Content-adaptive image compression and encryption via optimized compressive sensing with double random phase encoding driven by chaos

Zhihua Gan¹ · Xiuli Chai² · Jianqiang Bi³ · Xiuhui Chen²

Received: 28 July 2021 / Accepted: 26 November 2021 / Published online: 24 January 2022
© The Author(s) 2022

Abstract

With the advancement of multimedia technology and coming of big data era, the size of image data is significantly increased. However, the traditional image encryption methods cannot solve the emerging problems of efficient compression. To settle with this challenge, an effective content-adaptive image compression and encryption method based on compressive sensing and double random phase encoding (DRPE) is proposed in this paper. The original image is converted to one low-frequency part and three high-frequency parts by DWT and then permuted by sorting-based chaotic sequences. Afterward, a novel measurement matrix optimization algorithm based on adaptive step size is presented to measure the high-frequency components. To enhance the security of the scheme, the DRPE, quantization, and diffusion are successively performed on the complex matrix composed of the shuffled low-frequency component and three measurement value matrices to obtain the cipher image. Logistic-Sine chaotic system is utilized to produce the chaotic keystreams for the encryption process, and its system parameter and initial value are determined by the information entropy of the plain image and external key parameters, so that the proposed cipher can withstand known-plaintext and chosen-plaintext attacks effectively. Numerical experiments demonstrate the effectiveness of the proposed image compression and encryption algorithm.

Keywords Image compression and encryption · Chaotic system · Compressive sensing (CS) · Double random phase encoding (DRPE)

Introduction

With the rapid development of multimedia technology and the arrival of big data era, more and more high-resolution images are sampled, transmitted, and stored over the Internet. Some of them may contain private information. Therefore, compressing and encrypting images before transmission are necessary [1]. Recently, many image encryption methods have been introduced based on chaotic systems [2–4], such

as DNA sequence operations [5, 6], cellular automata [7], optical transform [8, 9], and others. However, these schemes cannot efficiently compress the images to save the transmission and storage pressures. Compressive sensing (CS) may compress, encrypt, and sample the plain image simultaneously [10–12], and some image encryption algorithms based on CS have been proposed accordingly.

In CS-based image encryption, measurement matrix (MM) is used as secret key [13], and it may be transmitted from the sender to the receiver for decryption. In the early age, the transmission of the whole measurement matrix may occupy huge amounts of storage space and transmission bandwidth [14, 15], which makes the secret key too large to be effectively distributed and stored. To settle this issue, chaotic systems are used to construct measurement matrix, and less parameters may get larger measurement matrix for CS. For instance, Zhou et al. [16] introduced a novel image compression–encryption hybrid algorithm based on key-controlled MM in CS, wherein the measurement matrices were generated by utilizing the circulant matrices and determining the

✉ Xiuli Chai
chaixiuli@henu.edu.cn

¹ School of Software, Intelligent Data Processing Engineering Research Center of Henan Province, Institute of Intelligent Network System, Henan University, Kaifeng 475004, China

² School of Artificial Intelligence, Henan University, Kaifeng 475004, China

³ School of Computer and Information Engineering, Henan Key Laboratory of Big Data Analysis and Processing, Henan University, Kaifeng 475004, China

original row vectors of the circulant matrices with one 1D logistic map. Huang et al. [17] proposed a compression–diffusion–permutation method for securing image, MM of CS was the Hadamard matrix generated by iterating a 2D Sine-Logistic modulation map, and using only a few keys of this chaos avoided the transmission and storage of the ordinary Gaussian matrix. In [18], a chaotic matrix was first produced by computing 1D logistic map with the initial value, and this matrix was quantified into -1 or 1 to get the Bernoulli random matrix for CS. Recently, Wang et al. [19] provided an adjustable visual image cryptosystem based on 6D hyperchaotic system and compressive sensing, 3D Chen chaotic system was applied to provide the measurement matrix of CS, and only three initial values need to be transmitted. In this article, 1D Logistic-Sine chaotic system (LSS) is utilized to generate the MM for CS.

Besides, the performance of MM may affect the quality of the reconstructed images [20], and some scholars devote to present high-performance MMs. For example, Endra et al. [21] optimized the MM by use of the modified closed equiangular tight frame. Luo et al. [22] generated a chaos-combined asymptotic deterministic random measurement matrix (CADRMM) by use of the Logistic map and Lissajous map to generate more random chaotic sequences. In [23], an asymptotical deterministic random measurement matrix based on information entropy and counter (ADM-MIC) was given to compress the plain image, 2D-LSCM chaotic system was utilized to generate the MM, and its parameters were controlled by information entropy of the plain image, so that random-like sequences may give more random MM and high-precision recovered images. In [24], 1D LSS was utilized to produce low-dimensional matrices, and then, they were extended with Kronecker product (KP) to get high-dimensional matrices, and the final measurement matrices were obtained by optimizing them with singular value decomposition (SVD). In this paper, a measurement matrix optimization algorithm based on adaptive step size is designed to improve the quality of the reconstructed image.

It is generally known that CS-based image encryption cannot attain perfect secrecy but computational secrecy [25]. Thus, some image encryption methods are combined with CS to enhance the security levels. Such as, a joint image compression–encryption scheme based on entropy coding and compressive sensing is given in [26], the higher bit planes of the plain image are manipulated entropy coding and the lower ones are performed CS compression. Sun et al. [27] provided an image encryption method based on CS and hyperchaotic map, row/column cyclic shift, and diffusion based on Galois field multiplication are utilized to upgrade the security level. Zhou et al. [28] proposed an image compression and encryption scheme by use of 2D CS and fractional Mellin transform, the plain image was measured from two directions to obtain the measurement value matrix,

and then, nonlinear fractional Mellin transform was utilized to confuse it. An image encryption algorithm based on memristive chaotic system, elementary cellular automata (ECA), and CS was presented in [29], the original image was processed by DWT to obtain the sparse coefficient matrix, and then, zigzag shuffling and ECA were combined to confuse the coefficient matrix to upgrade the reconstruction quality. Huo et al. [30] combined DNA encoding with CS to give a novel image compression–encryption hybrid scheme, the plain image was processed by DNA encryption, and then, the resulting image was measured by CS to find the cipher image.

It is no denying that although there are so many CS-based image encryption algorithms, some of them still have the shortcomings in the compression and security. For example, the relation of the image encryption method and plain image is a bit less, so that it is vulnerable to withstand chosen-plaintext and known-plaintext attacks; the quality of the recovered image is lower especially in the high compression condition; besides, the randomness of the final cipher image gotten by some ciphers is unsatisfactory to make it resist entropy attack, et al.

