Hindawi
Complexity
Volume 2020, Article ID 1987670, 18 pages
https://doi.org/10.1155/2020/1987670

Research Article

Parallel Encryption of Noisy Images Based on Sequence Generator and Chaotic Measurement Matrix

Jiayin Yu, Yaqin Xie, Shiyu Guo, Yanqi Zhou, and Erfu Wang

Electrical Engineering College, Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Erfu Wang; wangerfu@hlju.edu.cn

Received 23 December 2019; Revised 20 February 2020; Accepted 26 February 2020; Published 7 May 2020

Guest Editor: Viet-Thanh Pham

With the rapid development of information technology in today's society, the security of transmission and the storage capacity of hardware are increasingly required in the process of image transmission. Compressed sensing technology can achieve data sampling and compression at the rate far lower than that of the Nyquist sampling theorem and can effectively improve the efficiency of information transmission. Aiming at the problem of weak security of compressed sensing, this study combines the cryptographic characteristics of chaotic systems with compressed sensing technology. In the actual research process, the existing image encryption technology needs to be applied to the hardware. This paper focuses on the combination of image encryption based on compressed sensing and digital logic circuits. We propose a novel technology of parallel image encryption based on a sequence generator. It uses a three-dimensional chaotic map with multiple stability to generate a measurement matrix. This study also analyzes the effectiveness, reliability, and security of the parallel encryption algorithm for source noise pollution with different distribution characteristics. Simulation results show that parallel encryption technology can effectively improve the efficiency of information transmission and greatly enhance its security through key space expansion.

1. Introduction

Nowadays, the rapid evolution of information technology and data networks has brought great convenience to people's productivity and lives [1]. As the main carrier of information transmission, a network must store and forward a significant amount of information at any moment [2]. Among them, digital information is easy to store and forward, and noise does not accumulate, which makes it easy to store and transmit widely in the network. As an important information carrier in digital information, the digital image is widely used in national defense, education, medical treatment, finance, and other fields [3]. Effective encryption of digital image information can resist illegal attacks, malicious destruction, and destruction of information by criminals and realize the safe transmission of information [4]. In the traditional process of information transmission and encryption, the Nyquist sampling theorem is applied, which indicates that the sampling frequency must be more than twice the highest frequency when sampling a signal with limited bandwidth in order to ensure the complete recovery of the original signal from the sampling value [5]. In recent years, compressed sensing as a cryptosystem has attracted much attention owing to its low complexity and compressibility in the sampling process [6]. Compressed sensing can sample the compressible signal at the frequency far lower than that specified by Nyquist's sampling theorem and can ensure that the receiver can accurately reconstruct the original signal [7]. However, the encryption system under the traditional compressed sensing framework is vulnerable to plaintext attacks. To reduce the correlation between adjacent pixels of the encrypted image [8], an efficient image compression and encryption algorithm based on a chaotic system and compressed sensing was proposed in [9]. At the same time, owing to the use of diffusion and scrambling operations, the chaotic system has the characteristics of cryptography in order to achieve more effective encryption of image information.

Compressed sensing (CS), as a new signal sampling and compression technology [10], has been widely used in the

field of image processing since it was proposed [11]. Orsdemir et al. studied the robustness and security of CS-based encryption algorithms [12]. Schulz et al. analyzed the distortion performance of compressed sensing in image compression and compared it with traditional algorithms [13]. Fridrich discussed the relationship between discretization and chaotic cryptosystems and proposed a two-dimensional Baker-based symmetric image encryption algorithm. This algorithm uses image chaos to scramble and diffuse images to achieve image encryption [14]. Zhang proposed an image encryption algorithm about plaintext-related shuffling. This algorithm combines two types of diffusion operations and plaintext-related transformations to encrypt the image and uses hyper chaos to generate a keystream [15]. Enayatifar et al. proposed an image encryption scheme based on synchronous scrambling diffusion, using chaos mapping and a DNA encryption algorithm to diffuse and scramble pixels [16]. An image encryption algorithm based on two-dimensional sinusoidal coupled mapping and chaotic diffusion was proposed in the literature [17]. Chen et al. proposed an optical image conversion and encryption scheme based on a phase detection algorithm and incoherent superposition that can realize the conversion and encryption of color images and gray images [18]. Hua et al. used high-speed scrambling and pixel adaptation to encrypt an image. This can protect certain impulse noise and prevent data loss [19]. Gong et al. proposed an image encryption method combining a hyperchaotic system with a fractional-order discrete transform [20]. Zhang et al. [21] proposed an image encryption method combining orthogonal coding and double-random phase coding that can compress all images into random signals and diffuse them into stationary white noise. Wang et al. studied CS-based image optimization technology in three main aspects [22]. The signal after compressed sensing processing is optimized.

