Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **2**, March **2017**

Simultaneous Compression and Encryption of Video Sequences Based on 3D Compressive Sensing and 3D Discrete Fractional Random Transform

Qing-Zhu Wang[1], Xiao-Ming Chen[1,*] and Yi-Hai Zhu[2]

[1]School of Information Engineering, Northeast Electric Power University,
169 Changchun Road, Jilin, China
[2]Engineering Technology Center CRRC Changchun Railway Vehicles Co.,Ltd
*Corresponding author: 807372496@qq.com

Received June 2016; revised January, 2017

Abstract. *In this paper, we propose a novel video sequences compression and encryption method combining 3D compressive sensing (3D-CS) with 3D discrete fractional random transform (3D-DFrRT). In this scheme, the original video sequences were transformed with discrete wavelet and measured by three Gaussion random matrices to achieve compression and encryption simultaneously, and then the resulting 3D image was re-encrypted by Arnlod transform (AT) and 3D-DFrRT. Three random circular matrices used in 3D-FrRT were constructed by sine logistic modulation map. The three-dimensional smoothed ℓ_0-norm algorithm was adopted to obtain the decrypted video sequences. Simulation results verified the good compression performance, efficiency and security of the proposed method.*
Keywords: Compressive Sensing, Image encryption, Discrete fractional random transform, Smoothed ℓ_0-norm algorithm, Video sequence.

1. **Introduction.** Images, especially video sequences, are of much more significance with the development of networked multimedia, communication and propagation techniques. Nowadays, images or videos play a significant role in information communication. Therefore, to protect secret images, especially the videos, from leaking during the process of transmission and storage, a variety of encryption and compression schemes and systems have been proposed recently. The double random phase encoding (DRPE) [1] scheme has provided the foundation of a variety of theoretical and experimental studies in optical encryption. Subsequently, a novel optical authentication-based cryptography was proposed, combining the modified Gerchberg-Saxton algorithm with random sampling was proposed [2]. Moreover, a novel multiple-image encryption technique based on interference, two-beam interference, and radial shearing interference [3] were reported to enhance the security of a crypto-system. Some pixel diffusion tools were used in image encryption systems, e.g. fractional Fourier transform (FrFT) [4], Gyrator transform (GT) [5], Fresnel transform (FST) [6], and fractional random transform [7]. Unfortunately, these techniques used in image encryption were found to be vulnerable due to linearity.

A new sampling-reconstruction theory called compressive sensing [8] was later proposed, which can sample signals in the spatial domain and fulfill the compressive sampling simultaneously at a significantly lower rate than that of the Shannon-Nyquist sampling theorem. Subsequently, more CS-based image encryption schemes have been proposed. A digital image method [9] which can resist consecutive packet loss and malicious cropping attacks

by combining CS with bitwise XOR was investigated. Moreover, to achieve de-noising before encryption and compression, an image encryption technique was constructed by combining fractional Fourier transform with iterative kernel steering regression in double random phase encoding [10]. Lately, for resisting known and chosen plaintext attacks, Zhou et al. [11] proposed an image encryption scheme utilizing 2D-CS and fractional Mellin transform. Liu et al. [12] proposed an image compression, fusion and encryption method based on compressive sensing and chaos, which can ensure the efficiency and security of image transmission. Moqbool et al. [13] proposed an image compression and encryption scheme based on secure-JPEG encoding which can be used for lossless encryption and compression and lossy encryption and compression.

However, most previous image encryption techniques focus on methods for single images. In some cases, a multi-image or video sequence encryption and compression scheme is necessary. Consequently, multi-image encryption schemes have been widely studied. A double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform (DFrRT) was proposed [14], which strengthens the security in the spatial domain and the discrete fractional random transform domain by using a two-dimensional sine logistic modulation map. Alfalou et al. [15] proposed a method of simultaneous compression and encryption for color video images, with images compressed and encrypted into a single package, this highlights the benefits of DCT properties and digital print-based encryption to achieving image fusion and encryption simultaneously. Recently, to reduce the cost of data storage and collection time, Wei et al. [16] developed three-dimensional spare turntable microwave imaging based on compressive sensing, which proposed a fast sparse reconstruction algorithm called the 3D smoothed ℓ_0-norm (3D-SL0) algorithm.