Inspired by the above analyses, an effective content-adaptive image compression and encryption scheme based on compressive sensing and double random phase encoding (DRPE) is presented in this paper. Specifically, a measurement matrix optimization method for CS is designed, step size of gradient descent may be adjusted adaptively, and the stability of the algorithm is guaranteed. Besides, the integration of CS and DRPE may not only save hardware resources, but also improve the security of the proposed cipher. The contributions of our work can be summarized as follows:

1. We propose an effective image compression and encryption scheme by integrating CS and DRPE. CS is applied for compressing the plain image to narrow its size, and DRPE is used for diffusing the plain image to improve the security level of the proposed cipher.
2. We compress the plain image selectively by use of importance of the plain image, which can attain the balance of high-quality reconstruction image and high compression performance.
3. This paper designs a measurement matrix optimization algorithm based on adaptive step size, the threshold function is combined with Barzilai–Borwein method, Armijo criterion, and equiangular tight frame, so that the step size can be adjusted adaptively in the iteration, convergence speed of the algorithm is improved, and the stability of the algorithm is ensured.
4. The proposed cipher is highly sensitive to the plain image, and it is plain-image-content-adaptive. Logistic-Sine chaotic system is used to generate the chaotic keystreams for CS, DRPE, and diffusion, and its sys-

Fig. 1 Optical encryption setup based on DRPE

tem parameter and initial value are calculated by the information entropy of the plain image and external key parameters, so that different keystreams are produced for different original image, and the proposed cipher can resist known-plaintext and chosen-plaintext attacks effectively.

The rest of this paper is organized as follows. “**Preliminaries**” give the preliminaries, such as double random phase encoding, gram matrix and cross-correlation coefficient, overall correlation coefficient, QR decomposition, and gradient descent method. The proposed measurement matrix optimization algorithm and image compression and encryption scheme are depicted in “**The proposed measurement matrix optimization algorithm**” and “**The presented image compression and encryption scheme**”. Performance analyses of measurement matrix optimization algorithm and image compression and encryption algorithm are demonstrated in “**Performance analyses of measurement matrix optimization algorithm**” and “**Performance analyses of image compression and encryption algorithm**”, respectively. Finally, this paper is concluded in “**Conclusion**”.

Preliminaries

Double random phase encoding

Since optical encryption has many merits, such as parallel computation, fast running speed, and processing data in various transform domains, it attracts wide attention from researchers. Among them, double random phase encoding (DRPE) is an effective method and applied for image encryption [31]. As shown in Fig. 1, optical encryption setup based on DRPE mostly consists of two phase plates and two optical lens. The plain image is encoded randomly by the first phase plate, and then, the obtained image is converted to frequency domain by use of the Fourier transform of the first optical lens; subsequently, the gotten frequency data are encoded randomly by the second phase plate, and then, the cipher

image is found by performing inverse Fourier transform on it. The whole encryption process may be represented by

$$\Psi(x, y) = \text{FT}^{-1} \{ \text{FT} \{ f(x, y) \exp[i2\pi n(x, y)] \cdot \exp[i2\pi b(x, y)] \} \}, \quad (1)$$

where FT denotes the Fourier transform, FT^{-1} is its inverse operation, $f(x, y)$ is the plain image, $\Psi(x, y)$ is the cipher image, and $n(x, y)$ and $b(x, y)$ are two random phases.

Gram matrix and cross-correlation coefficient

The less the cross-correlation coefficient between the measurement matrix and sparse coefficient matrix is, the lower the correlation between them is, and the better the quality of the reconstructed image is. The cross-correlation coefficient may be computed by the following steps.

Let sparse coefficient matrix be $\Psi \in R^{N \times N}$, and measurement matrix be $\Phi \in R^{M \times N}$, and the multiplication between them is $D = \Phi\Psi$. The new matrix $\tilde{D}$ is obtained by manipulating normalized operation on every column of D , the maximum cross-correlation coefficient $\mu(D)$ between arbitrary two column vectors of $\tilde{D}$ may be computed by [32]

$$\mu(D) = \max_{i \neq j} \left\{ \frac{|d_i^T d_j|}{\|d_i\| \cdot \|d_j\|} \right\} = \max_{i \neq j} \left\{ |\tilde{d}_i^T \tilde{d}_j| \right\}, \quad (2)$$

where d_i and $\tilde{d}_i$ denote the column vectors of D and $\tilde{D}$, respectively, and $(\cdot)^T$ means the matrix transpose.

The Gram matrix G may be obtained by $G = \tilde{D}^T \tilde{D}$, and the maximum cross-correlation coefficient may be gotten by [33]

$$\mu = \max_{i \neq j} |g_{ij}|, \quad (3)$$

where g_{ij} is the element at row i and column j of G . Accordingly, the average cross-correlation coefficient μ_{av} of G may be defined as [34]

$$\mu_{av} = \frac{1}{n(n-1)} \sum_{i,j=1, i \neq j}^n |g_{ij}|, \quad (4)$$

where n is the total number of matrix elements.

To recover the original signal in CS, the following condition should be met [35]:

$$M > cK \cdot \mu^2(D) \cdot \log(N), \quad (5)$$

where N is the length of the signal, and parameter $c > 0$. From Eqs. (2–5), one may watch that when the cross-correlation coefficient $\mu(D)$ is less, the correlation of Φ and Ψ is lower [35], and the uncorrelation between them is stronger. Therefore, to improve the effect of reconstruction algorithm, one may optimize the measurement matrix by reducing the cross-correlation coefficient.

To find the minimum cross-correlation, an optimization method of measurement matrix based on equiangular tight frame (ETF) was proposed in [36], and then, Welch boundary is obtained [37]. For a certain space $R^{M \times N}$, the minimum value of cross-correlation coefficient μ is called as Welch boundary, that is, $\mu \geq \sqrt{(N-M)/(M(N-1))}$. If and only if the column vector of matrix D satisfies ETF, the inner product of any two columns of D is equal to $\sqrt{(N-M)/(M(N-1))}$, the equal sign in the above inequality holds, and here, M, N are the row and column of matrix Φ , respectively. Let $\mu(D) = \sqrt{(N-M)/(M(N-1))}$, and then, according to Eq. (6), the elements of Gram matrix G are contracted to make it approach to the ETF, and finally, the matrix H is obtained, and h_{ij}, g_{ij} are the elements located at the i th row and the j th column of H and G , respectively

$$h_{ij} = \begin{cases} \mu(D) \cdot \text{sign}(g_{ij}), & \mu(D) \leq |g_{ij}| \\ g_{ij}, & \mu(D) > |g_{ij}| \end{cases}. \quad (6)$$

Overall correlation coefficient

Reducing the square of non-zero eigenvalues of Gram matrix may effectively reduce the overall correlation coefficient between measurement matrix and sparse matrix. One finds that [38]

$$\sum_{s=1}^m \lambda_s = n \quad (7)$$

$$\sum_{s=1}^m (\lambda_s)^2 = \sum_{i,j}^n \left[\langle \tilde{d}_i, \tilde{d}_j \rangle \right]^2, \quad (8)$$

where λ_s ($s = 1, 2, \dots, m$) is the m th eigenvalue of Gram matrix, and $\tilde{d}_i$ is the i th column of $\tilde{D}$. From the definition of Gram matrix, it is evident that

$$\langle \tilde{d}_i, \tilde{d}_j \rangle = g_{ij}. \quad (9)$$

Normalize the column of $\tilde{D}$ to find that

$$g_{ij} = \langle \tilde{d}_i, \tilde{d}_j \rangle = 1. \quad (10)$$

Assuming that $\mu_{\text{all}} = \sum_{i \neq j} (g_{ij})^2$ is the overall correlation coefficient, and it may be expressed as

$$\begin{aligned} \mu_{\text{all}} &= \sum_{i \neq j} (g_{ij})^2 = \sum_{i,j=1}^n (g_{ij})^2 - \sum_{i=1}^n (g_{ii})^2 \\ &= \sum_{i,j=1}^n \left[\langle \tilde{d}_i, \tilde{d}_j \rangle \right]^2 - n = \sum_{s=1}^m (\lambda_s)^2 - n. \end{aligned} \quad (11)$$

