Hyperchaotic Bilateral Random Low-Rank Approximation Random Sequence Generation Method and Its Application on Compressive Ghost Imaging

Songyuan Tan[1,2], Jingru Sun[1,2*], Yiping Tang[2], Yichuang Sun[3] and Chunhua Wang[2]

[1*]Research Institute of Hunan University in Chongqing, Yubei District, 400039,Chongqing, China.
[2]College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, Hunan Province, China.
[3]School of Engineering and Computer Science, University of Hertfordshire, Hatfield, AL10 9AB, UK.

*Corresponding author(s). E-mail(s): jt_sunjr@hnu.edu.cn; Contributing authors: Tansongyuan@hnu.edu.cn; tangyiping@hnu.edu.cn; y.sun@herts.ac.uk; wch1227164@hnu.edu.cn;

Abstract

Hyperchaotic systems have been widely used in the field of communication and information security to generate random numbers due to their super-long sequences, pseudo-randomness, and unpredictability. However, chaotic systems still have certain periodicity and security risks. To improve the reliability of chaotic random sequences, in this paper, a new method of generating chaotic random sequences based on random bilateral projection is proposed. Through random bilateral projection algorithm, the matrix formed by chaotic sequences is decomposed into a noiseless low-rank matrix, sparse matrix, and noise matrix, and the noise matrix is retained as a random sequence, which can effectively remove the regular factors to improve the randomness of the generated sequence. To verify the effectiveness of the proposed sequence generation method, we apply it to the compressive ghost imaging encryption system, and through simulation verified that compared with the existing algorithms, the proposed random sequence generation method has better efficiency and randomness, and can improve the security and efficiency of the compressive ghost imaging system.

Keywords: bilateral random projection, hyperchaotic, image encryption, compressive ghost imaging

1 Introduction

Random number is the core of modern cryptography. A random and unpredictable random number is the security guarantee of modern secure communication[1]. The generation of random numbers has been one of the most popular research topics in recent years[2]. According to different entropy sources, random numbers can be divided into physical random numbers and pseudorandom numbers. The physical random number is generated by the natural unpredictability of random processes such as coin toss, dice roll, electronic noise, and photon noise, but the noise value of the physical random number generation method is too small and difficult to extract, cannot meet the requirements of the current communication system for long random sequence. Common pseudorandom number generation methods include linear feedback shift register [3, 4], Mason rotation algorithm [5], cellular automata [6], linear congruence generator [7], etc. In the process of pseudo-random number generation, a random number sequence with a balanced distribution of ’0’ and ’1’ can be generated by adjusting the algorithm parameters, which has the advantages of a high generation rate and easy access. The security of pseudo-random numbers depends on the complexity of the algorithm. With the improvement of computer computing ability, they are vulnerable to violent attacks and are cracked [8, 9]. Therefore, how to find a pseudo-random number generation algorithm with fast generation speed, high complexity, and not easy to be attacked has become the focus of pseudo-random number research.

Chaotic systems, due to their complex dynamic characteristics, inherent randomness, long-term unpredictability, and sensitivity to initial values [10, 11], have become widely used in cryptography, resulting in the emergence of a new research field known as chaotic cryptography [12, 13]. In particular, chaotic systems have become a common method for generating pseudorandom sequences. Chaotic systems can be divided into one-dimensional chaotic systems(ODCS) and high-dimensional hyperchaotic systems(HDHS). One-dimensional chaotic system is represented by one-dimensional logic map [14, 15], Sine map [16], tent map [17], and Hénon Map [18], etc. A lot of new ODCSs are generated from the above chaotic map. Hu et al. introduced a coupled chaotic system based on unit transformation [19], which can combine any two one-dimensional chaotic maps together to generate a new one-dimensional chaotic map with better performance. Zhou et al. proposed a new one-dimensional chaotic system by combining two existing seed maps. This results in larger chaotic ranges and better chaotic behavior [20].

One-dimensional chaotic system shows satisfactory chaotic behavior, but it is vulnerable to brute force attack due to its characteristics of fewer system parameters and simple chaotic orbit. HDHS has longer chaotic sequences and more complex chaotic behaviors and trajectories [21, 22]. Therefore, many stream cipher algorithms based on HDHS have been proposed[23–26]. Ghebleh et al have proposed a stream cipher algorithm based on the three-dimensional Arnold's cat map[27]. This algorithm has the ability to overcome sensitivity attacks. Chen et al have expanded the baker map to three dimensions, which is used to speed up the image encryption process[28]. Hua et al [29] propose a two-dimensional (2D) modular Chaotification system (2D-MCS) to improve the chaos complexity of any 2D chaotic map. [30] presented a stream cipher based on a two-dimensional coupled map lattice, in which the piecewise logistic map was used as the local chaotic map.

Researchers have proposed using memristor and neural networks to produce hyperchaotic systems, obtaining complex dynamic behaviors and providing new ideas for the construction of hyperchaotic systems[31–33]. Lai et al designed a Multiscroll Memristive Hopfield Neural Network yield multi double-scroll attractors[34]. Lin et al proposed designing multi-structure chaotic attractors in memristive neural networks[35].

However, chaotic systems realized on digital devices are subject to dynamic degradation. Although the generated chaotic orbit appears random, chaos is not entirely disordered[36, 37]. Once the chaotic sequence reaches a certain length, it becomes repetitive and predictable. As a result, the degradation of chaos-based stream ciphers can give rise to significant security risks[38]. Researchers in cryptography and chaotic systems have been exploring ways to eliminate repetition and achieve true randomness in chaotic sequences.

Bilateral random projection technology [39] is based on low-rank approximation, which decomposes the degenerate image matrix into low-rank matrix, sparse matrix, and noise matrix through image decomposition technology, where the low-rank matrix contains the regular information of the image, so it is widely used in image denoising. The noise matrix decomposes from the degenerate image matrix removes the regular information and has more randomness. Through bilateral random projection technology and a chaotic system, a new method to obtain natural random noise can be constructed.

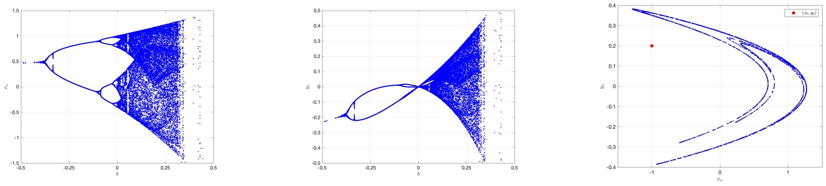
Based on the above analysis, this paper proposes a random sequence generation method based on bilateral random projection and HDHS. This method can effectively eliminate the regular information in the sequence, resulting in a genuinely random generated sequence. To verify the validity of the random sequence, we applied the generated random sequence to compressive sensing ghost image encryption system and achieved good encryption results.

The main contributions of this paper are as follows:

First, a method for generating random sequences using bilateral random projection technology and chaos systems is proposed. The random sequence generated by this method is closer to a true random sequence than that generated by a simple chaotic system.

Second, a more efficient compressive ghost imaging encryption architecture is proposed, which has higher execution efficiency and confidentiality.

