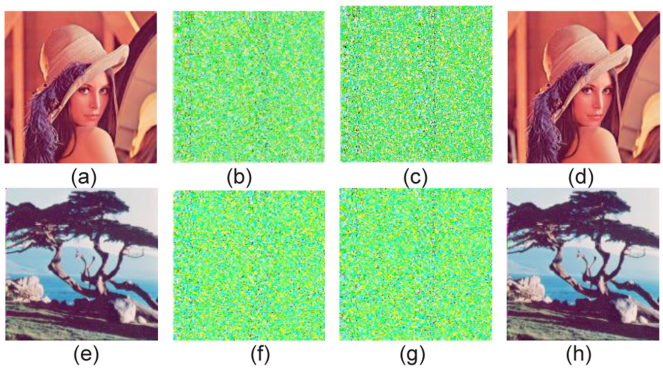


Fig. 5. (a) and (e) the original image, (b) and (f) the ciphertext, (c) and (g) the PK, (d) and (h) the decrypted image.

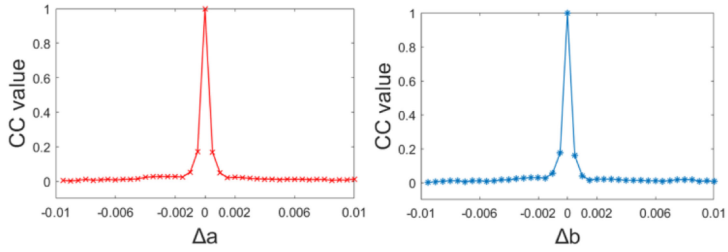


Fig. 6. The CC values with the change of order a and b of RPFrHT.

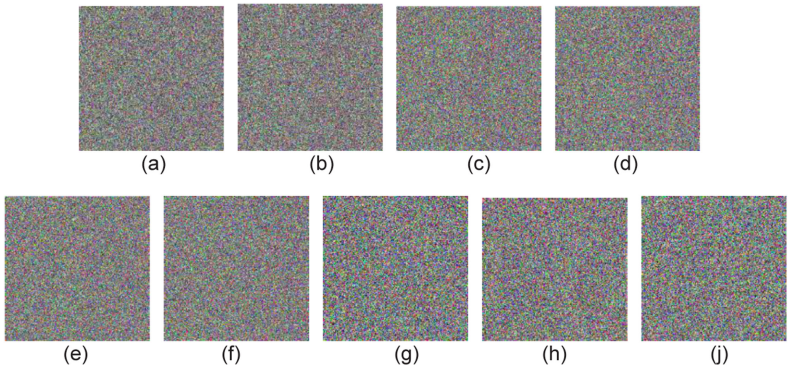


Fig. 7. The senitivity of (a) α_1, (b) α_2, (c) β_1, (d) β_2, (e) χ_0, (f) ς_0, (g) r_0, (h) r_1, and (j) $S(1, 1)$.

6. Security Analysis

When a new encryption scheme is developed, excellent security performance is required to be qualified. In this section, we have performed various tests on this scheme.

6.1 Key Sensitivity

For a secure encryption scheme, the cryptosystem must be highly sensitive to key changes. We test the scheme's sensitivity to keys. Fig. 6 shows the CC values with the change of the order *a* and *b* of RPFrHT. The change interval is $[-0.01, 0.01]$ with step size 0.0005. It can be seen that the CC value will change drastically only when the order changes slightly, which is about 20 times more sensitive than that of [40]. That is, the encryption scheme is sensitive to the variation.

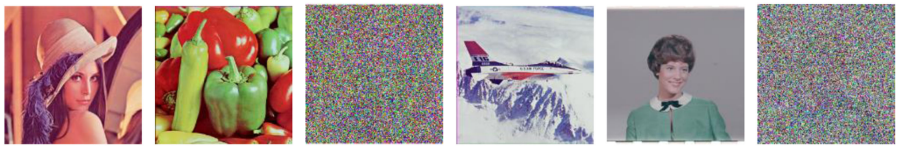


Fig. 8. (a) and (d) the original images, (b) and (e) the arbitary images, (c), and (f) the decrypted images.

Fig. 7 shows the sensitivity of α_1, α_2, β_1, β_2, χ_0, ς_0, r_0, r_1 and S (1,1). Fig. 7(a) and (b) are the decrypted images when α_1 and α_2 are increased by 10^{-15}. Fig. 7(c) and (d) are the decrypted images when β_1 and β_2 are increased by 10^{-16}. Fig. 7(e) and (f) are the decrypted images when χ_0 and ς_0 are increased by 10^{-16} and 10^{-15}, respectively. Fig. 7(g)–(j) are the decrypted images when r_0, r_1 and S (1, 1) are increased by 10^{-15}, 10^{-15} and 10^{-16}, respectively. We can't get any valid information from the decrypted images, which shows that the scheme has highly key sensitivity.

