Hindawi
Complexity
Volume 2020, Article ID 8815315, 13 pages
https://doi.org/10.1155/2020/8815315

Research Article

Protecting Compressive Ghost Imaging with Hyperchaotic System and DNA Encoding

Jingru Sun, Mu Peng, Fang Liu, and Cong Tang

College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

Correspondence should be addressed to Jingru Sun; jt_sunjr@hnu.edu.cn

Received 12 August 2020; Revised 14 September 2020; Accepted 17 September 2020; Published 5 October 2020

Academic Editor: Chun-Biao Li

As computational ghost imaging is widely used in the military, radar, and other fields, its security and efficiency became more and more important. In this paper, we propose a compressive ghost imaging encryption scheme based on the hyper-chaotic system, DNA encoding, and KSVD algorithm for the first time. First, a 4-dimensional hyper-chaotic system is used to generate four long pseudorandom sequences and diffuse the sequences with DNA operation to get the phase mask sequence, and then N phase mask matrixes are generated from the sequences. Second, in order to improve the reconstruction efficiency, KSVD algorithm is used to generate dictionary D to sparse the image. The transmission key of the proposed scheme includes the initial values of hyper-chaotic and dictionary D, which has plaintext correlation and big key space. Compared with the existing compressive ghost imaging encryption scheme, the proposed scheme is more sensitive to initial values and more complexity and has smaller transmission key, which makes the encryption scheme more secure, and the reconstruction efficiency is higher too. Simulation results and security analysis demonstrate the good performance of the proposed scheme.

1. Introduction

In recent years, with the rapid development of computer network and communication technology, information security issues have become more and more important. As an emerging optical imaging technology [1–3], CGI (computational ghost imaging) has attracted the attention of researchers once it had appeared and has been widely used in military, encryption, radar, and other fields [4, 5]. Therefore, the security of the CGI is especially vital.

CGI is developed based on ghost imaging technology [6], which can transmit image information through one optical path, with simple structure, strong anti-interference ability, and good imaging effect. In 2010, Clemente proposed an image encryption technology based on CGI [7]; as shown in Figure 1, this solution can encrypt plain-images into light intensity values and only requires a bucket detector without spatial resolution to receive the light intensity, which indicates a new research direction for optical information security [8]. To achieve high image reconstruction efficiency, Katz proposed a compressive ghost imaging (CSGI) scheme, which combines CGI with a compressive sensing (CS) algorithm to reduce the number of measurements required for image recovery by an order of magnitude [9–11].

Then, Durfin et al. proposed a CSGI encryption scheme [12]. Zhao et al. further improved the security of optical encryption by utilizing the high fault tolerance of QR encoding, which reduce the size of the transmitted images and enhance the robustness [13]. Wu et al. proposed an optical multiple-image encryption scheme based on CGI, and this method can transmit multiple images at the same time; but with the distance as the keys, it is vulnerable to brute-force attacks [14]. Zhu et al. use fingerprint technology to produce a phase modulation matrix, the fingerprint has the uniqueness, but it is easy to be obtained, and as a transmitted key, fingerprint is too big [15]. Li et al. proposed a multiple-image CSGI encryption method based on the LWT and XOR operations [16]. Most works in the literature fail to associate the key with plaintext image and have big transmission keys. This motivates us to look for a novel CSGI encryption method with plaintext correlation, smaller

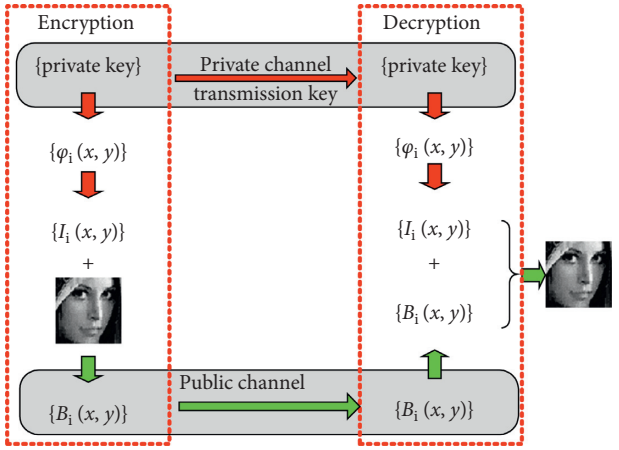


Figure 1: CGI encryption scheme.

transmission keys, larger key spaces, and high image reconstruction efficiency.

Chaos has many excellent characteristics, such as pseudorandomness, ergodicity, and sensitivity to initial points and parameters [17–23] and has been widely used in image encryption and privacy protection [24–28], communication encryption [29], and other fields. Chaotic systems can be divided into low-dimensional chaotic system and high-dimensional chaotic system. Low-dimensional chaotic systems such as Henon chaotic system [30, 31] and Tent map [32, 33] et al. were first used in the encryption system [34] but have been proved not security enough [35]. High-dimensional chaotic systems such as three-dimensional Lorenz chaotic systems [36, 37], and Chen System [38] and Yu System [39, 40] et al. have more dimensional and higher complexity. Especially hyper-chaotic systems [41, 42] have two or more Lyapunov exponents greater than 0 and larger key space and higher complexity. Hyper-chaotic systems have been wildly used in chaotic image encryption scheme [28, 43–45]. The DNA encoding and decoding technology [46] is a kind of biological method to process information, which has the characteristics of large-scale parallelism, high-storage density, ultra-low-power consumption, unique molecular structure, and intermolecular recognition mechanism. DNA has great development prospects in the field of information encryption [47–52]. In this paper, a CSGI encryption scheme based on the hyper-chaotic system, DNA and KSVD technologies is proposed. First, given four transmission keys, input the four keys as initial values to the hyper-chaotic-system; second, 4 long chaotic sequences are generated by a hyper-chaotic system, then three of them are arranged into a phase sequence, and the other sequence is used to produce a DNA sequence. Third, diffuse the phase sequence with the DNA sequence by DNA operation and then get phase modulation matrixes, which are used as the input of the spatial light modulator (SLM). At the same time, get dictionary matrix D with the original image by KSVD and achieve original signal sparse representation through D. Finally, complete the encryption of the scheme. Compared with the existing CSGI encryption scheme, the proposed scheme has smaller double transmission key, larger key space, high key sensitivity, plaintext correlation, and unpredictability. The use of DNA further increases the complexity and randomness of the encryption scheme.

The rest of this paper is organized as follows. In section 2, the basic theories of the CGI, hyper-chaotic system, DNA technology, compressed sensing, and singular value decomposition are described. In Section 3, the system framework of our proposed scheme and the generation process of phase mask matrixes are described in detail. The simulation results and security analysis are performed in section 4. The paper is summarized in section 5.