The paper is organized as follows: in section 2, we briefly introduce the basic techniques of bilateral random projection technology, the employed chaotic system, and compressive ghost imaging technology; In section 3, a random sequence generated method based on bilateral random projection and chaotic system is proposed and verified; In section 4, we apply the proposed random sequence to the compressive ghost imaging encryption system, and carry out experimental verification and comparison; Finally, we conclude the paper.



(a)

(b)

(c)

Fig. 1: Classical Hénon Maps under a=1.4 and $b \in (-0.5, 0.5)$, Bifurcation graphs(a), (b) and trajectory graphs(c).

2 The Preliminary Knowledge

2.1 Improved Hénon Map

Classical Hénon map is a widely used discrete-time dynamic system that can produce chaotic phenomena. It is mathematically defined as

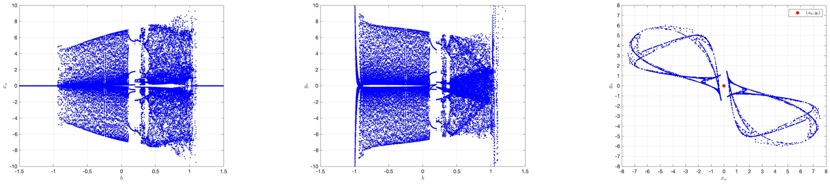
$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} . \tag{1}$$

When the parameter values are taken as $a = 1.4$ and $b = 0.3$ respectively, the chaotic system shows chaotic behavior. When a and b take other different values, the system can behave as a chaotic phenomenon, paroxysmal phenomenon, or converge to the periodic point, as shown in Fig. 1. The behavior characteristics of the system under different parameters can be seen from the track diagram.

However, from the mathematical equations, bifurcation diagrams, and trajectories, it can be seen that Hénon map has many remarkable characteristics.

First, their chaotic range is very narrow, the chaotic behavior is restricted to a specific range of parameters. As the number of parameters increases, the phase planes become less compact, leading their output values to diverge to infinity with the evolution of the system. Second, the scope of their confusion is discontinuous or even isolated. A small change in system parameters may transfer the parameters to the non-chaotic range. In addition, their output distribution is incomplete. Their trajectories can only access a small area on the phase plane and have obvious patterns. These characteristics may have negative impacts on some applications based on chaotic systems. Therefore, overcoming these shortcomings of the existing chaotic map can promote the application based on chaos. To solve the above problems, Hua et al. proposed a two-dimensional modular chaos system (2D-MCS) to improve the chaos complexity of any two-dimensional chaotic map[29]. Modular operation is a bounded operation, which can convert any input value into the range [0, N). Therefore, 2D-MCS can significantly improve the chaotic complexity of the existing two-dimensional chaotic map expand the chaotic range, and overcome the weaknesses of the existing two-dimensional chaotic map. Hénon's 2D-MCS can be expressed as

$$\begin{cases} x_{n+1} = (1 - \hat{a}x_n^2 + y_n) & mod\ N \\ y_{n+1} = \hat{b}x_n & mod\ N \end{cases}. \tag{2}$$



(a) (b) (c)

Fig. 2: Classical Zeraoulia-Sprott maps under a=3.8 and $b \in (-1.5, 1.5)$, Bifurcation graph (a), (b) and trajectory graph.

2.2 Improved Zeraoulia-Sprott Map

Zeraoulia-Sprott map designed by Zeraoulia and Sprott is a simple two-dimensional chaotic map, that can be denoted as Eq. (3), where a and b are its system parameters. As shown in Fig. 2, Zeraoulia-Sprott map has a rational fraction when $a = 3.8$ and $b = 0.6$, it shows classical chaotic behavior.

$$\begin{cases} x_{n+1} = \dfrac{-ax_n}{1 + y_n^2} \\ y_{n+1} = x_n + by_n \end{cases}. \tag{3}$$

Similarly, Zeraoulia-Sprott's 2D-MCS can be expressed as

$$\begin{cases} x_{n+1} = \dfrac{-\hat{a}x_n}{1+y_n^2} & mod\ N \\ y_{n+1} = (x_n + \hat{b}y_n) & mod\ N \end{cases}. \tag{4}$$

2.3 Bilateral Random Projection

Given a bilateral random projection (BRP) of a dense matrix $X \in R_{m\times n}(m>n)$, that is, $Y_1 = XA_1$ and $Y_2 = X^T A_2$, where $A_1 \in R_{m\times r}$ and $A_2 \in R_{n\times r}$ are Gaussian random matrices. Construct a fast rank-r approximation matrix L of X:

$$L = Y_1(A_2^T Y_1)^{-1} Y_2^T. \tag{5}$$

To improve the approximation accuracy of L, we use the original right random projection Y_1 to optimize the left projection matrix A_2, and then use Y_2 to optimize A_1. In particular, after $Y_1 = XA_1$, we update $A_2 = Y_1$, calculate the left random projection $Y_2 = X^T A_2$, then update $A_1 = Y_2$, and calculate the right random projection $Y_1 = XA_1$. Apply the new Y_1 and Y_2 to the above formula L, and a better low-rank approximation L will result. Here, the power scheme model is employed for optimization. Use matrix $\widetilde{X} = (XX^T)^q X$ instead of X to calculate bilateral random projection:

$$Y_1 = \widetilde{X}A_1, \quad Y_2 = \widetilde{X}^T A_2. \tag{6}$$

Then L is updated to $\widetilde{L}$:

$$\widetilde{L} = Y_1(A_2^T Y_1)^{-1} Y_2^T. \tag{7}$$

To further optimize the speed and accuracy of low-rank approximation to obtain the approximate value of X with rank r, we perform the QR decomposition of Y_1 and Y_2, namely:

$$Y_1 = Q_1 R_1, \quad Y_2 = Q_2 R_2. \tag{8}$$

Then the low-rank approximation of L can be rewritten as:

$$L = (\widetilde{L})^{\frac{1}{2q+1}} = Q_1[R_1(A_2^T Y_1)^{-1} R_2^T]^{\frac{1}{2q+1}} Q_2^T, \tag{9}$$

where q represents the number of cycles.

According to the low-rank decomposition theory, the degraded image matrix X can be decomposed into the sum of low-rank matrix L, sparse matrix S, and noise matrix N. The data before degradation can be approximated by low-rank matrix:

$$X = L + S + N. \tag{10}$$

In the formula (11), (12), $\| \bullet \|_F$ is the Frobenius norm, rank is the matrix rank, and card is the number of matrix components. L_t and S_t are the low-rank part and sparse part after t iterations respectively. S_t depends on the hard threshold of $X - L_t$, i.e.,

$$L_t = \underset{rank(L) \leq r}{\arg\min} \|X - L - S_{t-1}\|_F^2, \tag{11}$$

$$S_t = \underset{card(S) \leq k}{\arg\min} \|X - L_t - S\|_F^2, \tag{12}$$

$$S_t = \mathrm{wp}_k(X - L_t), \tag{13}$$

where wp_k $(X - L_t)$ is the matrix element hard threshold operator, which retains the largest k elements in $|X - L_t|$ and sets the other elements to 0. Repeat the above formula (11) to (13), until $\|X - L_t - S_t\|_F^2 / \|X\|_F^2$ is less than the set threshold, or the maximum number of iterations t_{max} is reached, the low-rank matrix L of X can be obtained.