To improve the computational efficiency of compressed sensing and the security of image encryption, a parallel image encryption technique based on a sequence signal generator was proposed. Regarding information security, the algorithm aims to provide a new data fusion processing technology, design a new encryption scheme, create a plan under the premise of guaranteeing the safety of image encryption, and minimize the decryption time to reduce information storage. This indirectly reduces the cost of information transmission and storage. Owing to the sensitivity of the initial value and the complex dynamic behavior of chaotic systems, pseudo-random sequences with randomness, relevance, and complexity can be provided. When designing a CS measurement matrix, this algorithm introduces a chaotic system, which has cryptographic characteristics achieved through scrambling and diffusion [23]. Li et al. [24] proposed an image communication system for IOT monitoring combined with CS model which helps reduce the image encryption/decryption time. Zhou et al. [25] proposed an algorithm by using double random-phase encoding and compressed sensing to enhance the security of digital image encryption with authentication capability. Shi et al. [26] proposed an image CS framework using convolutional neural network. The sampling network adaptively learns the sampling matrix from the training image. This study combines compressed sensing with chaotic cryptography to optimize the encryption effect and transmission efficiency of compressed sensing and greatly improve the key space.

In the actual information transmission process, noise cannot be avoided, and the existence of noise seriously affects the image quality. Aiming at the problem of noise-contaminated signals and whether the original signal can be reconstructed effectively after being encrypted and compressed by the compressed sensing algorithm, Section 4 of this article will focus on presenting the analysis of the encrypted observation when the plaintext contains noise. Whether the image can meet the encryption requirements and whether the reconstructed image is accurate will be assessed.

2. Compressed Sensing and Chaos Theory

Compressed sensing technology was originally developed using the sparsity or compressibility of signals, and its theory includes three key technologies [27]. The first is the sparse representation of the target signal in order to thin the signal to the extent possible [28]. In this, we need to obtain the transform domain that matches the target signal ψ. The second is the construction process of measurement matrix. The target signal is compressed and sampled after passing through the measurement matrix, so the design of the measurement matrix needs to ensure that the effective information contained in the target signal is not lost [29]. The receiver can effectively recover the target signal by using the sampling value. The third is the design of the reconstruction algorithm. The reconstruction algorithm finds the optimal solution of the target signal by solving the optimization problem [30]. Whether the reconstruction algorithm has accuracy, efficiency, and stability is also key in algorithm design.

Chaos used in this study is a new three-dimensional map with self-excited structures as proposed by Jiang et al. in 2016 [31]. This kind of chaotic system has hidden chaotic dynamics, which is a new topic in nonlinear science and has attracted extensive attention from mathematical and engineering researchers in recent years. This kind of self-excited three-dimensional mapping can provide a deeper understanding of the complex behavior of chaotic dynamics hidden in discrete mapping. At the same time, the stability of these chaotic systems can be analyzed based on the existence of fixed points. In this algorithm, a three-dimensional system with a single fixed point is used. The stability of the system will be analyzed by calculating the fixed point of the system.

2.1. Mathematical Representation of Compressed Sensing. Suppose that a two-dimensional signal X of size $N \times N$ is needed in the process of achieving compressed sensing to make the signal sparse. Under the corresponding sparse space of the signal, CS can achieve effective compression and sampling. Using equation (1), CS can generate the sparse representation of the signal X under ψ [32]:

$$X = \sum_{n=1}^{N} \psi_n s_n = \psi s, \tag{1}$$

where ψ is the sparse basis matrix and s is the projection under the sparse basis ψ. In equation (1), if there exist $K(K \ll N)$ nonzero coefficients, the signal X is said to be compressible under a sparse basis ψ, and the sparsity is K [25]. If there is a two-dimensional matrix ϕ of size $M \times N\,(M < N)$, then the original signal X can be converted into a signal of size $M \times N$ by the following equation:

