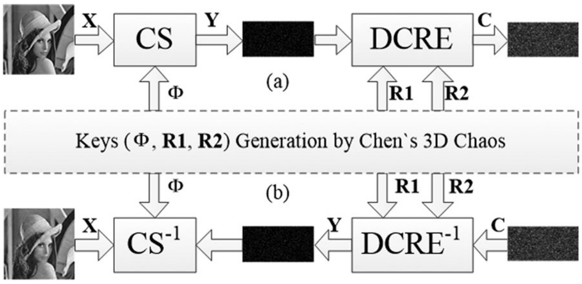
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Image Encryption Using Compressive Sensing and Detour Cylindrical Diffraction

Volume 10, Number 3, JUNE 2018

Jun Wang
Qiong-Hua Wang
Yuhen Hu, *Fellow, IEEE*



DOI: 10.1109/JPHOT.2018.2831252
1943-0655 © 2018 CCBY

IEEE photonics SOCIETY
IEEE

Image Encryption Using Compressive Sensing and Detour Cylindrical Diffraction

Jun Wang,[1] **Qiong-Hua Wang**,[1] **and Yuhen Hu,**[2] ***Fellow, IEEE***

[1]School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China
[2]Department of Electrical and Computer Engineering, University of Wisconsin - Madison, Madison, WI 53706 USA

DOI:10.1109/JPHOT.2018.2831252

Manuscript received March 22, 2018; revised April 21, 2018; accepted April 25, 2018. Date of publication April 30, 2018; date of current version May 15, 2018. This work was supported by in part by the National Key R&D Program of China under Grant 2017YFB1002900 and in part by the National Science Foundation of China under Grant 61320106015. Corresponding author: Qiong-Hua Wang (e-mail: qhwang@scu.edu.cn).

Abstract: An image compression and encryption method integrating compressive sensing (CS) and Detour Cylindrical-diffraction-based double Random-phase Encoding (DCRE) is proposed. The plaintext image is first compressed by CS and then encrypted by the DCRE algorithm. The existing integrated CS and double random phase encoding (DRPE) methods are known to be vulnerable to the plaintext attack and even ciphertext-only attack. The combination of CS and DCRE, however, will be free of the plaintext attack and ciphertext-only attack, free of phase retrieval attack and allows enlarged key space. Numerical simulation results demonstrate the effectiveness and flexibility of the proposed scheme.

Index Terms: Optical encryption, compressive sensing, cylindrical diffraction.

1. Introduction

To enhance information security, optical information processing methods have been developed to facilitate data securing, encryption, and authentication [1]–[5]. Among them, double random phase encoding (DRPE) proposed by Javidi, *et al.* [6] has become a widely adopted optical encryption technique. Unfortunately, current DRPE encryption approach is vulnerable to the chosen-plaintext attack and known-plaintext attack [7]–[9]. To mitigate these vulnerabilities, enhancements to DRPE have been proposed. For example, DRPE has been extended to the Fresnel transform [10], the fractional Fourier transform [11], and gyrator transform [12] domains. Other strategies, such as mixed phase-amplitude encoding [13], pixel randomization processing [14], phase truncation Fourier transform [15], [16], random sampling [17], phase truncation operations [18], and divergent illumination [19] have also been proposed for DRPE-based optical security systems. DRPE may also be enhanced by combining with the other imaging techniques such as coherent diffraction imaging [20], iterative computational algorithms [21]–[23], and photon-counting imaging [24], [25]. Previously, we proposed to incorporate asymmetric cylindrical diffraction and interference imaging [26] in order to ensure the DPRE based cryptosystem will resist phase retrieval attack.

Compressive sensing (CS) has received great attentions recently [27]–[29]. By exploiting the inherent sparsity (redundancy) in signals, the CS theory provides an optimization approach to reconstruct the original signal using a small subset of random measurements. Candes *et al.* [30] suggested that the measurement vectors obtained using random linear projection in CS can be regarded as the ciphertext with the measurement matrix playing the role of the secret key. Capitalizing this idea, Riverson *et al.* [31] combined CS and DRPE to restore images degraded by both diffraction and geometrical limited resolution. It has been proposed to first compressively sample the plaintext and then adopt DRPE to further encrypt the measurements [32]–[35]. These lead to the development of DRPE-then-CS cryptosystem [36], [37] and several cryptanalysis works [38]–[40]. Unfortunately, it is reported that some of these DRPE and CS based cryptosystems are vulnerable to the plaintext attack and the ciphertext-only attack [40]. By vector-matrix analysis on the equivalent of ciphertext of CS-then-DRPE or DRPE-then-CS, it is revealed that the combinations can be normalized as a single CS projection process whose equivalent measurement (key) matrix can be recovered by plaintext attack. It is also proved that the equivalent measurement matrix satisfies the restricted isometry property (RIP) [28], which make it possible to recover the plaintext with only a single-step ℓ_1 optimization.

To address this issue, we proposed a novel image compression and encryption scheme using the CS and Detour Cylindrical-diffraction based double Random-phase Encoding (DCRE). To the best of our knowledge, this approach has not been reported so far. Though the CS-DCRE also can be normalized as a single CS projection process, it is impossible to recover the plaintext with only a single-step ℓ_1 optimization since the equivalent measurement matrix of our scheme doesn't satisfy the RIP due to the asymmetric cylindrical diffraction of DCRE. Therefore, our scheme can resist the ciphertext-only attack even the plaintext attack. This is the main contribution of this paper compared with other DRPE and CS based cryptosystems. In this CS-DCRE system, the plaintext image is linearly projected onto measurement vectors. These measurements are then encrypted using DCRE which contains a two-step detour cylindrical diffraction process with double pseudo random phase masks (RPM) placed on both the object surface and the first diffraction surface. There are three random matrices, including the measurement matrix of CS and the two RPMs, which may be generated using a 3D chaos algorithm [41]. Their initial keys could be decided by the checksum of plaintext, which ensures the proposed scheme is sensitive to the plaintext and free of plaintext attack. The security of the proposed scheme is also improved in key space due to the use of two additional keys compared with the conventional CS-DRPE based methods [32] and DCRE [26]. Furthermore, CS-DCRE is free of phase-retrieval attack due to the cylindrical asymmetric diffraction [26]. Numerical simulation results demonstrate the effectiveness and flexibility of the proposed cryptosystem.

2. Reviews

2.1 Notations

In this paper, a lowercase and bold letter is reserved for a vector, a capital and bold letter for a matrix, respectively. A lowercase letter represents the entries of a vector or a matrix, or a variable, whereas a capital letter always denotes a constant. We adopt the 'vec' command as the vectorization operation that reshapes a matrix to a vector by stacking its columns. That is, $\mathbf{X} = [\mathbf{x}^1; \mathbf{x}^2; \ldots; \mathbf{x}^N] = \{\mathbf{x}_{i,j}\}^{M,N} = \{\mathbf{x}_{1,1}, \ldots, \mathbf{x}_{M,1}; \mathbf{x}_{1,2}, \ldots, \mathbf{x}_{M,2}; \ldots; \mathbf{x}_{1,N}, \ldots\ldots, \mathbf{x}_{M,N}\}$ represents the 2D primary image and $\mathbf{x} = \mathrm{vec}(\mathbf{X}) = [\mathbf{x}_{1,1}, \ldots, \mathbf{x}_{M,1}; \mathbf{x}_{2,1}, \ldots\ldots, \mathbf{x}_{M,N}]^T$ illustrates its vectorized version.

Besides, the superscript T is denoted as the transpose of a matrix, superscript * as its conjugate, and the superscript H as the conjugate transpose, i.e., $\mathbf{X}^H = \mathbf{X}^{*T}$. The subscript always demonstrates the dimension of the Fourier matrix, or the coordinate of a matrix entry. We use • and ⊗as the Hadamard and Kronecker products of two matrices, respectively.