To resist common attacks, and to shorten the transport and store burden, a new scheme combining 3D-CS with discrete fractional random transform is proposed in this paper. To reduce the cost of data acquisition, sparsification is applied to the video sequences before measuring. In the process of comprssion, three measurement matrices are used to measure the sparsed sequensces. After that, the resulting tensor image is re-encrypted by AT and 3D-FrRT, where three random circular matrices are constructed by sine logistic modulation mapping.

The remainder of this paper is organized as follows: In Section 2, basic fundamental knowledge is introduced. In Section 3, the proposed scheme is described in detail. In Section 4, numerical simulation results are given. Conclusions are stated in Section 5.

2. **Fundamental knowledge.**

2.1. **3D-CS.**

For a 3D signal $\mathcal{X}$ $(P\times Q\times K)$, the model of 3D-CS can be defined as:

$$\mathcal{S} = \mathcal{X} \times_1 \Phi_r \times_2 \Phi_c \times_3 \Phi_v \tag{1}$$

where $\mathcal{S} \in \mathcal{R}^{N\times M\times L}(N \leq P, M \leq Q, L \leq K)$ is an acquired tensor, $\times_n (n = 1, 2, 3)$ is the n-mode product of a tensor, Φ_r, Φ_c and Φ_v are sensing matrices. As for the reconstruction operation, which is critical of compressive sensing of recovering $\mathcal{X}$ from $\mathcal{S}$, it can be realized by solving the following sparsity-driven optimization problem:

$$\min_{\mathcal{S}} \|\mathcal{S}\|_0 \ s.t. \ \|\mathcal{S} - \mathcal{X} \times_1 \Phi_r \times_2 \Phi_c \times_3 \Phi_v\|_F \leq \epsilon \tag{2}$$

where $\|\cdot\|_F$ is the Frobenius norm of a tensor, and ϵ is a positive value bounded by the noise level.

2.2. **AT.** AT is proposed by Arnold in the research into ergodic theory, and it is commonly known as cat face transform [17]. The transform is a process of clipping and splicing that realign the pixel matrix of digital image. A matrix $I(x, y)$, sized $N \times N$, of AT can be expressed as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \tag{3}$$

where mod denotes the modulus after division, (x', y') denotes a new pixel position after AT. Here, x, y, x', $y' \in \{0, 1, 2, \ldots N-1\}$ is the pixel coordinate. It is clear that AT is actually a location moving of points, thus it can change the layout of gray values by changing the coordinates of pixels.

2.3. **DFrRT.** The DFrRT [18] can be defined as

$$\mathbf{R}^a = \mathrm{R}^a \mathrm{S} (\mathrm{R}^a)^T \tag{4}$$

where S is a target signal, a is the fractional order, R^a is the kernel transform and $(\mathrm{R}^a)^T$ denotes the transpose of R^a. The kernel transform is defined as

$$\mathrm{R}^a = \Lambda \mathrm{D}_R^a \Lambda^T \tag{5}$$

where $\Lambda\Lambda^T = 1$, and D_R^a is a diagonal matrix which can be defined as

$$\mathrm{D}_R^a = diag\{[1, \exp(-2\pi i \frac{1}{K}), \ldots, \exp(-2\pi i a \frac{N-1}{K}]\} \tag{6}$$

where K is the periodicity and matrix Λ is obtained by the eigenvector of a symmetric random matrix.

3. **The proposed scheme.** The proposed image sequence size with $M \times N \times Q$ compression and encryption scheme is illustrated in Figure 1, and corresponding process is as follows:

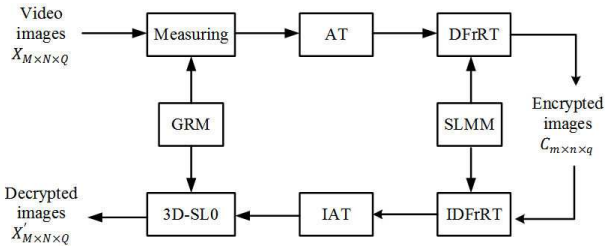

FIGURE 1. Schematic of the proposed images encryption and decryption scheme

Step 1. Sparsification. Sparsed representation of images can be realized by discrete wavelet transformation, where most transformed coefficients values are small, even zero, in the discrete wavelet domain.

