Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047233

ARTICLE

Color Image Compression and Encryption Algorithm Based on 2D Compressed Sensing and Hyperchaotic System

Zhiqing Dong[1], Zhao Zhang[1,*], Hongyan Zhou[2] and Xuebo Chen[2]

[1]School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, 114051, China

[2]School of Electronic and Information Engineering, University of Science and Technology Liaoning, Anshan, 114051, China

*Corresponding Author: Zhao Zhang. Email: zhangzhao333@hotmail.com

Received: 30 October 2023 Accepted: 24 December 2023 Published: 27 February 2024

ABSTRACT

With the advent of the information security era, it is necessary to guarantee the privacy, accuracy, and dependable transfer of pictures. This study presents a new approach to the encryption and compression of color images. It is predicated on 2D compressed sensing (CS) and the hyperchaotic system. First, an optimized Arnold scrambling algorithm is applied to the initial color images to ensure strong security. Then, the processed images are concurrently encrypted and compressed using 2D CS. Among them, chaotic sequences replace traditional random measurement matrices to increase the system's security. Third, the processed images are re-encrypted using a combination of permutation and diffusion algorithms. In addition, the 2D projected gradient with an embedding decryption (2DPG-ED) algorithm is used to reconstruct images. Compared with the traditional reconstruction algorithm, the 2DPG-ED algorithm can improve security and reduce computational complexity. Furthermore, it has better robustness. The experimental outcome and the performance analysis indicate that this algorithm can withstand malicious attacks and prove the method is effective.

KEYWORDS

Image encryption; image compression; hyperchaotic system; compressed sensing

1 Introduction

Owing to the advent of the big data era and multimedia technology, digital color images are applied in every field of people's lives with the advantages of high resolution and intuitive expression. However, there are also many security risks in image transmission while being convenient [1]. Therefore, many scholars have been attracted to studying more secure encryption schemes in this field. At present, techniques for text encryption have become increasingly mature within the information encryption domain [2]. However, with the emergence of digital color images, simple text encryption methods are no longer sufficient. With the improvement of technology, the means of attackers are also becoming increasingly sophisticated. In today's world, establishing a reliable and efficient encryption technique has become crucial [3].

American meteorologist E. Lorenz originally put up the idea of chaos in 1963. Unpredictability, unrepeatability, and nonrepeating ability define its behavior [4,5]. Consequently, numerous properties of chaotic systems apply to cryptography [6]. It has also aroused great interest in the last few decades [7]. Among the often employed chaotic systems are 1D chaotic systems [8], 2D chaotic systems [9], Multiple-dimensional chaotic systems, and hyperchaotic systems. In [10], a new chaotic system made up of two chaotic systems was used as an image encryption scheme. A new algorithm combining optics has been proposed by Liu et al. in [11]. In [12], a joint scrambling and diffusion scheme was proposed by Li et al. Reference [13] proposed a unique SCCM system that is 1D. Additionally, it provided a random DNA operation and SCCM-based image encryption technique. The scheme's strong encryption effect is confirmed by the experiment. Compared to high-dimensional chaotic systems, the nonlinear behavior of the hyperchaotic systems is more intricate and unpredictable [14]. These characteristics show that applying a hyperchaotic system to image encryption will enhance system security [15].

Due to the rapid development of compressed sensing (CS) technology [16], its application in image processing has attracted the attention of many scholars. CS can compress and encrypt the image simultaneously, so digital image processing using CS technology has become a new research hotspot [17,18]. It is highly concerned in many fields, like computer vision and wireless communication. Gong et al. proposed an advanced algorithm for compressing and encrypting images [19]. Arnold transformation is used to arrange the image's original, and then CS compresses and encrypts the resulting image. Subsequently, Zhang et al. proposed a cryptographic technique combining double random phase encoding with compressed sensing [20]. The scheme combines two images into one by encrypting and compressing them, increasing the difficulty of the algorithm. The scheme's efficacy and sophisticated nature are demonstrated by the experimental results. In [21], Chai et al. offered a block compression and multi-objective optimization-based image encrypting system. In [22], this research proposed a unique data transfer paradigm that combines a hybrid cloud with semi-tensor product compression sensing. The efficiency and security of this approach are shown by the results of the simulation. Currently, most CS cryptographic algorithms are used to process gray images [23], so effectively compressing and encrypting color images is a problem worth studying.

This paper presents a novel approach for image encryption that leverages 2D CS, the 4D hyperchaotic system, and the joint permutation diffusion (JPD) approach to address this issue. There are three stages to this paper's encryption algorithm. Firstly, generating initial values of hyperchaotic systems using the RSA algorithm. The system creates the matrix and chaotic sequence required for encryption. The Lorenz hyperchaotic system is prepared for the scrambling operation. Secondly, in the CS part, a grayscale mapping strategy is to process images and 2D CS to compress and quantify the mapped image. Among them, the 4D hyperchaotic system generates one measurement matrix, and the other is generated randomly, greatly increasing randomness. Finally, the encryption part encrypts the processed image using scrambling and spreading algorithms simultaneously. The decryption process consists of two distinct phases. The first step during the decryption process involves performing the inverse operation of JPD. Then, the 2DPG-ED algorithm decrypts the ciphertext image. Simulation experiments and performance analysis have demonstrated the effectiveness of the algorithm presented in this paper, showcasing its resilience against common attacks. After comparative analysis, the proposed algorithm has better encryption performance and less distortion ratio.

The remainder of this work is comprised of the following sections. Section 2 provides an overview of the preliminary work. Section 3 provides a detailed description of the proposed encryption scheme. Section 4 describes the experimental simulation results and analysis. Section 5 serves as the conclusion in the end.

2 Preliminary Work

2.1 The 4D Hyperchaotic System

A novel and extremely intricate 4D hyperchaotic system was suggested by [24]. Its definition is using the equation below:

$$\hat{x} = a\,(y - x - w) + byz, \hat{y} = c\,(4x + y) - xz, \hat{z} = dx - ez + xy, \hat{w} = rx + f\,(3yz + y^2), \tag{1}$$

here, $a = 80$, $b = 45$, $c = 22$, $d = 5$, $e = 21, f = 8$ and $60 \le r \le 322$.

The system's motion characteristics are represented by the Lyapunov exponent. For chaotic systems, they require at least one Lyapunov exponent to be positive. The system is said to be hyperchaotic when at least two of the exponents are positive. When $r = 100$, the Lyapunov exponents are $LE1 = 25.6206$, $LE2 = 11.2401$, $LE3 = 1.717\text{e}{-5}$, $LE4 = -115.0336$. Therefore, system Eq. (1) is in a state of hyperchaos. Fig. 1 depicts its hyperchaotic attractor when the initial condition is (0, 0.5, 0.5, 0.5).