$$Y = \phi X = \phi \psi S, \tag{2}$$

where Y is the measurement value and ϕ is the measurement matrix. On the basis of the known measurement value Y and measurement matrix ϕ, CS can reconstruct the signal X by solving the equation which is underdetermined. In the traditional underdetermined equation, there should be infinite solutions [33]; however, because s is sparse, conversion to an optimization problem is possible. The unique optimal solution of the underdetermined equation can be arrived at by obtaining the minimum norm L_0 in the following equation:

$$\begin{aligned} &\min \quad \|s\|_0 \\ &\text{s.t.} \quad Y = \phi \psi s, \end{aligned} \tag{3}$$

where $\|m\|$ represents the L_0 norm, s is recovery signal, and Y is the measurement signal. Because s is obtained using a sparse-basis transformation, the signal X can be recovered from the signal s through a single inverse transformation.

2.2. Three-Dimensional Map with Single Fixed Point. From the computational point of view, if the attractor domain of the attractor does not intersect with a small balanced neighborhood, then the former can be classified as a hidden attractor; otherwise, it is called a self-excited attractor [34]. Classical chaotic attractors, such as the Lorenz, Chua, Chen, and other chaotic systems, are self-excited attractors with one or more unstable equilibrium points. Self-excited attractors can be predicted by a standard calculation program, but there is no effective method to predict the existence of hidden attractors owing to the unpredictability of hidden attractor [35]. Hidden attractors can determine the success or failure of a project in engineering. It has become a new trend to study the continuous chaotic systems with implicit and multistable attractors.

This algorithm uses a three-dimensional chaotic map (SF1) with a single fixed point. The map was proposed in [31], which used a computer exhaustive search program to mine the hidden attractors contained in the map with stability. The mathematical expression is as follows:

$$\text{SFI} = \begin{cases} x_{k+1} = y_k, \\ y_{k+1} = z_k, \\ z_{k+1} = 0.6x_k + 0.39y_k + 0.65x_k^2 - 0.65y_k^2. \end{cases} \tag{4}$$

In order to solve the fixed points of the three-dimensional mapping above, it is first assumed that there are fixed points (x^*, y^*, z^*) in equation (4). The Jacobian matrix at the fixed point is shown as follows:

$$J = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0.6 + 1.3x^* & 0.39 - 1.3y^* & 0 \end{bmatrix}. \tag{5}$$

The characteristic equation of the above equation is shown in the following equation:

$$\det(\lambda I - J) = \lambda^3 + p\lambda^2 + q\lambda + r = 0, \tag{6}$$

where $p = -\text{tr}(J) = 0$, $q = -(0.39 + 1.35y^*)$, $r = \det(J) = -(0.6 + 1.3x^*)$, and tr is the trace of the Jacobian matrix. We can determine the unique fixed point $x^* = y^* = z^* = 0$ based on the definition of the fixed point. According to equation (6), the eigenvalues $|\lambda_1| = 0.7761$, $|\lambda_2| = 0.7761$, and $|\lambda_3| = 0.9962$ of the three-dimensional system shown in (4) can be obtained. The eigenvalues of the Jacobian matrix at this fixed point λ_1, λ_2, and λ_3 are all in the unit circle, that is, $|\lambda_i| < 1$. Therefore, the fixed point of the three-dimensional chaotic map is stable, that is, the chaotic map has the hidden chaotic attractor of the stable fixed point. Attractors of the chaotic maps are shown in Figure 1.

3. Parallel Compressed Sensing Encryption Algorithm Based on Sequence Generator

In the image encryption and transmission process, the complete image can be transmitted directly or by row or column. The efficiency of image transmission depends on the dimensions of the image information. In order to improve the efficiency of encryption and transmission, this study designs a block and parallel compressed sensing encryption algorithm. We study this problem in detail and introduce a logic circuit-based compressed sensing encryption method in [36]. Based on this algorithm, this paper makes a further study. By selecting appropriate block dimensions, the image is divided into blocks, and the blocks are encrypted and transmitted in parallel. This method can greatly improve the transmission efficiency of the image. In the process of designing the measurement matrix, this algorithm is based on the sensitivity and pseudorandom performance of chaotic signals to initial values, as well as the cryptographic characteristics of chaos under the mechanism of diffusion and scrambling. Combined with the feature that compressed sensing needs to rely on a measurement matrix for compressed sampling, the security of a traditional compressed sensing framework is not high, and the reconstruction wastes a large amount of storage resources.