Step 2. Measuring. The measurements matrices Φ_1, Φ_2 and Φ_3 can be constructed by Gaussion random matrix (GRM). Typically, the size of Φ_1, Φ_2 and Φ_3 are set as $m \times M$,$n \times N$,$q \times Q$ $(m \leq M, n \leq N, q \leq Q)$. Meanwhile acquired image tensor $\mathcal{Z}_{m\times n\times q}$ with the size of $m \times n \times q$ obtained by preforming following projection expression

$$\mathcal{Z} = \mathcal{X} \times_1 \Phi_1 \times_2 \Phi_2 \times_3 \Phi_3 \tag{7}$$

Step 3. $\mathcal{Z}'_{m\times n\times q}$ obtained by AT.

$$\mathcal{Z}'_{m\times n\times q} = AT(\mathcal{Z}_{m\times n\times q}) \tag{8}$$

Step 4. Obtain encryption image sequences $\mathcal{C}_{m\times n\times q}$ by performing 3D-DFrRT on the $\mathcal{Z}'_{m\times n\times q}$. Random matrix obtained as

$$\mathrm{P} = \frac{\eta \mathrm{Q}_1 + (1-\eta)\mathrm{Q}_2}{2} \tag{9}$$

where $0 < \eta < 1$, random circular matrices Q_1 and Q_2 can be constructed by following expression

$$\begin{aligned} \mathrm{Q}(i,1) &= \lambda \mathrm{Q}(i-1,N) \\ \mathrm{Q}(i,2:N) &= \mathrm{Q}(i-1,1:N-1) \end{aligned} \tag{10}$$

The first element of vector $\mathrm{Q}(i,1)$ is set as $\lambda \mathrm{Q}(i-1,N)$, where $2 \le i \le M$ and $\lambda > 1$. The initial row of vector Q, i.e., $\mathrm{Q}(1,:)$, is generated by sine logistic modulation map (SLMM) [19]

$$\begin{cases} x_{i+1} = \tau(\sin(\pi y_{i+1}) + \rho) x_i (1-x_i) \\ y_{i+1} = \tau(\sin(\pi x_{i+1}) + \rho) x_i (1-x_i) \end{cases} \tag{11}$$

where better chaotic performance generated when ρ close to 3. Encryption image sequences generated through following transform expression:

$$\mathcal{C}_{m\times n\times q} = \mathcal{G}_{m\times n\times q} \tag{12}$$

where $\mathrm{R}_1(m\times m)$, $\mathrm{R}_2(n\times n)$ and $\mathrm{R}_3(q\times q)$ are kernel matrices. Here, a different kernel matrix was used in tensor multiplication, where the kernel matrix can be constructed by using different initial values. It can be called 3D-DFrRT. For simplicity, we set $\mathrm{R}_1 = \mathrm{R}^a$, $\mathrm{R}_2 = (\mathrm{R}^a)^T$, $\mathrm{R}_3 = -\mathrm{R}^a$.

By executing the process which is depicted in Figure 1, decryption images can be obtained with correct keys (order of 3D-DFrRT and measurements of 3D-CS) in the inverse operation. Actually, Eq. (2) can be solved directly through 3D-SL0 which use a continuous function to approximate the ℓ_0-norm of a tensor and apply a fast gradient-based method to find a sparse solution. An expression is defined

$$F_\sigma(\mathcal{X}) = \sum_{m=1}^{M}\sum_{n=1}^{N}\sum_{k=1}^{K} \exp\left(-\frac{|\mathcal{X}_{m,n,k}|^2}{2\sigma^2}\right) \tag{13}$$

Obviously, if σ is sufficiently small, Eq. (14) can be renewed as

$$\max_{\mathcal{S}} F_\sigma(\mathcal{X}) \ s.t. \ \|\mathcal{S} - \mathcal{X} \times_1 \Phi_r \times_2 \Phi_c \times_3 \Phi_v\|_F \le \epsilon \tag{14}$$

For small values of σ, it is difficult to maximize F_σ because F_σ is highly unsmooth with a lot of local maxima. However, it becomes smoother with larger values of σ and contains less local maximum values. Consequently, a decreasing sequence of σ, initialized with a large value, was used in this algorithm.

The pseudo-code used for tensor-based encoding and decoding are presented in Algorithm 1 and Algorithm 2 which combined with 3D-SL0 algorithm [16].