6.2 Key Space

From the perspective of cryptography, the size of the key space must be no less than 2^{100} to ensure the security of the cryptosystem. In the proposed scheme, the keys designed during the encryption process are independent. The key sensitivity of orders a and b is about 0.002, that is, the key space is not less than $10^2 \times 10^2$. From the Section 6.1, we can compute the size of key space is $10^{2+2+15+15+16+16+16+15+15+15+16} = 10^{143} \approx 2^{478}$.

6.3 Chosen-Plaintext Attack

It is well known that there are four types of traditional attacks, namely, cipher-only attack, known-plaintext attack, chosen-cipher attack and chosen-plaintext attack. Among them, the chosen-plaintext attack is the most vulnerable to attack. Therefore, if a cryptosystem could defend against chosen-plaintext attack, it can resist other attacks.

Based on the proposed cryptosystem, the attacker may use any images to encrypt and obtain a fake private key, then use the obtained fake private key to decrypt the ciphertext. The decrypted image is shown in Fig. 8(c) and (f), in which Fig. 8(a) and (d) are the original images, Fig. 8(b) and (e) are the arbitrary images, respectively. We can't obtain any valid information, which indicates that the proposed cryptosystem has high security and strong robustness to resist chosen plaintext attack.

6.4 Correlation Coefficient Analysis

Correlation coefficient is an important index to measure the quality of cryptosystem. The correlation between adjacent pixels of the ciphertext is very small in a good cryptosystem. In this simulation, we selected 10000 pairs of adjacent pixels from the original and encrypted images, and measured their correlation coefficients in the horizaontal, vertical and diagonal directions. The results are shown in Table 2. It can be seen that there are significant corrtlations between adjacent pixels of the original images, while there are almost no correlations in the corresponding encrypted images. It proved that the proposed cryptosystem breaks the correlation of the original images.

6.5 Robustness Analysis

The noise and occlusion attacks are often used to test the robustness of an image encryption scheme.

TABLE 2
Correlation Coefficient of Adjacent Pixels

		Original image			Encrypted image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	R	0.93272	0.95319	0.88826	0.00138	0.00026	0.00019
	G	0.94953	0.9667	0.91887	0.00090	0.00573	0.00090
	B	0.91669	0.94123	0.8633	0.00171	0.00064	0.00075
Peppers	R	0.92418	0.93526	0.88191	0.00002	0.00009	0.00007
	G	0.94039	0.95119	0.90672	0.00152	0.00026	0.00013
	B	0.90075	0.92137	0.85998	0.00031	0.00004	0.00002
Tree	R	0.93339	0.9377	0.88852	0.00100	0.00888	0.00098
	G	0.96225	0.95315	0.92559	0.00172	0.00116	0.00131
	B	0.95019	0.94874	0.91692	0.00213	0.00308	0.00059
Airplane	R	0.89533	0.84644	0.79132	0.00042	0.00009	0.00015
	G	0.88905	0.88011	0.82226	0.00298	0.00007	0.00061
	B	0.91608	0.86437	0.83951	0.00011	0.00018	0.00011

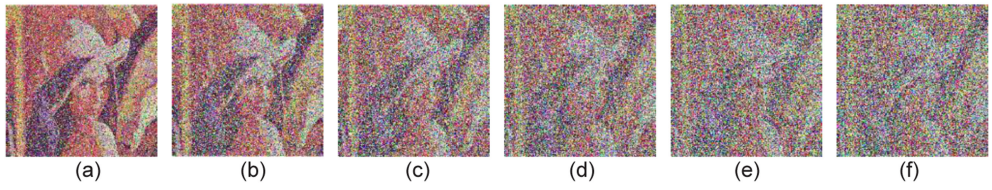


Fig. 9. Decrypted image with noise intensity: (a) 0.1, (b) 0.2, (c) 0.3, (d) 0.4, (e) 0.5, and (f) 0.6.