2. Basic Theories

2.1. CGI. In CGI, as shown in Figure 2, a spatial laser beam transmits through a spatial light modulator (SLM), which introduces an arbitrary phase mask matrix $\varphi(x, y)$, generating a spatially incoherent beam. Knowing the random phase and the distribution of laser light field $U_{\text{in}}(x, y)$, one can evaluate the distribution of the light intensity $U_i(x, y)$ right after the SLM:

$$U_i(x, y) = U_{\text{in}}(x, y)e^{i\varphi_i(x,y)}. \tag{1}$$

Through Fresnel diffraction, the light field distribution of signal light in front of object plane is the same as reference light, the light travels to the object plane which is z distance away from the SLM, and the speckle filed $I_i(x, y)$ can be calculated:

$$I_i(x, y) = \left|U_i(x, y) \otimes h_z(x, y)\right|^2, \tag{2}$$

where $h_z(x, y)$ is the transfer function in the spatial domain at a distance z, $\otimes$ represents the convolution operation, and $I_i(x, y)$ is defines as the reference light. The signal light intensities detected by a bucket detector placed behind the object, which can be represented by a transmission function of the object $T(x, y)$ and written as

$$B_i = \int \mathrm{d}x\mathrm{d}y I_i(x, y)T(x, y). \tag{3}$$

To construct the object's transmission function $T(x, y)$, the reference light speckle filed $I_i(x, y)$ cross-correlated with the signal light intensities B_i:

$$G(x, y) = \frac{1}{N}\sum_{i=1}^{N}(B_i - B)I_i(x, y), \tag{4}$$

where $G(x, y)$ denotes the recovered object information, $\langle\cdot\rangle = (1/N)\sum_i \cdot$ is an ensemble average over N measurements, $I_i(x, y)$ is calculated by the receiver according to equation (2), and B is the average value for the measured components $\{B_i\}$ [53].

2.2. Hyper-Chaotic System. In our proposed CSGI encryption scheme, the phase mask matrix required on the SLM is generated by the hyper-chaotic system:

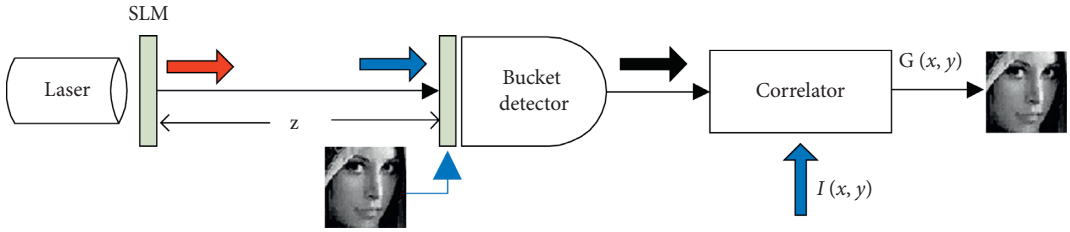


Figure 2: The basic theory of CGI.

$$\begin{cases} \dot{x} = a(y - x) + yz, \\ \dot{y} = bx - y - xz + w, \\ \dot{z} = xy - cz, \\ \dot{w} = dw - xz. \end{cases} \tag{5}$$

By setting parameters $a = 35$, $b = 3/8$, $c = 55$, and $d = 1.3$, we obtain four Lyapunov exponents, including two positive Lyapunov exponents, $\lambda_1 = 1.4164$ and $\lambda_2 = 0.5318$, a zero Lyapunov exponent $\lambda_3 = 0$, and a negative Lyapunov exponent $\lambda_4 = -39.1015$ [54]. By this means, the system exhibits hyper-chaotic behavior. Figure 3 depicts the phase portraits of the hyper-chaotic system. Here, we take the fourth-order Runge-Kutta method to solve (5) and obtain the four hyper-chaotic sequences.

2.3. DNA. DNA is a long-chain polymer, and the basic elements are four nucleic acid bases, namely, A (adenine), C (cytosine), G (guanine), and T (thymine), where A and T, C and G are complementary, respectively. In a binary system, 0 and 1 are complementary. It can be concluded that 00 and 11 are complementary, and 10 and 01 are complementary. Encoding the four bases A, C, G, and T with 0 and 1, eight encoding methods can be obtained, as shown in Table 1. Each of the DNA coding rules corresponds to an operation rule, and the following algorithm is based on the encoding rule 1 and rule 2. According to the binary calculation rule, we can get the corresponding rules of DNA addition, subtraction, and complement rule listed in Tables 2 and 3.

2.4. Compressed Sensing. Compressed sensing technology uses sparse basis such as DCT or DFT to represent the signal sparsely, measures the signal based on Gaussian random matrix, and then reconstructs the signal based on $L1$ norm and other algorithms.

Suppose a signal is $x \in \mathbb{R}^{N\times 1}$, before sampling the signal x, select a suitable and orthogonal sparse base $\Psi \in \mathbb{R}^{N\times N}$ to sparsely represent the signal x as

$$x = \Psi s, \tag{6}$$

where s is the sparse representation of x on a sparse basis Ψ. s has K nonzero elements, and other $N - K (N \gg K)$ elements' values are 0.

Sparse operation and the measurement matrix must satisfy restricted isometry property (RIP). Discrete cosine transform, fast-Fourier transform, etc. are common sparse operations.

During measuring x, in order to reduce the number of the measurements and ensure that the measuring result contain as much information of x as possible, we need an appropriate measurement matrix $\Phi \in \mathbb{R}^{M\times N}$ $(M < N)$. Bernoulli matrix, Gaussian distribution matrix, Hadamar matrix, Toeplitz matrix, etc. are often used in compressed sensing technology. The measurement of signal x can be expressed as

$$y = \Phi x = \Phi\Psi s = \Theta s, \tag{7}$$

where $\Phi\Psi = \Theta$ is a sensor matrix and $y \in \mathbb{R}^{M\times 1}$ is the measurement result.

In the end, use the compressed sensing reconstruction algorithm to reconstruct $\tilde{s}$ from y:

$$\begin{aligned} &\tilde{s} = \min \|\tilde{s}\|_{L_1} = \min \left\|\Psi^T x\right\|_{L_1} \\ &\text{s.t.} \quad y = \Phi x = \Theta s. \end{aligned} \tag{8}$$

The approximate solution vector can be obtained by applying inverse transformation for $\tilde{s}$:

$$\tilde{x} = \Psi\tilde{s}. \tag{9}$$

2.5. Singular Value Decomposition (SVD). Suppose a real matrix $E_K' \in \mathbb{R}^{m\times n}$ can be decomposed can be decomposed into

$$E_K' = \mathrm{UEV}^T, \tag{10}$$

where $E \in \mathbb{R}^{m\times n}$ is a singular value matrix whose nonzero elements are only located on the diagonal. $U \in \mathbb{R}^{m\times m}$ and $V \in \mathbb{R}^{n\times n}$ are both-unit orthogonal matrices, and U means the left singular matrix and V means the right singular matrix, respectively. Generally, E is represented as

$$E = \begin{bmatrix} \sigma_1 & 0 & 0 & 0 & 0 \\ 0 & \sigma_1 & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}_{m\times n}. \tag{11}$$

Decomposing E_K' by equation (10), then we can get

$$\begin{aligned} E_K' E_K'^T &= \mathrm{UEV}^T \mathrm{VE}^T U^T = \mathrm{UEE}^T U^T, \\ E_K'^T E_K' &= \mathrm{VEU}^T \mathrm{UE}^T V^T = \mathrm{VEE}^T V^T. \end{aligned} \tag{12}$$