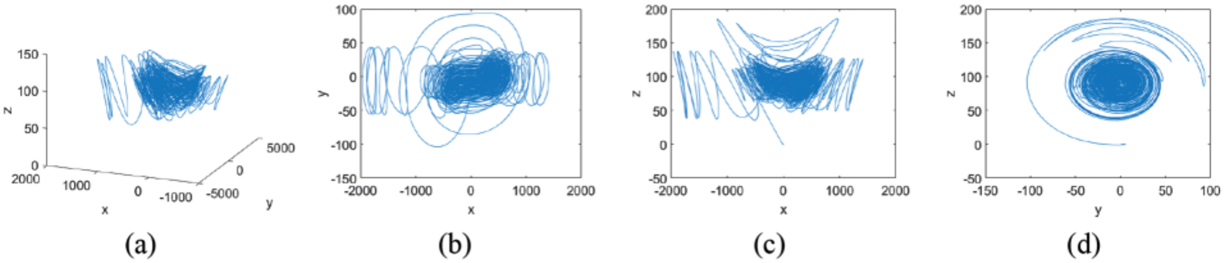
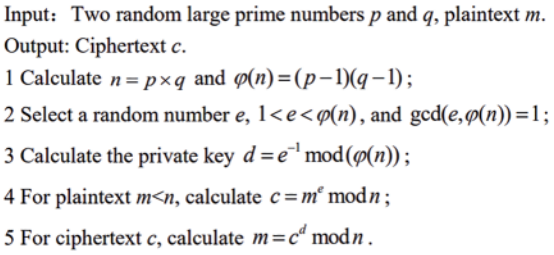


Figure 1: The system (1)'s hyperchaotic attractor at $r = 100$. The projections are as follows: (a) in x−y−z, (b) in x−y, (c) in x−z, and (d) in y−z

2.2 RSA Algorithm

In 1977, Rivest, Shamir, and Adleman proposed the public-key cryptography known as RSA. It is an asymmetric cryptographic algorithm [25]. It can be used to encrypt and digitally sign data, and for encryption and decoding, the system requires two distinct keys. The most extensively researched algorithm for public-key cryptography is the RSA algorithm. It has been put forth for almost 30 years and has also faced criticism on several occasions. The process of generating ciphertext using the RSA algorithm is shown in Fig. 2.



Input：Two random large prime numbers p and q, plaintext m.

Output: Ciphertext c.

1 Calculate $n = p \times q$ and $\varphi(n) = (p-1)(q-1)$;

2 Select a random number e, $1 < e < \varphi(n)$, and $\gcd(e, \varphi(n)) = 1$;

3 Calculate the private key $d = e^{-1} \bmod (\varphi(n))$;

4 For plaintext m<n, calculate $c = m^e \bmod n$;

5 For ciphertext c, calculate $m = c^d \bmod n$.

Figure 2: RSA algorithm

2.3 2D CS

In the process of sampling the signal, the signal compression is completed simultaneously by the CS theory; therefore, many image compression and encryption techniques employ CS theory [26]. For 2D CS, consider an $N \times N$ image P, in sparse form, which can be expressed as: $\beta = \Psi P \Psi^T$, β is a sparse representation of the P, Ψ is an $N \times N$ orthogonal base. Two measurement matrices: Φ_1 and Φ_2. They are needed for the 2D image P sampling and compression processes. The dimension of both matrices is $M \times N\,(M < N)$. Y's measurement value is represented as a $M \times M$ matrix. It can be expressed as: $Y = \Phi_1 P \Phi_2^T$, where Φ_1 and Φ_2 meet the Restricted Isometry Property (RIP). Furthermore, by figuring out the following equation: $min\, \|\beta\|_0$ s.t. $Y = \Phi_1 P \Phi_2^T$, where $\|\beta\|_0$ is the l_0 norm of β, we may precisely recreate P from Y.

An orthogonal matching pursuit algorithm is the primary CS reconstruction method [27], a reconstruction algorithm based on smooth l_0 norm [28], a base tracking algorithm, gradient projection for sparse reconstruction [29], etc. The reconstruction algorithm in this paper adopts the 2DPG-ED method [30]. Under the premise of fast signal reconstruction, the algorithm ensures the quality of the image reconstruction by keeping the image information.

3 The Proposed Encryption Scheme

3.1 Encryption Process

Fig. 3 depicts the encryption processing flowchart; a further discussion of the procedure will follow:

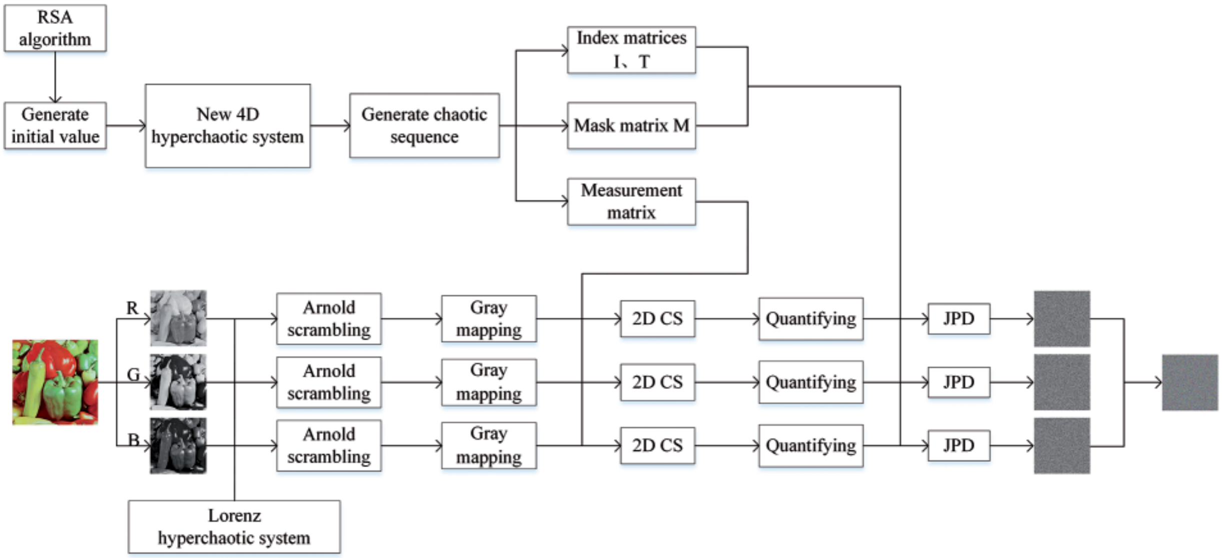


Figure 3: The procedure flow chart for the image encryption

Step 1: Generate initial values for the hyperchaotic system Eq. (1). At random, four large positive integers (m_1, m_2, m_3, m_4) are chosen. According to Fig. 2, then the public key (e, n) will be used for the computation of $c_i = m_i^e \bmod n$, $i = 1, 2, 3, 4$. Using Eq. (2), the initial value of the 4D hyperchaotic system is computed as the final step.

$$x_0 = sqrt(\log(c_1 + m_1)), y_0 = sqrt(\log(c_2 + m_2)), z_0 = sqrt(\log(c_3 + m_3)), w_0 = sqrt(\log(c_4 + m_4)). \tag{2}$$

Step 2: Generate a chaotic sequence. Based on the initial values Eq. (2), the system Eq. (1) generates a sufficiently long sequence iteratively. In the jth iteration, it is possible to obtain four status values $r^j = \left\{x_j, y_j, z_j, w_j\right\}$. Upon completing the iteration, by joining all the r^j $(j = 1, 2, \cdots, n)$, it can obtain the hyperchaotic sequence S. It is shown in the Eq. (3).