Combining Eq. (7) with Eq. (11), the problem of minimizing overall correlation coefficient can be transformed into the following optimization problem:

$$\min \mu_{\text{all}} = \sum_{s=1}^m (\lambda_s)^2 - n \quad \text{s.t.} \quad \sum_{s=1}^m \lambda_s = n. \quad (12)$$

From Eq. (12), one may see that when the square sum $\sum_{s=1}^m (\lambda_s)^2$ of the eigenvalues of the Gram matrix is minimum, the global correlation coefficient μ_{all} may get the minimum value. Since $\sum_{s=1}^m \lambda_s = n$, when $\lambda_1 = \lambda_2 = \dots = \lambda_n = n/m$, μ_{all} may reach the minimum. Specifically, first, find the eigenvalues of Gram matrix, then set all the non-zero eigenvalues as the average value n/m , which not only makes the sum of the eigenvalues constant, but also renders the square sum of the eigenvalues the lowest [39].

QR decomposition

First, the measurement matrix Φ is decomposed by standard QR decomposition to obtain matrix Q and R . As for R , its principal diagonal elements are much larger than the non-diagonal elements [40], and then, one sets all non-diagonal elements to 0 to get matrix $\hat{R}$; thus, the new measurement matrix $\hat{\Phi} = Q\hat{R}$ is obtained. The detailed steps are as follows.

Step 1: First, get a random measurement matrix $\Phi = R^{M \times N}$;

Step 2: Perform transpose operation on matrix Φ to get Φ^T , and then manipulate QR decomposition on Φ^T to obtain $\Phi^T = QR$;

Step 3: Make all the non-diagonal elements of matrix R be zero to obtain the matrix $\hat{R}$;

Step 4: $\hat{\Phi}$ is obtained by replacing R with $\hat{R}$ in step 2, and then, its transpose $\hat{\Phi}^T$ is the optimized result.

Through the above steps, the minimum singular value of the measurement matrix is increased by QR decomposition,

so that the independence of the column vectors of the measurement matrix is improved, the purpose of optimizing the measurement matrix is achieved, and accordingly, the quality of reconstructed image is improved.

Gradient descent method

In this article, gradient descent method (GDM) is utilized to lessen the cross-correlation between the measurement matrix and sparse matrix. The optimization problem of measurement matrix may be derived to the following unconstrained optimization one:

$$\min_G \|G - H_2\|_F^2 = \min_{\Phi} \|\Psi^T \Phi^T \Phi \Psi - H_2\|_F^2, \quad (13)$$

where $\|\cdot\|_F$ is the Frobenius norm, G is the Gram matrix, H_2 is gotten by contracting threshold function, Φ is the measurement matrix, and Ψ is the sparse matrix. GDM is applied for renewing the measurement matrix, and the detailed steps are as follows.

First, to get the optimal measurement matrix, one function is defined as

$$J(\Phi) = \|\Psi^T \Phi^T \Phi \Psi - H_2\|_F^2. \quad (14)$$

Next, the gradient of measurement matrix Φ is obtained by

$$\begin{aligned} \frac{\partial J(\Phi)}{\partial \Phi} &= \frac{\partial}{\partial \Phi} \{\text{tr}(\Psi^T \Phi^T \Phi \Psi - H_2)^T (\Psi^T \Phi^T \Phi \Psi - H_2)\} \\ &= 4\Phi \Psi (\Psi^T \Phi^T \Phi \Psi - H_2) \Psi^T, \end{aligned} \quad (15)$$

where $\text{tr}(\cdot)$ is the trace of the matrix. Subsequently, regenerate the matrix Φ_{i+1} by

$$\Phi_{i+1} = \Phi_i - \beta \frac{\partial J(\Phi)}{\partial \Phi} = \Phi_i - \eta \Phi_i \Psi (\Psi^T \Phi_i^T \Phi_i \Psi - H_2) \Psi^T, \quad (16)$$

where iteration step size $\eta = 4\beta$ ($\beta > 0$).

Barzilai–Borwein strategy [41] is utilized to infer the iteration step η_i , and it may be computed by

$$\begin{aligned} \eta_i &= \arg \min_{i \in R} \|\eta S_{i-1} - Y_{i-1}\|^2 \quad \text{or} \\ \eta_i &= \arg \min_{i \in R} \|S_{i-1} - \eta^{-1} Y_{i-1}\|^2, \end{aligned} \quad (17)$$

where $S_{i-1} = \Phi_i - \Phi_{i-1}$, $Y_{i-1} = Q_i - Q_{i-1}$, $Q_i = \Phi_i \Psi (\Psi^T \Phi_i^T \Phi_i \Psi - H_2) \Psi^T$. Through computing Eq. (17), two iteration steps are obtained and shown as

$$\eta_i = \frac{\langle S_{i-1}, S_{i-1} \rangle}{\langle Y_{i-1}, S_{i-1} \rangle} \quad \text{or} \quad \eta_i = \frac{\langle S_{i-1}, Y_{i-1} \rangle}{\langle Y_{i-1}, Y_{i-1} \rangle}. \quad (18)$$

Specifically, one of them may be applied for achieving the adaptive adjustment of steps. To ensure the convergence of GDM, Armijo criterion [42] is adopted and the following inequality must hold:

$$J(\Phi_i + \eta_i P_i) \leq J(\Phi_i) + \sigma \eta_i \langle P_i, \nabla J(\Phi_i) \rangle, \quad (19)$$

where $P = -\nabla J(\Phi_i)$, $\nabla J(\Phi_i) = \partial J / \partial \Phi = 4\Phi \Psi (\Psi^T \Phi^T \Phi \Psi - H_2) \Psi^T$, $0 < \sigma < 1$. If the relative change rate r of the objective function of two adjacent iterations satisfies Eq. (20), the iteration is terminated [42]

$$r = \left| \frac{J(\Phi_i) - J(\Phi_{i-1})}{J(\Phi_{i-1})} \right| < \varepsilon, \quad (20)$$

where $0 < \varepsilon < 1$.

To reduce the cross-correlation between the measurement matrix and sparse matrix, GDM is adopted. In the optimization process, the flexible iteration step is utilized; thus, the proposed method is more flexible and efficient compared with the fixed number of iterations.

The proposed measurement matrix optimization algorithm

To obtain better measurement matrix, we present an adaptive iteration step optimization method, as shown in Fig. 2. The detailed operation steps are as below.