Algorithm 1
Input: 3D image $\mathcal{X}_{M\times N\times Q}$ 1) Sparsification; 2) Sensing matrices Φ_1, Φ_2, Φ_3; 3) AT; 4) 3D-DFrRT: a) Initial $x(1)$, $y(1)$; b) Obtain vector x, y according to Eq. (11); c) Construct random matrix P according to Eq. (9) and Eq. (10); d) Obtain matrix D_R^a and R^a; e) Tensor product R_1, R_2, R_3. Output: $\mathcal{C}_{m\times n\times q}$

Algorithm 2

Input: $\mathcal{C}_{m\times n\times q}$;

1) 3D-IDFrRT:
   a) Initial $x(1)$, $y(1)$;
   b) Obtain vector x, y according to Eq. (11);
   c) Construct random matrix P according to Eq. (9) and Eq. (10);
   d) Obtain matrix D_R^a and R^{-a};
   e) Tensor product R_1', R_2', R_3'.
2) IAT;
3) 3D-SL0:

Initialization:

(1) $\hat{\mathcal{X}}_0 \leftarrow \mathcal{S} \times_1 \Phi_r^\dagger \times_2 \Phi_c^\dagger \times_3 \Phi_v^\dagger$, $A^\dagger$ is a pseudo-inverse of A;
(2) Decreasing sequence σ, i.e. $[\sigma_1 \dots \sigma_J]$;

For $j = 1, \dots, J$:

(a) Let $\sigma = \sigma_j$.
(b) Maximize (approximately) the function F_σ on the feasible set $\mathbb{X} = \{\mathcal{X} | \| \mathcal{S} - \mathcal{X} \times_1 \Phi_r \times_2 \Phi_c \times_3 \Phi_v \|_F \leq \epsilon\}$ using L iterations of the steepest ascent algorithm (followed by projection onto the feasible set):

– Initialization: $\mathcal{X} = \hat{\mathcal{X}}_{j-1}$;

– **For** $l = 1 \dots L$ (loop L times):

i. Calculate $\Delta\mathcal{X} \triangleq [\sigma_{m,n,k}]$,where $\sigma_{m,n,k} = \mathcal{X}_{m,n,k} \exp(-(|\mathcal{X}_{m,n,k}|^2/2\sigma^2))$;
ii. Let $\mathcal{X} \leftarrow \mathcal{X} - \mu\Delta\mathcal{X}$ (where μ is a small positive constant);
iii. Project $\mathcal{X}$ back onto the feasible set $\mathbb{X}$:

$$\mathcal{X} \leftarrow \mathcal{X} - (\mathcal{X} \times_1 \Phi_r \times_2 \Phi_c \times_3 \Phi_v - \mathcal{S}) \times_1 \Phi_r^\dagger \times_2 \Phi_c^\dagger \times_3 \Phi_v^\dagger$$

(c) Set $\hat{\mathcal{X}}_j = \hat{\mathcal{X}}$.

Final answer $\hat{\mathcal{X}} = \hat{\mathcal{X}}_J$.

Output: $\mathcal{X}'_{M\times N\times Q}$

4. **Experimental results and performance analyses.** In this section, simulations were performed by MATLAB 2014(b) on a 64-bit computer. Original video image resources "Anchorwoman" and "News", with size of $128 \times 128 \times 128$, and eight images, which were selected randomly, are shown in Figure 2(a). Discrete symelt8 wavelet was applied to the sparse transform process. Parameters involved in the process were taken as: $\lambda_1 = 3$, $\lambda_2 = 4$ in Eq. (10), $\alpha = 0.35$, $K = 4$ in Eq. (6), $\eta = 0.345$ in Eq. (9) and $\tau = 1$, $\rho = 3$, $x_0 = 0.3456$, $y_0 = 0.8765$ in Eq. (11) in 3D-DFrRT. Encrypted and decrypted results are showed in Figure 2(b) and Figure 2(c).

4.1. **Performance of reconstruction.** One of the most prominent advantages of our scheme is that compression and encryption of video sequences could be realized simultaneously. In Figure 3 and Table 1, compression performance (e.g. relations between the compression ratio (CR) and the peak signal-to-noise ratio (PSNR)) among different compression and encryption method have been compared, i.e. Zhous method [11], Lius method [12] and our method. It indicate that our scheme exhibits a relatively superior reconstruction performance. Our scheme has relatively much higher PSNR than Zhous scheme and Lius scheme with the same CR. It should be pointed out that Alfalous method [15] has relatively good performance, but we cannot ignore that its CR cannot be changed for video sequenes, compared to our scheme where the CR can be setted according to autors need. In Alfalous scheme, if 128 images are inputted, then the CR is 1/128 and the PSNR is 14.35 dB, which is not acceptable for a video. Experimental results indicate that the reconstruction quality of our method remains acceptable to some degree with different ratios, i.e. the compression ability of the proposed scheme is great enough and useful for transmission and storage.