2.4 Compressive Ghost Imaging

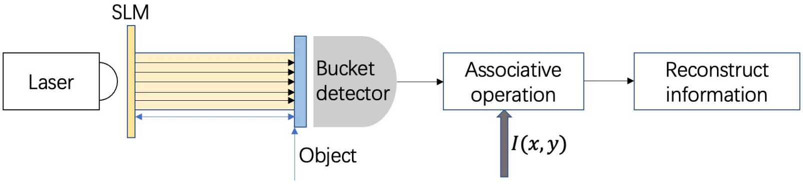


Fig. 3: Compressive ghost imaging scheme.

As shown in Fig. 3, an arbitrary phase mask matrix $\varphi(x, y)$ is introduced into the spatial light modulator (SLM), and the spatial laser beam is transmitted through the SLM to generate a spatial incoherent beam[40]. Given the distribution of random phase and incident light field $U_{in}(x, y)$, we can evaluate the distribution of light intensity $U_i(x, y)$ after SLM:

$$U_i\,(x, y) = U_{in}\,(x, y)\, e^{i\varphi_i(x,y)}. \tag{14}$$

After Fresnel diffraction, the light propagates to the object plane where the distance space modulator is z. The light field distribution of the signal light in front of the object plane is the same as that of the reference light. The object is a compressed image that has already been compressed using compressive sensing algorithms.

The speckle light field intensity $I_i(x, y)$ can be calculated according to Eq. (15),

$$I_i(x, y) = |U_i(x, y) \otimes h_z(x, y)|^2, \tag{15}$$

which is defined as the reference light, where $h_z(x, y)$ is the transfer function at the distance z in the spatial domain, and $\otimes$ represents the convolution operation.

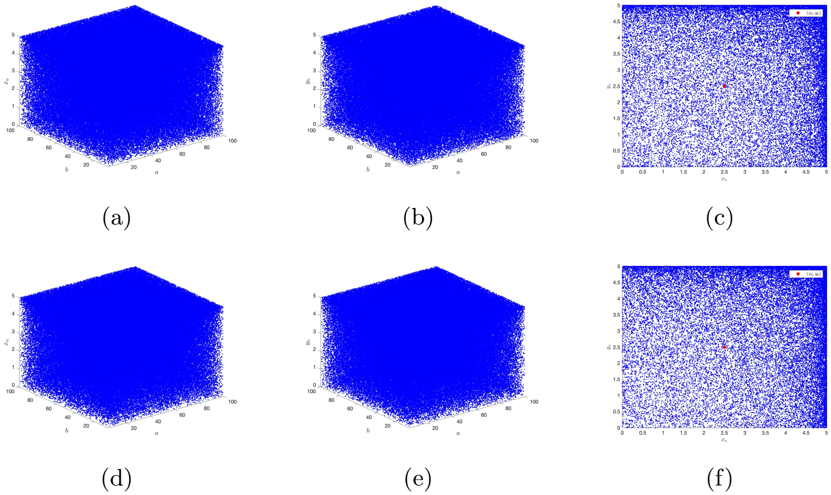
The transfer function $T(x, y)$ of the object is used to represent the signal light intensity received by the bucket detector placed behind the object. This function modulates the light field, as shown in Eq. (16).

$$B_i(x, y) = \int dxdyI_i(x, y)T(x, y). \tag{16}$$

To reconstruct the transmission function $T(x, y)$ of the object, the receiver correlates the calculated reference light intensity $I_i(x, y)$ with the received signal light intensity $B_i(x, y)$, which can be described as:

$$G(x, y) = \frac{1}{N}\sum_{i=1}^{N}(B_i(x, y) - B(x, y))I_i(x, y), \tag{17}$$

where $G(x, y)$ represents the recovered object information, $(1/N)\sum \cdot$ calculates the ensemble average of N measurements, and B represents the average value of the measured component B_i.



(a) (b) (c)

(d) (e) (f)

Fig. 4: Bifurcation and trajectory diagrams of 2D-MCS, (a)-(c)Hénon's 2D-MCS, (d)-(f)Zeraoulia-Sprott's 2D-MCS.

2.5 Orthogonal Matching Pursuit Algorithm

The basic principle of the OMP algorithm: For a non-homogeneous linear system of equations, given A and b, to recover x, it is necessary to fully utilize the sparsity of x, where b is a linear combination of the column vectors of matrix A, which is the result obtained by weighting x with the column vectors of matrix A. Due to the sparsity of x, it indicates that only a few column vectors in A contribute to b. Identify these column vectors that contribute significantly to b, and at the same time, based on the positions of the column vectors in A, the positions of the non-zero elements in x can be determined.

The detailed process of the OMP algorithm is as follows:

The inputs of the algorithm are the measurement matrix $X \in R^{N\times d}$, the observation vector $y \in R^N$, and the sparsity W of the signal x under sparse transformation basis Ψ. The output of the algorithm is the estimated value $\widetilde{x}$ of the ideal signal. $\Lambda_m (m = 1, 2, ..., d)$ is an index set, and residual $r_m \in R^N$.

Step 1: Initialize the residual $r_0 = y$, index set $\Lambda_0 = \emptyset$, measurement matrix $\Phi = \emptyset$, iteration number $t = 1$, and the result of signal x after sparse transformation is s.

Step 2: Search for index λ_t. By solving formula (18), the index λ_t corresponding to subscript t can be found.

$$\lambda_t = \arg\max_{j\notin\Lambda_{t-1}} |\langle r_{t-1}, \varphi_j\rangle|, \tag{18}$$

where $\varphi_j (j = 1, 2, ..., d)$ is the column vector of the measurement matrix $\Phi = [\varphi_1\varphi_2...\varphi_d]$.

Step 3: Update index set and measurement matrix. $\Lambda_t = \Lambda_{t-1} \cup \lambda_t$, $\Phi_t = [\Phi_{t-1}\varphi_{\lambda_t}]$.

Step 4: Using the least squares method to solve formula (19):

$$s_t = \arg\min_{s} \|\Phi_t\widetilde{s} - y\|_2. \tag{19}$$

Step 5: Update residual $r_t = y - \Phi_t\widetilde{s}_t$, $t = t + 1$.

Step 6: If $t < W$, return to step 2.

Step 7: The estimated value of the final output s is $\widetilde{s} = \widetilde{s}_t$, and the estimated value of the signal $\widetilde{x}$ is obtained using formula (20).

$$\widetilde{x} = \Psi\widetilde{s}. \tag{20}$$

3 Random Sequence Generation Method and Its Application

3.1 Random Sequence Generation Method

In this part, an improved Hénon Map, an improved Zeraoulia-Sprott map, and a bilateral random projection algorithm are employed to construct a really random sequence.

3.1.1 Performance Analysis of Chaotic System

In Fig. 4. (a)-(c) are the bifurcation diagrams and trajectory diagrams of Hénon's 2D-MCS, and (d)-(f) are the bifurcation diagrams and trajectory diagrams of Zeraoulia-Sprott's 2D-MCS, both number of mod operations is 5. It can be seen that under all given parameter settings, the variables x and y can randomly access the entire region of the phase plane, and the output can be randomly distributed on the entire phase plane. This shows that the improved 2D - MCS chaotic map has more complex chaotic behavior and wider chaotic range than the original chaotic map, and can achieve robust chaotic behavior.