2.2 Theory of Compressive Sensing

The CS is originally developed as a revolutionary data acquisition technique that exploits the sparsity or compressibility. For a 1D discrete signal $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N)^T$, $\mathbf{x}$ is said to be K-sparse if $\mathbf{x}$ can be well approximated using only K coefficients under some linear transform $\mathbf{x} = \Psi\mathbf{s}$, where Ψ is the

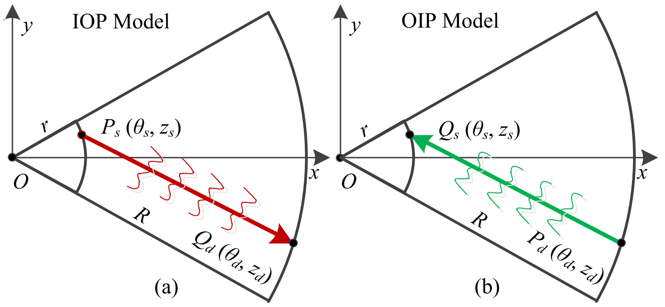


Fig. 1. Illustration of cylindrical diffraction in top-view. (a) IOP Model, (b) OIP Model.

sparsifying basis and **s** is the transform coefficient vector with at most K $<<$ N (significant) nonzero entries. The CS measures signal via the following linear projection,

$$\mathbf{y} = \Phi\mathbf{x} = \Phi\Psi\mathbf{x} = \Theta\mathbf{s}, \tag{1}$$

where **y** is the measurement vector with $K << N$ entries, Φ represents the $M \times N$ measurement matrix, and Θ is the sensing matrix. For 2D or high-dimensional signals, they can be vectorized to 1D format by stacking their columns. The CS theory implies that **x** can be faithfully recovered with overwhelming probability from only $M = O(K \log N)$ measurements, in the case that Θ satisfies the restricted isometry property (RIP) [28]. In such scenarios, the reconstruction of **x** can be preceded by solving the following ℓ_1-norm minimization problem:

$$\min \|\mathbf{s}\|_1 \quad \text{s.t.} \quad \mathbf{y} = \Theta\mathbf{s}. \tag{2}$$

Popular matrices families that satisfy RIP in k order including Gaussian and Bernoulli ensembles with $K = \mathrm{O}(k \log M)$ rows, which are well known as it is universally incoherent with popular orthonormal sparsifying bases. For example, if Φ is a random matrix of Gaussian entries and Ψ is an arbitrary orthonormal sparsifying basis, the resultant sensing matrix in the transform domain $\Theta = \Phi\Psi$ is also a Gaussian matrix, and hence satisfy RIP requirements [42].

2.3 Cylindrical Diffraction Theory

In the cylindrical diffraction theory [43]–[45], the object and the observation surfaces are concentric cylindrical surfaces as shown in Fig. 1, where R and r denote the radii of the inner and outer surfaces, respectively. Obviously, there are two, inside-out and outside-in, propagation models in the cases that objects are placed on the inside and outside surfaces as shown in Fig. 1(a) and (b), respectively.

In both cases of inside-out propagation (IOP) and outside-in propagation (OIP) models, the object and observation points can be represented by $P_s(\theta_s, z_s)$ and $Q_d(\theta_d, z_d)$ in cylindrical coordinate, respectively. Here, (θ_s, z_s) and (θ_d, z_d) are the coordinates of azimuthal and vertical directions, respectively. And z_s and z_d are in range of $-H/2$ to $H/2$, where H is the height of the cylindrical surface. In our previous researches [45], we have proposed a unified and accurate diffraction calculation for IOP and OIP models of two concentric cylindrical surfaces. If the distributions on the source and destination surfaces are represented by $u_s(\theta_s, z_s)$ and $u_d(\theta_d, z_d)$, respectively, the destination distributions can be calculated by

$$u_d(\theta_d, z_d) = C \iint_c u_s(\theta_s, z_s) \cos\alpha \times e^{jkL} \times L^{-1} d\theta_s dz_s,$$
$$\cos\alpha = [R_d - R_s \cos(\theta_d - \theta_s)] \times L^{-1}, L = \left[R_d^2 + R_s^2 - 2R_d R_s \cos(\theta_d - \theta_s)) + (z_d - z_s)^2\right]^{1/2}, \tag{3}$$

where k and c denote the wavenumber of the incident light and the cylindrical source surface, respectively, C and L denote a constant and the propagation distance, respectively, and cos α denotes the obliquity factor. The fast calculation algorithm also has been proposed as

$$\begin{aligned} u_d &= u_s * h = \mathcal{F}^{-1}[\mathcal{F}(u_s) \times \mathcal{F}(h)], \\ h &= C \times e^{ikL} \times [R_d - R_s \cos\theta] \times L^{-2}, \end{aligned} \tag{4}$$

where $\mathcal{F}$ and $\mathcal{F}^{-1}$ denote the forward and inverse Fourier transforms, respectively, h and $*$ denote the unified kernel function and the convolution integral, respectively, and the two propagation models of IOP and OIP are specified as

$$\begin{aligned} h_I &= C \times e^{ikL} \times [R - r\cos\theta] \times L^{-2} \cdots\cdots \text{IOP}, \\ h_O &= C \times e^{ikL} \times [r - R\cos\theta] \times L^{-2} \cdots\cdots \text{OIP}. \end{aligned} \tag{5}$$

3. Principle

3.1 Cylindrical Diffraction in Vector-Matrix Form

In this paper, we try to present a new view point of the cylindrical diffraction calculation in vector-matrix form for security analysis. The $\mathbf{F}_N$ is defined as the Fourier matrix which can convert the DFT of a length$-N$ signal through matrix multiplication, i.e., DFT($\mathbf{x}$) $= \mathbf{F}_N\mathbf{x}$. The formula of $\mathbf{F}_N$ is described in (6), where $w = e^{-2\pi i/N}$ is a primitive Nth root of unity [46].

$$\mathbf{F}_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & \cdots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \cdots & w^{(N-1)(N-1)} \end{bmatrix}. \tag{6}$$

Both of the Fourier matrix $\mathbf{F}_N$ and its conjugate transpose F_N^H are symmetric and unitary, i.e., (7) always holds [46].

$$\mathbf{F}_N = \mathbf{F}_N^T, \mathbf{F}_N^{-1} = \mathbf{F}_N^H = \mathbf{F}_N^{HT}. \tag{7}$$

With the definition of Fourier matrix, the 2D $M \times N$ DFT and IDFT can be respectively described as [46],

$$\mathcal{F}(\mathbf{P}_{M\times N}) = \mathbf{F}_M \mathbf{P}_{M\times N} \mathbf{F}_N, \mathcal{F}^{-1}(\mathbf{P}_{M\times N}) = \mathbf{F}_M^H \mathbf{P}_{M\times N} \mathbf{F}_N^H. \tag{8}$$

If $\mathbf{U_s}$ and $\mathbf{U_d}$ denote the input and output matrix, respectively, the cylindrical diffraction calculation can be rewritten as

$$\begin{aligned} \mathbf{U_d} &= \text{Cydi}_\text{I}(\mathbf{U_s}) = \mathcal{F}^{-1}(\mathcal{F}(\mathbf{H_I}) \,.\, \mathcal{F}(\mathbf{U_s})) = \mathbf{F}_M^H((\mathbf{F}_M \mathbf{H_I} \mathbf{F}_N) \,.\, (\mathbf{F}_M \mathbf{U_s} \mathbf{F}_N))\mathbf{F}_N^H \cdots\cdots \text{IO}P, \\ \mathbf{U_d} &= \text{Cydi}_\text{O}(\mathbf{U_s}) = \mathcal{F}^{-1}(\mathcal{F}(\mathbf{H_O}) \,.\, \mathcal{F}(\mathbf{U_s})) = \mathbf{F}_M^H((\mathbf{F}_M \mathbf{H_O} \mathbf{F}_N) \,.\, (\mathbf{F}_M \mathbf{U_s} \mathbf{F}_N))\mathbf{F}_N^H \cdots\cdots \text{OIP}, \end{aligned} \tag{9}$$

where Cydi$_\text{I}$ and Cydi$_\text{O}$ denote the cylindrical diffractions of IOP and OIP models, respectively. And $\mathbf{H_I}$ and $\mathbf{H_O}$ denote their kernel function matrices, respectively.