$$S = \left\{r^1, r^2, \cdots, r^n\right\} = \{x_1, y_1, z_1, w_1, \cdots, x_n, y_n, z_n, w_n\} = \{r_1, r_2, r_3, r_4, \cdots, r_{4n-3}, r_{4n-2}, r_{4n-1}, r_{4n}\}. \tag{3}$$

Step 3: Generate mask matrix M and index matrices I, T. The chaotic sequences are utilized to select four sequences at random, r_1, r_2, r_3, and r_4, which are then arranged in ascending order to generate si_1, si_2, si_3, and si_4. Matrices I, T and M, specifically, they are described as follows: $I(i,j) = si_1(\mathrm{mod}(i + si_2(j) - 1, w) + 1)$, $T(i,j) = si_3(\mathrm{mod}(i + si_4(j) - 1, w) + 1)$. Next, a sequence r_5 is chosen at random, and $M = reshape\left(\mathrm{mod}(((r_5 - \lfloor r_5 \rfloor) \times 2^{32}), 256), [h, w]\right)$, to obtain matrix M, here, w denotes the image's width and h its height.

Step 4: Generate the measurement matrix. First, remove the first 3001 items from the chaotic sequence S to obtain better randomness. The chaotic sequence S is standardized through formulas, and the measurement matrix $Phi1$ is obtained. A slight disturbance Pe is added to x every 1000 iterations to make it more complex. Then, assume that $Phi2$ are random matrices of size $M \times N$.

$$Phi1 = \begin{bmatrix} S_1 & S_{M+1} & \cdots & S_{M(N-1)} \\ S_2 & S_{M+2} & \cdots & S_{M(N-1)+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_M & S_{2M} & \cdots & S_{MN} \end{bmatrix}. \tag{4}$$

Step 5: The optimized Arnold transformation. The pseudo-random numbers a and b are obtained using the Lorenz hyperchaotic system. The matrix of images is transformed into a vector A' in one dimension. Obtaining an updated coordinate position (p', q'), perform the scrambling operation at any given point coordinate location $(1, j)$ of the vector A' to acquire the image U. Its representation is shown in Eq. (5).

$$\begin{bmatrix} p' \\ q' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \begin{bmatrix} 1 \\ j \end{bmatrix}. \tag{5}$$

Step 6: Mapping of the grey values of the scrambled image to the range −128 to 128 using a grey mapping strategy, which can be the form of the following: $U^{\xi} = U - F$, where F is a template matrix with entries all of 128, U^{ξ} is a mapping of U, and U represents the encrypted image from the above steps.

Step 7: Make use of the measurement matrix that was produced in Step 4. Another measurement matrix is produced at random. To sample the mapping of the confused image, 2D CS is applied. $Y^{\xi} = AU^{\xi}B^T = AUB^T - AFB^T = Y - Y_F$, where A is $Phi1$ and B is $Phi2$, Y, Y^{ξ} and Y_F denote 2D measurements of U, U^{ξ} and F.

Step 8: To get the bitstream, put Y^{ξ} into the scalar quantization (SQ) encoder.

Step 9: Conduct JPD operations on preprocessed images. Give an ordinary image with a channel P. Using the matrix generated in Step 3, perform joint permutation, and diffusion operations. The following Eq. (6) can be used to explain it. It is split up into three sections. Finally, the ciphertext image C is acquired.

$$C_{I_{i,j},j} = \begin{cases} mod(M_{i,j} \oplus (P_{T_{j,I_{i,j}},I_{i,j}} + P_{I_{h,w},w}), F), if\ i = 1, j = 1 \\ mod(M_{i,j} \oplus (P_{T_{j,I_{i,j}},I_{i,j}} + C_{I_{i-1,w},w}), F), if\ i \neq 1, j = 1 \\ mod(M_{i,j} \oplus (P_{T_{j,I_{i,j}},I_{i,j}} + C_{I_{i,j-1},j-1}), F), if\ j \neq 1 \end{cases}, \tag{6}$$

here, i and j denote the matrix's positions.

3.2 Decryption and Reconstruction Algorithm

As depicted in Fig. 4, decryption corresponds to the reverse process of encryption. In particular, original images are reconstructed using the 2DPG-ED reconstruction technique in the decryption process.

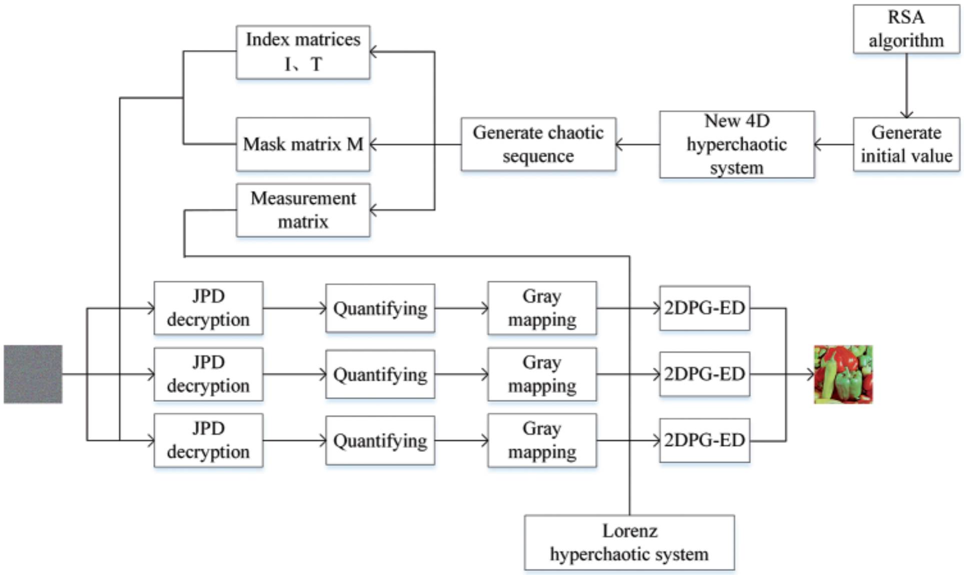


Figure 4: The procedure flow chart for the image decryption

Step 1: For ciphertext image C, the combined scrambling and diffusion procedures are reversed. The JPD decryption algorithm can be described by formulas using the index matrices I and T generated in Step 3 of 3.1, and the mask matrix M.

$$D_{T_{j,I_{i,j}},I_{i,j}} = \begin{cases} mod(M_{i,j} \oplus (C_{I_{i,j},j} - D_{I_{h,w},w}), F), if\ i = 1, j = 1 \\ mod(M_{i,j} \oplus (C_{I_{i,j},j} - D_{I_{i-1,w},w}), F), if\ i \neq 1, j = 1 \\ mod(M_{i,j} \oplus (C_{I_{i,j},j} - C_{I_{i,j-1},j-1}), F), if\ j \neq 1 \end{cases}. \tag{7}$$

Step 2: Estimating the Y^{ξ}, referred to as $\hat{Y}^{\xi}$, can be restored on the side of the decoder using inverse quantization. After that, we can use the formula to get Y's estimate: $\hat{Y} = \hat{Y}^{\xi} + Y_F$.