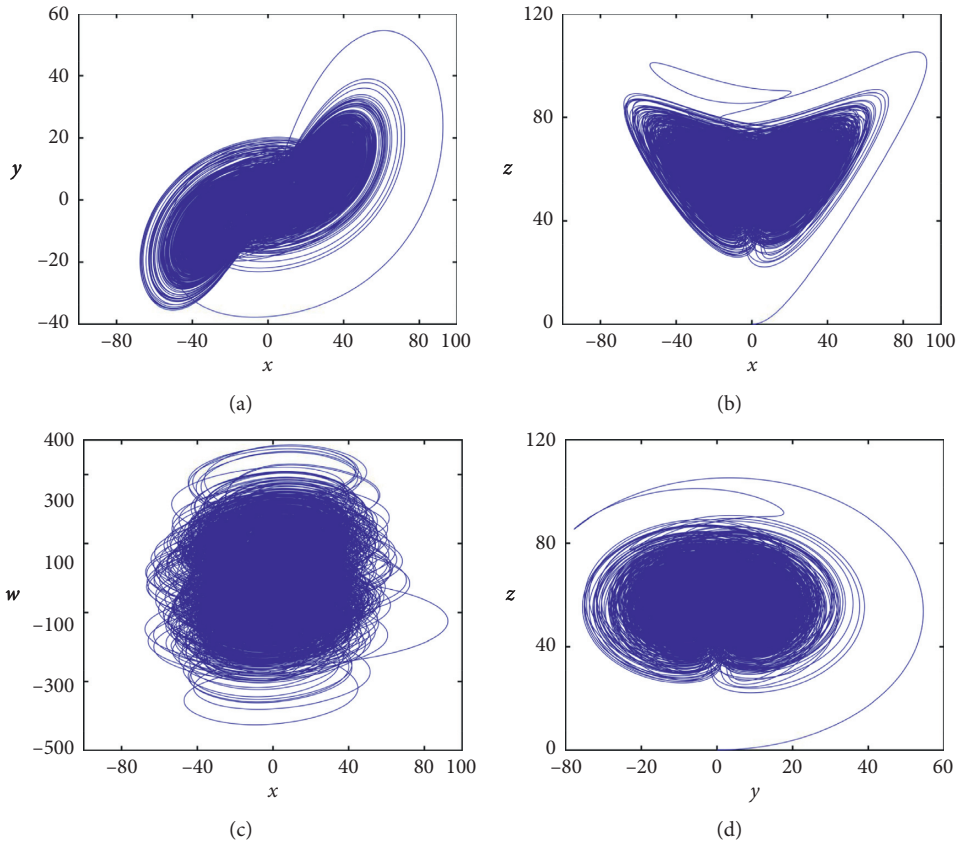


Figure 3: Phase portraits. (a) $x - y$ plane. (b) $x - z$ plane. (c) $x - w$ plane. (d) $y - z$ plane.

Table 1: DNA encode rule.

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

Table 2: DNA encode rule.

Addition	A	C	G	T	Subtraction	A	C	G	T
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

Table 3: DNA encode rule.

Complement	1	2	3	4	5	6
A	T	T	C	C	G	G
T	C	G	G	A	C	A
C	G	A	T	G	A	T
G	A	C	A	T	T	C

With the eigen-decomposition of $E_K^{'}E_K^{'T}$ and $E_K^{'T}E_K^{'}$, the left singular matrix U and the right singular matrix V can be obtained.

3. Proposed Encryption Scheme of CSGI

The proposed encryption scheme of CSGI includes three main parts: the generated of the phase mask φ, original image sparse presentation, and CSGI encryption. Next, the implementation processes will be introduced in detail.

3.1. Generation of the Phase Mask Matrix. Chaotic systems have some significant features, such as deterministic, pseudorandomness, and ergodicity, and they are sensitive to initial points and parameters. Supposing that the original image is denoted as T, whose size is $M \times M$, the initial values are x_0, y_0, z_0, and w_0 and the N phase mask matrices $\varphi(x, y)$ can be realized as follows:

(1) Use the initial values x_0, y_0, z_0, and w_0 to produce four pseudorandom sequences C_x, C_y, C_z, and C_w by iterating equation (5) for $M_0 + L$ times, where $L = M \times M$. To get rid of transient effect, we discard the first M_0 numbers of each sequence.

(2) Define two L length sequences, named Phase_s and DNA_s:

$$\text{Phase\_}s[i] = \frac{C\_x(i) + C\_y(i), C\_z(i)}{3} \times 10^{16} \bmod 256,$$
$$\text{DNA\_}s[i] = C\_w(i) \times 10^{16} \bmod 256. \tag{13}$$

(3) Convert sequences Phase_s and DNA_s to binary sequence, and then convert Phase_s and DNA_s into DNA sequence $L \times 4$P_sb and DNA_sb, respectively according to DNA encoding rules 1 and 3.

(4) According to the DNA complement rule and

$$P\_\text{st}[i] = \begin{cases} \text{DNA\_}C1\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = A \text{ and } i \bmod 2 = 0, \\ \text{DNA\_}C2\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = C \text{ and } i \bmod 2 = 0, \\ \text{DNA\_}C3\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = G \text{ and } i \bmod 2 = 0, \\ \text{DNA\_}C4\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = T \text{ and } i \bmod 2 = 0, \\ \text{DNA\_}C5\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = A \text{ and } i \bmod 2 = 1, \\ \text{DNA\_}C6\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = C \text{ and } i \bmod 2 = 1, \\ \text{DNA\_}C3\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = G \text{ and } i \bmod 2 = 1, \\ \text{DNA\_}C4\,(p\_\text{sb}[i]) \text{ if DNA\_sb}[i] = T \text{ and } i \bmod 2 = 1, \end{cases} \tag{14}$$

the new sequence P_st can be obtained.

(5) Convert the sequence $P\_\text{st}[i]$ to decimal, and normalize the phase values so that they are uniformly distributed in the range $[0, 2\pi]$:

$$P\_\text{st}[i] = \bmod (P\_\text{st}[i], 2 \times \pi). \tag{15}$$

(6) Transform the sequence $P\_\text{st}[i]$ into $M \times M$ pixels, and obtain phase mask matrix:

$$\varphi(x, y) = P\_\text{st}[i]. \tag{16}$$

(7) Set $x_0 = C\_x(L-1)$, $y_0 = C\_y(L-1)$, $z_0 = C\_z(L-1)$, and $w_0 = C\_w(L-1)$, and repeat step 1 to step 6 $N-1$ times, and then we can get N phase mask matrices $\varphi(x, y)$.

3.2. Original Image Sparse Presentation with KSVD. Suppose the original signal (image) is a matrix $X \in \mathbb{R}^{m \times n}$. $D \in \mathbb{R}^{m \times K}$ is dictionary matrix, and each column of the dictionary is called atomic vector d_k. S is the sparse matrix. Ideally, there is $X = \text{DS}$, with the original signal X sparse representation through D. Therefore, solving the dictionary matrix and sparse matrix can be converted into an optimization problem as follows:

$$\begin{aligned} &\min_{D,S} \quad \|X - \text{DS}\|_F^2 \\ &\text{s.t} \quad \forall i, \ \|s_i\|_0 \le T_0, \\ &\min_{D,S} \quad \sum_i \|s_i\|_0, \\ &\text{or s.t.} \min_{D,S} \quad \|X - \text{DS}\|_F^2 \le \varepsilon, \end{aligned} \tag{17}$$

where s_i $(i = 1, 2, \ldots, K)$ is the row vector of the sparse matrix S and $\|s_i\|_0 \le T_0$ is the limitation, namely, each row of the sparse matrix has nonzero elements as few as possible. This problem can be converted to a nonconstrained optimization problem by using Lagrangian multiplier method, which is

$$\min_{D,S} \|X - \text{DS}\|_F^2 + \lambda \|s_i\|_1. \tag{18}$$

In order to simplify the optimization problem, $\|s_i\|_0$ is replaced by $\|s_i\|_1$.