The Lyapunov Exponent (LE) represents the numerical characteristics of the average exponential divergence rate of adjacent trajectories in phase space. Fig. 5 (a) (b) show the LE of classical Hénon and Zeraoulia-Sprott, and Fig. 5 (c) (d) show the LE of Hénon's 2D-MCS and Zeraoulia-Sprott's 2D-MCS. The improved chaotic system not only has positive and more extensive LEs in all parameter settings but also has two positive LEs, showing hyperchaotic behavior.

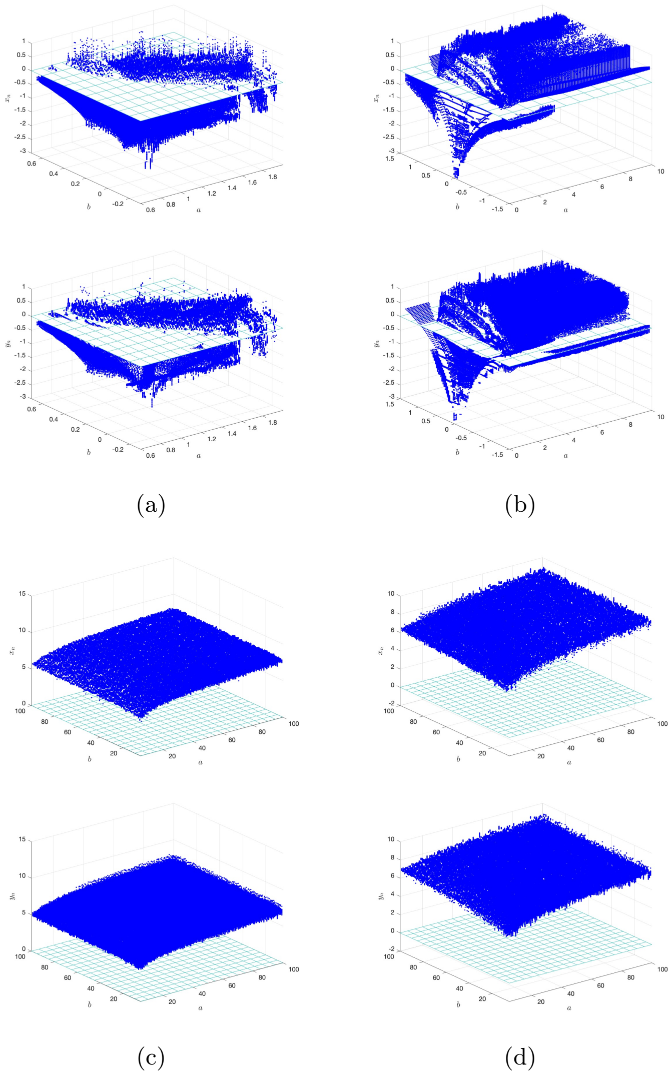
3.1.2 Random Sequence Generation Process

Assume that the original image size is $M \times M$. As shown in Fig 6, there are 5 steps in the random sequence process.

Step 1: Set the initial value, and iteratively generate four pseudorandom sequences with the length of $M + R$, where $R = M \times M/4$. The first M of each pseudorandom sequence will be discarded to eliminate the transient effect;

Step 2: Discard the first M of each pseudorandom sequence, and then combine the four pseudorandom sequences to generate a sequence X with a length of $R \times 4$, and reconstruct the sequence X into a matrix with a size of $M \times M$. According to section 2.3, initialize low-rank matrix L, sparse matrix S, and Gaussian random matrix A_1, set $L = X$, $S = 0$.

Step 3: Optimize $\hat{L} = [(X - S_{t-1})(X - S_{t-1})^T]^q (X - S_{t-1})$. Calculate the right random projection matrix $Y_1 = LA_1$, and update $A_2 = Y_1$. Calculate the left random projection matrix $Y_2 = L^T A_2$, and update $A_1 = Y_2$. If the number of cycles does not reach $q + 1$ (To simplify the calculation, q is set to 1.), cyclically update Y_1 and Y_2. Otherwise, proceed to the next step.



(a)

(b)

(c)

(d)

Fig. 5: Two LEs of different 2D chaotic systems. (a)Hénon map, (b)Zeraoulia-Sprott map, (c)Hénon's 2D-MCS, (d)Zeraoulia-Sprott's 2D-MCS.

Step 4: Calculate the QR decomposition of Y_1 and Y_2 to further solve $L = (\widetilde{L})^{\frac{1}{2q+1}} = Q_1[R_1(A_2^T Y_1)^{-1} R_2^T]^{\frac{1}{2q+1}} Q_2^T$. Make $S = |X - L|$, keep the elements larger than 140 in $|X - L|$, and set other elements to 0.

Step 5: Calculate the noise matrix $N = X - L - S$ as the random sequence.

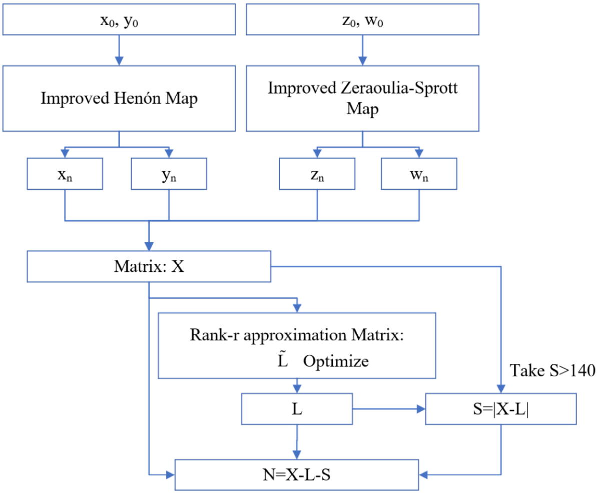


Fig. 6: Flow chart of random sequence generation.

3.2 Compressive Ghost Image Encryption Scheme

The encryption process is as follows:

Step 1: Input the plaintext image and key, sparsely represent the original image using the KSVD algorithm[40], and obtain the dictionary matrix D and the sparse image.

Step 2: Construct the phase mask matrix N of SLM with the random sequence generated in section 3.1.2 and perform phase modulation on the laser beam.

Step 3: The distance between the image and the SLM is z. By Fresnel diffraction, the light field intensity $I_i(x, y)$ can be obtained before the image according to formula (15).

Step 4: After the light is irradiated onto the image, the barrel detector receives the total light intensity. Total light intensity $B_i(x, y)$ is calculated according to formula (16).

Step 5: If Measurement K times, repeat step 2-4 K times. To obtain K phase mask matrixes and K signal intensities.

Step 6: The initial value of the chaotic system is transmitted through a private channel as the transmission key. $B_i(x, y)$ is transmitted through a common channel.

Decryption process:

Step 1: The receiver receives the transmission key through a private channel and calculates N random phase mask matrices using the received transmission key according to the method in section 3.1.2.

Step 2: Obtain N random phase mask matrices, to get the same light field intensity $I_i(x, y)$ with the Fresnel diffraction theorem as step 3 in section 3.2.