Step 3: To decode the final color image P, the 2DPG-ED algorithm rebuilds the image.

4 Simulation Results and Analysis

In this study, simulation tests on a 64-bit machine are accomplished using Matlab R2016a. The Lorenz hyperchaotic system's starting value is as follows: $x_0 = 1.1$, $y_0 = 2.2$, $z_0 = 3.3$, and $w_0 = 4.4$. Within the trial, test images of the size 256 × 256 and 512 × 512 are selected for evaluation. Assuming that universality remains, the compression ratio in the compression sensing process is set to 0.9.

4.1 Evaluation of Encryption and Decryption Effects

The test images include 256 × 256 color images: House, Tree, and 512 × 512 color images: Lena, Baboon, and Black. It should be noted that due to the limited space of the paper, the size of the above two types of color images presented in this paper is the same. However, in the actual simulation experiment, the pixels of these two types of images are different. Fig. 5 shows the experimental results. There is no observable information about the original image in the concealed image. The size of the image is different in the compressed encrypted version and the original. The visual differences between the original and restored images are not very noticeable.

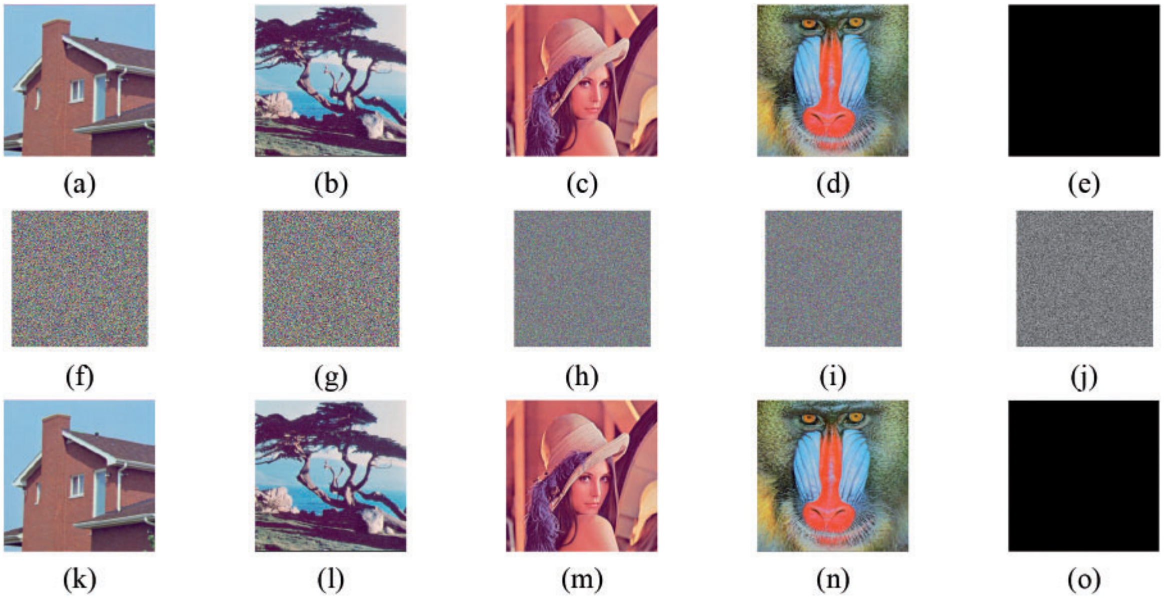


Figure 5: The experimental simulation results are obtained by using the scheme in this paper, where the original images are situated in the first row, compressed encrypted images are in the second row, and reconstructed images are in the third row

4.2 Statistic Analysis

Typically, two statistical qualities used in statistical analysis: histogram analysis and correlation analysis. These statistical properties can be used to assess the efficacy of encryption techniques.

4.2.1 Histogram Analysis

Histogram analysis is a useful tool for evaluating the security and effectiveness of encryption schemes. Attackers who use statistical analysis to break passwords do so by examining the statistical trends in both plaintext and ciphertext. To resist statistical attacks, the histogram of the encrypted images should exhibit a uniform appearance. Fig. 6 makes it evident that a clear statistical rule is displayed in the plaintext image histogram. However, the ciphertext image histogram is uniform, and it is impossible to get any information from it. Experiments have shown that the encryption algorithm has strong anti-histogram statistical performance.

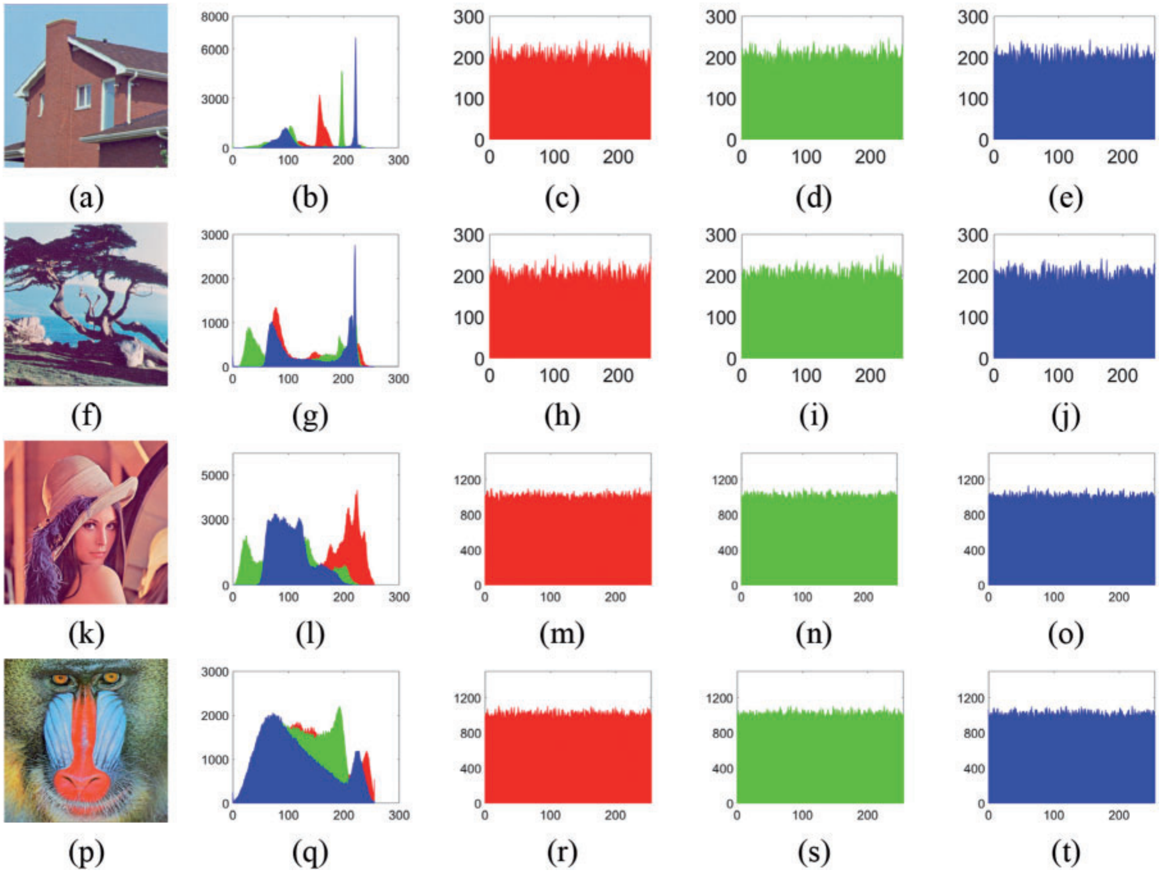


Figure 6: Histogram analysis, where (a), (f), (k), and (p) are original images, (b), (g), (l), and (q) are histograms of original images, the remaining images are the three channels histograms of the encrypted images R, G, and B