So, the main problem is converted to D and S two objective optimization problems, and the common method of S optimizing is orthogonal matching pursuit (OMP) algorithm, which has been discussed in [55]. The optimization of D can be described as follows:

Suppose the sparse matrix S is known, we can implement the columnwise update of dictionary matrix D. s_k^T is the k-th row vector of S, and E_k denotes residual, so

$$\begin{aligned}\|X - \mathrm{DS}\|_F^2 &= \left\|X - \sum_{j=1}^{K} d_j s_j^T\right\|_F^2 \\ &= \left\|\left(X - \sum_{j\neq k} d_j s_j^T\right) - d_k s_k^T\right\|_F^2 = \left\|E_k - d_k s_k^T\right\|_F^2,\end{aligned} \tag{19}$$

where $E_k = X - \sum_{j\neq k} d_j s_j^T$. Aforementioned optimization question can be converted into

$$\min_{d_k, s_k^T} \left\|E_k - d_k s_k^T\right\|_F^2, \tag{20}$$

where d_k and s_k^T become the variables to optimize, and equation (20) can be described as a least squares problem which can be solved by using SVD. Extract all nonzero terms of E_k and then rebuild new matrix E_k'. Hence, the optimization turns into

$$\min_{d_k, s_k^T} \left\|E_k' - d_k s_k^T\right\|_F^2. \tag{21}$$

Through SVD, we can get

$$E_k' = \mathrm{UEV}^T. \tag{22}$$

Replace d_k with the first column vector u_1 of left singular matrix, and then get one column of D. Multiply the first row of right singular matrix and the largest singular value; afterwards, we can obtain s_k^T. Replace s_k^T of sparse matrix S with the new result. Singular values of E should be ordered from largest to smallest.

Repeat the above steps to update each column of dictionary, and then we can gain the final dictionary matrix D and sparse matrix S from original signal.

3.3. CSGI Encryption. Figure 4 shows the process of CSGI encryption. The detailed steps are as follows:

(1) The phase masks matrices $\varphi(x, y)$ generated in Section 3.1 are uploaded to SLM, and the laser beam is phase modulated by SLM according to equation (1).

(2) The sparse matrix S and dictionary matrix D are gained by sparse representation of the original image according to Section 3.2.

(3) The sparse matrix S is placed at z distance from the SLM. According to Fresnel diffraction, we can get the light field distribution that can be obtained in the front of the image, and the light field intensity $\{I_i(x, y)\}$ can be further obtained according to equation (2).

(4) The total light intensity $\{B_i(x, y)\}$ can be calculated by a bucket detector behind the image according to equation (3).

(5) The initial values of the chaotic system and dictionary matrix D transmit through the private channel as the transmission key. And, $\{B_i(x, y)\}$ transmits through the public channel.

3.4. Decryption Process. Figure 5 shows the decryption process, and the detailed steps are as follows:

(1) The transmission key is received through the private channel x_0, y_0, z_0, w_0, and D, and the random phase mask matrices are calculated using the received transmission key according to the method in Section 3.1.

(2) The same computed intensity patterns $I_i(x, y)$ are obtained as step 3 of Section 3.3.

(3) The computed intensity patterns $I_i(x, y)$ are correlated with the total intensities of the light field $\{B_i(x, y)\}$ received from the public mode, and the estimated matrix $\widetilde{S}$ of S is reconstructed, according to equation (3).

(4) According to $\widetilde{X} = D\widetilde{S}$, use dictionary matrix D to reconstruct the original image from $\widetilde{S}$.

4. Simulation Results and Security Analysis

In this part, the proposed scheme is simulated with MATLAB R2016a to verify the feasibility.

As shown in Figure 6(a), a grayscale image of 128×128 size is used as the original image. The initial values of the hyper-chaotic system are set as $(x_0 = 1, y_0 = 0.949, z_0 = 1$, and $w_0 = 1)$, and then referring to the mentioned point in Section 3, we obtain N different random phase mask matrices and the sparse representation of original image which is shown in Figures 6(b) and 6(c). The following is the brief descriptions of the computational complexity of our algorithm and comparison with other algorithms.

In generation of phase mask matrix, the size of gray image is $m \times m$, the main operations are "addition", "multiplication," and "mod", and then the operand is $N(40m^2 + 19M_0)$, where N is the number of measurements. In the step of sparse representation, the main operation is the computation of sparse matrix S and dictionary matrix D, the operand is $5m^3$ where the number of iterations is 10, and for projection and image reconstruction, the operand is $4\,\mathrm{Nm}^2$ and $4m^3$, respectively. In order to guarantee the quality of results, we set $N \gg m$ in our experiments. The total operand is $N(44m^2 + 19M_0) + 4m^3$, because the generation of phase mask matrix and sparse representation can be performed simultaneously. Therefore, the computational complexity of CSGI can be expressed as $\Theta(\mathrm{Nm}^2)$. Compared with other algorithms, the computational complexity of using QR code and compressed sensing to encrypt the image (QR-CGI-OE) [13] is $\Theta(\mathrm{Nm}^2)$. And, the method based on the LWT, XOR

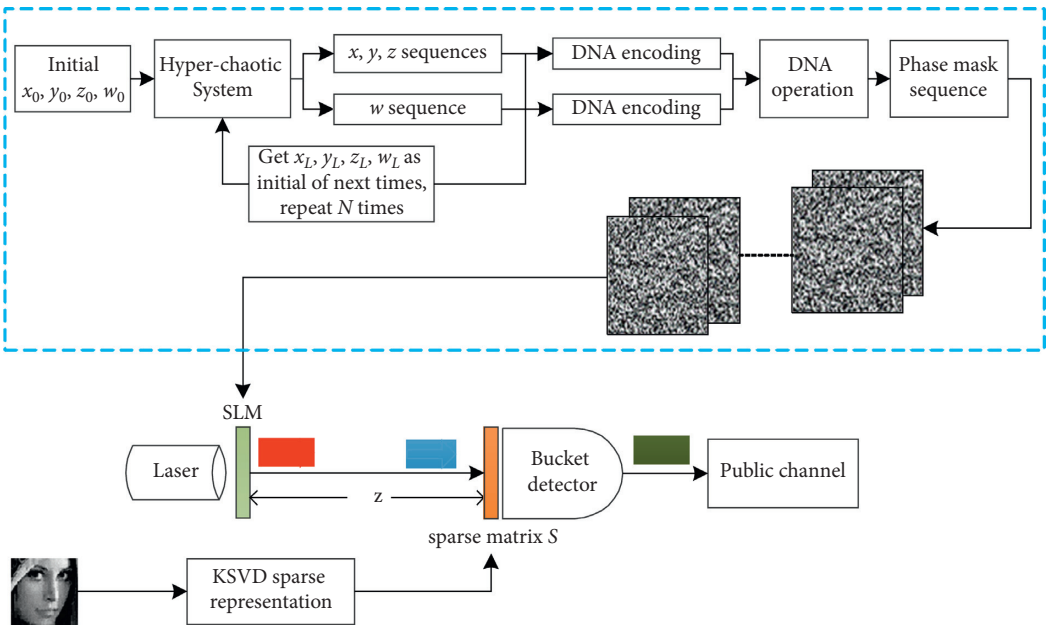


Figure 4: CSGI encryption.