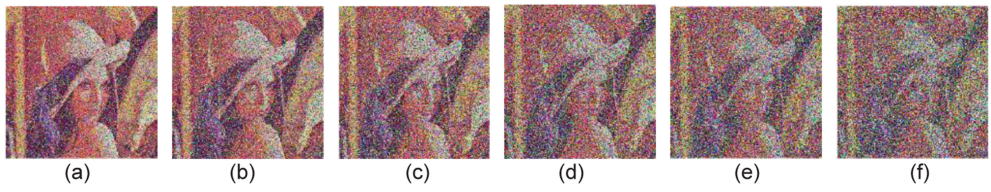


Fig. 10. Decrypted image when obscured the encrypted image by (a) 30 × 30 × 3, (b) 40 × 40 × 3, (c) 50 × 50 × 3, (d) 60 × 60 × 3, (e) 70 × 70 × 3, and (f) 80 × 80 × 3 pixels.

The ciphertext is inevitably polluted by noise during transmission. We tested the effects of noise on the cryptosystem and set the encrypted image to be contaminated by Gaussian noise as follows:

$$E' = E(1 + kG), \tag{30}$$

where E and E' denote encrypted image and noise-contaminated encrypted image, respectively. G is a Gaussian random noise with a mean of 0 and a variance of 0.05, and k denotes a Gaussian noise intensity coefficient.

Fig. 9(a)–(f) are the decrypted images when ciphertext are polluted with noise intensity k = 0.1, 0.2, 0.3 0.4, 0.5 and 0.6, respectively. In those case, we can still distinguish the features of the images, which represents that the proposed scheme is robust to noise attack.

Some information may lose when a ciphertext is transmitted over a communication channel. In order to test the robustness of the proposed scheme against data loss, we obscured the encrypted image by 30 × 30 × 3, 40 × 40 × 3, 50 × 50 × 3, 60 × 60 × 3, 70 × 70 × 3, 80 × 80 × 3 pixels, the corrsponding decrypted images are shown in Fig. 10. The decrypted images have original information, which indicates that some data lost, the remaining pixels still contain global information, the proposed scheme can withstand a certain amount of data loss.

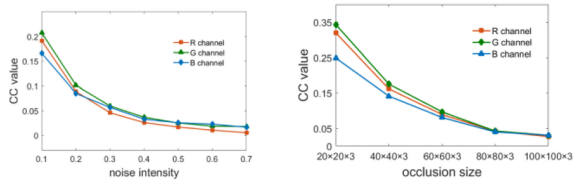


Fig. 11. The CC values (a) with the change of noise intensity and (b) the change of occlusion size.

TABLE 3
The Comparison of Key Space

	This work	Ref. [43]	Ref. [44]	Ref. [45]	Ref. [46]	Ref. [47]	Ref. [48]
Key space	$10^{143}\approx 2^{478}$	10^{98}	2^{199}	2^{294}	2^{299}	2^{440}	2^{128}

TABLE 4
The Comparison of Correlation Coefficient

		Encrypted image		
		Horizontal	Vertical	Diagonal
The proposal	R	0.00138	0.00026	0.00019
	G	0.00090	0.00573	0.00090
	B	0.00171	0.00064	0.00075
Ref [43]	R	-0.00147	0.00242	-0.00234
	G	0.00029	0.00072	-0.00016
	B	0.00262	-0.00192	-0.00744
Ref [45]	R	0.00270	-0.01670	0.00330
	G	-0.01240	0.01530	-0.00040
	B	0.00220	-0.01270	-0.00270
Ref [46]	R	-0.01240	-0.00010	-0.00550
	G	-0.00380	0.00590	-0.00860
	B	0.00750	-0.00620	0.00060
Ref [49]	R	0.00100	-0.00140	-0.00190
	G	-0.00056	-0.00130	-0.00022
	B	-0.00025	0.00180	0.00022

Fig. 11(a) and (b) are the CC values with the change of noise intensity and occlusion size, respectively. As we can see, this scheme can resist noise attack and data loss attack effectively.

7. Comparison and Discussion

7.1 Comparison

In this section, the scheme is compared with other mehods in literature to prove that the scheme is reliable and safe. Table 3 provides a comparison of the key space among the proposed scheme and other schemes which are symmetric encryption. It shows that the key space of the proposed scheme is large enough to resist brute force attacks, and attackers can't correctly decrypt images through large-scale exhaustive searches. Table 4 shows a comparison of correlation coefficient with other schemes, which shows our scheme has superior performances in adjacent pixels correlation.