3.2 DCRE in Vector-Matrix Form

To apply the cylindrical diffraction theory to encrypt an image, DRPE scheme is a common approach. However, directly twice diffractions are impracticable because of sampling issue of too big difference of sampling pitches. To conquer this issue, an algorithm of DCRE was proposed as shown in Fig. 2 [26].

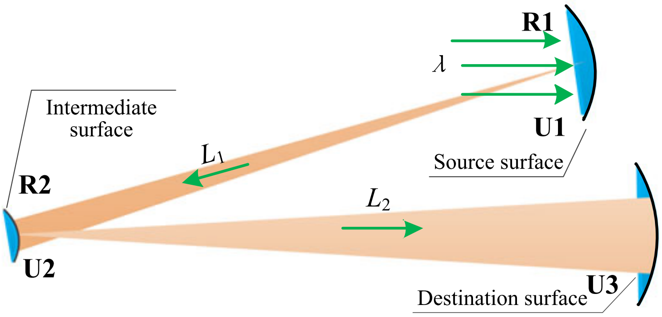


Fig. 2. Principle of DCRE.

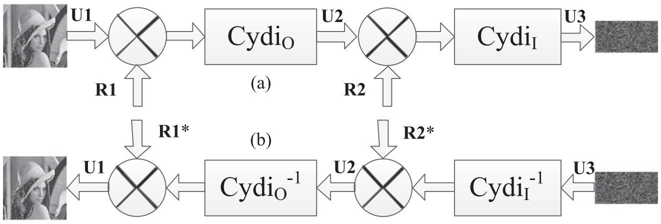


Fig. 3. Block diagrams of DCRE: (a) encryption, (b) decryption.

The random phase masks (**R1** and **R2**) are cylindrical surfaces which have radii of R_1, and r, respectively. The input object, which is bonded to the first random phase mask at the source surface, is also cylindrical surface with radius of R_1. The object wave, **U1**, modulates by the **R1** and propagates to the intermediate surface, on which the distributions is **U2**. After reflection and modulation by **R2**, the wave field continuously propagates to the destination surface, on which the distributions is **U3**. The block diagram of DCRE is shown in Fig. 3. The ciphertext can be written in matrix form as

$$\begin{aligned}\mathbf{U2} &= \text{Cydi}_\text{O}\left(\mathbf{U1}\,.\,\mathbf{R1}\right) = \mathcal{F}^{-1}\left(\mathbf{H}_\mathbf{F}^\mathbf{O}\,.\,\mathcal{F}\left(\mathbf{U1}\,.\,\mathbf{R1}\right)\right),\\ \mathbf{U3} &= \text{Cydi}_\text{I}\left(\mathbf{U2}^*\,.\,\mathbf{R2}\right) = \mathcal{F}^{-1}\left(\mathbf{H}_\mathbf{F}^\mathbf{I}\,.\,\mathcal{F}\left(\mathbf{U2}^*\,.\,\mathbf{R2}\right)\right)\\ &= \mathcal{F}^{-1}\left(\mathbf{H}_\mathbf{F}^\mathbf{I}\,.\,\mathcal{F}\left(\left(\mathcal{F}^{-1}\left(\mathbf{H}_\mathbf{F}^\mathbf{O}\,.\,\mathcal{F}\left(\mathbf{U1}\,.\,\mathbf{R1}\right)\right)\right)^*\,.\,\mathbf{R2}\right)\right),\end{aligned} \tag{10}$$

where $\mathbf{H}_\mathbf{F}^\mathbf{I}$ and $\mathbf{H}_\mathbf{F}^\mathbf{O}$ denote the Fourier transform of the kernel function matrices of IOP and OIP models, respectively. Here, $\mathbf{H}_\mathbf{F}^\mathbf{I} = \mathbf{F}_M\mathbf{H}_\mathbf{I}\mathbf{F}_N$ and $\mathbf{H}_\mathbf{F}^\mathbf{O} = \mathbf{F}_M\mathbf{H}_\mathbf{O}\mathbf{F}_N$, and * denotes conjugate of matrix. It is worthy to denote that DRPE is an example of DCRE scheme; three even more random phase encoding is theoretically feasible.

3.3 DCRE Combining With CS

The cryptosystem integrating CS with DCRE can achieve compression and encryption simultaneously. The flowchart of encryption and decryption with can be depicted in Fig. 4.

In encryption, the plaintext or object image **X** is firstly compressively sampled and subsequently encrypted using DCRE, as illustrated in Fig. 4(a). The encryption process can be summed as

$$\begin{aligned}\mathbf{y} &= \text{vec}(\mathbf{Y}) = \Phi\text{vec}(\mathbf{X}) = \Phi\mathbf{x},\\ \mathbf{C} &= \text{Cydi}_\text{I}\left(\left(\text{Cydi}_\text{O}\left(\mathbf{Y}\,.\,\mathbf{R1}\right)\right)^*\,.\,\mathbf{R2}\right).\end{aligned} \tag{11}$$

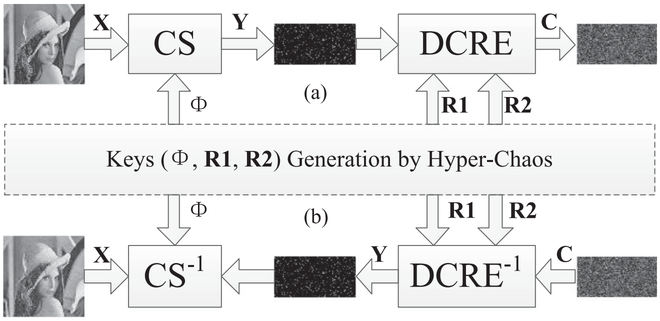


Fig. 4. Proposed Scheme: (a) encryption and (b) decryption processes.

For ciphering with CS-DCRE architecture, random phase masks **R1** and **R2** of DCRE, the measurement matrix Φ of CS jointly consist of the secret key of the concatenated cryptosystem. The keys can be generated by Chen's 3D chaos algorithm [41].

Decryption is the inverse of encryption and should be traded as a two-step separate operation. The ciphertext should be firstly decrypted by the DCRE decoder and then reconstructed by ℓ_1 optimization, i.e.,

$$\mathbf{Y} = \mathrm{Cydi}_{\mathrm{O}}^{-1}\left(\mathrm{Cydi}_{\mathrm{I}}^{-1}(\mathbf{C})\,.\,\mathbf{R2}^{*}\right)^{*}.\,\mathbf{R1}^{*},$$
$$\min\|\mathbf{s}\|_1 \quad \text{s.t.} \quad \mathbf{y} = \mathrm{vec}(\mathbf{Y}) = \Theta\mathbf{s}, \tag{12}$$

where $\mathrm{Cydi}_{\mathrm{I}}^{-1}$ and $\mathrm{Cydi}_{\mathrm{O}}^{-1}$ denote the inverse processes of IOP and OIP models, respectively.