Input: Sparse matrix Ψ , parameter η_0, σ, λ and threshold value μ ;

Optimization objective: Minimizing $\mu_{av}(D)$ as small as possible, and $D = \Phi \Psi$, Φ is the measurement matrix, d_i, d_j are the i th column and j th column of matrix D , respectively;

Output: The optimized measurement matrix $\Phi = \hat{\Phi}_i$.

Step 1: Initialize some parameters, including measurement matrix $\Phi_0 \in R^{M \times N}$ and parameter η_0, σ, λ .

Step 2: Obtain the matrix D by $D = \Phi_0 \Psi$, the Gram matrix G by use of $G = \tilde{D}^T \tilde{D}$, and then normalize the column of G .

Step 3: Perform eigenvalue decomposition on G to get $G' = V H_1 V^{-1}$, fix the non-zero elements in the diagonal matrix H_1 as N/M to find matrix $\hat{H}_1$, and, finally, get matrix $G'' = V \hat{H}_1 V^{-1}$, where M, N are the row and column of measurement matrix.

Step 4: Shrink the non-diagonal element of G'' according to Eq. (6) to get new matrix H_2 .

Step 5: Regenerate Φ_i by use of GDM via

$$\Phi_{i+1} = \Phi_i - \eta_i \Phi_i \Psi (\Psi^T \Phi_i^T \Phi_i \Psi - H_2) \Psi^T, \quad (21)$$

where $\eta_i > 0$ denotes the i th iteration step size.

Fig. 2 Flowchart of the proposed measurement matrix optimization method

Step 6: Judge whether η_i satisfies Eq. (19), if so, perform step 7; otherwise, $\eta_i = \lambda \eta_i$, and $0 < \lambda < 1$, and then, go to step 6 to rejudge the condition again.

Step 7: Determine whether Φ_i satisfies Eq. (20), if so, manipulate step 8; otherwise $i = i + 1$, and then, go to step 4.

Step 8: Transpose Φ_i to Φ_i^T , and then, perform QR decomposition on Φ_i^T to obtain $\Phi_i^T = QR$.

Step 9: Set all the non-diagonal element of R as zero, and obtain a new matrix $\hat{R}$.

Step 10: Obtain the matrix $\hat{\Phi}_i^T = Q\hat{R}$, and the optimized measurement matrix $\hat{\Phi}_i$ may be obtained by transposing $\hat{\Phi}_i^T$.

The presented image compression and encryption scheme

Generating the system parameter and initial value of chaotic system

In this paper, LSS is used to produce key sequences for image encryption, and it is derived by

$$x(n+1) = \text{mod}(ux(n)(1-x(n)) + (4-u)\sin(\pi x(n))/4, 1), \quad (22)$$

where u is the system parameter, $u \in (0, 4]$, and x is the state variable.

To improve the dependence of plain image and image encryption scheme, the plain image characteristic information is applied for generating the system parameter and initial value of the LSS chaotic system. First, compute the information entropy h of plain image P sized of MN ; next, calculate the system parameters and initial value of LSS by

$$\begin{cases} u = \text{mod}((h \times t_1 + t_2 \times t_3 + t_4) \times 10^6, 1) \\ x(1) = \text{mod}((h + t_1 \times t_2 \times t_3 \times t_4) \times 10^6, 4) \end{cases}, \quad (23)$$

where mod is the modular operation, and external key parameters $t_1, t_2, t_3, t_4 \in (0, +\infty)$.

The adoption of information entropy of the plain image enhances the relationship between the algorithm and the plain image, so that the proposed method may resist chosen-plaintext and known-plaintext attacks effectively. For successful decryption, the information entropy should be sent to the receiver through a secure channel.

Producing the chaotic measurement matrix

In this section, two chaotic measurement matrices will be constructed and optimized according to “The proposed measurement matrix optimization algorithm”, and then, the optimized matrices are utilized to perceive the plain image. The generation process of the measurement matrix is as below.

Step 1: Iterate LSS system with the obtained u and $x(1)$ for $(n_0 + MN)$ times, remove the previous n_0 values ($n_0 > 500$) to avoid the harmful effect, and obtain the chaotic sequences X_1 .

Step 2: Pick out the previous pq elements from X_1 to get the sequence X_2 , and then obtain X_3 by preprocessing X_2 via

$$X_3(n) = 1 - 2X_1(n), \quad (24)$$

where $p = \text{ceil}(CR_1 M/2)$, $q = \text{ceil}(N/2)$, $CR_1 = 0.5$, ceil is a rounding up function, and $n = 1, 2, \dots, pq$.

Step 3: Construct the measurement matrix Φ_1 sized of $p \times q$ by use of X_3

$$\Phi_1 = \sqrt{\frac{2}{p}} \begin{pmatrix} X_3(1) & \cdots & X_3(p(q-1)+1) \\ \vdots & & \vdots \\ X_3(p) & \cdots & X_3(pq) \end{pmatrix}, \quad (25)$$

where $\sqrt{2/p}$ is the normalized coefficient.

Step 4: First, pick out the previous $p'q$ elements from X_1 to get the sequence X'_2 , next preprocess it according to Eq. (24) to find the sequence X'_3 , and finally generate another measurement matrix Φ_2 sized of $p' \times q$ via

$$\Phi_2 = \sqrt{\frac{2}{p'}} \begin{pmatrix} X'_3(1) & \cdots & X'_3(p'(q-1)+1) \\ \vdots & & \vdots \\ X'_3(p') & \cdots & X'_3(p'q) \end{pmatrix}, \quad (26)$$

where $p' = \text{ceil}(\text{CR}_2 M/2)$, $\text{CR}_2 = 0.25$ and $\sqrt{2/p'}$ is the normalized coefficient.

Generating the mask matrix for DRPE

In the proposed image encryption, DRPE is applied for confusing the measurement values of the plain image to upgrade the confusion effect, and its mask matrix is produced by the following steps.

Step 1: Collect the previous $MN/16$ elements from chaotic sequences X_1 to obtain X_4 , and then sort X_4 in ascending order to get chaotic sequence X_5 and the corresponding index sequence D sized of $1 \times MN/16$ according to

$$[X_5, D] = \text{sort}(X_4). \quad (27)$$

Step 2: Pick out the previous $MN/4$ elements from chaotic sequence X_1 to get X_6 , and then draw the last $MN/4$ elements from X_1 to find X_7 ; subsequently, process sequences X_6, X_7 according to Eq. (28) to get sequences X_8, X_9 , and then resize them to obtain two mask matrices X_{10}, X_{11} sized of $M/2 \times N/2$

$$\begin{cases} X_8 = \text{mod}(((X_6 + X_7) \times 10^6), 1) \\ X_9 = \text{mod}((X_6 \times 10^3 + X_7 \times 10^3) \times 10^6, 1) \end{cases}. \quad (28)$$

Step 3: Pick out the first $MN/2$ elements from chaotic sequence X_1 to get X_{12} , draw the last $MN/2$ elements from it to obtain X_{13} , and then modify them by use of Eq. (29) to get X_{14} and X_{15} with size of $1 \times MN/2$

$$\begin{cases} X_{14} = \text{floor}(\text{mod}(((X_{12} + X_{13}) \times 10^6), 256)) \\ X_{15} = \text{floor}(\text{mod}((X_{12} + X_{13} + X_{14}) \times 10^6, 256)) \end{cases}. \quad (29)$$

Step 4: Resize X_{14} and X_{15} to obtain the mask matrices X_{16} and X_{17} sized of $M/2 \times N$ for diffusion.