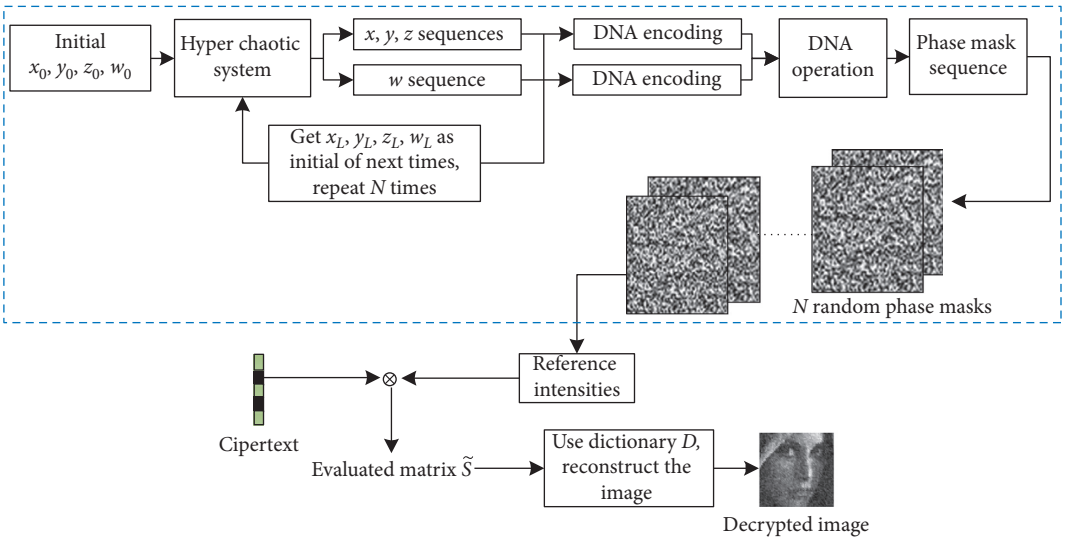
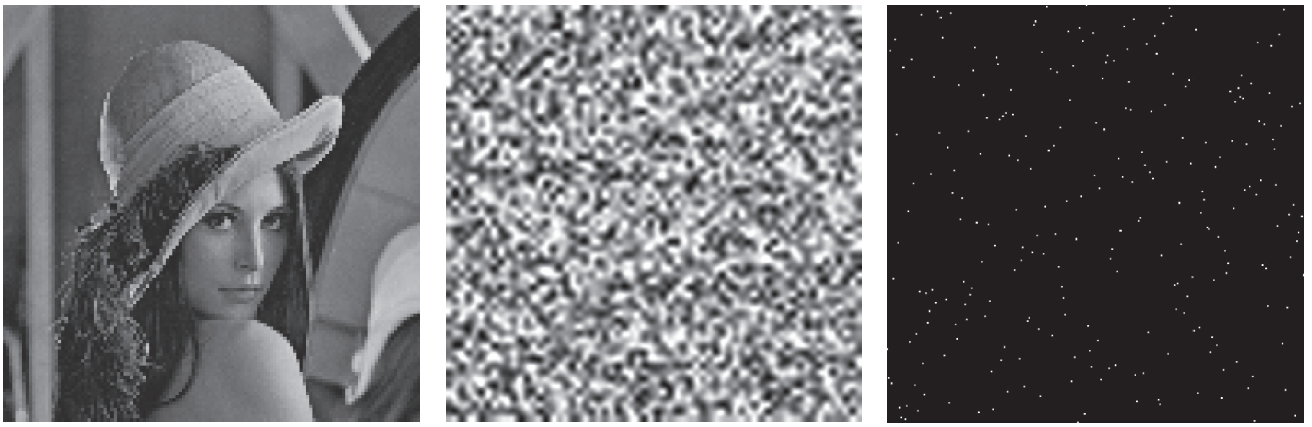


Figure 5: CSGI encryption.



(a) (b) (c)

Figure 6: Continued.

(d)

Figure 6: (a) The original image. (b) The random phase mask matrix. (c) The spares matrix. (d) The reconstructed image.

(a) (b) (c)

Figure 7: Reconstructed images for the sample object. (a) The original image. The reconstructed image with (b) the correct keys and (c) the incorrect keys.

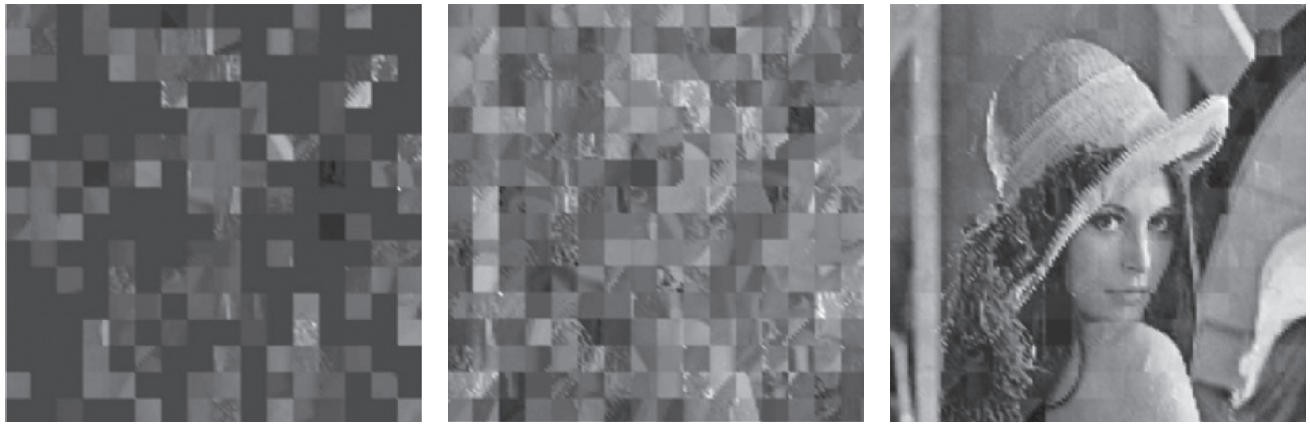
operations (XOR-LWT-OE) [16], spends most time on the process of measurement, whose computational complexity can be expressed as $\Theta(Nm^2)$. These illustrate that the computational complexity of the method used in this paper is identical to some relatively new algorithms', whereas our algorithm have better performance and less times of the measurement, which is stated below.

During the encryption of the CSGI, the wavelength of the plane wave is selected $0.532\,\mu m$. The image is placed at a distance $z = 200$ mm from the SLM, and the transmitted light is collected into a bucket detector. Then, the image can be reconstructed according to Section 3.4 and Figure 6(c).

4.1. Key Space Analysis. If the cryptographic scheme has enough large key space, it can resist brute-force attacks. Here, the transmission keys are x_0, y_0, z_0, w_0, and D. D is smaller and can be ignored. The operational precision of the computer is $10^{16} \approx 2^{52}$, and the key space of our proposed scheme is $2^{52} \times 2^{52} \times 2^{52} \times 2^{52} \approx 2^{208}$, which is much larger than the security requirement of the key space 2^{100}. Thus, the key space of our proposed scheme is strong enough and can effectively resist brute-force attacks.

4.2. Key Sensitivity Analysis. A highly secure computation ghost imaging system must be sensitive to the key. To verify the security performance of our proposed scheme, a security test is carried out. The private keys are set as ($x_0 = 1, y_0 = 0.949, z_0 = 1$, and $x_0 = 1$). In decryption process, we change the value of the private keys to ($x_0' = 1 + 10^{-15}, y_0' = 0.949, z_0' = 1$, and $w_0' = 1$) and then use to reconstruct the image. The sampled object is shown in Figure 7. Obviously, the information related to the plaintext image cannot be obtained when the private key is changed slightly.

4.3. Correlation Analysis. To evaluate the quality of the reconstructed image, the correlation coefficient between the reconstructed image G and the original image T can be calculated by



(a) (b) (c)

Figure 8: Reconstructed images with different measurements. The measurement and r_{TG} of is (a) 1000, 0.2418, (b) 2000, 0.5494, and (c) 2800, 0.9533.