3.4 Equivalent of the Ciphertext

We try to present the ciphertext in an equivalent matrix form. We have the matrix form of ciphertext as,

$$\mathbf{y} = \mathrm{vec}(\mathbf{Y}) = \Phi\mathrm{vec}(\mathbf{X}),$$
$$\mathbf{Y1} = \mathbf{F}_M^H\left(\mathbf{H}_{\mathbf{F}}^{\mathbf{O}}\,.\,(\mathbf{F}_M\,(\mathbf{Y}\,.\,\mathbf{R1})\,\mathbf{F}_N)\right)\mathbf{F}_N^H,$$
$$\mathbf{C} = \mathbf{F}_M^H\left(\mathbf{H}_{\mathbf{F}}^{\mathbf{I}}\,.\,(\mathbf{F}_M\,((\mathbf{Y1})^{*}\,.\,\mathbf{R2})\,\mathbf{F}_N)\right)\mathbf{F}_N^H. \tag{13}$$

Firstly, let us consider the equivalent form of the proposed DCRE. Let **P** and **R** be 2D $M \times N$ matrix, it is found that (14) always holds, where diag(vec(**R**)) is the $MN \times MN$ diagonal matrix with entries are vec(**R**) from the upper-left to the lower-bottom corner.

$$\mathrm{vec}(\mathbf{R}\,.\,\mathbf{P}) = \mathrm{vec}(\mathbf{R}\,.\,\mathbf{P}) = \mathrm{diag}(\mathrm{vec}(\mathbf{R}))\mathrm{vec}(\mathbf{P}) = \mathrm{diag}(\mathrm{vec}(\mathbf{P}))\mathrm{vec}(\mathbf{R}). \tag{14}$$

A is an $M \times N$ matrix and **B** is a $P \times Q$ matrix, then the Kronecker product $\mathbf{A} \otimes \mathbf{B}$ is the $MP \times NQ$ block matrix [47], and there are properties as:

$$(\mathbf{A} \otimes \mathbf{B})^H = \mathbf{A}^H \otimes \mathbf{B}^H,$$
$$\mathrm{vec}(\mathbf{C}) = \mathrm{vec}(\mathbf{AYB}) = (\mathbf{B}^T \otimes \mathbf{A})\mathrm{vec}(\mathbf{Y}). \tag{15}$$

By using these matrix properties, we can get equivalent form of the first step of DCRE ciphertext, as demonstrated:

$$\begin{aligned}\mathrm{vecs}\,(\mathbf{Y1}) &= \left(\mathbf{F}_N^H \otimes \mathbf{F}_M^H\right) \mathrm{d}i\mathit{ag}\left(\mathrm{vec}\left(\mathbf{H}_{\mathbf{F}}^{\mathbf{O}}\right)\right) \mathrm{vec}\left(\mathbf{F}_M\,(\mathbf{Y}\,.\,\mathbf{R1})\,\mathbf{F}_N\right)\\ &= \left(\mathbf{F}_N^H \otimes \mathbf{F}_M^H\right) \mathrm{d}i\mathit{ag}\left(\mathrm{vec}\left(\mathbf{H}_{\mathbf{F}}^{\mathbf{O}}\right)\right) \left(\mathbf{F}_N \otimes \mathbf{F}_M\right) \mathrm{d}i\mathit{ag}\left(\mathrm{vec}\left(\mathbf{R1}\right)\right) \mathrm{vec}(\mathbf{Y})\\ &= \mathbb{F}^H\,\mathbb{H}_{\mathbf{O}}\mathbb{F}\mathbb{R}\mathbf{1}\mathrm{vec}(\mathbf{Y}).\end{aligned} \tag{16}$$

where $\mathbb{F}$ is the Kronecker product of $\mathbf{F}_N$ and $\mathbf{F}_M$, $\mathbb{H}_{\mathbf{O}} = \text{diag}(\text{vec}(\mathbf{H}_{\mathbf{F}}^{\mathbf{O}}))$, $\mathbb{H}_{\mathbf{I}} = \text{diag}(\text{vec}(\mathbf{H}_{\mathbf{F}}^{\mathbf{I}}))$, $\mathbb{R}\mathbf{1} = \text{diag}(\text{vec}(\mathbf{R1}))$, $\mathbb{R}\mathbf{2} = \text{diag}(\text{vec}(\mathbf{R2}))$. They are all with size $MN \times MN$, with the size of $\mathbf{Y}$ is $M \times N$ and will be vectorized to $\mathbf{y}$ with size MN $\times$ 1. Further, we can achieve the equivalent form of DCRE ciphertext, as

$$\text{vec}(\mathbf{C}) = \mathbb{F}^H \mathbb{H}_{\mathbf{I}} \mathbb{F} \mathbb{R}\mathbf{2}\text{vec}(\mathbf{Y1})^* = \mathbb{F}^H \mathbb{H}_{\mathbf{I}} \mathbb{F} \mathbb{R}\mathbf{2} \mathbb{F}^T \mathbb{H}_{\mathbf{O}}^* \mathbb{F}^* \mathbb{R}\mathbf{1}^* \text{vec}\left(\mathbf{Y}^*\right). \tag{17}$$

And if $\mathbf{T}$ is defined as the product of $\mathbb{F}^H \mathbb{H}_{\mathbf{I}} \mathbb{F} \mathbb{R}\mathbf{2} \mathbb{F}^T \mathbb{H}_{\mathbf{O}}^* \mathbb{F}^* \mathbb{R}\mathbf{1}^*$, we obtain

$$\mathbf{c} = \mathbf{T}\mathbf{y}^* = \mathbf{T}\Phi^*\Psi^*\mathbf{s}^*. \tag{18}$$

Here, we achieve an equivalent matrix form for the ciphertext of CS-DCRE scheme.

3.5 RIP Performance and Security Analysis

The proposed scheme of DCRE combining with CS works with RIP. Here, we try to illustrate whether matrix $\mathbf{T}\Phi$ in (14) also satisfies the RIP with same order of matrix Φ in (1). If they are the same, the decryption of the concatenated systems could be unified to a single step ℓ_1 optimization procedure,

$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \mathbf{c} = \mathbf{T}\Phi^*\Psi^*\mathbf{s}^* = \mathbf{T}\Theta^*\mathbf{s}^*. \tag{19}$$

Fortunately, the two orders are not the same,

$$\begin{aligned} \mathbf{T}\mathbf{T}^H &= \mathbb{F}^H \mathbb{H}_{\mathbf{I}} \mathbb{F} \mathbb{R}\mathbf{2} \mathbb{F}^T \mathbb{H}_{\mathbf{O}}^* \mathbb{F}^* \mathbb{R}\mathbf{1}^* \left(\mathbb{F}^H \mathbb{H}_{\mathbf{I}} \mathbb{F} \mathbb{R}\mathbf{2} \mathbb{F}^T \mathbb{H}_{\mathbf{O}}^* \mathbb{F}^* \mathbb{R}\mathbf{1}^*\right)^H \neq \mathbf{I}, \\ &\|\mathbf{T}\Phi\mathbf{s}\|_2 \neq \|\Phi\mathbf{s}\|_2. \end{aligned} \tag{20}$$

In matrix $\mathbf{T}$, although matrices F, $\mathbf{F}^H$, $\mathbb{R}\mathbf{1}$ and $\mathbb{R}\mathbf{2}$ are unitary matrices, but matrices $\mathbb{H}_\text{I}$ and $\mathbb{H}_\text{O}$ are not. Therefore, matrix $\mathbf{T}$ is not unitary matrix. In other words, the complete DCRE and CS operations cannot be normalized as an equivalent CS procedure. Although $\mathbf{T}\Phi$ serve as the equivalent measurement matrix, the proposed scheme is safety to plaintext attack and ciphertext-only attack with **R1**, **R2**, and Φ serve as secret keys.