The complete image compression and encryption method

In this section, the proposed image compression and encryption method based on compressive sensing and DRPE is described in detail. First, the plain image is transformed to a low frequency and three high-frequency components by use of discrete wavelet transformation (DWT). Second, the four components are shuffled by index sequences, the obtained high-frequency components are compressed by CS, and a complex matrix is obtained by integrating them with the shuffled low-frequency component. Third, the complex matrix is processed by DRPE, quantization, and diffusion to get the cipher image. Since the low-frequency component contains important information of the plain image, it is not compressed. For the high-frequency components have less plain information, they are compressed to save storage room and transmission bandwidth. Compressing the plain image selectively based on importance of the plain image may not only ensure the quality of reconstructed images, but also reduce the data redundancy. Besides, the adoption of permutation and DRPE improves the security of the proposed cipher. The complete image encryption process is shown in Fig. 3, and the detailed steps are as below.

Step 1: Perform DWT on plain image P sized of $M \times N$ to get the low-frequency component LL and high-frequency components LH, HL, HH sized of $M/2 \times N/2$.

Step 2: As described in “Generating the system parameter and initial value of chaotic system”, obtain the system parameter u and initial value $x(1)$ of LSS system by use of information entropy h and keys t_1, t_2, t_3, t_4 .

Step 3: Convert LL, LH, HL , and HH to sequences LL_1, LH_1, HL_1 , and HH_1 sized of $1 \times MN/4$, respectively. Next, utilize index sequence D gotten in “Generating the mask matrix for DRPE” to shuffle them to obtain sequences LL_2, LH_2, HL_2, HH_2 via

$$\begin{cases} LL_2(i) = LL_1(D(i)) \\ LH_2(i) = LH_1(D(i)) \\ HL_2(i) = HL_1(D(i)) \\ HH_2(i) = HH_1(D(i)) \end{cases}, \quad (30)$$

where $i = 1, 2, \dots, MN/4$.

Step 4: As demonstrated in “Producing the chaotic measurement matrix”, produce two measurement matrices: Φ_1 sized of $p \times q$ and Φ_2 sized of $p' \times q$, where $p = \text{ceil}(\text{CR}_1 M/2)$, $p' = \text{ceil}(\text{CR}_2 M/2)$, $q = \text{ceil}(N/2)$, $\text{CR}_1 = 0.5$ and $\text{CR}_2 = 0.25$.

Step 5: Resize sequences LL_2, LH_2, HL_2, HH_2 to matrices LL_3, LH_3, HL_3, HH_3 sized of $M/2 \times N/2$, respectively. Subsequently, optimize Φ_1 and Φ_2 according to “The proposed measurement matrix optimization algorithm”, and then mea-

Fig. 4 The flowchart of the image decryption process

Influence of measurement matrix optimization on reconstruction effect

To analyze the effect of measurement matrix optimization on reconstruction effect, compression rate CR of the plain image varies from 0.3, to 0.5, 0.7, and 0.9, the reconstructed Lena is obtained under the optimized and unoptimized conditions, and the results are shown in Fig. 5.

As shown in Fig. 5 that first, after the measurement matrix is optimized, the recovered Lena image is clearer than that without optimization, just like the plain image, indicating the effectiveness of our optimization method; second, when CR = 0.3, the reconstructed Lena image gotten by our scheme has higher quality than that in [43, 44], especially around the eyes. Besides, the PSNR values between the reconstruction image and plain image are illustrated in Fig. 6 with CR changing from 0.1 to 0.9. From Fig. 6, one may conclude that PSNR gotten by our optimization method is the largest than [43, 44], and the proposed optimization algorithm can improve PSNR obviously when the compression ratio is small, especially from 0.2 to 0.4.

Influence of different chaotic systems on reconstruction effect

In the image encryption based on CS, measurement matrix is used as secret key, and it should be sent to the receiver for decryption. To reduce the transmission cost, chaotic systems are applied to generate measurement matrix, less parameters as secret key may produce larger measurement matrix. In this section, the effect of different chaotic system on reconstruction quality is analyzed. Chaotic systems are chosen as Tent map, Logistic map, and Logistic-Tent chaotic system (LTS), and they are described by

$$X_{n+1} = \begin{cases} rX_n/2, & X_n < 0.5 \\ r(1 - X_n)/2, & X_n \geq 0.5 \end{cases} \quad (35)$$

$$X_{n+1} = rX_n(1 - X_n) \quad (36)$$

$$\begin{aligned} v_{n+1} &= \text{LTS}(r, v_n) \\ &= \begin{cases} (rv_n(1 - v_n) + (4 - r)v_n/2) \bmod 1, & v_n < 0.5 \\ (rv_n(1 - v_n) + (4 - r)(1 - v_n)/2) \bmod 1, & v_n \geq 0.5 \end{cases} \end{aligned} \quad (37)$$

where system parameter $r \in (0, 4]$ and state variables are $X_n, v_n \in (0, 1)$.

The measurement matrix is produced by chaotic system, OMP is the reconstruction method, other parameters are set as in “Performance analyses of measurement matrix optimization algorithm”, and the PSNR between the recovered image and original image are listed in Table 1. From Table 1, one may conclude that when the measurement matrix is not optimized, the PSNR values gotten by different chaotic systems change a lot, and the maximum deviation is 6.61 dB for the same CR. Besides, after the measurement matrix is optimized, PSNR values obtained by different chaos are closer, and the maximum deviation decreases to 3.2 dB. Additionally, PSNR values are more than 30 dB with the optimized measurement matrix under the condition that CR = 0.6, and when the LSS is utilized, the largest PSNR is obtained. All in all, the reconstruction quality of the proposed image encryption is enhanced by optimizing the measurement matrix, and different chaotic systems may be used, broadening the selection range of chaotic system.

Performance stability analysis

A good optimization method should have stable performance after repeated use. When Gaussian random matrix is adopted, as for its randomness, the simulation results may be different for different test; thus, the PSNR of the same optimization algorithm is different under the same compression ratio. PSNR values gotten by 50-time manipulation are demonstrated in Fig. 7, with CR = 0.3.

Fig. 5 The reconstructed Lena image with different CR for every row

As is evident from Fig. 7 that PSNR values improve a lot after the measurement matrix is optimized, PSNR values change dramatically with the unoptimized measurement matrix, but when it is optimized, PSNR value varies very

slow and is concentrated around 22 dB, which may indicate that the proposed measurement matrix optimization method makes the performance more stable.