3.1. Algorithm Principle. This algorithm adopts a combination of a digital logic circuit and compressed sensing theory. First, the binary sequence signal of the length is generated through the sequence signal generator, and the binary sequence signal is taken as the "modulation signal." Based on chaotic system's sensitivity to the "tiny disturbance" of the initial conditions, for chaotic systems, the initial value of any small changes can directly affect the entire

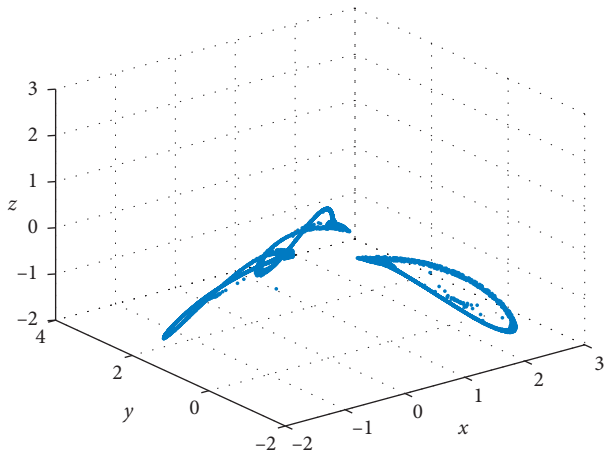


Figure 1: SF1 attractor.

chaos matrix generation. In this way, the security of image encryption can be improved. Second, the chaos matrix disturbed by the initial value is taken as the measurement matrix, and the compressed sensing process is used to encrypt the image. In this study, a 256×256 image is segmented into eight blocks by columns, and the image is segmented and compressed in parallel. In order to better present the chaotic cryptographic characteristics, this algorithm diffuses and scrambles the compressed sampled cipher text image so that the energy blocks gathered in blocks in the cipher text image after block encryption can be evenly distributed. This is distributed on the entire image to achieve effective encryption and efficient transmission of the image information. The realization principle diagram of this algorithm is shown in Figure 2.

3.2. Sequence Signal Generator Mode. In this study, a shift register with feedback logic circuit is designed, as shown in Figure 3. If the number of bits of the sequence signal is m and the number of bits of the shift register is n, then $2^n \geq m$ should be used. For example, to generate a set of 8 bit sequence signals such as 00101110 (time sequence from left to right), a 3 bit shift register and a feedback logic circuit can be used to form the required signal generator. The shift register outputs the serial output signal from end Q_2, that is, the required sequence signal.

The sequence signal generated according to the requirements can list the state transition table that the shift register should have, as shown in Table 1. Starting from the requirements of state transition, the requirements for the value of input D_0 of the shift register are obtained. According to the value requirements, the functional relationship between D_0 and Q_2 and Q_1 and Q_0 can be obtained as shown in the following formula:

$$D_0 = Q_2 Q_1' Q_0 + Q_2' Q_1 + Q_2' Q_0'. \tag{7}$$

The state transition table is shown in Table 1.

The clock signal is continuously added to the counter, and the state of $Q_2 Q_1 Q_0$ circulates continuously according to the order given in Table 1. Q_2 is the output end of the sequence signal, and the feedback logic circuit in the generator can be used as the key to modulate the initial value of the chaotic system. It should be noted that the purpose of generating different sequence signals can be realized only by modifying the functional relationship of the feedback logic circuit, so this circuit possesses the characteristics of flexibility and convenience.

3.3. Parallel Compressed Sensing. In this study, the initial value of the chaotic system is fine-tuned by the binary sequence signal generated in the previous section, and different chaotic matrices are generated as the measurement matrices to realize the compressed sensing process. In the image process compression and encryption using compressed sensing, it is necessary to set the compression ratio, adjust the dimensions of the measurement matrix according to the size of the compression ratio, and realize the compression sampling process of the sparse image. In this algorithm, the sparse plaintext image is evenly divided into eight blocks according to the column, and the size of each block is 256×32. Compared with the transmission by column, eight-block parallel transmission can effectively improve the efficiency. The parallel compression sampling process is shown in Figure 4.