4. Results

To verify the proposed CS-DCRE scheme which is based on CS and DCRE, numerical simulations have been conducted on a Matlab R2017a platform with Processor Intel Core i7 @ 2.4 GHz, Memory 8.0 GB RAM, and 64-bit OS Win10. The R_2, H, r, and λ are independent and can be used as the cylindrical diffraction keys, and the two random phase masks and one random matrix are generated by Chen's 3D chaos algorithm with keys of x_0, y_0, z_0, pa, pb, and pc, which consist the encryption keys of CS-DCRE. In the simulations, let the diffraction parameters of r, R_1, R_2, H, λ be 10, 200, 220, 32, 480 mm, respectively, i.e., supposing the compression ratio (CR) be 0.5. Here, CR is defined as the ratio of data amount of compressed image divided by that of original image. And let keys of x_0, y_0, z_0, pa, pb, and pc be 0.116, 0.795, 0.467, 35, 3, and 28, respectively. The correlation coefficient (CC) and PSNR are employed to evaluate the encryption performance or reconstruction quality. Here, if $\mathbf{X}$ and $\mathbf{C}$ denote the original and different images, respectively, the CC and PSNR are defined as

$$\begin{aligned} \text{CC} &= \left[\text{cov}\left(\mathbf{X}, \mathbf{C}\right)\right] / \left(\sigma_{\mathbf{X}} \times \sigma_{\mathbf{C}}\right), \\ \text{PSNR} &= 10\log_{10}\left(MN \times MAX^2 / \|\mathbf{X} - \mathbf{C}\|_1^2\right), \end{aligned} \tag{21}$$

where cov denotes the cross-covariance, σ denotes standard deviation, *MN*, denote the image size. And here *MAX* is 255, the maximum gray level of an image.

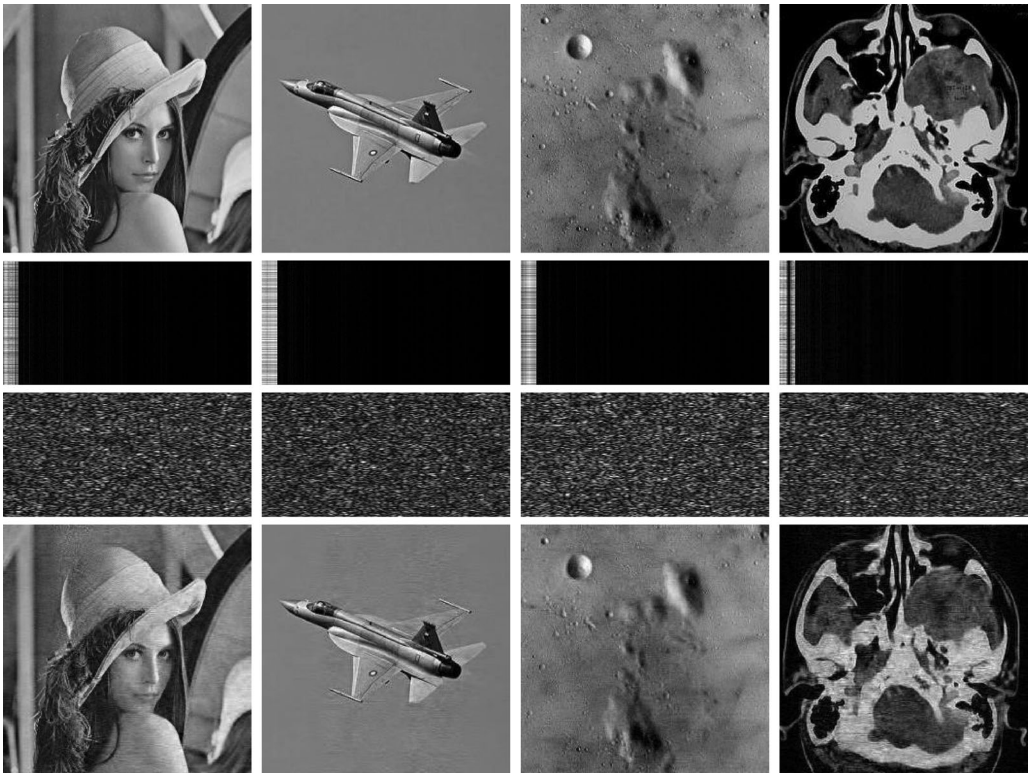


Fig. 5. Simulation results: Row 1 is original images; Row 2 is corresponding compressed images of row 1 with compression ratio of 0.5; Row 3 is corresponding encrypted images of row 2; Row 4 is corresponding decrypted images of row 3. The images in Row 1 are Lena, Aircraft, Moon, Brain.

4.1 Encryption and Decryption Results

We employed four types of images, Lena, Aircraft, Moon and Brain (256 × 256 pixels), as input plaintext image to demonstrate the correctness and the security of the cryptosystem, as shown in Figs. 5 and 6.

The CS compression and DCRE encryption and decryption results of the proposed method are shown in Fig. 5 Row 2, Row 3, and Row 4, respectively. The CC values of corresponding to Fig. 5 Row 3 are 0.0039, −0.0019, 0.0014, and −0.0083, respectively. The PSNR values of corresponding to Fig. 4 Row 4 are 29.88, 35.95, 31.24, and 26.95 dB, respectively. As shown in Fig. 5 Row 2, the compressed results by CS don't show good noise-like property, although it is verified by subjective observation that the no information of the original object can be recognized. When the CS is combined with the DCRE, the encrypted images show very good noise-like property, which it is also verified by their CC values.

The decrypted results of Lena are shown in Fig. 6(a)–(m) with wrong keys of x_0, y_0, z_0, pa, pb, pc, λ, H, r, R_2, Φ, **R**1, and, **R**2, respectively. Results of Fig. 6(k)–(m) show that if any one of three keys (R1, R2, and Φ as shown in Fig. 4) is wrong, which means even any two of three keys are known, none of the actual image information can be found. These results also show that the attacker cannot catch any information of the original object by subjective observation without keeping all correct keys.

4.2 Histogram and CC

The histogram of an image shows the distribution of pixel values. Fig. 7(a)–(d) illustrate the equalized histograms of the images of Lena, Aircraft, Moon and Brain, respectively. In these figures, red, green,