Fig. 6 PSNR vs CR

Table 1 PSNR gotten by different chaotic systems (unit: dB)

Chaotic system	CR		
	0.3	0.6	0.9
Tent			
Unoptimized	14.58	26.37	31.55
Optimized	21.76	30.01	34.99
Increase	7.18	3.64	3.44
Logistic			
Unoptimized	10.54	28.54	32.64
Optimized	18.56	30.03	34.99
Increase	8.02	1.49	2.35
LSS			
Unoptimized	17.15	28.59	32.81
Optimized	21.83	30.07	35.32
Increase	4.68	1.48	2.51
LTS			
Unoptimized	10.54	28.54	32.64
Optimized	18.56	30.03	34.99
Increase	8.02	1.49	2.35

Performance analyses of image compression and encryption algorithm

Encrypted images and decrypted images

In the experiment, the external keys are randomly set as $t_1 = 0.2358$, $t_2 = 1.3545$, $t_3 = 10.8949$, $t_4 = 100.1564$, parameters to optimize measurement matrix are fixed as $\eta = 10^{-6}$, $\lambda = 10^{-3}$, $\sigma = 10^{-2}$, and OMP is utilized for reconstruction. Lena, Peppers sized of 512×512 , Lena sized of 1024×1024 , Lena, Einstein, Peppers sized of 256×256 , color Lena sized of 256×256 are used to test, and $CR = 0.5$. The encryption

Fig. 7 PSNR values vs experiment times

and decryption results are shown in Figs. 8 and 9. Wherein, in Fig. 8a–i are the plain image, encryption image, and decryption image of Lena512, Peppers512, and Lena1024, respectively.

In Fig. 9a–c are the plain image Lena256 and its encryption and decryption images, d–f are the plain image Einstein256 and its encryption and decryption images, g–i are the plain image Peppers256 and its encryption and decryption images, and j–l are the color plain image Lena and its encryption and decryption images. From Figs. 8 and 9, one may conclude that the encryption images have been compressed a half, their appearances are all noisy, nothing useful information may be derived from them, and thus, the plain image information is protected effectively; the decrypted images are just their corresponding plain images, indicating the effectiveness of the decryption method. Besides, the proposed image compression and encryption method may be applied for color image.

Comparison analyses of measurement matrix

In this section, the performance of our generated measurement matrix is compared with Toplitz, Gaussian, and Bernoulli measurement matrix. The plain images shown in Figs. 8 and 9 are used as test images, compression ratio is set as $CR = 0.5$, and the PSNR values gotten by different measurement matrices are computed and listed in Fig. 10. As is evident from Fig. 10 that among the five test images, the PSNR values gotten by our method are the largest than Toplitz, Gaussian, and Bernoulli measurement matrix, indicating the effectiveness of our measurement matrix generation method. Additionally, Lena512 (shown in Fig. 8a) is used as test image, the PSNR between the decrypted image and plain image is computed and listed in Table 2, and $CR = 0.5$. From Table 2, one may watch that PSNR value gotten by our method is more than Refs. [20, 45], verifying the satisfactory compression performance of the proposed scheme.

Fig. 8 Encryption and decryption images sized of 512×512 and 1024×1024

Key space analyses

The key space should be large enough to make the image encryption withstand any kinds of brute force attacks [24, 29]. The key used in our algorithm consists of (1) the information entropy h of plain image; (2) the external key t_1, t_2, t_3, t_4 ; (3) intermittent parameters $L_{\max}, L_{\min}, LL_{\max}$, and $LL_{\min}$. If the computation precision of the computer is 10^{-14} , our key space is about $(10^{14})^5 = 10^{70} > 2^{210}$, much larger than the general requirements of 2^{100} to resist brute force attack [46]. Table 3 gives the comparison results of key space with other algorithms. As can be seen, our key space is larger than that in Refs. [47–49], indicating that our image encryption may withstand brute force attack effectively.

Histogram analyses

Histogram plots the distribution information of image pixels [50]. A good image encryption should generate cipher image with uniform histogram to prevent hackers from obtaining plain image information from them. The histograms of plain image Lena sized of 256×256 and its cipher image sized of 128×256 are shown in Fig. 11. It is evident from Fig. 11 that the histogram of plain image demonstrates very obvious statistical information; conversely, that of cipher image is evenly distributed and nothing useful information may be found, indicating that the proposed image encryption may resist the statistical attack effectively.

Fig. 9 Encryption and decryption images sized of 256×256

Fig. 10 PSNR values for different measurement matrices

Table 2 PSNR values between our algorithm and others

Algorithm	Ours	Ref. [45]	Ref. [20]
PSNR (dB)	31.5328	31.5	<26.7

Table 3 Comparison results of key space

Algorithm	Ours	Ref. [47]	Ref. [48]	Ref. [49]
Key space	2^{210}	2^{138}	2^{130}	2^{192}

Correlation of adjacent pixels

It is generally known that adjacent pixels of a meaningful plain image have strong correlations, and a cipher image gotten by a good encryption method is noise-like, and adjacent pixels have no correlations. To visually plot the correlation distribution of adjacent pixels, 7000 pairs of pixels are randomly chosen from the plain image Lena256 and its cipher image and their distribution are presented in Fig. 12. It may be seen that the distributions of plain image are concentrated in horizontal, vertical, and diagonal directions, indicating high correlation. While the distributions of cipher image are distributed evenly in these directions, indicating no-correlation.

Additionally, to assess the correlation of two adjacent pixels in horizontal, vertical, and diagonal directions, the correlation coefficient CC of two adjacent pixels is defined by [45]

$$CC = \frac{L \sum_{i=1}^L (x_i y_i) - \sum_{i=1}^L x_i \sum_{i=1}^L y_i}{\sqrt{\left(L \sum_{i=1}^L x_i^2 - \left(\sum_{i=1}^L x_i \right)^2 \right) \left(L \sum_{i=1}^L y_i^2 - \left(\sum_{i=1}^L y_i \right)^2 \right)}}, \quad (38)$$

where x_i and y_i denote two different pixels in one image, and L is the total number of selected pixels.

Randomly choose 7000 pairs of pixels from plain images and their cipher images, calculate the CCs of adjacent pixels in horizontal, vertical, and diagonal directions, and list them in Table 4. As may be watched from Table 4 that the CCs of cipher images are very small, indicating that the corre-

lation of adjacent pixels has been removed effectively, and the proposed image encryption may resist statistical attack well. Besides, Table 5 gives the comparison results with other studies for Lena256 image. It is evident that CCs gotten by our scheme are all less than those in Refs. [51–53].

Information entropy

Shannon [54] introduced information entropy to describe the randomness and unpredictability of an information source in 1949. It may be computed by [55]

$$H(m) = \sum_{i=0}^{2^n-1} v(m_i) \log \frac{1}{v(m_i)}, \quad (39)$$

where $v(m_i)$ is the probability of pixel v_i . For a truly random source composed of 2^8 symbols, the entropy should ideally be 8. The information entropies of the plain images and cipher images are shown in Table 6. It is evident from Table 6 that the information entropy of the cipher image gotten by our image encryption is larger than 7.99, very close to 8, indicating that the plain image information is effectively concealed. Table 7 gives the comparison results with other methods. From Table 7, we may watch that the information entropy of our algorithm is larger than that in Refs. [14, 20, 45].