It should be noted that although the parallel compressed sensing image encryption scheme can effectively and reliably encrypt the image, it is not bereft of some defects. Since the plaintext image is sampled as a block, the energy of each block in the measured value is stored centrally. To overcome this defect, we adopt diffusion and scrambling operations to evenly distribute the energy of the cipher text image in the entire image. The reference formula for the diffusion process is as follows:

$$Q^*(n) = Q(n) \oplus k_d(n) \oplus Q^*(n-1), \tag{8}$$

where $Q(n)$ is the current operated element, $Q^*(n)$ is the output cipher element, $Q^*(n-1)$ is the previous cipher element, and $k_d(n)$ is the corresponding key stream.

3.4. Encryption Performance Analysis. We select a 256×256 gray image "Pepper" from the standard test gallery. The image is sparsed by using a discrete wavelet transform, and the sparse image is divided into eight parts. Each part has dimensions of 256×32. The initial value of the chaotic system is as follows: $x(1) = 0.17$, $y(1) = 1.63$, and $z(1) = -1.18$. According to the method detailed in Section 3.1, the sequence signal generator is designed to generate the binary signal 00101110. When the sequence signal is 1, the initial value of chaos is fine-tuned to a step size of 10^{-8}. When the sequence signal is 0, the initial value at this point is kept unchanged to generate the chaotic signal. The chaos matrix is used as the measurement matrix, and eight subblocks of the image are compressed and sampled in parallel by means of compressed sensing. The dimensions of the measurement matrix in the encryption process are 190×256, so the compression ratio is 74.2%. Finally, the encrypted cipher text image is diffused. Figure 5 shows the

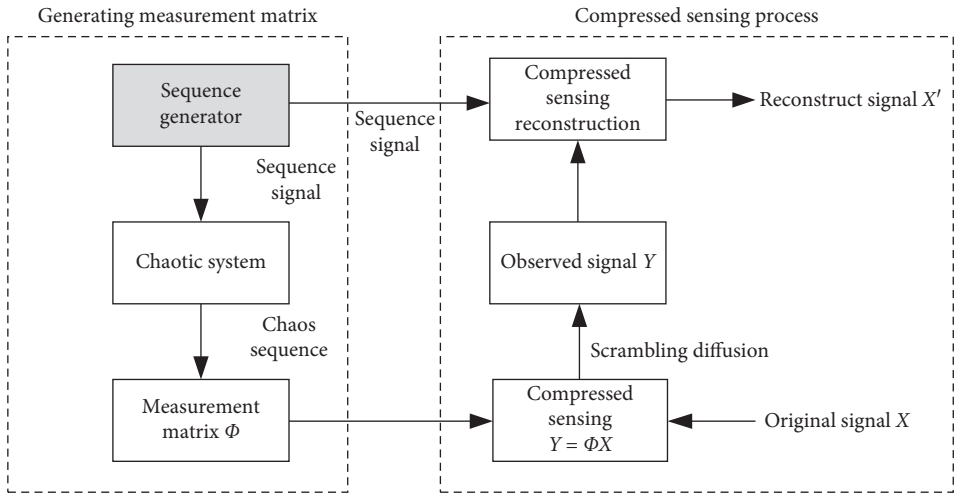


Figure 2: Parallel compression sensing encryption algorithm based on sequence generator.

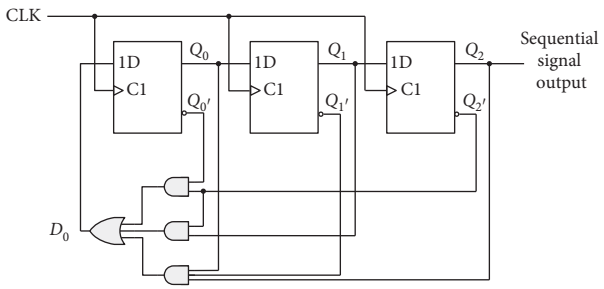


Figure 3: Signal generator based on shift register.

Table 1: Circuit state transition.

CLK	Q_2	Q_1	Q_0	D_0
0	0	0	0	1
1	0	0	1	0
2	0	1	0	1
3	1	0	1	1
4	0	1	1	1
5	1	1	1	0
6	1	1	0	0
7	1	0	0	0
8	0	0	0	1

original image, encrypted image, diffused image, and difference between the encrypted image and diffused image.