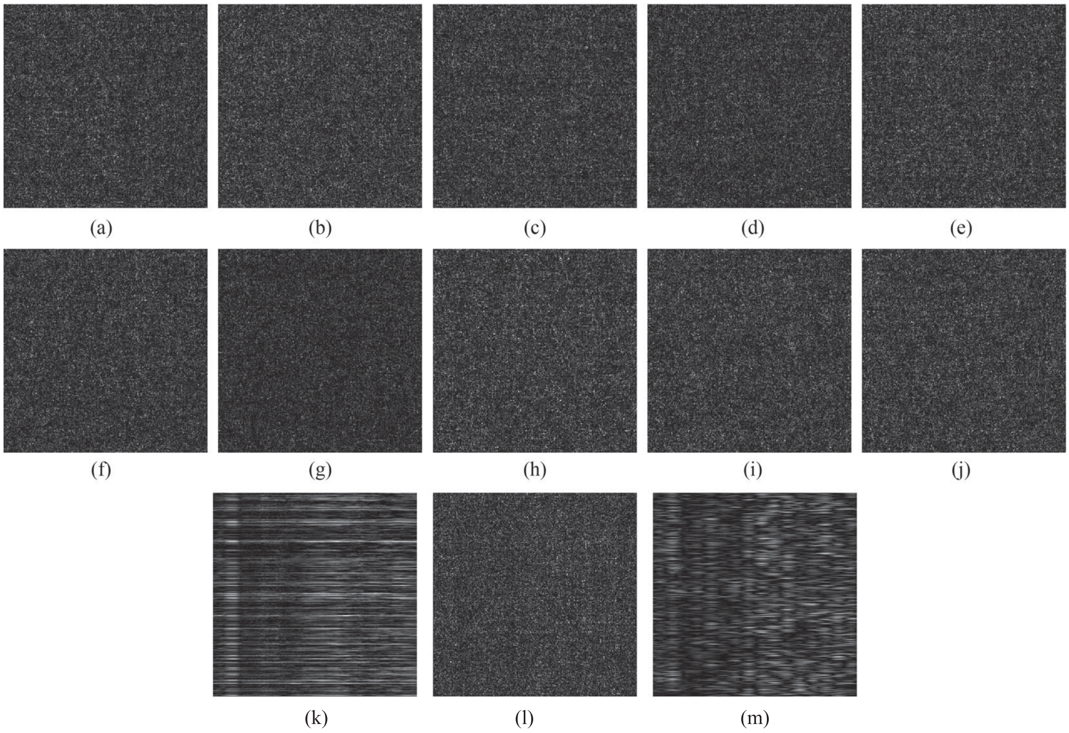


Fig. 6. Results with wrong keys: (a) x_0; (b) y_0; (c) z_0; (d) pa; (e) pb; (f) pc; (g) λ; (h) H; (i) r; (j) R_2; (k) Φ; (l) $\mathbf{R}1$; (m) $\mathbf{R}2$.

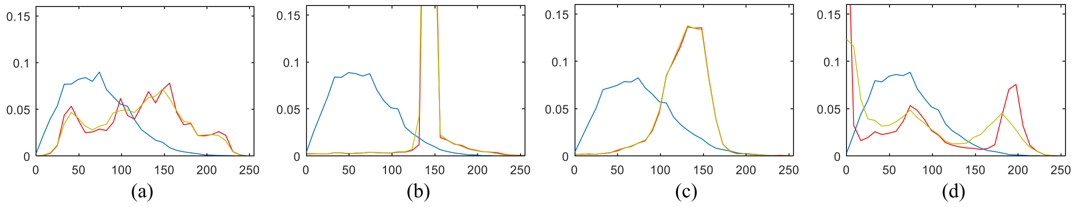


Fig. 7. Histograms of (a) Lena; (b) Aircraft; (c) Moon; (d) Brain; And those of plaintext images with red line, ciphertext images with blue line, reconstructed images with green line.

and blue lines denote the results of plain, cypher, and reconstructed images, respectively. It is clear from Fig. 7 that the histograms of the reconstructed images are almost the same with those of the original images. While the histograms of the proposed scheme result in the Rayleigh noise-like distributions, and statistical attack is not effective to our algorithm.

Ciphered image should also have no correlation with the plain image. The CC values results of different compression ratio are shown in Fig. 8 for Lena, Aircraft, Moon and Brain. When the CR is 1, it means the DCRE plays alone without CS. The CC values are ranged from -0.0357 to 0.0714. These results show that all the ciphered image shows good noise-like property, although the reconstructed image maybe not good when the CR is too small, i.e., CR < 0.3. It is also verified that CS combining with DCRE compresses and encrypts images well, simultaneously.

4.3 Key Space and Sensitivity

To provide an encryption scheme with high security, the key space should be large enough to make any brute force attack ineffective. The total key space is generally decided by the keys in the

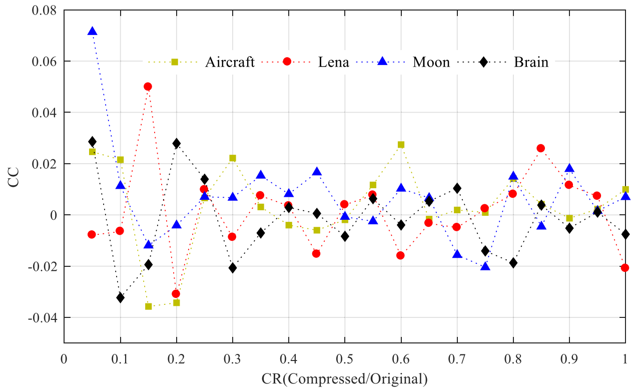


Fig. 8. CC results response to the variant of CR.

TABLE 1
Key Sensitive Result

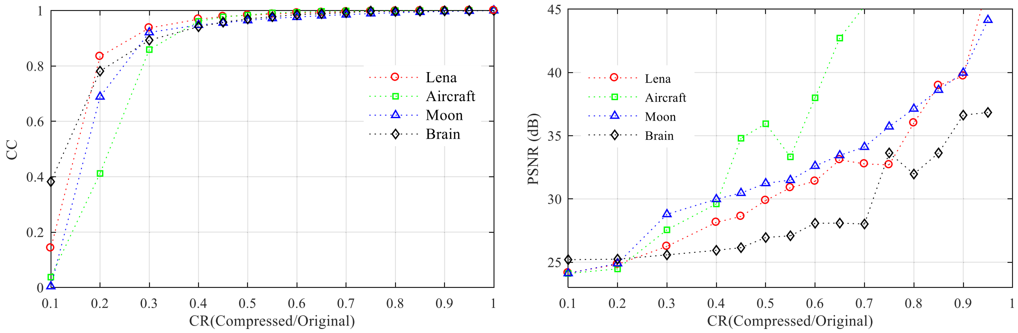
Modified secret keys	CCs of plain and reconstructed images with tiny wrong in keys			
	Lena	Aircraft	Moon	Brain
$x_0' = x_0 + 10^{-16}$	0.0065	-0.0010	0.0163	-0.0083
$y_0' = y_0 + 10^{-16}$	-0.0088	-0.0035	0.0140	0.0016
$z_0' = z_0 + 10^{-15}$	0.0072	0.0079	-0.0042	0.0009
$pa' = pa + 10^{-14}$	0.0010	0.0026	0.0126	0.0106
$pb' = pb + 10^{-15}$	-0.0098	-0.0009	-0.0044	0.0005
$pc' = pc + 10^{-14}$	-0.0010	-0.0048	0.0246	0.0006
$\lambda' =\lambda + 10^{-7}$	-0.0057	0.0107	0.0265	-0.0056
$H' =H + 10^{-4}$	-0.0053	0.0019	0.0060	0.0015
$r' =r + 10^{-4}$	0.0049	0.0029	0.0109	0.0058
$R_2' = R_2 + 10^{-4}$	**0.0166**	**0.0143**	**0.0289**	**0.0662**

scheme include the initial conditions and control parameters of the 3D chaos system (x_0, y_0, z_0, pa, pb, pc) and the diffraction system parameters (λ, r, H, R_2). Compared with CS-DRPE or DCRE, the proposed CS-DCRE has two additional keys. We have done many experiments to get the fact that we can decrypt the ciphered images unless we know x_0 within error 10^{-16}, y_0 within error 10^{-16}, z_0 within error 10^{-15}, pa within error 10^{-14}, pb within error 10^{-15}, pc within error 10^{-14}, λ within error 10^{-7}, H within error 10^{-15}, r within error 10^{-15}, R_2 within error 10^{-15}. The key space of the proposed algorithm is $10^{16} \times 10^{16} \times 10^{15} \times 10^{14} \times 10^{15} \times 10^{14} \times 10^{7} \times (2^4)^3 \approx 2^{109}$, which is big enough to resist all kinds of brute-force attacks.

A good image encryption algorithm is supposed to be sensitive to its key and own big key space. The keys used in the proposed algorithm consist of (x_0, y_0, z_0, pa, pb, pc) and (λ, r, H, R_2). The key sensitive results of CC values of plaintext and reconstructed image with tiny wrong in keys are shown in Table 1. Therefore, the sensitive of our proposed scheme is verified from the above results.