4.2.2 *Correlation Analysis*

Strong correlations exist between neighboring pixels in plaintext images; a pixel often leaks information about the pixels that surround it. So, to avoid statistical attacks, these strong correlations must be broken. It can be computed using the formula that follows.

$$Cor\left(X\right) = \left(\sum_{i=1}^{m}\left(x_i - E\left(x\right)\right)\left(y_i - E\left(y\right)\right)\right) \Big/ \sqrt{\sum_{i=1}^{m}\left(x_i - E\left(x\right)\right)^2 \sum_{i=1}^{m}\left(y_i - E\left(y\right)\right)^2},$$

here, x_{i} and y_{i} represent two pixels chosen at random from the test images, and m is 5000 pairs.

According to Fig. 7, the pixels in the original image are strongly associated with each other. However, in encrypted images, pixel distribution is uniform and uncorrelated. Table 1 gives the correlations between images in ciphertext and plaintext. When calculating correlations, all pixels in images are involved. From Table 1, we observe that the correlation coefficients of the original images are all nearly to 1, indicating strong correlations in the original images. On the other hand, all of the ciphertext images have very low correlations that are almost equal to 0.

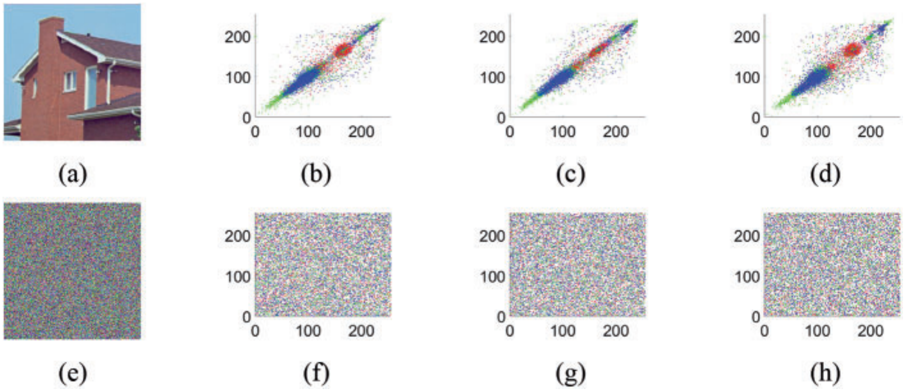


Figure 7: Correlation analysis. The last three columns represent the horizontal, vertical, and diagonal correlations of plaintext and ciphertext images, which correspond to the matching values in the first column

Table 1: Correlation coefficients analysis

Image		Original image			Encrypted image		
		Horizontal direction	Vertical direction	Diagonal direction	Horizontal direction	Vertical direction	Diagonal direction
House256	R	0.9683	0.9734	0.9104	0.0035	0.0011	0.0018
	G	0.9807	0.9403	0.9259	0.0027	0.0048	0.0018
	B	0.9833	0.9325	0.9632	0.0014	0.0043	0.0015
Tree256	R	0.9570	0.9319	0.9133	−0.0094	−0.0021	−0.0016
	G	0.9675	0.9421	0.9294	−0.0081	0.0036	0.0054
	B	0.9576	0.9367	0.9230	0.0022	−0.0016	0.0013
Lena512	R	0.9799	0.9880	0.9672	0.0079	0.0064	0.0063
	G	0.9708	0.9820	0.9553	−0.0088	0.0087	−0.0050
	B	0.9386	0.9583	0.9219	0.0040	0.0070	0.0048
Baboon512	R	0.9250	0.8609	0.8439	0.0023	0.0068	0.0012
	G	0.8804	0.7650	0.7365	−0.0022	0.0023	0.0018
	B	0.9291	0.8784	0.8587	0.0086	−0.0013	0.0042

4.3 Information Entropy Analysis

In the field of image encryption, information entropy analysis is the process of calculating and analyzing the entropy of encrypted images. It can evaluate the confidentiality and randomness of the image achieved by an encryption algorithm. The theoretical value of the encrypted picture for color image intensities ranging from 0 to 255 is 8. The computation formula that is employed is $H(X) = -\sum_{i=0}^{L} p(i) \log_2 p(i)$, here, L denotes the total number of grey levels in the image, and $P(i)$ represents the probability or likelihood of the occurrence of a specific grey value i.

In Table 2, the values of three channels of color test images are all around 7.997. However, the same images are used for testing in the [12], and all ciphertext images have a lower information entropy than the encryption method used in this paper. Therefore, entropy attacks can be resisted with this encryption scheme.

Table 2: Information entropy analysis

Image		Size	R	G	B
House256	Original image	256 × 256	6.4311	6.5389	6.2320
	Encrypted image	230 × 230	**7.9971**	**7.9970**	**7.9971**
	Reference [12]	230 × 230	7.9960	7.9964	7.9970
	Reference [25]	230 × 230	7.9967	7.9965	7.9965
Tree256	Original image	256 × 256	7.2104	7.4136	6.9207
	Encrypted image	230 × 230	**7.9967**	**7.9969**	**7.9968**
	Reference [12]	230 × 230	7.9962	7.9964	7.9962
	Reference [25]	230 × 230	7.9964	7.9964	7.9966
Lena512	Original image	512 × 512	7.2531	7.5940	6.9684
	Encrypted image	461 × 461	**7.9993**	**7.9992**	**7.9992**
	Reference [12]	461 × 461	7.9991	7.9991	7.9990
	Reference [25]	461 × 461	7.9992	7.9991	7.9992
Baboon512	Original image	512 × 512	7.7067	7.4744	7.7522
	Encrypted image	461 × 461	**7.9992**	**7.9993**	**7.9993**
	Reference [12]	461 × 461	7.9990	7.9991	7.9991
	Reference [25]	461 × 461	7.9992	7.9991	7.9992

4.4 Analysis of Resisting Differential Attacks

Differential attacks analyze the differences between pairings of plaintext and the matching ciphertext to deduce the encryption algorithm's key or internal structure.