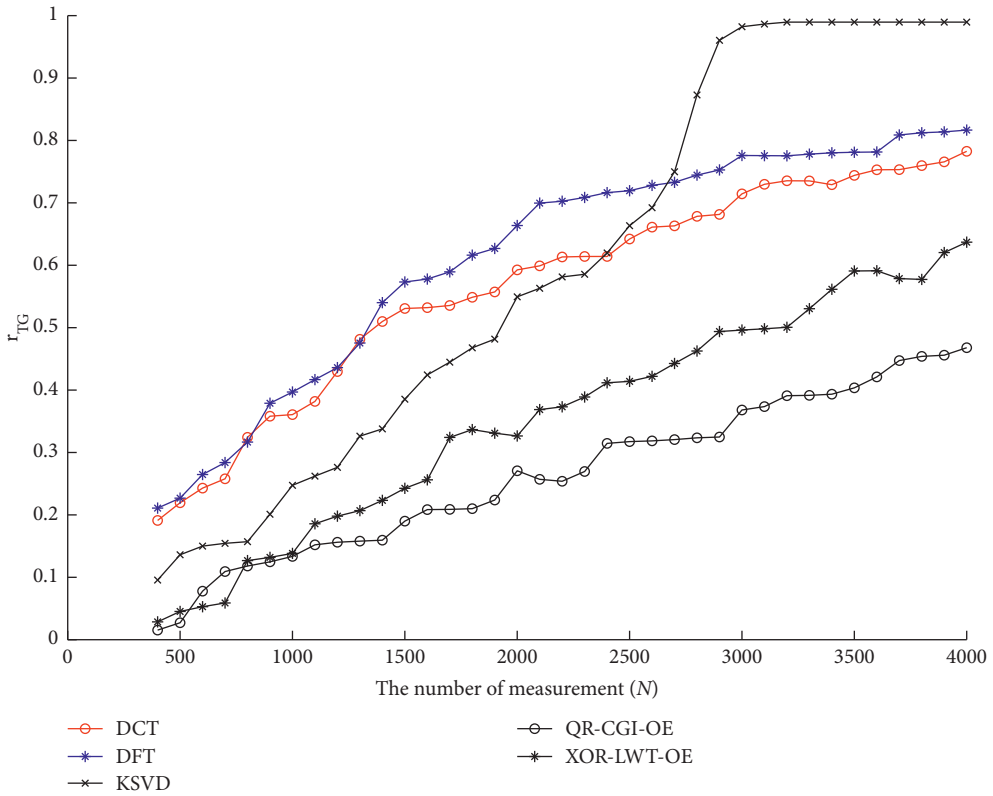


Figure 9: The relation curve of correlation coefficient r_{TG} with the measurement based on DCT, DFT, KSVD, QR-CGI-OE, and XOR-LWT-OE.

$$r_{TG} = \frac{E(T - E(T))(G - E(G))}{\sqrt{D(T)D(G)}}, \tag{23}$$

where $D(T)$ and $D(G)$ are the square deviations of the reconstructed image and the original image, respectively, $D(x) = (1/N)\sum_{i=1}^{N}(x_i - E(x))^2$ and $E(x) = (1/N)\sum_{i=1}^{N} x_i$. The larger the correlation coefficient, the better the imaging effect. Ideally, the correlation coefficient $r_{TG} = 1$.

In order to get a good reconstruction result, we performed a lot of experiments by changing the measurement N. The r_{TG} value of Figures 8(a)–8(c) is 0.2418, 0.5494, and 0.9533 Obviously, from left to right, the reconstructed image is getting better.

The comparison experiments for compressed sensing using different sparse basis such as DCT, DFT, and KSVD are conducted on Lena. Besides, simulation of QR-CGI-OE

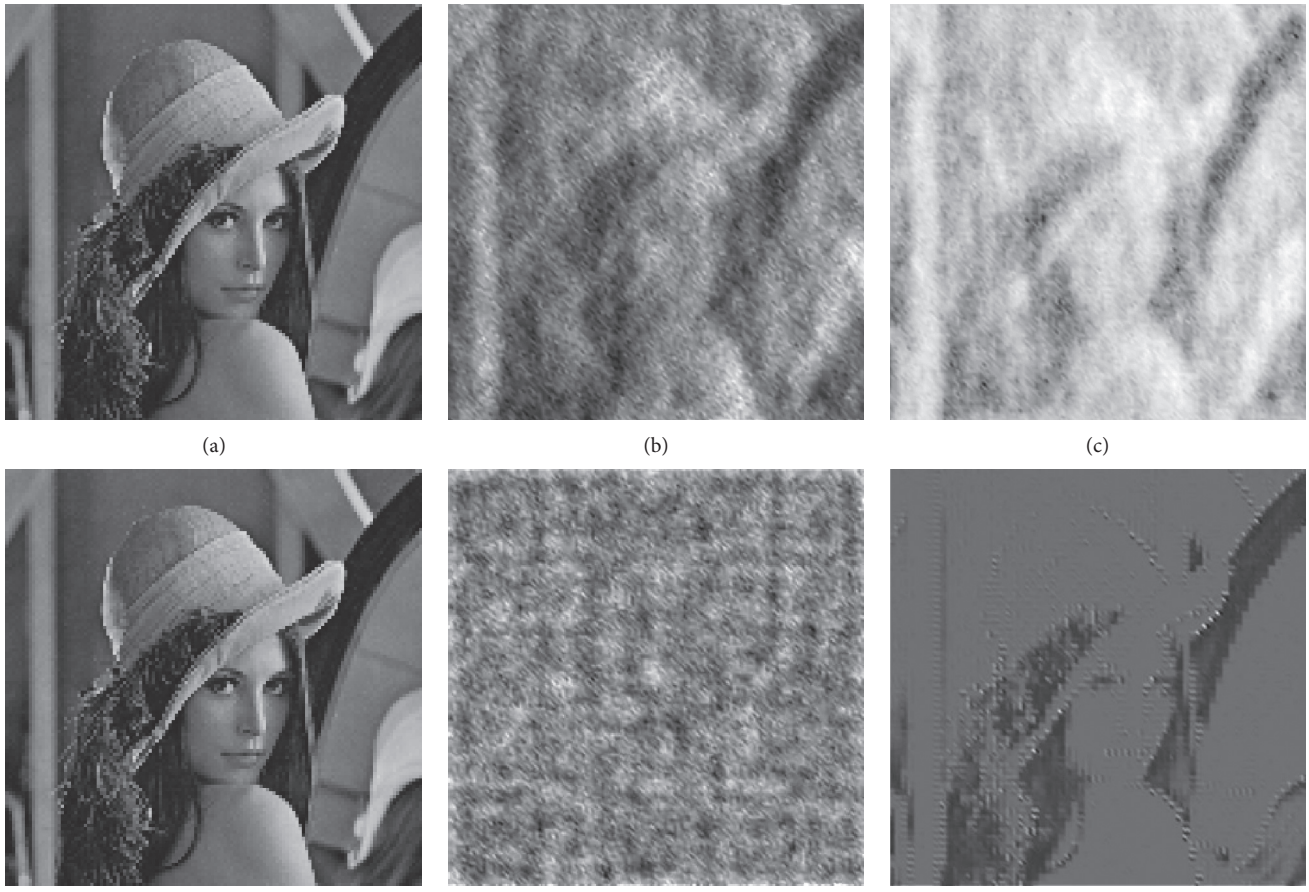


Figure 10: The reconstructed image based different sparse transformation. (a) The original image of Lena. (b–f) The reconstructed image based on DCT, DFT, and KSVD sparse representation, respectively, and QR-CGI-OE AND XOR-LWT-OE algorithms.

and XOR-LWT-OE is conducted in this experiment. Figure 9 shows the curve of the correlation coefficient change with the measurement based on several different means, the abscissa represents the number of measurements, the ordinate represents the correlation coefficient between the decrypted image and the original image. As shown in Figure 9, the correlation coefficient increases with the increase of measurement. The reconstructed image with high quality can be obtained with the increase of the measurement number. In addition, the result suggests that based on KSVD sparse representation, a high-quality image can be reconstructed in less measurements than other methods.