7.2 Discussion

Current color-image encryption algorithms are classified into two categories, one is individual encryption, which encrypts each channel individually, the other is sequential encryption, which encrypts each channel in turn. As shown in Fig. 12, (a), the proposed 3DVD, realizes three-component

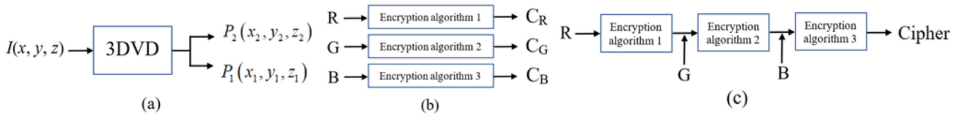


Fig. 12. The process of (a) our technique and (b) sequential image encryption.

encryption with one action, and each channel has the same encryption strength. Fig. 12(b) is the diagram of common individual encryption, which encrypts each channel individually. In this case, attackers can obtain most of the information of the original color image only by attacking one of the channels. The proposed 3DVD can reduce this risk, because it encrypts three channels with one action, in which every channel is encrypted uniformly not individually. Fig. 12(c) is the diagram of common sequential encryption, and each channel is encrypted in turn, which results in the last encrypted channel having weakest and fewest constraint because it is decrypted first when attacked. Each channel of the color image has the outline information of the whole image, and as long as one channel is decrypted, the attacker basically gets most of information of the original image. For example, in paper [39], the author processes phase-truncated Fresnel transform (PRFrT) on R, G and B channel sequentially. In the process of attack, only RPM R_1 and R_2, secret keys P_5 and P_6 are needed to decrypt the B channel. However, to decrypt the G channel, P_3 and P_4 are additionally required. To decrypt the R channel, additional constraints P_1, P_2, P_3 and P_4 are required. Therefore, this kind of encryption scheme has a vulnerable channel, while the proposed 3DVD can achieve three-component encryption with one action, which avoids the vulnerable channel, and strengthens the security.

8. Conclusions

In this paper, we propose a novel 3DVD for color-image encryption, which provides a reliable security constraint. It decomposes 3D vectors in random planes with random sizes, which outputs the real ciphertext. Moreover, we employ an 1D chaos with strong chaotic performances, and RPFrHT to cooperate 3DVD for a color-image cryptosystem. The 3DVD realizes a three-component encryption with one action, which reduces the single-channel attack risk in individual encryption and avoids the vulnerable channel in sequential color-image encryption. The proposed cryptosystem gives real outputs for reducing the amount of data, which is convenient for recording and transmission. Besides, it has large key space, high key sensitivity, and robustness resisting various attack.