4.4 Compression and Reconstruction Performances

In this section, the compression and reconstruction performances are discussed. CR is one important aspect of the compression algorithms, and the reconstructed quality is another aspect. CC and PSNR values are employed to evaluate it in this paper. The results of reconstructed image quality



(a) (b)

Fig. 9. Quality of the reconstructed images of (a) CCs and (b) PSNRs in red, green, blue, and dark makers for Lena, Aircraft, Moon, and Brain, respectively, with different compression ratios.

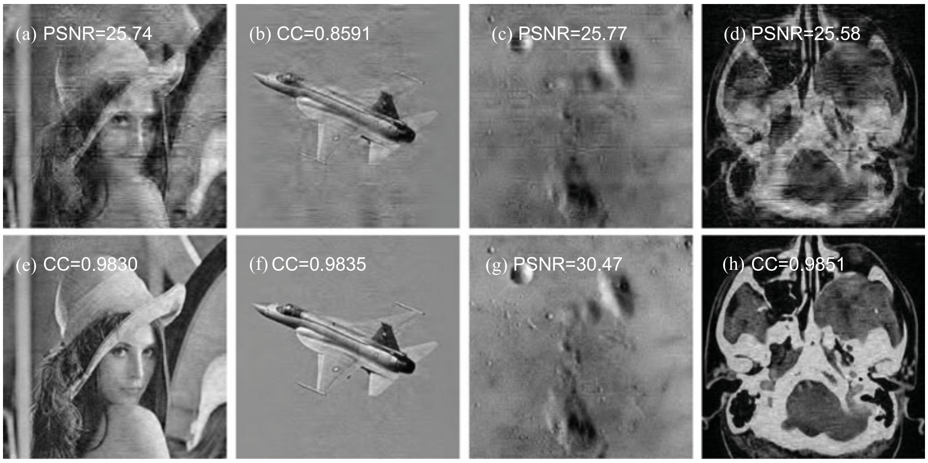


Fig. 10. Reconstructed result images of acceptable (row 1) and good (row 2) quality standards for (a) Lena with $CR = 0.25$, (b) Aircraft with $CR = 0.30$, (c) Moon with $CR = 0.25$, (d) Brain with $CR = 0.30$, (e) Lena with $CR = 0.5$, (f) Aircraft with $CR = 0.45$, (g) Moon with $CR = 0.45$, (h) Brain with $CR = 0.6$.

in CC and PSNR with the different *CRs* are shown in Fig. 9(a) and (b), respectively, for test images of Lena, Aircraft, Moon and Brain.

From these results, it clearly shows that the reconstructed image quality is degraded rapidly when CR < 0.3 from the CC results, although different types of images have difference. We can denote two quality lines of either CC > 0.85 or PSNR > 25 dB and either CC > 0.98 or PSNR > 30 dB for acceptable and good qualities, respectively, i.e., the image quality for Lena is acceptable when CR ≥ 0.3 since the CC $= 0.8342$, and good when CR ≥ 0.5 since the CC $= 0.9830$. Other image qualities have the similar situation. The corresponding results are shown in Fig. 10.

The above results show that our proposed scheme is flexible for different types of images in different application scenario, and also verify the feasibility of our proposed compression and encryption, simultaneously.

4.5 Potential Attacks Analysis

An excellent cryptosystem should be sensitive to the plaintext. Therefore, the six keys of chaos algorithm could be decided by the checksum of the plaintext, i.e.,:

$$x'_0 = x_0 + \text{checksum},$$
$$\text{checksum} = \text{mod}(sum, M \times N)/(M \times N), \tag{22}$$

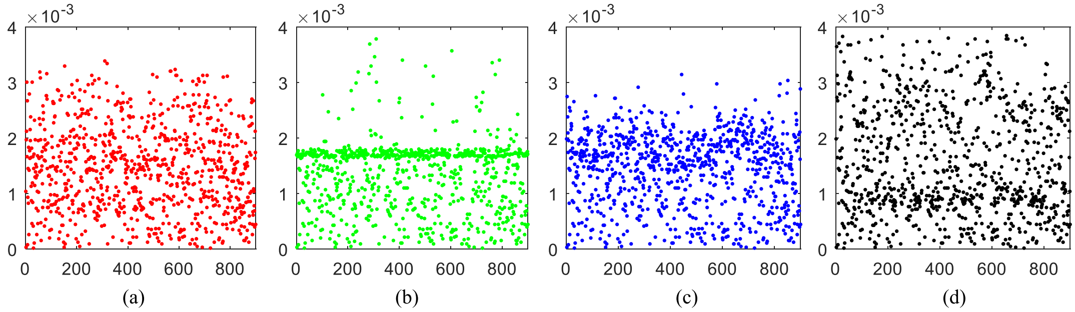


Fig. 11. Results of absolute change of the checksums. (a) Lena; (b) Aircraft; (c) Moon; (d) Brain.

TABLE 2
Comparison of Potential Attacks Test

Attack test types	Different schemes			
	CS-DCRE	DCRE [26]	CS-DPRE [32]	DPRE [6]
plaintext attack	Pass	No Pass	No Pass	No Pass
ciphertext-only attack	Pass	No Pass	No Pass	No Pass
phase-retrieval attack	Pass	Pass	No Pass	No Pass
differential attack	Pass	No Pass	No Pass	No Pass
brute-force attack	Pass	Pass	Pass	Pass

where mod denotes modulus operation, and *sum* is the sum of all pixel values of the plaintext image. The checksums of Lena, Aircraft, Moon, and Brain are 0.7271, 0.0923, 0.7633, and 0.9136, respectively. Fig. 11(a)–(d) show absolute change of checksums (ACC) when the plaintext images change a random value in one random position for Lena, Aircraft, Moon, and Brain, respectively. Here, 900 positions are randomly selected for every plaintext. The minimum of the 3600 ACCs is 1.5259e-5 which is not zero although it is so small. Since the initial values of the 3D chaos algorithm are highly sensitive as shown in Table 1, the proposed scheme should be highly sensitive to plaintext, which ensures the cryptosystem could resist plaintext attack, i.e., differential attack.

As analyzed in Section 3.5, the proposed scheme is safety to ciphertext-only attack and plaintext attack. Since the DCRE scheme can resist phase-retrieval attack [26], [48], the scheme combining CS and DCRE could resist phase-retrieval attack too. The comparison of potential attacks test for some conventional schemes are shown in Table 2. The comparison shows that the proposed scheme can resist several attacks and has higher security than the conventional schemes have such as DPRE [6], DCRE [26] and CS-DPRE [32].

5. Conclusion

We proposed an image cryptosystem based on the CS-then-DCRE architecture, which could simultaneously compress and encrypt image with high security. Through the analysis on the equivalent ciphertext of CS-DCRE in vector-matrix form, we proved that the CS-DCRE can be normalized as a single CS projection process. However, the equivalent measurement matrix of our scheme can't satisfy the RIP due to the asymmetric cylindrical diffraction of DCRE, which makes it impossible to recover the plaintext with only a single-step $\ell 1$ optimization. Therefore, our scheme can resist ciphertext-only attack and even plaintext attack. Furthermore, the encryption keys could be decided by the checksum of plaintext, which ensures the proposed scheme is sensitive to plaintext and free of plaintext attack. In addition, our scheme is free of phase-retrieval attack because of the asymmetric cylindrical diffraction. The security of the proposed scheme is also improved in key space due to two additional keys compared with the conventional CS-DRPE [32] and DCRE [26]. Numerical simulation results demonstrate the effectiveness and flexibility of the proposed cryptosystem.

References

[1] B. Javidi *et al.*, “Roadmap on optical security,” *J. Opt.*, vol. 18, no. 8, Jul. 2016, Art. no. 083001.

[2] A. Carnicer and B. Javidi, “Optical security and authentication using nanoscale and thin film structures,” *Adv. Opt. Photon.*, vol. 9, no. 2, pp. 218–256, 2017.