Make measurement 3000 times on Lena, and the reconstructed images are shown in Figures 10(b)–10(f). The r_{TG} value of DCT, DFT, QR-CGI-OE, XOR-LWT-OE, and KSVD is 0.7353, 0.7821, 0.4540, 0.6248, and 0.9729, respectively. Then, we compare maximum r_{TG} and measurements of KSVD with other sparse basics and algorithms, as shown in Table 4. By the way, after measuring 7100 times, the decrypted QR code can just be recognized and original image can be restored in QR-CGI-OE.

4.4. NIST Statistical Test. In this paper, the NIST SP 800-22 test suite [56] is used to analyse randomness and discover potential defects in the structure of the pseudorandom sequence generator. During the test, we used the default values that came with the NIST test. The test result is expressed as p. According to NIST test rules, to pass the test, p has to be greater than 0.01. The pseudorandom sequences generated by the hyper-chaotic map are successfully passed the NIST SP 800-22 statistical test. The test results are listed in Table 5.

Table 4: The best reconstructed r_{TG} and measurement of different sparse basis and other algorithms.

Sparse basis or algorithms	Max r_{TG}	Measurement
No sparse representation	0.8243	18000
DCT	0.8478	6400
DFT	0.8439	5300
QR-CGI-OE	0.8210	7100
XOR-LWT-OE	0.9343	6200
KSVD	**0.9729**	**3000**

4.5. Noise Addition. As the phase mask matrices may be attacked by noise, to test the robustness of this scheme, we add Gaussian noise, salt and pepper noise, and speckle noise on the phase mask matrices, respectively. As shown in Figure 11, Figure 11(a) is the decryption image when the

Table 5: NIST statistical test result.

Statistical test	X		Y		Z		W	
	p value	Result	p value	Result	p value	Result	p value	Result
Frequency	0.105232	Passed	0.150434	Passed	0.200545	Passed	0.331051	Passed
Block frequency	0.553902	Passed	0.426452	Passed	0.626177	Passed	0.788040	Passed
Runs	0.873186	Passed	0.072802	Passed	0.893688	Passed	0.216107	Passed
Longest run	0.713956	Passed	0.935258	Passed	0.497594	Passed	0.985966	Passed
Rank	0.357115	Passed	0.437155	Passed	0.771378	Passed	0.193581	Passed
FFT	0.291282	Passed	0.840006	Passed	0.186356	Passed	0.354010	Passed
Non-overlapping template	0.263903	Passed	0.640982	Passed	0.886167	Passed	0.433739	Passed
Overlapping template	0.121652	Passed	0.468763	Passed	0.969480	Passed	0.660406	Passed
Universal	0.522018	Passed	0.532899	Passed	0.257854	Passed	0.881329	Passed
Linear complexity	0.985256	Passed	0.847794	Passed	0.913437	Passed	0.824185	Passed
Serial test-1	0.271726	Passed	0.082269	Passed	0.368673	Passed	0.229263	Passed
Serial test-2	0.437868	Passed	0.130755	Passed	0.308462	Passed	0.182765	Passed
Approximate entropy	0.992196	Passed	0.939959	Passed	0.214085	Passed	0.105079	Passed
Cumulative sums	0.116982	Passed	0.083702	Passed	0.182438	Passed	0.182438	Passed
Random excursions	0.030601	Passed	0.058385	Passed	0.054319	Passed	0.200294	Passed
Random excursions variant	0.040671	Passed	0.470229	Passed	0.032714	Passed	0.042780	Passed

(a) (b) (c)

Figure 11: The decrypted images when the phase mask matrices are attacked by noise, and the measurement is 3000. (a) Gaussian noise: mean value is zero, variance is 0.005 and $r_{TG} = 0.9549$. (b) Salt and pepper noise: density is 0.005 and $r_{TG} = 0.9306$. (c) Speckle noise: mean is zero, variance is 0.01, and $r_{TG} = 0.9119$.

phase mask matrices are added; for Gaussian noise, mean value is zero and variance is 0.005 and $r_{TG} = 0.9549$; Figure 11(b) is added Salt and pepper noise, density is 0.005, and $r_{TG} = 0.9306$; Figure 11(c) is added speckle noise, mean is zero, variance is 0.01, and the $r_{TG} = 0.9119$. Obviously, the proposed scheme can resist noise attacks well.

5. Conclusion

In this paper, a CSGI encryption scheme based on hyper-chaotic-system and DNA and KSVD technology is proposed for the first time. The hyper-chaotic system is used to generate four long pseudorandom sequences, the sequences are diffused with DNA operation, and then the phase mask matrices for encryption can be obtained. The original image is sparse by dictionary D generated by KSVD. The transmission key of the scheme is composed with the initial values of the hyper-chaotic system and the dictionary D. Compared with the existing scheme, the proposed scheme has a small transmission key which ensures the security of the private key, big key space, highly sensitive to the key, high complexity, and strong plaintext correlation and ensures the security of the scheme. Simulation results and security analysis show that the proposed scheme can resist most of the known attacks well and has high security and great performance.

Data Availability

The data used to support the findings of the study are available from the corresponding author upon request.

Conflicts of Interest

All authors declare that they have no conflicts of interest.

Acknowledgments

This work was supposed by the Science and Technology Project of Hunan Provincial Communications Department, China (Grant No.2018037), and the National Nature Science Foundation of China (Grant nos. 61674054 and 91964108).

References

[1] D. N. Klyshko, "A simple method of preparing pure states of an optical field, of implementing the Einstein-Podolsky-Rosen experiment, and of demonstrating the complementarity principle," *Soviet Physics Uspekhi*, vol. 31, no. 1, pp. 74–85, 1988.

[2] T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," *Physical Review A*, vol. 52, no. 5, pp. R3429–R3432, 1995.

[3] R. S. Bennink, S. J. Bentley, and R. W. Boyd, "Two-Photon" coincidence imaging with a classical source," *Physical Review Letters*, vol. 89, no. 11, Article ID 113601, 2002.

[4] L. Tang, Y. Bai, C. Duan, S. Nan, Q. Shen, and X. Fu, "Effects of incident angles on reflective ghost imaging through atmospheric turbulence," *Laser Physics*, vol. 28, no. 1, Article ID 015201, 2017.

[5] Y. Gao, Y. Bai, and X. Fu, "Point-spread function in ghost imaging system with thermal light," *Optics Express*, vol. 24, no. 22, pp. 25856–25866, 2016.

[6] J. H. Shapiro, "Computational ghost imaging," *Physical Review A*, vol. 78, no. 6, Article ID 061802, 2008.

[7] P. Clemente, V. Durán, V. Torres-Company, and J. Lancis, "Optical encryption based on computational ghost imaging," *Optics Letters*, vol. 35, no. 14, pp. 2391–2393, 2010.