Robustness analyses

Cropping attack analysis

Figure 13 displays the cipher images with different cropping attacks and their corresponding decrypted images. It may be seen from Fig. 13 that when the data loss varies from 16×16 to 4×256 , to 256×4 , to $256 \times 4 \times 2$, the plain image information may still be recovered, indicating that the proposed method may resist cropping attacks to a certain extent.

Noise attack analysis

In this section, Lena is used as plain image, its encrypted image is added different Gaussian noise (GN), Salt & Pepper noise (SPN), Speckle noise (SN), and then, the decrypted images are shown in Figs. 14, and 15 gives the PSNR values between the decrypted images and the original image. From Figs. 14 and 15, one may watch that first, as for SPN, PSNR values are higher than 30 dB, they are about stable when the noise intensity changes, which means that our algorithm has highly robustness to SPN; second, as for GN and SN, the PSNR values change dramatically; when noise intensity is 0.000007, the PSNR is lower than 20 dB, but one may find the plain image information from the recover images.

Fig. 11 Histogram of plain image and cipher image

Fig. 12 Correlation between adjacent pixels of plain image and cipher image: **a** horizontal correlation of plain image, **b** vertical correlation of plain image, **c** diagonal correlation of plain image, **d** horizontal correlation of cipher image, **e** vertical correlation of cipher image, and **f** diagonal correlation of cipher image

Conclusively, the proposed image encryption may withstand noise attacks effectively.

Conclusion

This paper introduced an effective image compression and encryption method based on CS and DRPE. First, the plain

Table 4 Correlation coefficients between adjacent pixels in the plain image and cipher image

Image	Horizontal	Vertical	Diagonal
Lena512			
Plain image	0.9846	0.9707	0.9598
Cipher image	− 0.0056	− 0.0181	0.0067
Peppers 512			
Plain image	0.9822	0.9813	0.9693
Cipher image	− 0.0082	0.0034	0.0041
Lena256			
Plain image	0.9692	0.9391	0.9205
Cipher image	− 0.0138	− 0.0027	− 0.0026
Einstein256			
Plain image	0.9253	0.9084	0.8566
Cipher image	0.0017	0.0005	0.0007
Peppers256			
Plain image	0.9511	0.9399	0.9015
Cipher image	0.0045	0.0025	− 0.0024

Table 5 Comparison results on correlation coefficient with others

Algorithm	Ours	Ref. [51]	Ref. [52]	Ref. [53]
Horizontal	− 0.0038	− 0.000573	− 0.0017	− 0.0027
Vertical	− 0.0027	− 0.003637	− 0.0027	− 0.0033
Diagonal	− 0.0026	− 0.003021	− 0.0027	− 0.0035

Table 6 Information entropy of plain image and cipher image

Image	Lena512	Peppers512	Lena256	Einstein256	Peppers256
Plain image	7.4476	7.5740	7.5683	6.8841	7.5251
Cipher image	7.9974	7.9972	7.9969	7.9961	7.9964

Table 7 Comparison with other algorithms for Lena512

Image	Ours	Ref. [45]	Ref. [20]	Ref. [14]
Lena512	7.9974	7.9219	7.9960	7.9969

image is decomposed to one low-frequency component and three high-frequency components by use of DWT, and shuf-

Fig. 13 Cropping attack results

Fig. 14 Noise attack results

Fig. 15 PSNR under different noise intensities

fled by index vectors generated from chaotic sequences. Next, shuffled high-frequency components are measured by optimized measurement matrix produced by a novel measurement matrix optimization algorithm based on adaptive step size. Subsequently, a new complex matrix is found by combining the shuffled low-frequency component and three measurement value matrices. Finally, the cipher image is

obtained by performing DRPE, quantization, and diffusion on the complex matrix. The proposed cipher is content-adaptive, since the information entropy of the plain image is applied for generating initial value of the LSS chaotic system, and the iterated chaotic sequences are utilized in the complete encryption stage. Through the performance analyses and comparison of the proposed image encryption, our method has been proven to have large key space, highly sensitive key, resistance to statistical attacks, and it can be applied for image secure transmission and storage.

Acknowledgements All the authors are deeply grateful to the editors for smooth and fast handling of the manuscript. The authors would also like to thank the anonymous referees for their valuable suggestions to improve the quality of this paper. This work is supported by the National Natural Science Foundation of China (Grant no. 61802111, 61872125, 61871175), and Science and Technology Foundation of Henan Province of China (Grant no.182102210027, 182102410051) and the Key Science and Technology Project of Henan Province (Grant no. 201300210400, 212102210094).

Author contributions All authors contributed to the study conception and design. Material preparation, data collection, and analysis were performed by ZG, XC, JB, and XC. The first draft of the manuscript was written by ZG and XC. All authors commented on this version of the manuscript. All authors read and approved the final manuscript.

Funding This work is supported by the National Natural Science Foundation of China (Grant nos. 61802111, 61872125, 61871175), and Science and Technology Foundation of Henan Province of China (Grant no. 182102210027, 182102410051).

Availability of data and materials The authors declare that data and materials will be made available on reasonable request.

Code availability The authors declare that the code will be made available on reasonable request.

Declarations

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

Ethics approval Our research is not involved in human participants and animals.

Consent to participate All the listed authors have participated actively in the study.