Step 3: Associate the calculated light field intensity $I_i(x, y)$ with the total light intensity received from the common channel according to formula (17), and reconstruct the original image using the OMP algorithm and dictionary D.

4 Simulation Results and Security Analysis

To verify the feasibility of the proposed solution, we conducted simulations using MATLAB R2016a.

4.1 Simulation Results

Select "Lena", "Pepper", and "Baboon" grayscale images with a size of 128 * 128 as the original images for testing, as shown in Fig. 7. (a)-(c). Obtain K different random phase mask matrices according to the method proposed in section 3.1.2, where the random phase mask matrix is shown in Fig 7. (d)-(f). Fig. 7. (g)-(i) show their sparse matrix respectively. Fig. 7. (j)-(l) shows the reconstruction results of this scheme, and it can be seen that the reconstruction effect is good.

4.2 Key Sensitivity Analysis

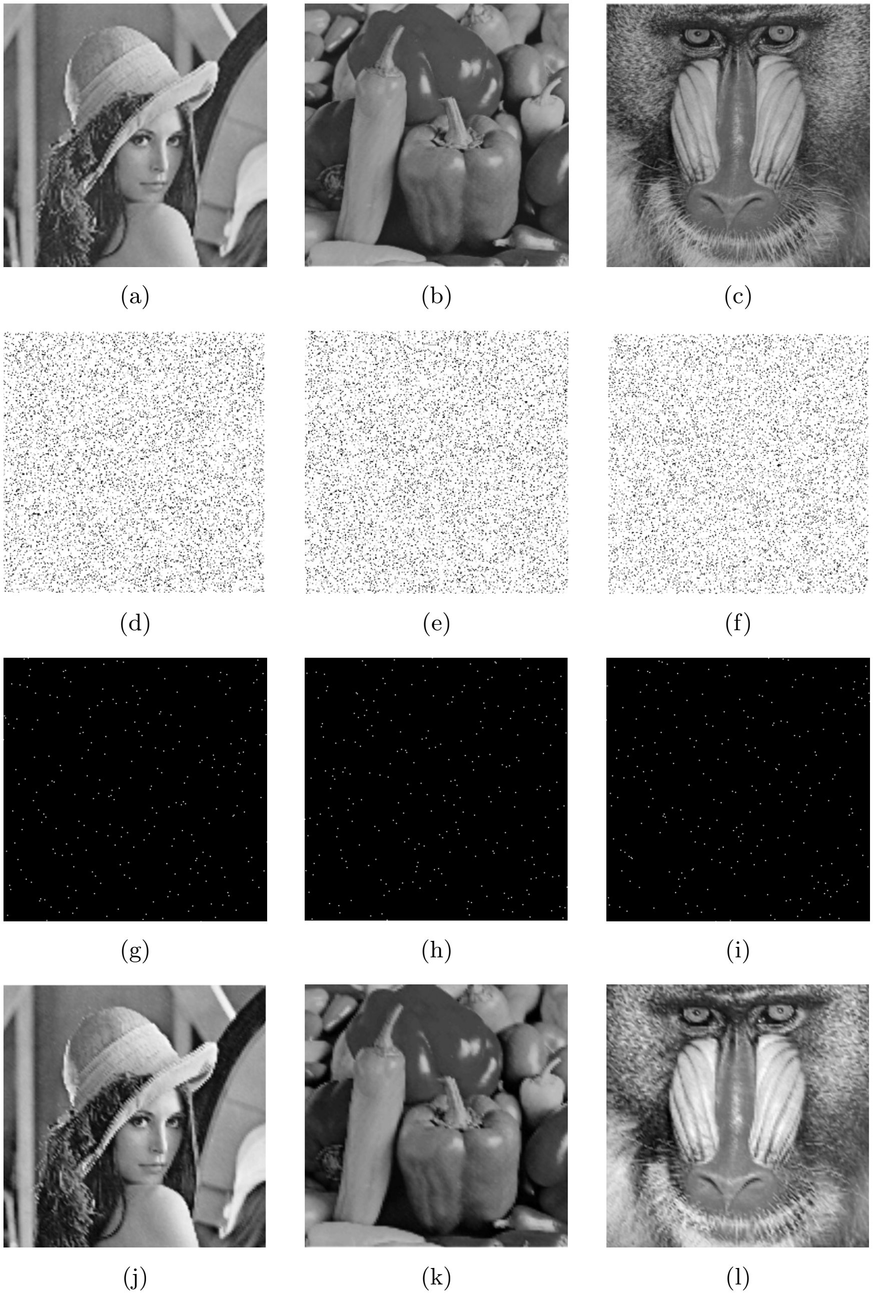
The key sensitivity of chaotic ciphers refers to the sensitivity of the initial state of the chaotic map and the sensitivity of the control parameters. During the encryption and decryption process, if there is a slight change in the initial key, information related to the plaintext image cannot be obtained, resulting in image reconstruction failure. This paper sets the initial private keys to x_0=3.11; $y_0 = 0.566$; $z_0 = 3$; w_0=0.5. During the decryption process, modify the private keys to $x_0 = 3.11 + 10^{-15}$; $y_0 = 0.566$; $z_0 = 3$; $w_0 = 0.5$. As shown in Fig 8, it is evident that when the initial key is slightly changed, the original image cannot be restored, satisfying the key sensitivity requirements.

4.3 Correlation Analysis

The correlation coefficient is the linear description of the degree of approximation between the two. Generally speaking, the closer to 1, the more closely the two have a linear relationship, and the better the imaging effect. The quality of the reconstructed image can be evaluated by calculating the correlation coefficient between the reconstructed image G and the plaintext image T using the formula,

$$r_{TG} = \frac{E(T - E(T))(G - E(G))}{\sqrt{D(T)D(G)}}, \tag{21}$$

where $D(T)$, and $D(G)$ are the variances of the reconstructed image and the original image, respectively. $D(x) = (1/K)\sum_{i=1}^{K}(x_i - E(x))^2$ and $E(x) = (1/K)\sum_{i=1}^{K} x_i$. Fig. 9 shows the reconstructed images under different measurement times, with r_{TG} values from (a) to (d) being 0.2829, 0.5041, 0.8618, and



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Fig. 7: Encryption and decryption results of different samples, where (a)-(c) are the original images, (d)-(f) are the random phase mask matrices, (g)-(i) are sparse matrixes of original images, (j)-(l) are reconstruction images.

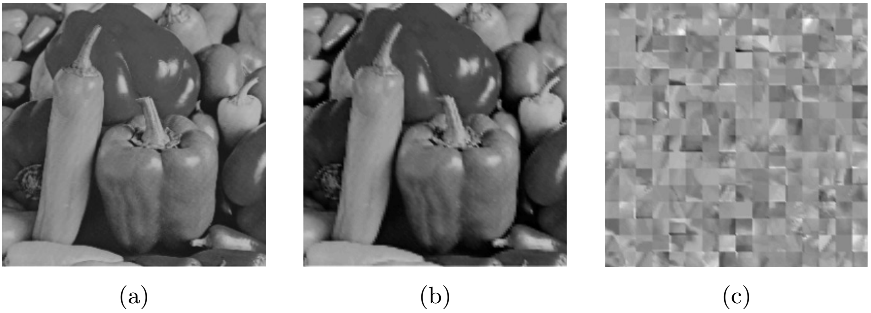


Fig. 8: Result of key sensitivity analysis. (a) Original image pepper, (b) Reconstructed image with correct keys, (c) Reconstructed image with error keys.