The two metrics used to assess the difference between two images are the Unified Average Changing Intensity (UACI) and the Number of Pixels Change Rate (NPCR). The calculation formulas are $NPCR = \sum_{ij} D(i,j)/(M \times N) \times 100\%$ and $UACI = \sum_{ij} |c_1(i,j) - c_2(i,j)|/255/(M \times N) \times 100\%$, here, M and N stand for the rows and columns of images. Then, the theoretical value for NPCR is 99.6094%. The theoretical value for UACI is 33.4635%. Table 3 confirms that the encryption scheme's NPCR and UACI calculation results are nearly to theoretical standard values, proving the algorithm's robustness against attacks based on differences.

Table 3: Differential attacks analysis

Image		Ours			Reference [12]		
		R	G	B	R	G	B
House256	NPCR	99.6110	99.6070	99.6087	99.6330	99.6310	99.6220
	UACI	33.4317	33.4702	33.4245	27.2350	27.1270	27.2300
Tree256	NPCR	99.6110	99.6087	99.6030	99.5560	99.6250	99.6190
	UACI	33.4315	33.4761	32.4824	30.0800	30.2750	29.9630
Lena512	NPCR	99.6120	99.6091	99.6130	99.6130	99.6210	99.6110
	UACI	33.0701	33.5607	32.6035	33.0070	33.0950	33.0730
Baboon512	NPCR	99.6080	99.6140	99.6095	99.6203	99.6144	99.6085
	UACI	33.4450	33.5354	33.4520	33.3946	33.5394	33.4437

4.5 Key Analysis

4.5.1 Key Space Analysis

The key space refers to the complete set of possible values that a cryptographic key can take. Its size has a direct impact on the password system's security. In the algorithm of this paper, two hyperchaotic systems make up the key space. Even if only one iteration is performed, the precision of the computation is 10^{-15}, and the key space in this paper can reach $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{120}$. As stated by [31], this cryptosystem is theoretically resistant to violence when the key space is greater than 2^{100}. As a result, this algorithm is capable of withstanding strong attacks.

4.5.2 Key Sensitivity Analysis

In an ideal encryption system, with the correct key, it is possible to recover ordinary images completely, and any little alteration to the key will produce entirely different decoded images. In the experiment, we used one of the keys $x_0 + 10^{-14}$. The decrypted result is shown in Fig. 8. We cannot see any information objects from it. Therefore, we can deduce that this article's encryption algorithm key is so sensitive that even little adjustments to the key will not be able to restore the original image.

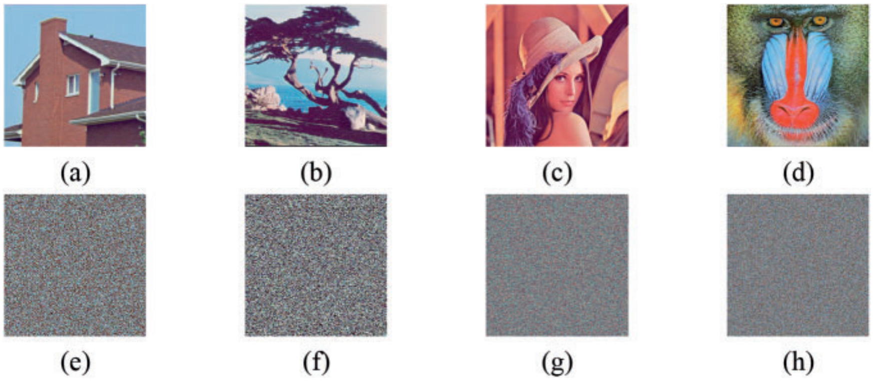


Figure 8: Key sensitivity analysis

4.6 Robustness Analysis

4.6.1 Anti-Cropping Attack

Certain portions of an image will inevitably sustain damage during processing, transmission, and storage. A strong encryption method ought to be capable of resisting cropping attacks. To simulate the process of image destruction, we cropped the ciphertext image, as illustrated in Fig. 9.

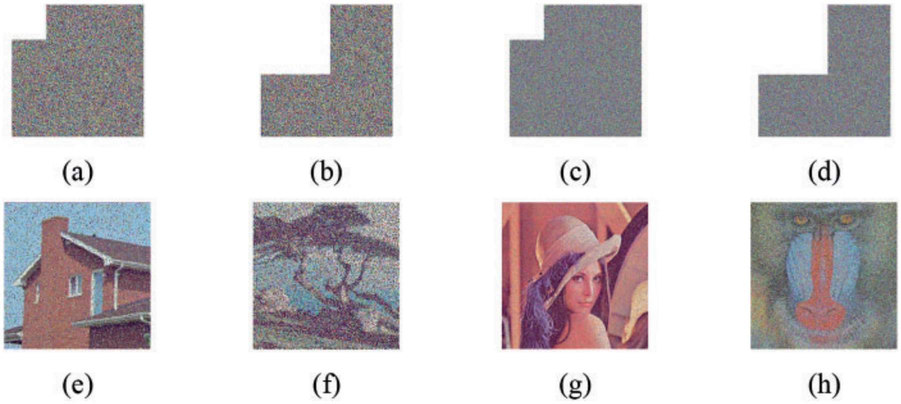


Figure 9: Anti-cropping attack analysis. (a)–(d) show cropped images with 1/16 and 1/4 of different sizes of ciphertext cropped, and (e)–(h) display the reconstructed images that match the ciphertext image that was attacked with the cropping techniques. The experimental simulation findings illustrate that the majority of the initial image information remains intact in the encoded and reconstructed ciphertext image despite the cropping attack. This suggests that the approach may provide a degree of resistance against cropping attacks

Figs. 9a–9d show cropped images with 1/16 and 1/4 of different sizes of ciphertext cropped, and Figs. 9e–9h display the reconstructed images that match the ciphertext image that was attacked with the cropping techniques. The experimental simulation findings illustrate that the majority of the initial image information remains intact in the encoded and reconstructed ciphertext image despite the cropping attack. This suggests that the approach may provide a degree of resistance against cropping attacks.

4.6.2 Anti-Noise Attack

The encryption system ought to be able to fend off malicious noise attacks directed at the encrypted image. Therefore, as an example, let us consider adding salt and pepper noise. We conducted a simulation experiment as displayed in Fig. 10.

Figs. 10a–10c illustrate the images depicting salt and pepper noise with concentrations of 0.001, 0.05, and 0.1, respectively. Additionally, Figs. 10d–10f present the reconstructed images that match the noise-affected ciphertext images. The experimental results indicate that the restored image can reveal information associated with the original image, suggesting that this approach can withstand noise attacks.

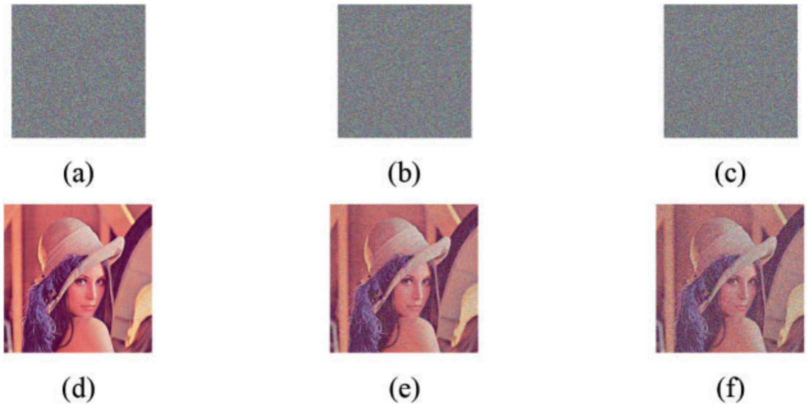


Figure 10: Anti-noise attack analysis

4.7 Compression Performance Analysis

The compression performance is assessed through the use of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) values. PSNR is one of the indicators for measuring image quality. In domains like image compression, it is often used to measure signal reconstruction quality. Mean Square Error (MSE), which is $MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [P(i,j) - I(i,j)]^2$, here, P represents the original image of size, whereas I denotes a noisy image. Then, PSNR is based on the definition of MSE. PSNR can be defined as: $PSNR = 10 \times \log_{10} \left(255^2/MSE\right)$.