As can be seen from Figure 5, the algorithm described in this study presents a snowflake shape after encrypting sparse images, and it is unable to distinguish any information related to plaintext by the naked eye. From a subjective perspective, it can be considered that this algorithm achieves effective encryption of plaintext. Next, the encryption effect and reconstruction effect are analyzed from an objective perspective to verify that this algorithm can achieve the secure encryption and effective decryption of plaintext images. Figure 6 shows the original image, diffused image, and their histograms.

The histogram in Figure 6(c) can clearly reflect the distribution of pixel values, from which we can obtain relevant information of the image. However, the pixel values in Figure 6(d) are evenly distributed within the range [0, 255]. Different from the normal image, the attacker cannot obtain any valid information of the original image from the encrypted image. From the perspective of the histogram, this algorithm achieves effective encryption of the plaintext image.

Information entropy is an index used in information theory to measure the amount of information. Conversely, the more chaotic the system, the higher the information entropy. For image information, the image information entropy with high information is lower, while the image information entropy with low effective information is higher. The higher the entropy is, the more evenly the energy distribution in the image is and the less information the attacker can obtain. Table 2 shows the change of information entropy with the compression ratio when the compression rate changes.

As can be seen from the table, the entropy value of the image encrypted by the algorithm in this study is close to 8, indicating that the algorithm achieves secure encryption of the image.

3.5. Decryption (Reconstruction) Effect and Performance. This algorithm uses compressed sensing to encrypt the image. The decryption process can be regarded as the inverse operation of the encryption process. The decryption process can also be seen as the reconstruction process of the image. First, the cipher text is antidiffused, and the formula is shown as (9). The receiving end generates sequence signals according to the key it holds and generates the initial value control parameters of the measurement matrix. The chaotic matrix is restored according to the control parameters, and the measurement matrix is obtained. The sparse signal is reconstructed by solving the optimization problem. The formula for solving the optimization problem is shown in (10). Finally, the plaintext image is restored by using equation (11).