Consent for publication All the listed authors have agreed to publish our article in Complex & Intelligent Systems.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Ye HS, Zhou NR, Gong LH (2020) Multi-image compression–encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion. *Signal Process* 175:107652
- Ye GD, Pan C, Huang XL, Mei QX (2018) An efficient pixel-level chaotic image encryption algorithm. *Nonlinear Dyn* 94:745–756
- Wang M, Wang X, Zhao T, Zhang C, Xia Z, Yao N (2021) Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme. *Inf Sci* 544:1–24
- Li XJ, Mou J, Xiong L, Wang ZS, Xu J (2021) Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption. *Opt Laser Technol* 140:107074
- Wen WY, Wei KK, Zhang YS, Fang YM, Li M (2020) Colour light field image encryption based on DNA sequences and chaotic systems. *Nonlinear Dyn* 99:1587–1600
- Wang XY, Wang Y, Zhu XQ, Luo C (2020) A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. *Opt Lasers Eng* 125:105851
- Chai XL, Gan ZH, Yang K, Chen YR, Liu XX (2017) An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process Image Commun* 52:6–19
- Zhang YB, Zhang L, Zhong Z, Yu L, Shan MG, Zhao YG (2021) Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation. *Opt Lasers Eng* 143:106626
- Yu SS, Zhou NR, Gong LH, Nie Z (2020) Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. *Opt Lasers Eng* 124:105816
- Donoho DL (2006) Compressed sensing. *IEEE Trans Inf Theory* 52:1289–1306
- Fan HJ, Zhou KL, Zhang E, Wen WY, Li M (2020) Subdata image encryption scheme based on compressive sensing and vector quantization. *Neural Comput Appl* 32:12771–12787
- Zhou SW, He Y, Liu YH, Li CQ, Zhang JM (2021) Multi-channel deep networks for block-based image compressive sensing. *IEEE Trans Multimed* 23:2627–2640
- Zhang YS, Zhang LY, Zhou JT, Liu LC, Chen F, He X (2016) A review of compressive sensing in information security field. *IEEE Access* 4:2507–2519
- Hu G, Xiao D, Wang Y, Xiang T (2017) An image coding scheme using parallel compressive sensing for simultaneous compression–encryption applications. *J Vis Commun Image Rep* 44:116–127
- Wang KS, Wu XJ, Gao TG (2021) Double color images compression–encryption via compressive sensing. *Neural Comput Appl*. <https://doi.org/10.1007/s00521-021-05921-y>
- Zhou NR, Zhang AD, Zheng F, Gong LH (2014) Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Opt Laser Technol* 62:152–160
- Huang H, He X, Xiang Y, Wen WY, Zhang YS (2018) A compression–diffusion–permutation strategy for securing image. *Signal Process* 150:183–190
- Hua ZY, Zhang KY, Li YM, Zhou YC (2021) Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. *Signal Process* 183:107998
- Wang XY, Ren Q, Jiang DH (2021) An adjustable visual image cryptosystem based on 6D hyperchaotic system and compressive sensing. *Nonlinear Dyn* 104:4543–4567
- Zhou NR, Jiang H, Gong LH, Xie XW (2018) Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Opt Lasers Eng* 110:72–79
- Endra RS (2013) Compressive sensing-based image encryption with optimized sensing matrix. *IEEE Int Conf Comput Intell Cybern* 2013:122–125
- Luo YL, Lin J, Liu JX, Wei DQ, Cao LC, Zhou RL, Cao Y, Ding XM (2019) A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Process* 161:227–247
- Gan ZH, Bi JQ, Ding WK, Chai XL (2021) Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption. *Neural Comput Appl*. <https://doi.org/10.1007/s00521-021-05937-4>
- Chai XL, Wu HY, Gan ZH, Han DJ, Zhang YS, Chen YR (2021) An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. *Inf Sci* 556:305–340
- Zhang YS, Zhou JT, Chen F, Zhang LY, Wong KW, He X, Xiao D (2016) Embedding cryptographic features in compressive sensing. *Neurocomputing* 205:472–480
- Song YJ, Zhu ZL, Zhang W, Guo L, Yang X, Yu H (2019) Joint image compression–encryption scheme using entropy coding and compressive sensing. *Nonlinear Dyn* 95:2235–2261

27. Xu QY, Sun KH, He SB, Zhu CX (2020) An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Opt Lasers Eng* 134:106178
28. Zhou NR, Li HL, Wang D, Pan SM, Zhou ZH (2015) Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. *Opt Commun* 343:10–21
29. Chai XL, Zheng XY, Gan ZH, Han DJ, Chen YR (2018) An image encryption algorithm based on chaotic system and compressive sensing. *Signal Process* 148:124–144
30. Huo DM, Zhu XH, Dai GZ, Yang HC, Zhou X, Feng MH (2020) Novel image compression–encryption hybrid scheme based on DNA encoding and compressive sensing. *Appl Phys B Lasers Opt* 126:45
31. Jiang X, Xiao Y, Xie YY, Liu BC, Ye YC, Song TT, Chai JX, Liu Y (2021) Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding. *Opt Commun* 484:126683
32. Wang F, Xu J, Fan QJ (2021) Statistical properties of the detrended multiple cross-correlation coefficient. *Commun Nonlinear Sci* 99:105781
33. Rudelson M, Vershynin R (2008) On sparse reconstruction from Fourier and Gaussian measurements. *Commun Pure Appl Math* 61:1025–1045
34. Elad M (2007) Optimized projections for compressed sensing. *IEEE Trans Signal Process* 55:5695–5702
35. Szarek SJ (1991) Condition numbers of random matrices. *J Complex* 7:131–149
36. Welch L (1974) Lower bounds on the maximum cross correlation of signals. *IEEE Trans Inf Theory* 20:397–399
37. Abolghasemi V, Ferdowsi S, Sanei S (2012) A gradient based alternating minimization approach for optimization of the measurement matrix in compressive sensing. *Signal Process* 92:999–1009
38. Ma YL, Pei LY, Jiang H (2017) Improved optimization algorithm for measurement matrix in compressed sensing. *J Signal Process* 33:192–197
39. Liu JP, Yang CY, Fang J, Wei G (2016) Improved optimization algorithm of the Gram measurement matrix based on gradient projection. *J Huazhong Univ Sci Technol (Natural Science Edition)* 44:062–066
40. Sahoo JK, Behera R, Stanimirovic PS, Katsikis VN (2020) Computation of outer inverses of tensors using the QR decomposition. *Comput Appl Math* 39:199
41. Zhao W, Chen YY, Liu JK (2020) An effective first order reliability method based on Barzilai–Borwein step. *Appl Math Model* 77:1545–1563
42. Shen ZY, Wang LX (2019) Adaptive step-size method for measurement matrix iterative optimization. *Comput Eng Appl* 55:266–270
43. Lan MR (2017) Research on optimization and reconstruction algorithm of measurement matrix based on compressive sensing. Nanjing University of Posts and Telecommunications
44. Fang J (2015) Research on the measurement matrix and reconstruction algorithm in compressed sensing. South China University of Technology
45. Luo YL, Zhou RL, Liu JX, Cao Y, Ding XM (2018) A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. *Nonlinear Dyn* 93:1165–1181
46. Li C, Zhang Y, Xie EY (2019) When an attacker meets a cipher-image in 2018: a year in review. *J Inf Secur Appl* 48:102361
47. Pak C, Huang LL (2017) A new color image encryption using combination of the 1D chaotic map. *Signal Process* 138:129–137
48. Wang XY, Zhang JJ, Cao GH (2019) An image encryption algorithm based on ZigZag transform and LL compound chaotic system. *Opt Laser Technol* 119:105581
49. Man ZL, Li JQ, Di XQ, Liu X, Zhou J, Wang J, Zhang XX (2021) A novel image encryption algorithm based on least squares generative adversarial network random number generator. *Multimed Tools Appl* 80:27445–27469
50. Chai XL, Zhi XC, Gan ZH, Zhang YS, Chen YR, Fu JY (2021) Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption. *Signal Process* 183:108041
51. Yao SY, Chen LF, Zhong Y (2019) An encryption system for color image based on compressive sensing. *Opt Laser Technol* 120:105703
52. Chai XL, Fu XL, Gan ZH, Lu Y, Chen YR (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process* 155:44–62
53. Wang XY, Zhao HY, Wang MX (2019) A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices. *Opt Laser Technol* 115:42–57
54. Shannon CE (1949) Communication theory of secrecy systems. *Bell Labs Tech J* 28:656–715
55. Yang FF, Mou J, Liu J, Ma CG, Yan HZ (2020) Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. *Signal Process* 169:107373

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.