4.2. **Time complexity.** It is necessary to analyze the time complexity of an encryption scheme. "Lena" and "Pepper", with different size of 128×128, 256×256 and 512×512, were used to test the time complexity. The proposed scheme for two images with size of 128×128 is 0.191240 s. Table 2 lists several image encryption schemes for different sizes of images. Actually, the encryption time of the proposed scheme for the video sequence "Anchorwoma" with size of $128 \times 128 \times 128$ is 1.932093s. It is a relatively fast video image compression and encryption scheme. Therefore, the proposed scheme requires small storage space and has a higher encryption speed.

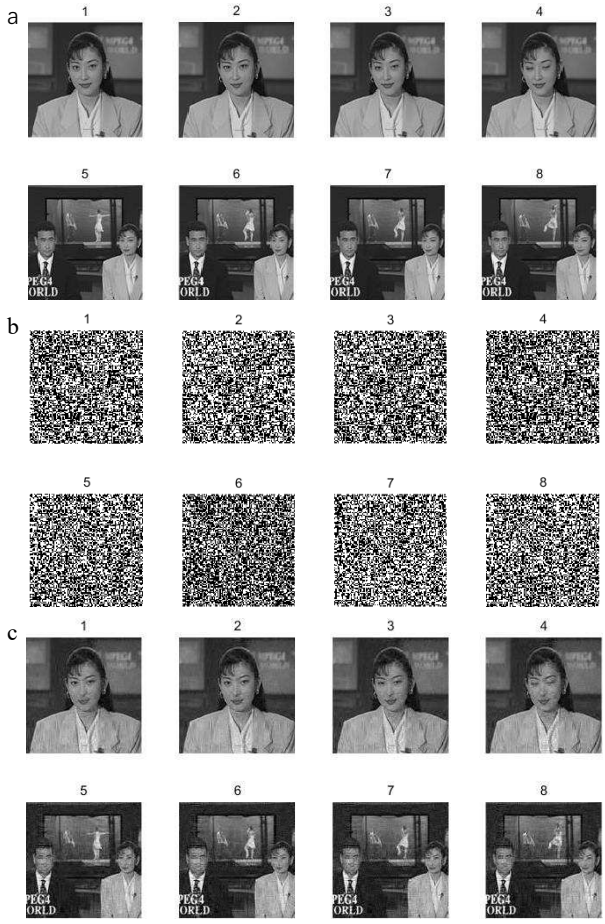

FIGURE 2. a : Images of "Anchorwoman" and "News", b : Encrypted "Anchorwoman" and "News", c : Decrypted "Anchorwoman" and "News"

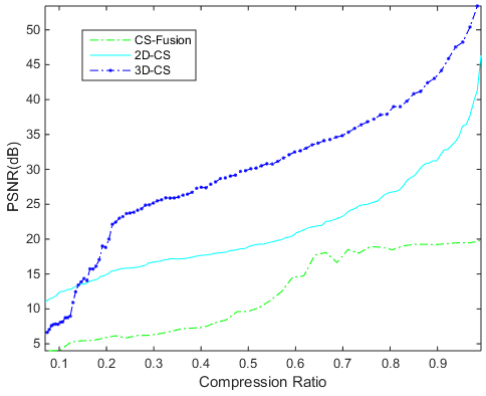

FIGURE 3. Reconstruction performance of video sequence

TABLE 1. Reconstruction quality at different compression ratios

CR(%)	CS-Fusion PSNR(dB)	2D-CS PSNR(dB)	3D-CS PSNR(dB)
10.77	4.07	12.49	8.15
24.22	5.84	15.82	23.67
35.25	6.77	17.17	26.05
53.93	11.23	19.27	30.81
72.53	18.01	24.41	35.88
90.84	19.36	32.79	44.16

TABLE 2. Encryption time (second) of the scheme for different sizes of images

Image size	$2 \times 128 \times 128$	$2 \times 256 \times 256$	$2 \times 512 \times 512$
Liu's scheme [20]	0.517253	1.378824	8.283544
Liao's scheme [21]	0.416732	1.035171	4.143523
Zhou's scheme [14]	0.247012	0.552962	1.890441
Maqbool's scheme[13]	0.689931	1.130806	4.302622
The proposed scheme	0.191240	0.310630	0.410849