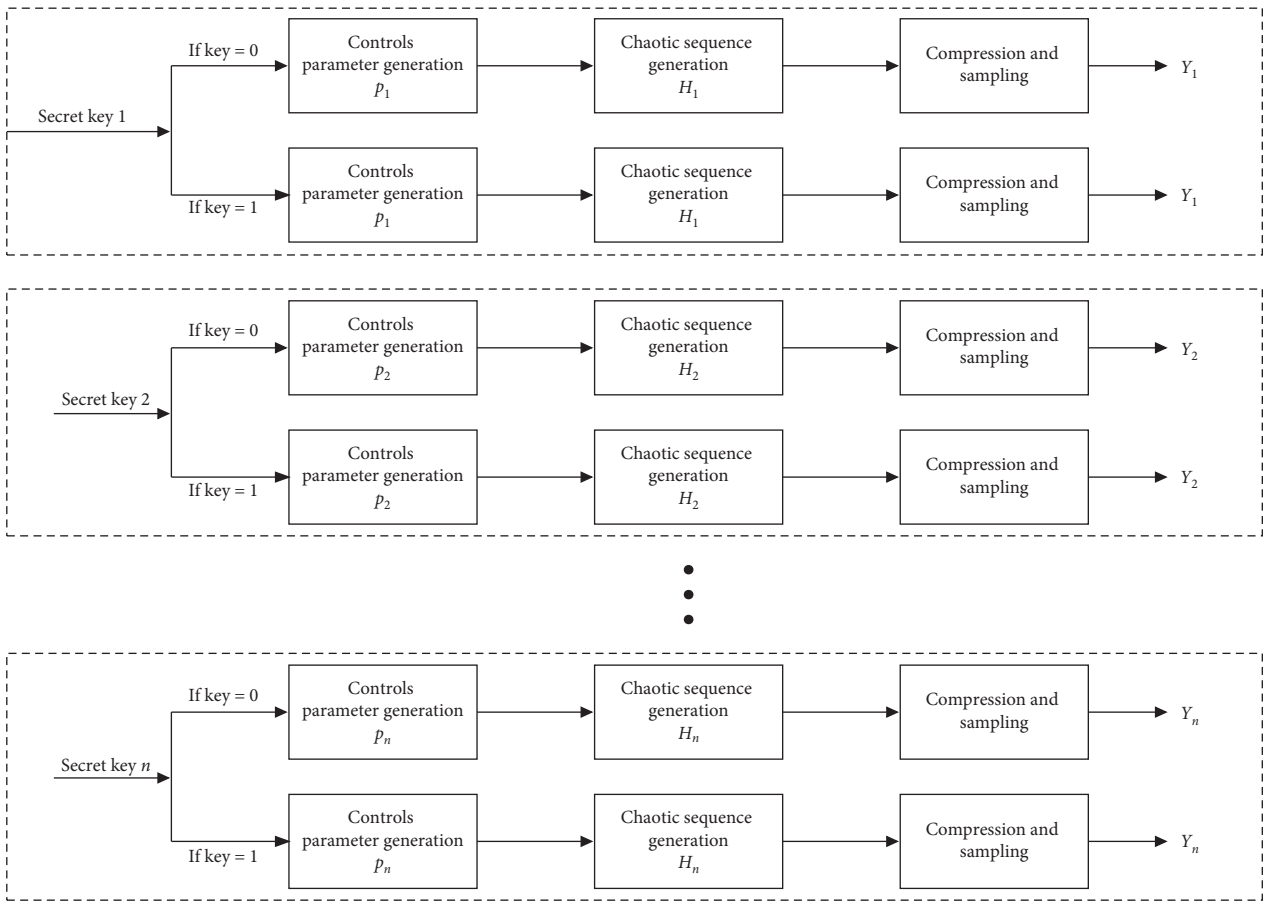


Figure 4: Parallel sampling compression of compressed sensing process.

$$Q(n) = Q^*(n) \oplus Q^*(n-1) \oplus k_d(n), \tag{9}$$

$$\begin{aligned} &\widehat{s}_i = \arg\min_{s_i \in R^N} \left\| s_i \right\|_1 \\ &\text{s.t. } \widehat{y}_i = \phi_i x_i = \phi_i \psi_i s_i, \\ &\qquad\qquad i = 1, \ldots, N, \end{aligned} \tag{10}$$

$$\widehat{x}_i = \psi \widehat{s}_i. \tag{11}$$

According to the above process, the original image, reconstructed image, and their histograms are shown in Figure 7.

According to Figure 7(b), we see that this algorithm can achieve reconstruction of cipher text. The image reconstruction reflects a clear image of effective information. Comparing Figures 7(c) and 7(d) of the histogram, the reconstructed image can be found in the original image and the pixel distribution is basically similar, and we can assume that this algorithm can realize image reconstruction.

Structural similarity is an index that measures the similarity of two images, and the value ranges from 0 to 1. The closer the similarity to 1, the higher the similarity of two images; otherwise, the greater the difference. Table 3 shows the structural similarity between the original image and reconstructed image at different compression rates.

As can be seen from Table 3, with an increasing compression rate, the image similarity also increases. When the compression rate is about 74.2%, the image can recover over 90%. However, the similarity of cipher text is very low, which indicates that this algorithm can achieve the image encryption requirements.

4. Encryption and Decryption Algorithms for Noisy Images and Performance Analysis

In the process of actual transmission, the information is composed of different kinds of noise pollution. Noise may be derived from the source with the noise of the signal, from the transmission channel through additive noise, or can be derived from the actual produced physical noise. The existence of noise affects the accuracy of information transmission. This section will present the analysis of whether the algorithm can still effectively encrypt and successfully reconstruct the image when the noise is mixed at the source.

4.1. Encryption and Reconstruction Results. This study intends to add Gaussian noise and salt-and-pepper noise to the original image, sparse the original image containing noise, and compress and perceive the sampling encryption. This is used to verify whether the compressed sensing image encryption technology optimized by this algorithm has the