References

[1] W. Xu, Z. Geng, Q. Zhu, and X. Gu, "A piecewise linear chaotic map and sequential quadratic programming based robust hybrid particle swarm optimization," *Inf. Sci.*, vol. 218, pp. 85–102, 2013.
[2] X. Wang, W. Zhang, W. Guo, and J. Zhang, "Secure chaotic system with application to chaotic ciphers," *Inf. Sci.*, vol. 221, pp. 555–570, 2013.
[3] E. Solak and C. Cokal, "Algebraic break of image ciphers based on discretized chaotic map lattices," *Inf. Sci.*, vol. 181, pp. 227–233, 2011.
[4] A. Kanso, H. Yahyaoui, and M. Almulla, "Keyed hash function based on a chaotic map," *Inf. Sci.*, vol. 186, pp. 249–264, 2012.
[5] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Process.*, vol. 93, no. 11, pp. 3039–3052, 2013.
[6] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, no. 0, pp. 80–94, 2015.
[7] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.
[8] L. Zhang, X. Hu, Y. Liu, K.-W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 10, pp. 3653–3659, 2014.
[9] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurc. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[10] Q. Gong, H. Wang, Y. Qin, and Z. Wang, "Modified diffractive-imaging-based image encryption," *Opt. Laser. Eng.*, vol. 121, pp. 66–73, 2019.
[11] Y. Qin, Z. Wang, H. Wang, and Q. Gong, "Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code," *Opt. Laser. Technol.*, vol. 103, pp. 93–98, 2018.
[12] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser. Technol.*, vol. 57, pp. 327–342, 2014.
[13] S. Jiao, C. Zhou, Y. Shi, W. Zou, and X. Li, "Review on optical image hiding and watermarking techniques," *Opt. Laser. Technol.*, vol. 109, pp. 370–380, 2019.
[14] N. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Opt. Commun.*, vol. 284, pp. 3234–3242, 2011.
[15] H. Xu *et al.*, "Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain," *Opt. Commun.*, vol. 402, pp. 302–310, 2017.
[16] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process*, vol. 138, pp. 129–137, 2017.
[17] I. Bashkirtseva and L. Ryashko, "Stochastic sensitivity analysis of noise-induced intermittency and transition to chaos in one-dimensional discrete-time system," *Physica A.*, vol. 392, pp. 295–306, 2013.
[18] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Process*, vol. 144, pp. 444–452, 2018.
[19] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process*, vol. 92, pp. 1101–1108, 2012.
[20] R. C. Hilborn, *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, 2nd ed., New York, NY, USA: Oxford University Press, 2001.
[21] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, pp. 767–769, 1995.
[22] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, 2000.
[23] J. Wu, F. Guo, Y. Liang, and N. Zhou, "Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform," *Optik-Int. J. Light Electron Opt.*, vol. 125, no. 16, pp. 4474–4479, 2014.
[24] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, pp. 762–764, 1999.
[25] Y. Liu, J. Du, J. Fan, and L. Gong, "Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation," *Multimedia Tools Appl.*, vol. 74, no. 9, pp. 3171–3182, 2015.
[26] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.*, vol. 35, pp. 118–120, 2010.
[27] J. Cai, X. Shen, M. Lei, C. Lin, and S. Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Lett.*, vol. 40, pp. 475–478, 2015.
[28] S. Jiao, J. Feng, and Y. Gao, "Visual cryptography in single-pixel imaging," *Opt. Exp.*, vol. 28, no. 5, pp. 7301–7313, 2020.
[29] G. Luan, A. Li, D. Zhang, and D. Wang, "Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain," *IEEE. Photoni. J.*, vol. 11, no. 1, Feb. 2019, Art. no. 6900207.
[30] J. Cai and X. Shen, "Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Laser. Technol.*, vol. 95, pp. 105–112, 2017.
[31] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyperchaotic system," *J. Syst. Softw.*, vol. 85 no. 2, pp. 290–299, 2012.
[32] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016.
[33] K. G. Larkin, "The spiral phase transform," *Phase Estimation in Optical Interferometry*, P. Rastogi, E. Hack, Eds., Boca Raton, FL, USA: CRC Press, 2014, pp. 121–139.
[34] K. Nadeau, A. Durkin, and B. Tromberg, "Advanced demodulation technique for the extraction of tissue optical properties and structural orientation contrast in the spatial frequency domain," *J. Biomed. Opt.* vol. 19, 2014, Art. no. 056013.
[35] X. Deng and D. Zhao, "Single-channel color image encryption based on asymmetric cryptosystem," *Opt. Laser. Technol.*, vol. 44, pp. 136–140, 2012.
[36] Q. Yuan, X. Yang, and L. Gao, "Color image single-channel encryption based on tricolor grating theory," *Opt. Lett.*, vol. 5, pp. 147–149, 2019.
[37] Z. Zhu, X. Chen, C. Wu, J. Wang, W. Wang, "An asymmetric color-image cryptosystem based on spiral phase transformation and equal modulus decomposition," *Opt. Laser. Technol.*, vol. 126, 2020, Art. no. 106106.
[38] S. M. Lamine and B. Ibtissem, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear. Dyn.*, vol. 94, pp. 723–744, 2018.
[39] Y. Wang, C. Quan, and C. J. Tay, "Optical color image encryption without information disclosure using phase-truncated fresnel transform and a random amplitude mask," *Opt. Commun.*, vol. 344, pp. 147–155, 2015.
[40] Y. Zhou, L. Bao, and C. L. Philip Chen, "A new 1D chaotic system for image encryption," *Signal Process*, vol. 97, pp. 172–182, 2014.
[41] X. Kang and R. Tao, "Color image encryption using pixel scrambling operator and reality-preserving MPFRHT," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 7, pp. 1919–1932, Jul. 2019.
[42] S.-C. Pei, C.-C. Tseng, M.-H. Yeh, and J. J. Shyu, "Discrete fractional hartley and fourier transforms," *IEEE Trans. Circuits Syst. II. Analog Digit. Signal Process.*, vol. 45 no. 6, pp. 665–675, Jun. 1998.
[43] X. Kang and R. Tao, "Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 6, pp. 1595–1607, Jun. 2019.

[44] J. Chen, L. Chen, L. Y. Zhang, and Z. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dyn.*, vol. 96, pp. 301–322, 2019.
[45] X. Chai, X. Zheng, Z. Gan, and Y. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," *Neural Comput. Appl*, 2019, doi: 10.1007/s00521-019-04312-8.
[46] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dyn.*, vol. 90, pp. 855–875, 2019.
[47] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dyn.*, vol. 95, pp. 2797–2824, 2019.
[48] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on imprived random number generator and its implementation," *Nonlinear Dyn.*, vol. 95, pp. 1781–1805, 2019.
[49] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dyn.*, vol. 94, pp. 723–744, 2018.