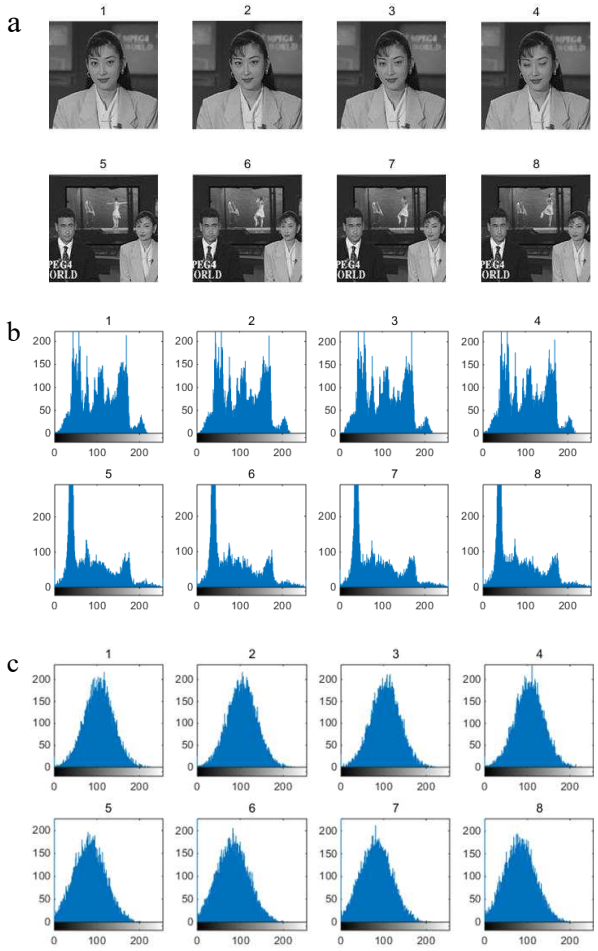

FIGURE 4. a : Original images, b : Original histograms, c : Ciptertext histograms

4.3. **Histograms.** A good encryption scheme usually has the ability to transform an original image with high correlations among neighborhood pixels into a random-like one, i.e. the histograms of the encrypted images are fairly uniform in distribution or similar. According to Figure 4, the sum histograms of the original images are different from each other, while the histograms of the ciphertext images are similar, and illegal users cannot obtain any valid information from this statistical property.

4.4. **Correlation coefficient.** Usually, the correlation coefficient value of two adjacent pixels with distribution in the horizontal, vertical, and diagonal directions of the original image is close to 1, whereas it is close to 0 in an encrypted image encrypted by a good encryption scheme. In this study, 14,400 adjacent pixel pairs in the horizontal directions were selected randomly from both original images and encrypted images. As shown in Figure 5, there was a strong correlation between two adjacent pixels which distributed

regularly in the original images, whereas encrypted images had a weak correlation and were distributed dispersedly. Table 3 shows the horizontal correlations in plaintext and ciphertext. Results demonstrated that the proposed scheme can resist statistical analysis since attacks cannot get the useful information easily.

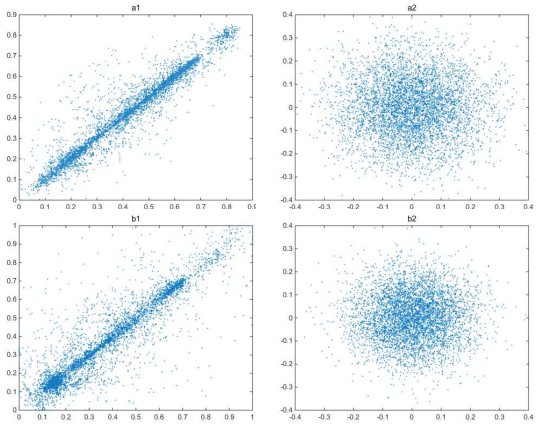

FIGURE 5. Correlation distribution of two horizontally adjacent pixels in: (a1) Original "Anchorwoman"; (a2) Encrypted "Anchorwoman"; (b1) Original "News"; (b2) Encrypted "News"

TABLE 3. Correlation coefficients of adjacent pixels of six images within the sequence

Images	Horizontal	Vertical	Diagonal	Images	Horizontal	Vertical	Diagonal
"1"	0.9564	0.9475	0.9481	"4"	0.9567	0.9479	0.9485
Encrypted "1"	-0.0937	-0.1395	-0.1374	Encrypted 4""	-0.0938	-0.1405	-0.1385
"2"	0.9565	0.9476	0.9482	"5"	0.9567	0.9477	0.9483
Encrypted "2"	-0.0939	-0.1404	-0.1383	Encrypted "5"	-0.0938	-0.1403	-0.1382
"3"	0.9567	0.9473	0.9479	"6"	0.9566	0.9477	0.9483
Encrypted "3"	-0.0931	-0.1393	-0.1371	Encrypted "6"	-0.0910	-0.1318	-0.1297