SSIM is defined as $SSIM(x,y) = \left(\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)\right)/\left(\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)\right)$. Usually, SSIM with a range of values above 0.9 is considered an image of high quality.

As shown in the experimental results in Table 4, as an example, three channels of color images are used in this section. A higher PSNR value indicates a lower level of image distortion, resulting in a reconstructed image that closely resembles the original. As the compression ratio (CR) decreases, the reconstruction effect becomes worse, but important information can still be distinguished from it.

Table 4: PSNR and SSIM of the original image and reconstructed image

Image	CR	PSNR			SSIM		
		R	G	B	R	G	B
House256	0.9	41.5035	41.5153	40.2329	0.9652	0.9655	0.9577
	0.7	37.4520	37.9081	36.4775	0.9193	0.9318	0.9115
	0.5	34.3997	34.2699	33.3641	0.8610	0.8771	0.8474
Tree256	0.9	36.9224	36.9596	35.7426	0.9481	0.9548	0.9337
	0.7	32.3189	31.8310	31.0656	0.8810	0.9012	0.8588
	0.5	28.6948	26.9180	27.8649	0.7909	0.8209	0.7871

4.8 Running Time Analysis

The results of these evaluations are presented in Table 5, demonstrating that the encryption and decryption time differs according to the size of the images. The reconstruction time is often longer than the encryption time owing to this paper's combination of compressed sensing. Compared to [12] and [25], the combination of CS technology with the scheme in this paper results in a shorter encryption time. However, the decryption time is longer due to the extended duration required by the reconstruction algorithm. After comprehensive consideration, our algorithm has a slight advantage.

Table 5: Running time analysis

Image	Encryption time (s)			Decryption time (s)		
	Ours	Reference [12]	Reference [25]	Ours	Reference [12]	Reference [25]
House256	0.26834	2.33764	0.55346	2.71117	0.26988	0.45401
Tree256	0.28299	2.07799	0.38486	2.22668	0.27961	0.44971
Lena512	1.28151	3.96321	1.70280	4.23535	1.68899	1.77177
Baboon512	1.28066	4.32917	1.48969	4.36212	1.81652	1.62893

4.9 Ablation Experiment Analysis

This part of this paper underwent ablation experiments and was divided into five parts, and the effectiveness of each part is evaluated as follows:

(1) Only Arnold scrambling of images is carried out. Image scrambling plays a role in hiding and protecting image information, which can be encrypted and transmitted and used as a pre-processing of image processing.

(2) Only JPD encryption of images is carried out. When combined with a hyperchaotic system, they are indeed commonly employed as encryption methods.

(3) Only CS. Using the CS algorithm to process the image can compress and encrypt the image simultaneously.

(4) Arnold scrambling and JPD operations are carried out. The encryption performance is improved when the two image processing techniques are combined.

(5) The scheme of this paper. The combination of the encryption method and compression method makes image encryption more perfect.

Specifically, take a color picture of House with a size of 256 × 256 as an example. Table 6 includes the correlation coefficient, with the horizontal value taken as an example. Simulation experiments have demonstrated the effectiveness of the solution in this paper, which combines chaotic encryption with CS.

From Table 6, schemes (1)–(4) do not have as good of an encrypting effect as the one suggested in this study. Although some schemes have short encryption and decryption times, the encryption effect is poor. Image encryption should not only look at the time but also need to combine ciphertext image performance. Consequently, the experiment proves the effectiveness of the scheme.

Table 6: Ablation experiment analysis

Scheme	Encryption time (s)	Decryption time (s)	Information entropy			Correlation coefficient		
			R	G	B	R	G	B
(1)	0.07012	0.05876	6.4311	6.5389	6.2320	0.0183	0.0204	0.0209
(2)	0.26953	0.25946	7.9968	7.9965	7.9964	−0.0137	−0.0233	0.0121
(3)	0.06404	2.65594	6.6179	7.1741	7.3265	0.0296	−0.0155	−0.0180
(4)	0.31406	0.30617	7.9965	7.9968	7.9963	0.0162	−0.0125	0.0354
(5)	**0.26834**	**2.71117**	**7.9971**	**7.9970**	**7.9971**	**0.0035**	**0.0027**	**0.0014**

5 Conclusions

This work introduces a technique for color image compression and encryption that combines the hyperchaotic system with 2D CS. Firstly, this algorithm scrambles the original image. Subsequently, the scrambled image is compressed and encrypted simultaneously. Finally, for the sake of encryption security, the compressed and encrypted images are double-encrypted to achieve the ciphertext image. While decrypting, a reasonable image reconstruction algorithm is adopted to improve the reconstruction effect and reduce computational complexity. Experimental results show that it effectively resists several common attacks. Compared with existing advanced image encryption schemes, the proposed in this paper outperforms other schemes in performance and attack resistance. The validity of the encryption scheme has been verified. However, the decryption time is long, and we must improve it in our future work.

Acknowledgement: The editors and anonymous referees whose comments and recommendations have helped to improve this work are greatly appreciated by the authors. The authors would like to express their gratitude for the guidance and support provided by the research group.

Funding Statement: This work was supported in part by the National Natural Science Foundation of China under Grants 71571091, 71771112, the State Key Laboratory of Synthetical Automation for Process Industries Fundamental Research Funds under Grant PAL-N201801, and the Excellent Talent Training Project of University of Science and Technology Liaoning under Grant 2019RC05.

Author Contributions: The following contributions to the work are confirmed by the authors: study conception and design: Zhiqing Dong, Zhao Zhang; gathering of data: Zhiqing Dong; analysis and interpretation of results: Zhiqing Dong, Hongyan Zhou; draft manuscript preparation: Zhiqing Dong, Zhao Zhang, Hongyan Zhou, Xuebo Chen. All authors have thoroughly reviewed the results and have provided their approval for the manuscript in its final form.

Availability of Data and Materials: Data and materials are available upon request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Liang, H. Peng, L. Li, F. Tong, S. Bao and L. Wang, "A secure and effective image encryption scheme by combining parallel compressed sensing with secret sharing scheme," *J. Inf. Secur. Appl.*, vol. 75, pp. 103487, 2023. doi: 10.1016/j.jisa.2023.103487.