[8] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," *Applied Physics Letters*, vol. 101, no. 10, Article ID 101108, 2012.

[9] O. Katz, Y. Bromberg, and Y. Silberberg, "Compressive ghost imaging," *Applied Physics Letters*, vol. 95, no. 13, Article ID 131110, 2009.

[10] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Optics and Lasers in Engineering*, vol. 121, pp. 203–214, 2019.

[11] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2d-slim," *Optics and Lasers in Engineering*, vol. 134, Article ID 106178, 2020.

[12] V. Duran, P. Clemente, E. Tajahuerce et al., "Optical encryption with compressive ghost imaging," in *Proceedings of the 2011 Conference on Lasers & Electro-Optics Europe & 12th European Quantum Electronics Conference CLEO EUROPE/EQEC*, Munich, Germany, May 2011.

[13] S. Zhao, L. Wang, W. Liang, W. Cheng, and L. Gong, "High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique," *Optics Communications*, vol. 353, pp. 90–95, 2015.

[14] J. Wu, Z. Xie, Z. Liu, W. Liu, Y. Zhang, and S. Liu, "Multiple-image encryption based on computational ghost imaging," *Optics Communications*, vol. 359, pp. 38–43, 2016.

[15] J. Zhu, X. Yang, X. Meng et al., "Computational ghost imaging encryption based on fingerprint phase mask," *Optics Communications*, vol. 420, pp. 34–39, 2018.

[16] X. Li, X. Meng, X. Yang et al., "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme," *Optics and Lasers in Engineering*, vol. 102, pp. 106–111, 2018.

[17] G. Álvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[18] H. Lin, C. Wang, and Y. Tan, "Hidden extreme multistability with hyperchaos and transient chaos in a Hopfield neural network affected by electromagnetic radiation," *Nonlinear Dynamics*, vol. 99, no. 3, pp. 2369–2386, 2020.

[19] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2322–2335, 2019.

[20] H. Lin, C. Wang, Y. Sun, and W. Yao, "Firing multistability in a locally active memristive neuron model," *Nonlinear Dynamics*, vol. 100, no. 4, pp. 3667–3683, 2020.

[21] Y. Wang, T. Lei, X. Zhang, C. Li, and S. Jafari, "Hyperchaotic oscillation in the deformed rikitake two-disc dynamo system induced by memory effect," *Complexity*, vol. 2020, Article ID 8418041, 10 pages, 2020.

[22] Q. Deng, ""Multi-scroll hidden attractors with two stable equilibrium points," *Chaos*," *An Interdisciplinary Journal of Nonlinear Science*, vol. 29, Article ID 093112, 2019.

[23] X. Zhang, C. Wang, W. Yao, and H. Lin, "Chaotic system with bondorbital attractors," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2159–2174, 2019.

[24] C. Xu, J. Sun, and C. Wang, "An image encryption algorithm based on random walk and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 30, no. 4, Article ID 2050060, 2020.

[25] F. Yu, Z. Zhang, L. Liu et al., "Secure communication scheme based on a new 5D multistable four-wing memristive hyperchaotic system with disturbance inputs," *Complexity*, vol. 2020, no. 9, pp. 1–16, 2020.

[26] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm," *Optics and Lasers in Engineering*, vol. 128, Article ID 105995, 2020.

[27] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[28] C. Xu, J. Sun, and C. Wang, "A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems," *Multimedia Tools and Applications*, vol. 79, no. 9-10, pp. 5573–5593, 2020.

[29] F. Yu, L. Liu, H. Shen et al., "Dynamic analysis, circuit design, and synchronization of a novel 6D memristive four-wing hyperchaotic system with multiple coexisting attractors," *Complexity*, vol. 2020, Article ID 5904607, 17 pages, 2020.

[30] J. Li and H. Liu, "Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," *IET Information Security*, vol. 7, no. 4, pp. 265–270, 2013.

[31] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[32] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[33] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[34] L. Liu, Q. Zhang, and X. Wei, "A rgb image encryption algorithm based on DNA encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[35] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, 2018.

[36] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Engineering Applications of Artificial Intelligence*, vol. 25, no. 4, pp. 753–765, 2012.

[37] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Optics and Lasers in Engineering*, vol. 77, pp. 118–125, 2016.

[38] G. Chen and T. Ueta, "Yet another chaotic attractor," *International Journal of Bifurcation and Chaos*, vol. 9, no. 7, pp. 1465-1466, 1999.

[39] F. Yu, L. Liu, H. Shen et al., "Multistability analysis, coexisting multiple attractors and FPGA implementation of Yu-Wang four-wing chaotic system," *Mathematical Problems in Engineering*, vol. 2020, Article ID 7530976, 16 pages, 2020.

[40] F. Yu, S. Qian, X. Chen et al., "A new 4D four-wing memristive hyperchaotic system: dynamical analysis, electronic circuit design, shape synchronization and secure communication," *International Journal of Bifurcation and Chaos*, vol. 30, no. 10, Article ID 2050147, 2020.

[41] Q. Deng, C. Wang, and L. Yang, "Four-Wing hidden attractors with one stable equilibrium point," *International Journal of Bifurcation and Chaos*, vol. 30, no. 6, Article ID 2050086, 2020.

[42] F. Yuan, Y. Deng, Y. Li, and G. Chen, "A cascading method for constructing new discrete chaotic systems with better randomness," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 5, Article ID 053120, 2019.

[43] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Article ID 107484, 2020.

[44] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, Article ID 1950115, 2019.

[45] J. Sun, C. Li, T. Lu, A. Akgul, and F. Min, "A memristive chaotic system with hypermultistability and its application in image encryption," *IEEE Access*, vol. 8, 2020.

[46] X. Zheng, J. Xu, and W. Li, "Parallel DNA arithmetic operation based on n-moduli set," *Applied Mathematics and Computation*, vol. 212, no. 1, pp. 177–184, 2009.

[47] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[48] X. Wang, Y. Wang, X. Zhu, and S. Unar, "Image encryption scheme based on Chaos and DNA plane operations," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26111–26128, 2019.

[49] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.

[50] K. A. K. Patro, B. Acharya, and V. Nath, "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation," *IETE Technical Review*, vol. 37, no. 3, pp. 223–245, 2019.

[51] K. A. K. Patro, M. P. J. Babu, K. P. Kumar, and B. Acharya, "Dual-layer DNA-encoding-decoding operation based image encryption using one-dimensional chaotic map," in *Proceedings of the Advances in Data and Information Sciences–ICDIS 2019*, pp. 67–80, Agra, India, March 2019.

[52] L. M. Zhang, K. H. Sun, W. H. Liu, and S. B. He, "A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations," *Chinese Physics B*, vol. 26, no. 10, pp. 98–106, 2017.

[53] Y. Bromberg, O. Katz, and Y. Silberberg, "Ghost imaging with a single detector," *Physical Review A*, vol. 79, no. 5, Article ID 053840, 2009.

[54] N. Yujun, W. Xingyuan, W. Mingjun, and Z. Huaguang, "A new hyperchaotic system and its circuit implementation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3518–3524, 2010.

[55] T. T. Cai and L. Wang, "Orthogonal matching pursuit for sparse signal recovery with noise," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4680–4688, 2011.

[56] A. L. Rukhin, J. Soto, J. R. Nechvatal et al., "SP 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Applied Physics Letters*, vol. 22, no. 7, pp. 1645–2179, 2010.