4.5. **Sensitivity of the keys.** Apparently, the security of the proposed encryption scheme is mainly determined by the initial values of the 3D-DFrRT, i.e. α, x_0, y_0, x_1, y_1, x_2 and y_2. As is illustrated in Figure 6, using incorrect keys of $\alpha' = -0.37$, $K' = 4.3$, $x_0' = 0.3456 + 10^{-16}$, $y_0' = 0.8765 + 10^{-15}$ ($x_0 = x_1 = x_2, y_0 = y_1 = y_2$), any information from the decrypted images cannot be obtained visually when small deviation is added to the initial value.

4.6. **Key space analysis.** According to an ideal cryptosystem, the size of key space should be large enough to make the brute-force attack infeasible, namely the total number of different keys used in the encryption and decryption process should be large. In the encryption process, the key spaces of the initial values α, x_0, y_0, x_1, y_1, x_2 and y_2 were denoted by s_1, s_2, s_3, s_4, s_5, s_6 and s_7, respectively. The simulation results in Figure 6 show that the entire key space of the cryptosystems was $s_1 \times s_2 \times s_3 \times s_4 \times s_5 \times s_6 \times s_7 = 10^{96}$. It indicates that the key space is sufficiently to frustrate brute-force attacks.

4.7. **Noise attack analysis.** When considering the robustness against noise, a Gaussian random noise was added to the ciphertext of "Anchorwoman" as

$$\mathrm{C}' = \mathrm{C} + k\mathrm{G} \tag{15}$$

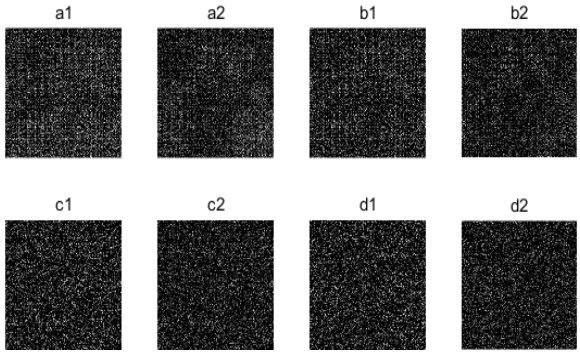

FIGURE 6. Decrypted image with incorrect keys: $(\mathrm{a1}, \mathrm{a2})\alpha' = -0.37$, $(\mathrm{b1}, \mathrm{b2})K' = 4.3$, $(\mathrm{c1}, \mathrm{c2})x_0' = 0.3456 + 10^{-16}$, $(\mathrm{d1}, \mathrm{d2})y_0' = 0.8765 + 10^{-15}$

where, C′ and C are the noise-affected ciphertext images and original images, respectively. k is the noise intensity and G is a Gaussian random noise with zero-mean and identity standard deviation. Figure 7 shows the decrypted images of "Anchorwoman" when k is set to 1, 3, 5, 7, 9 and 11. Similar results can be obtained for image "News". As Figure 7 shows, the content of the decrtypted images can be recognized despite noise interference and the proposed encryption scheme has high robustness against noise attack.

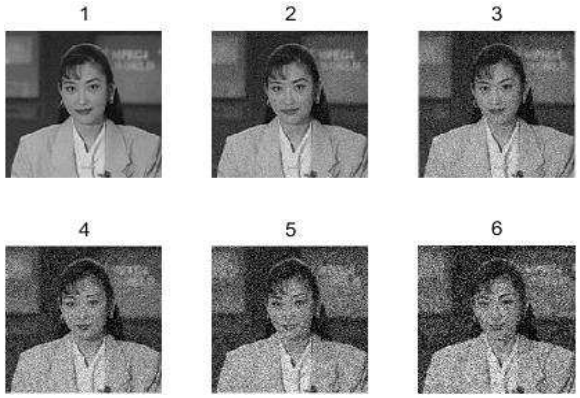

FIGURE 7. Decrypted images with coefficient K, (K=1, 3, 5, 7, 9, 11, respectively)