0.9978. It can be indicated that the closer r_{TG} is to 1, the better the reconstructed image effect.

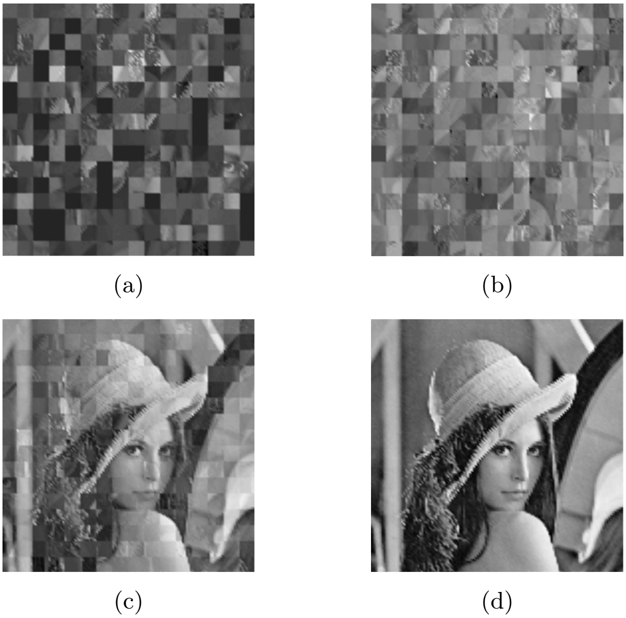


Fig. 9: Reconstructed images under different measurement times. (a) Measurement times=1000, (b) Measurement times=2000, (c) Measurement times=2800, (d) Measurement times=3000.

4.4 Sparse Method Analysis

We compare compressed sensing sparse methods KSVD with DCT and DFT. Fig. 10 shows the comparison results. It can be observed that after approximately 2700 reconstructions, the reconstruction effect based on KSVD sparse representation is outstanding. When the number of reconstructions reaches around 3000, the r_{TG} value of the reconstructed image based on KSVD sparse representation can achieve an almost perfect score of 1, while the r_{TG} value of the reconstructed image based on DCT and DFT sparse representation is less than 0.8. This is sufficient to demonstrate that the image reconstruction scheme based on KSVD is excellent.

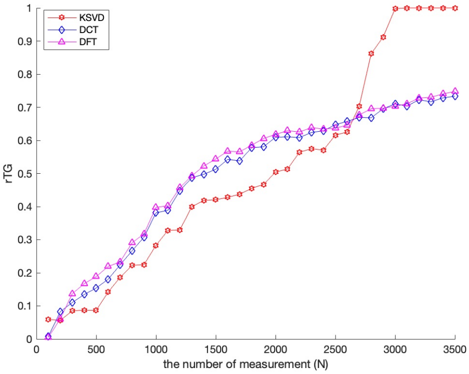
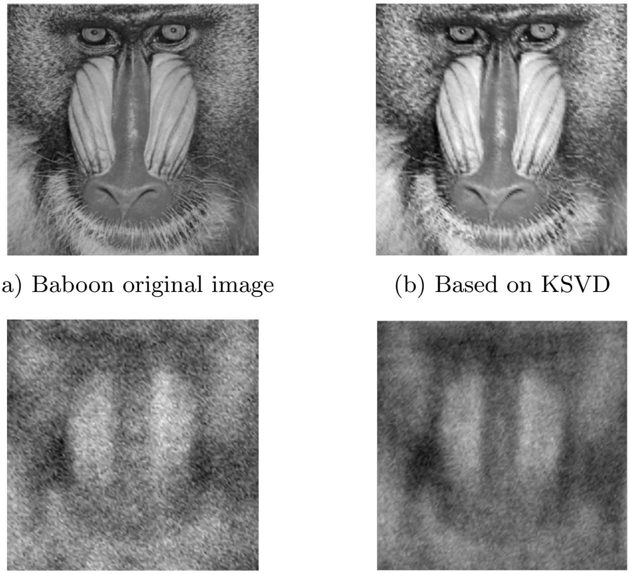


Fig. 10: Relationship curve of correlation coefficient and measurement frequency based on sparse representations of KSVD, DCT, and DFT.



(a) Baboon original image

(b) Based on KSVD

(c) Based on DCT

(d) Based on DFT

Fig. 11: Reconstructed image based on KSVD, DCT, DFT sparse representation.

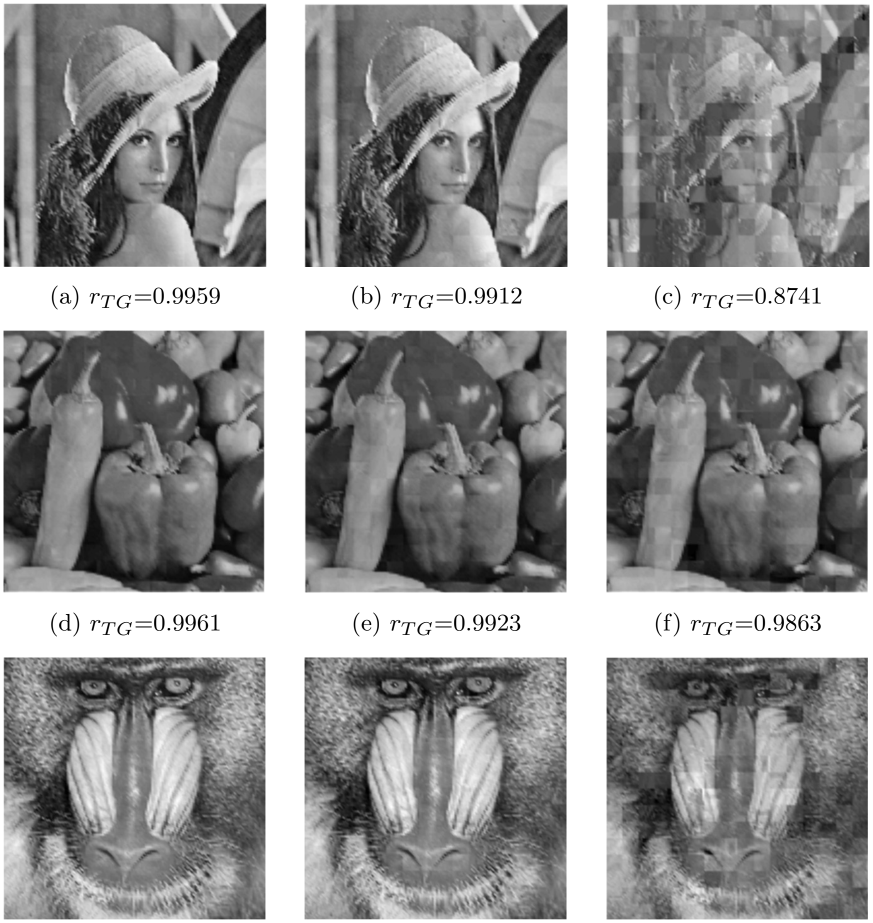
Fig. 11 shows the reconstructed images based on different sparse methods for 3000 measurements, with the r_{TG} values of 1, 0.6442, and 0.8433 for (b)-(d) respectively.