[3] O. Matoba, T. Nomura, E. P. Cabré, M. S. Millán, and B. Javidi, “Optical techniques for information security,” *Proc. IEEE*, vol. 97, no. 6, pp. 1128–1148, Jun. 2009.

[4] A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,” *Adv. Opt. Photon.*, vol. 1, no. 3, pp. 589–636, 2009.

[5] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, 2014.

[6] P. Refregier and B. Javidi, “Optical image encryption based on input plane and fourier plane random encoding,” *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[7] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” *Opt. Lett.*, vol. 30, no. 13, pp. 1644–1646, 2005.

[8] X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” *Opt. Lett.*, vol. 31, no. 8, pp. 1044–1046, 2006.

[9] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” *Opt. Exp.*, vol. 15, no. 16, pp. 10253–10265, 2007.

[10] G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, 2004.

[11] 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.

[12] N. Singh and A. Sinha, “Gyrator transform-based optical image encryption, using chaos,” *Opt. Lasers Eng.*, vol. 47, no. 5, pp. 539–546, 2009.

[13] X. C. Cheng *et al.*, “Security enhancement of double-random phase encryption by amplitude modulation,” *Opt. Lett.*, vol. 33, no. 14, pp. 1575–1577, 2008.

[14] A. Elshamy *et al.*, “Optical image encryption based on chaotic baker map and double random phase encoding,” *IEEE J. Lightw. Technol.*, vol. 31, no. 15, pp. 2533–2539, Aug. 2013.

[15] W. Qin and X. Peng, “Asymmetric cryptosystem based on phase-truncated Fourier transforms,” *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, 2010.

[16] X. Wang and D. Zhao, “Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated fourier-transform-based encryption using a random amplitude mask,” *Opt. Lett.*, vol. 38, no. 18, pp. 3684–3686, 2013.

[17] X. Wang, W. Chen, and X. Chen, “Optical information authentication using compressed double random phase encoded images and quick-response codes,” *Opt. Exp.*, vol. 23, no. 5, pp. 6239–6253, 2015.

[18] X. Deng and D. Zhao, “Single-channel color image encryption based on asymmetric cryptosystem,” *Opt. Laser Technol.*, vol. 44, no. 1, pp. 136–140, 2012.

[19] X. Wang, G. Zhou, C. Dai, and J. Chen, “Optical image encryption with divergent illumination and asymmetric keys,” *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7801908.

[20] C. Shen, J. Tan, C. Wei, and Z. Liu, “Coherent diffraction imaging by moving a lens,” *Opt. Exp.*, vol. 24, no. 15, pp. 16520–16529, 2016.

[21] H. Hwang, H. Chang, and W. Lie, “Fast double-phase retrieval in fresnel domain using modified gerchberg-saxton algorithm for lensless optical security systems,” *Opt. Exp.*, vol. 17, no. 16, pp. 13700–13710, 2009.

[22] X. Wang, W. Chen, and X. Chen, “Optical encryption and authentication based on phase retrieval and sparsity constraints,” *IEEE Photon. J.*, vol. 7, no. 2, Apr. 2005, Art. no. 7800310.

[23] Z. Liu, C. Shen, J. Tan, and S. Liu, “A recovery method of double random phase encoding system with a parallel phase retrieval,” *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7801807.

[24] E. Perez-Cabre, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” *Opt. Lett.*, vol. 36, no. 1, pp. 22–24, 2011.

[25] A. Markman, B. Javidi, and M. Tehranipoor, “Photon-counting security tagging and verification using optically encoded QR codes,” *IEEE Photon. J.*, vol. 6, no. 1, Feb. 2014, Art. no. 6800609.

[26] J. Wang, X. Li, Y. Hu, and Q. Wang, “Phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and double-random phase encoding,” *Opt. Commun.*, vol. 410, pp. 468–474, 2018.

[27] E. Candes, J. Romberg, and T. Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,” *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[28] D. Donoho, “Compressed sensing,” *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[29] E. Candes and M. Wakin, “An introduction to compressive sampling,” *IEEE Trans. Signal Process.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[30] E. Candes and T. Tao, “Near-optimal signal recovery from random projections: Universal encoding strategies?” *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.

[31] Y. Rivenson, A. Stern, and B. Javidi, “Single exposure super-resolution compressive imaging by double phase encoding,” *Opt. Exp.*, vol. 18, no. 14, pp. 15094–15103, 2010.

[32] P. Lu, Z. Xu, X. Lu, and X. Liu, “Digital image information encryption based on compressive sensing and double random-phase encoding technique,” *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 16, pp. 2514–2518, 2013.

[33] X. Liu, W. Mei, and H. Du, “Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain,” *J. Modern Opt.*, vol. 61, no. 19, pp. 1570–1577, 2014.

[34] B. Deepan, C. Quan, Y. Wang, and C. J. Tay, “Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique,” *Appl. Opt.*, vol. 53, no. 20, pp. 4539–4547, 2014.

[35] Q. Liu, Y. Wang, J. Wang, and Q. Wang, “Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain,” *Opt. Rev.*, vol. 25, no. 1, pp. 1–10, 2018.

[36] J. Li, H. Li, J. Li, Y. Pan, and R. Li, “Compressive optical image encryption with two-step-only quadrature phase shifting digital holography,” *Opt. Commun.*, vol. 344, pp. 166–171, 2015.

[37] N. Rawat, B. Kim, I. Muniraj, G. Situ, and B. Lee, “Compressive sensing based robust multispectral double-image encryption,” *Appl. Opt.*, vol. 54, no. 7, pp. 1782–1793, 2015.

[38] Z. Liu, C. Shen, J. Tan, and S. Liu, “A recovery method of double random phase encoding system with a parallel phase retrieval,” *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7801807.

[39] T. Li, Z. Miao, and Y. Shi, “Ciphertext-only attack on phase-shifting interferometery-based encryption,” *IEEE Photon. J.*, vol. 9, no. 5, Oct. 2017, Art. no. 7803108.

[40] J Chen, Y Zhang, and LY Zhang, “On the security of optical ciphers under the architecture of compressed sensing combining with double random phase encoding,” *IEEE Photon. J.*, vol. 9, no. 4, Apr. 2017, Art. no. 7802711.

[41] G. Chen, Y. Mao, and C. Chui, “A symmetric image encryption based on 3D chaotic cat maps,” *Chaos Soliton. Fract.*, vol. 21, pp. 749–761, 2004.

[42] T. Do, L. Gan, N. Nguyen, and T. Tran, “Fast and efficient compressive sensing using structurally random matrices,” *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 139–154, Jan. 2012.

[43] Y. Sando, M. Itoh, and T. Yatagai, “Fast calculation method for cylindrical computer-generated holograms,” *Opt. Exp.*, vol. 13, pp. 1418–1423, 2005.

[44] J. Wang, Q. Wang, and Y. Hu, “Fast diffraction calculation of cylindrical computer generated hologram based on outside-in propagation model,” *Opt. Commun.*, vol. 403, pp. 296–303, 2017.

[45] J. Wang, Q. Wang, and Y. Hu, “Unified and accurate diffraction calculation between two concentric cylindrical surfaces,” *J. Opt. Soc. Amer. A*, vol. 35, no. 1, pp. A45–A52, 2018.

[46] K. Rao, D. Kim, and J. Hwang, *Fast Fourier Transform-Algorithms and Applications*. New York, NY, USA: Springer-Verlag, 2011.

[47] J. W. Brewer, “A note on kronecker matrix products and matrix equation systems,” *SIAM J. Appl. Math.*, vol. 17, no. 3, pp. 603–606, 1969.

[48] J. R. Fienup, “Phase retrieval algorithms: A comparison,” *Appl. Opt.*, vol. 21, no. 15, pp. 2758–2769, 1982.