[2] Y. Tao, W. Cui, and Z. Zhang, "Spatiotemporal chaos in multiple dynamically coupled map lattices and its application in a novel image encryption algorithm," *J. Inf. Secur. Appl.*, vol. 55, pp. 102650, 2020. doi: 10.1016/j.jisa.2020.102650.

[3] C. Xu, D. Li, K. Guo, Z. Yin, and Z. Guo, "Computational ghost imaging with key-patterns for image encryption," *Opt. Commun.*, vol. 537, pp. 129190, 2023. doi: 10.1016/j.optcom.2022.129190.

[4] E. Gokcay and H. Tora, "A novel data encryption method using an interlaced chaotic transform," *Expert. Syst. Appl.*, vol. 237, pp. 121494, 2024. doi: 10.1016/j.eswa.2023.121494.

[5] X. Y. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, 2019. doi: 10.1016/j.ins.2019.02.049.

[6] A. Mehmood, A. Shafique, S. A. Chaudhry, M. Alawida, A. N. Khan, and N. Kumar, "A time-efficient and noise-resistant cryptosystem based on discrete wavelet transform and chaos theory: An application in image encryption," *J. Inf. Secur. Appl.*, vol. 78, pp. 103590, 2023. doi: 10.1016/j.jisa.2023.103590.

[7] M. Tang, G. Zeng, Y. Yang, and J. Chen, "A hyperchaotic image encryption scheme based on the triple dislocation of the Liu and Lorenz system," *Optik*, vol. 261, pp. 169133, 2022. doi: 10.1016/j.ijleo.2022.169133.

[8] M. J. Wang, M. Y. An, X. A. Zhang, and H. H. C. Iu, "Feedback control-based parallel memristor-coupled sine map and its hardware implementation," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 70, pp. 4251–4255, 2023. doi: 10.1109/TCSII.2023.3293109.

[9] J. Y. Wang, X. H. Song, H. Q. Wang, and A. A. Abd El-Latif, "Applicable image security based on new hyperchaotic system," *Symmetry*, vol. 13, no. 12, pp. 2290, 2021. doi: 10.3390/sym13122290.

[10] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process*, vol. 97, pp. 172–182, 2014. doi: 10.1016/j.sigpro.2013.10.034.

[11] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography," *Opt. Laser Technol.*, vol. 127, pp. 106171, 2020. doi: 10.1016/j.optlastec.2020.106171.

[12] T. Li, J. Shi, and D. Zhang, "Color image encryption based on joint permutation and diffusion," *J. Electron. Imaging*, vol. 30, pp. 013008, 2021. doi: 10.1117/1.JEI.30.1.013008.

[13] Q. Liang and C. X. Zhu, "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding," *Opt. Laser Technol.*, vol. 160, pp. 109033, 2023. doi: 10.1016/j.optlastec.2022.109033.

[14] W. Dong, Q. Li, Y. Tang, M. Hu, and R. Zeng, "A robust and multi chaotic DNA image encryption with pixel-value pseudorandom substitution scheme," *Opt. Commun.*, vol. 499, pp. 127211, 2021. doi: 10.1016/j.optcom.2021.127211.

[15] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, pp. 29–37, 2012. doi: 10.1016/j.optcom.2011.08.079.

[16] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, pp. 1289–1306, 2006. doi: 10.1109/TIT.2006.871582.

[17] Y. Xiao, L. Jiang, and Z. Wang, "Convergence of compressed sensing encryption and deep network recovery in RoF system," *Opt. Commun.*, vol. 548, pp. 129835, 2023. doi: 10.1016/j.optcom.2023.129835.

[18] J. Cai, A. Wen, P. Li, H. Zhuo, W. Zhang, and Y. Y. Dong, "Instantaneous photonic frequency measurement based on compressive sensing," *Opt. Commun.*, vol. 530, pp. 129189, 2023. doi: 10.1016/j.optcom.2022.129189.

[19] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, 2019. doi: 10.1016/j.optlastec.2019.01.039.

[20] R. Zhang and D. Xiao, "Double image encryption scheme based on compressive sensing and double random phase encoding," *Mathematics*, vol. 10, pp. 1242, 2022. doi: 10.3390/math10081242.

[21] X. Chai, J. Fu, Z. Gan, Y. Lu, and Y. Zhang, "An image encryption scheme based on multi-objective optimization and block compressed sensing," *Nonlinear Dyn.*, vol. 108, pp. 2671–2704, 2022. doi: 10.1007/s11071-022-07328-3.

[22] X. L. Chai, J. Y. Fu, Z. H. Gan, Y. Lu, Y. S. Zhang and D. J. Han, "Exploiting Semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission," *IEEE Int. Things J.*, vol. 10, pp. 7380–7392, 2023. doi: 10.1109/JIOT.2022.3228781.

[23] Y. Chen, C. Zhang, M. Cui, Y. Luo, T. Wu and X. Liang, "Joint compressed sensing and JPEG coding based secure compression scheme in OFDM-PON," *Opt. Commun.*, vol. 510, pp. 127901, 2022. doi: 10.1016/j.optcom.2022.127901.

[24] L. Chen, S. Tang, Q. Li, and S. Zhong, "A new 4D hyperchaotic system with high complexity," *Math. Comput. Simulat.*, vol. 146, pp. 44–56, 2018. doi: 10.1016/j.matcom.2017.10.002.

[25] R. Lin and S. Li, "An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm," *Secur. Commun. Netw.*, vol. 2021, pp. 1–18, 2021. doi: 10.1155/2021/5586959.

[26] D. Huo *et al.,* "A visually meaningful double-image encryption scheme using 2D compressive sensing and multi-rule DNA encoding," *Complex Intell. Syst.*, vol. 9, pp. 4783–4803, 2023. doi: 10.1007/s40747-023-00989-6.

[27] M. Imaduddin, Farikhin, and S. Hariyanto, "Analysis of orthogonal matching pursuit using orthogonal bases on digital image," *J. Phys. Conf. Ser.*, vol. 1776, pp. 012053, 2021. doi: 10.1088/1742-6596/1776/1/012053.

[28] J. H. Liu, S. K. Xu, X. Z. Gao, and X. Li, "Compressive radar imaging methods based on fast smoothed L0 algorithm," *Proc. Eng.*, vol. 29, pp. 2209–2213, 2012. doi: 10.1016/j.proeng.2012.01.289.

[29] M. A. T. Figueiredo, R. D. Nowak, and S. J. Wright, "Gradient Projection for sparse reconstruction: Application to compressed sensing and other inverse problems," *IEEE J. Sel. Top. Signal Process.*, vol. 1, pp. 586–597, 2008. doi: 10.1109/JSTSP.2007.910281.

[30] B. Zhang, D. Xiao, and Y. Xiang, "Robust coding of encrypted images via 2D compressed sensing," *IEEE Trans. Multimedia*, vol. 22, pp. 2656–2671, 2020. doi: 10.1109/TMM.2020.3014489.

[31] R. Montero-Canela, E. Zambrano-Serrano, E. I. Tamariz-Flores, J. M. Munoz-Pacheco, and R. Torrealba-Melendez, "Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks," *Ad Hoc Netw.*, vol. 97, pp. 102005, 2020. doi: 10.1016/j.adhoc.2019.102005.