4.5 Noise Attack Analysis

In practical situations, the system operation process may be affected by environmental factors such as noise attacks. Therefore, we need to test the robustness of the system to demonstrate that the scheme has good noise resistance performance. To simulate the situation of the phase mask matrix under noise attack, we added Gaussian noise to the phase mask matrix. Fig. 12 shows the reconstructed image of the phase mask matrix under Gaussian noise attack with a mean of 0 and different variances for 3000 measurements (the variances of Gaussian noise added to the phase mask matrix from left to right for each row of images are 0.05, 0.1, and 0.2 respectively).

Observing the decrypted image, it can be seen that the scheme has high robustness and can effectively resist noise attacks.

From the relationship curve in Fig. 10, it can be seen that as the number of measurements increases, the correlation coefficient increases. Therefore, when the noise is high, we can also increase the number of measurements appropriately to reduce the impact of noise. Gaussian noise with a mean of 0 and



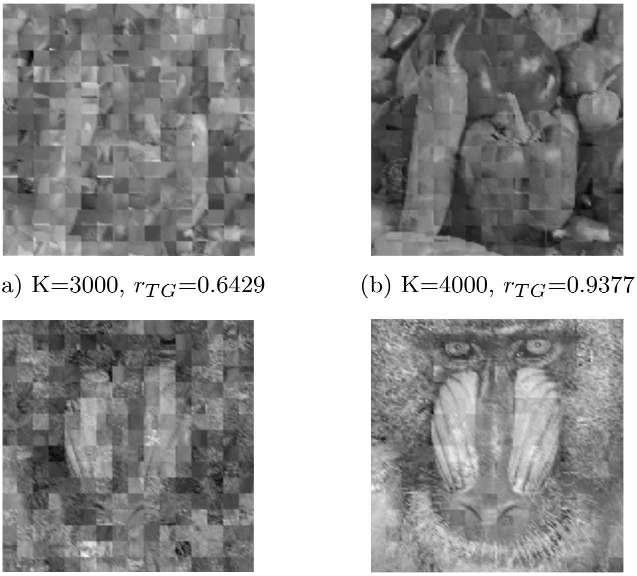
(a) r_{TG}=0.9959 (b) r_{TG}=0.9912 (c) r_{TG}=0.8741

(d) r_{TG}=0.9961 (e) r_{TG}=0.9923 (f) r_{TG}=0.9863

(g) r_{TG}=0.9964 (h) r_{TG}=0.9908 (i) r_{TG}=0.9236

Fig. 12: Reconstructed images of phase mask matrices under Gaussian noise attacks with 0.05, 0.1, and 0.2 variances (from left to right).

a variance of 0.5 was added to the phase mask matrix, as shown in Fig. 13. When the number of measurements reached 4000, the reconstruction effect was significantly improved compared to 3000.



(a) K=3000, r_{TG}=0.6429

(b) K=4000, r_{TG}=0.9377

(c) K=3000, r_{TG}=0.6430

(d) K=4000, r_{TG}=0.9208

Fig. 13: Reconstructed images under high Gaussian noise interference.

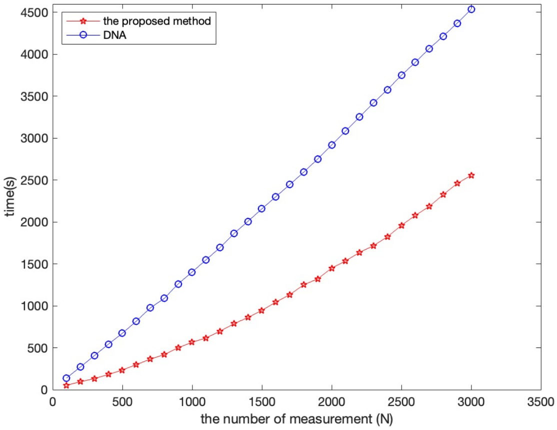


Fig. 14: Comparison curve of encryption system running time.

4.6 Efficiency Analysis

This paper enhances the randomness of chaotic sequences by using bilateral random projection algorithm, which also improves its execution efficiency. To demonstrate, we compared system execution time with reference [40], which used DNA encoding and decoding method to generate SLM. As shown in Fig. 14, two curves represent the time it takes for the entire system to run after using DNA diffusion and the method proposed in this paper to process chaotic sequences under the same number of measurements. The encryption system proposed in this paper has greatly improved its operational efficiency.

4.7 NIST Statistical Testing

The NIST random number testing method is a standardized testing method used to evaluate the quality of random number generators. This testing method includes a series of statistical tests to detect whether a random number sequence has characteristics such as uniformity, independence, and long periodicity. Through these tests, it can be determined whether a random number generator is safe and reliable enough. We use the NIST SP 800-22 random number test set to verify the quality of the random number generator [41, 42]. The test results are shown in Table. 1. All P-Values are greater than 0.01, pass the NIST request.

Table 1: NIST statistical test result

Statistical test	P-Value	Result
Frequency	0.739918	Passed
Block frequency	0.355920	Passed
Cumulative sums	0.534146	Passed
Runs	0.519628	Passed
Longest run	0.696792	Passed
Rank	0.739918	Passed
FFT	0.532620	Passed
Non-overlapping template	0.350485	Passed
Overlapping template	0.122325	Passed
Universal	0.213309	Passed
Approximate entropy	0.267986	Passed
Random excursions	0.159079	Passed
Random excursions variant	0.173900	Passed
Serial test-1	0.066882	Passed
Serial test-2	0.510663	Passed
Linear complexity	0.416601	Passed

5 Conclusion

This paper proposed a bilateral random projection based hyperchaotic random sequence generation method. The method first employs hyperchaotic systems to generate original random sequences, then utilizes bilateral random projection and low-rank decomposition theory to enhance the randomness, by removing regular factors from the sequence. We employed the random sequence generation method to realize the compressive ghost imaging encryption system. The experiment result shows that the proposed random sequence generation method can generate high randomness sequences. The generated random phase mask matrix is applied to the compressive ghost imaging encryption system based on KSVD sparse representation, and compared with the previous work the scheme proposed in this paper can reduce the system running time, improve imaging efficiency, and has higher robustness.

Acknowledgments. This work was supported by the National Natural Foundation of China (62171182), the Natural Science Foundation Project of Chongqing, Chongqing Science and Tech Commission n (CSTB 2022NSCQ-M SX0770)

Data Availability. Data sharing is not applicable to this article, as no datasets were generated or analyzed during the current study.