5. **Conclusion.** An image compression-encryption scheme based on 3D-CS and 3D-DFrRT was proposed in this paper. Sparsification using discrete wavelet was adapted before video sequences were compressed and encrypted. Three measurement matrices were constructed by GRM and the random circular matrices were controlled by SLMM. The advantage of compressive sensing theory was fully realized to cut down the size of the original video images in the compression process. The resulting tensor image was re-encrypted by AT and the 3D-FrRT which was controlled by three different kernel matrices. The decryption process was the inverse operation related to the encryption process, and a 3D-SL0 algorithm was adapted in the reconstruction operation. Image pixels were changed greatly through AT, which strengthened the security of the scheme. Simulation results indicated that the proposed video images compression and encryption method was effective. It not only has good compression performance, but also is able to stand against statistical attack and noise attack. In summary, in certain cases, this technique is a good compression and encryption method for video sequences.

Acknowledgment. This work was supported by National Natural Science Foundation of China (61301257). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier planerandom encoding, *Optics Letters*, vol.20, no.7, pp.767–769, 1995.
[2] W. Chen, X. Chen, Optical multiple-image authentication based on modified GerchbergSaxton algorithm with random sampling, *Optics Communications*, vol.318, no.5, pp.128132, 2014.
[3] D. Lu, W. He, Enhancement of optical image encryption based on radial shearing interference, *Optics Communications* , vol.336, no.10, pp.7783, 2015.
[4] B. Hennelly, J. Sheridan, Optical image encryption by random shifting in fractional Fourier domains, *Optics Letters* , vol.28, no.4, pp.267–271, 2003.
[5] N. Singh, A. Sinha, Gyrator transform-based optical image encryption, using chaos, *Optics & Lasers in Engineering*, vol.47, no.5, pp.539–546, 2009.
[6] G. Situ, J. Zhang, Double random-phase encoding in the Fresnel domain, *Optics Letters*, vol.29, no.14, pp.1584–6, 2004.
[7] Z. Liu, H. Zhao, S. Liu, A discrete fractional random transform, *Optics Communications*, vol.255, no.4, pp.357–365, 2006.
[8] D. Donoho, Compressed Sensing, *IEEE Transactions on Information Theory*, vol.52, no.4, pp.1289–1306, 2006.
[9] R. Huang, K. Sakurai, A Robust and Compression-Combined Digital Image Encryption Method Based on Compressive Sensing, *International Conference on Intelligent Information Hiding & Multimedia Signal Processing. IEEE Computer Society* , pp.105–108, 2011.
[10] N. Rawat, R. Kumar, B. Lee, Implementing compressive fractional Fourier transformation with iterative kernel steering regression in double random phase encoding, *Optik - International Journal for Light and Electron Optics*, vol.125, no.18, pp.5414–5417, 2014.
[11] N. Zhou, H. Li, D. Wang, et al, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, *Optics Communications*, vol.343, pp.10–21, 2015.
[12] X. Liu, W. Mei, H. Du, Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos, *Optics Communications*, vol.366, pp.22–32, 2016.
[13] S. Maqbool, N. Ahamad, A. Muhammad, et al, Simultaneous Encryption and Compression of Digital Images Based on Secure-JPEG Encoding, *Pattern Recognition*, Springer International Publishing, 2016.
[14] N. Zhou, J. Yang, C. Tan, et al, Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform[J]. Optics Communications, *Optics Communications*, vol.354, pp.112–121, 2015.
[15] A. Alfalou, C. Brosseau, N. Abdallah, Simultaneous compression and encryption of color video images, *Optics Communications*, vol.338, pp.371–379, 2015.
[16] W. Qiu, J. Zhou, H. Zhao, et al, Three-Dimensional Sparse Turntable Microwave Imaging Based on Compressive Sensing, *IEEE Geoscience & Remote Sensing Letters*, vol.12, no.4, pp.826–830, 2015.
[17] V. Arnold, A. Avez, Ergodic problems of classical mechanics, *Benjamin*, 1968.
[18] J. Guo, Z. Liu, S. Liu, Watermarking based on discrete fractional random transform, *Optics Communications*, vol.272, no.2, pp.344–348, 2007.
[19] Z. Hua, Y. Zhou, C. Pun, et al, 2D Sine Logistic modulation map for image encryption, *Information Sciences*, vol.297, pp.8094, 2014.
[20] Z. Liu, M. Gong, Y. Dou, et al, Double image encryption by using Arnold transform and discrete fractional angular transform, *Optics & Lasers in Engineering*, vol.50, no.2, pp.248–255, 2012.
[21] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, *Signal Processing*, vol.90, no.9, pp.2714–2722, 2010.