Declarations

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

References

[1] Yu, F., Li, L., Tang, Q., Cai, S., Xu, Q.: A survey on true random number generators based on chaos. Discrete Dynamics in Nature and Society **2019**(1), 1–10 (2019)

[2] Hullermeier, E., Rifqi, M.: A Fuzzy Variant of the Rand Index for Comparing Clustering Structures. In: in Proc. IFSA/EUSFLAT Conf., pp. 1294–1298 (2009)

[3] Lewis, T.G., Payne, W.H.: Generalized feedback shift register pseudorandom number algorithm. Journal of the ACM **20**(3), 456–468 (1973)

[4] Gonzalez-Diaz, V.R., Pareschi, F., Setti, G., Maloberti, F.: A pseudorandom number generator based on time-variant recursion of accumulators. IEEE Transactions on Circuits Systems II Express Briefs **58**(9), 580–584 (2011)

[5] Matsumoto, M., Nishimura, T.: Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Transactions on Modeling and Computer Simulation **8**(1), 3–30 (1998)

[6] Cerda, J.C., Martinez, C.D., Comer, J.M., Hoe, D.H.K.: An efficient FPGA random number generator using lfsrs and cellular automata. In: 2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 912–915 (2012)

[7] Kao, C., Wong, J.Y.: An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus smaller than 2. Journal of Statistical Computation Simulation **54**(1-3), 29–35 (1996)

[8] Shannon, C.E., Shannon, C.: Communication theory of secrecy systems. Bell Systems Technical Journal **28**(4), 656–715 (1949)

[9] Wang, X., Yu, H.: How to break MD5 and other hash functions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 19–35 (2005). Springer

[10] Lin, H., Wang, C., Du, S., Yao, W., Sun, Y.: A family of memristive multibutterfly chaotic systems with multidirectional initial-based offset boosting. Chaos, Solitons Fractals **172**, 113518 (2023)

[11] Ma, J.: Energy function for some maps and nonlinear oscillators. Applied Mathematics and Computation **463**, 128379 (2024)

[12] Ma, X., Wang, C., Qiu, W., Yu, F.: A fast hyperchaotic image encryption scheme. International Journal of Bifurcation and Chaos **33**(05), 2350061 (2023)

[13] Zhu, Y., Wang, C., Sun, J., Yu, F.: A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. Mathematics **11**(3) (2023)

[14] Wang, C., Wang, X., Xia, Z., Zhang, C.: Ternary radial harmonic fourier moments based robust stereo image zero-watermarking algorithm. Information Sciences **470**, 109–120 (2019)

[15] May, R.M.: Simple mathematical models with very complicated dynamics. Nature **261**(5560), 459–467 (1976)

[16] Pak, C., Huang, L.: A new color image encryption using combination of the 1D chaotic map. Signal Processing **138**(SEP.), 129–137 (2017)

[17] Li, C., Luo, G., Qin, K., Li, C.: An image encryption scheme based on chaotic tent map. Nonlinear Dynamics **87**, 127–133 (2017)

[18] Suneel, M.: Cryptographic pseudo-random sequences from the chaotic Hénon map. Sadhana **34**(5), 689–701 (2006)

[19] Hu, G., Li, B.: Coupling chaotic system based on unit transform and its

applications in image encryption. Signal Processing **178**, 107790 (2021)

[20] Zhou, Y., Bao, L., Chen, C.L.P.: A new 1d chaotic system for image encryption. Signal Processing **97**, 172–182 (2014)

[21] Yu, F., Liu, L., Qian, S., Li, L., Huang, Y., Shi, C., Cai, S., Wu, X., Du, S., Wan, Q.: Chaos-based application of a novel multistable 5D memristive hyperchaotic system with coexisting multiple attractors. Complexity **2020**, 1–19 (2020)

[22] Ding, D., Wang, J., Wang, M., Yang, Z., Wang, W., Niu, Y., Xu, X.: Controllable multistability of fractional-order memristive coupled chaotic map and its application in medical image encryption. The European Physical Journal Plus **138**(10), 908 (2023)

[23] Ma, X., Wang, C.: Hyper-chaotic image encryption system based on N+ 2 ring Joseph algorithm and reversible cellular automata. Multimedia Tools and Applications, 1–26 (2023)

[24] Cheng, S., Sun, J., Xu, C.: A color image encryption scheme based on a hybrid cascaded chaotic system. International Journal of Bifurcation and Chaos **31**(09), 2150125 (2021)

[25] Xu, C., Sun, J., Wang, C.: A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems. Multimedia Tools and Applications **79**(9-10), 5573–5593 (2020)

[26] Lai, Q., Hu, G., Erkan, U., Toktas, A.: A novel pixel-split image encryption scheme based on 2d salomon map. Expert Systems with Applications **213**, 118845 (2023)

[27] Ghebleh, M., Kanso, A.: A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation **19**(6), 1898–1907 (2014)

[28] Mao, Y.B., Chen, G.R., Lian, S.G.: A novel fast image encryption scheme based on 3D chaotic baker maps. International Journal of Bifurcation and Chaos in Applied Sciences and Engineering (10), 14 (2004)

[29] Hua, Z., Zhang, Y., Zhou, Y.: Two-dimensional modular chaotification system for improving chaos complexity. IEEE Transactions on Signal Processing **68**, 1937–1949 (2020)

[30] Liu, Z., Wang, Y., Zhao, Y., Zhang, L.Y.: A stream cipher algorithm based on 2D coupled map lattice and partitioned cellular automata. Nonlinear Dynamics **101**, 1383–1396 (2020)

[31] Ma, M., Xiong, K., Li, Z., He, S.: Dynamical behavior of memristor-coupled heterogeneous discrete neural networks with synaptic crosstalk. Chinese Physics B (2023)

[32] Lai, Q., Yang, L., Chen, G.: Design and performance analysis of discrete memristive hyperchaotic systems with stuffed cube attractors and ultraboosting behaviors. IEEE Transactions on Industrial Electronics, 1–10 (2023)

[33] Bao, H., Chen, Z., Chen, M., Xu, Q., Bao, B.: Memristive-cyclic hopfield neural network: spatial multi-scroll chaotic attractors and spatial initial-offset coexisting behaviors. NONLINEAR DYNAMICS (2023)

[34] Lai, Q., Wan, Z., Zhang, H., Chen, G.: Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption. IEEE Transactions on Neural Networks and Learning Systems **34**(10), 7824–7837 (2023)

[35] Lin, H., Wang, C., Xu, C., Zhang, X., Iu, H.H.: A memristive synapse control method to generate diversified multistructure chaotic attractors. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **42**(3), 942–955 (2022)

[36] Hu, Z., Wang, C.: Hopfield neural network with multi-scroll attractors and application in image encryption. Multimedia Tools and Applications, 1–21 (2023)

[37] Xie, Z., Sun, J., Tang, Y., Tang, X., Simpson, O., Sun, Y.: A K-SVD based compressive sensing method for visual chaotic image encryption. Mathematics **11**(7), 1658 (2023)

[38] Arroyo, D., Li, C., Li, S., Alvarez, G., Halang, W.A.: Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos, Solitons Fractals **41**(5), 2613–2616 (2009)

[39] Zhou, T., Tao, D.: Bilateral random projections. In: International Symposium on Information Theory (2012)

[40] Sun, J., Peng, M., Liu, F., Tang, C.: Protecting compressive ghost imaging with hyperchaotic system and DNA encoding. Complexity **2020**, 1–13 (2020)

[41] Pareschi, F., Rovatti, R., Setti, G.: On statistical tests for randomness included in the nist sp800-22 test suite and based on the binomial distribution. IEEE Transactions on Information Forensics and Security **7**(2), 491–505 (2012)

[42] Zhu, S., Ma, Y., Lin, J., Zhuang, J., Jing, J.: More powerful and reliable second-level statistical randomness tests for nist sp 800-22, pp. 307–329 (2016). Springer