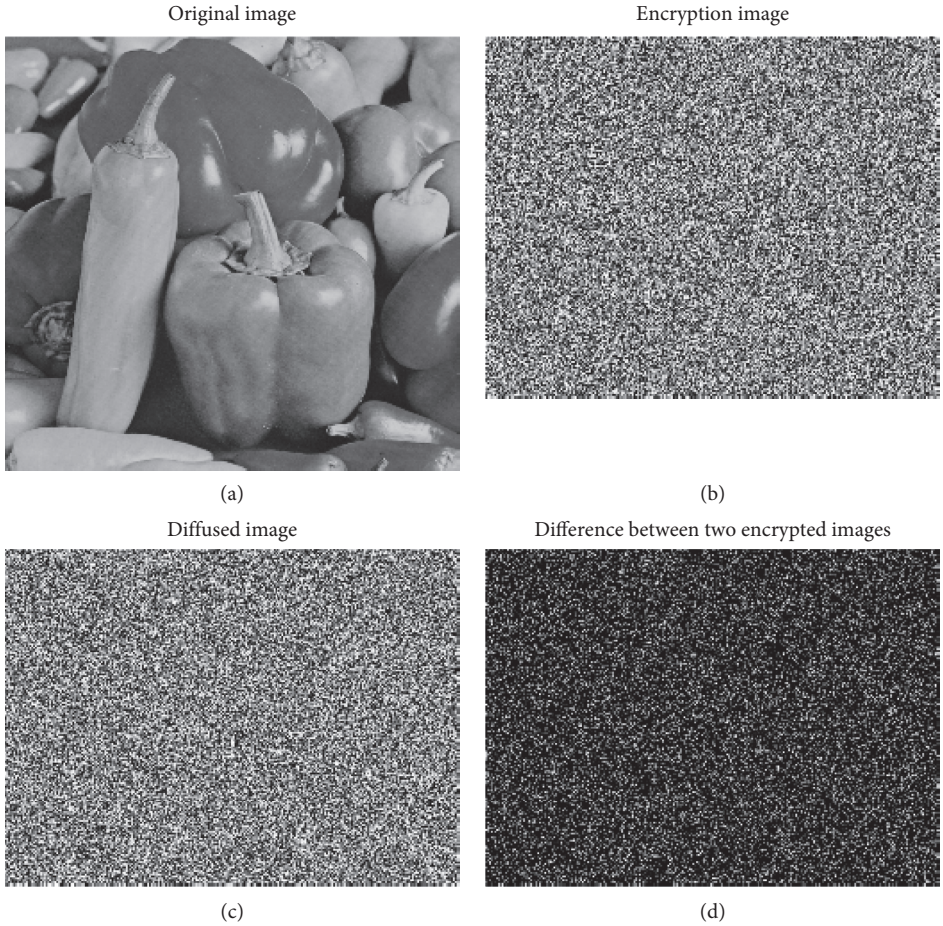


Figure 5: Results of gray image parallel compression perception encryption: (a) original image, (b) compressed sensing encrypted image, (c) diffused cipher text image, and (d) difference between (b) and (c).

ability to resist source noise. The salt-and-pepper noise used in this section has a noise density of 0.02, average Gaussian noise of 0, variance of 0.01, and compression ratio of 0.8. First, it is determined whether the image with noise can be reconstructed at the receiving end. The simulation results and histogram of adding salt-and-pepper noise to the original image are shown in Figure 8, and the simulation results and histogram of adding Gaussian noise are shown in Figure 9.

As can be seen from Figures 8(b) and 9(b), after adding noise to the original signal, the cipher text image encrypted by the algorithm in this study still resembles a snowflake, and the useful information in the image cannot be identified by observation. The histograms of Figures 8(e) and 9(e) are evenly distributed, indicating that we have successfully hidden the effective information of the original image, and the attacker cannot attack the algorithm using a statistical attack. Figures 8(c) and 9(c) show the recovered images of the encrypted image after the reconstruction algorithm. It can be seen that although the image still contains noise, the reconstructed image can be restored to the original image after filtering. It shows that the algorithm has a certain ability to resist the source noise. Since the intensity and variance of the noise we added to the original picture are both low, by comparing Figures 8(d), 8(f), 9(d), and 9(f), we can see that the image is polluted with salt-and-pepper noise. The reconstructed image has a better restoration effect after reconstruction, the image is clear, the histogram distribution is similar to the original image, and the signal contaminated by Gaussian noise is greatly affected, but it can still effectively recover the original information.

4.2. Encryption Performance Analysis. When the information entropy of the image is low, it is vulnerable to malicious attacks and tampering by criminals. For encrypted images, the higher the information entropy is, the more uniform the energy distribution in the image is and the less useful information an attacker can obtain from the grayscale distribution. Table 4 shows the changes in the entropy of the encrypted image when the compression ratio changes during the compression and encryption process. The noise intensity of the salt-and-pepper noise selected during the experiments in this section is 0.02; the mean and variance of the Gaussian noise are 0.2 and 0.01, respectively; and the compression rate of the compressed sensing process is 74.2%. In the table, I represents the noise intensity, M represents the mean, and V represents the variance.

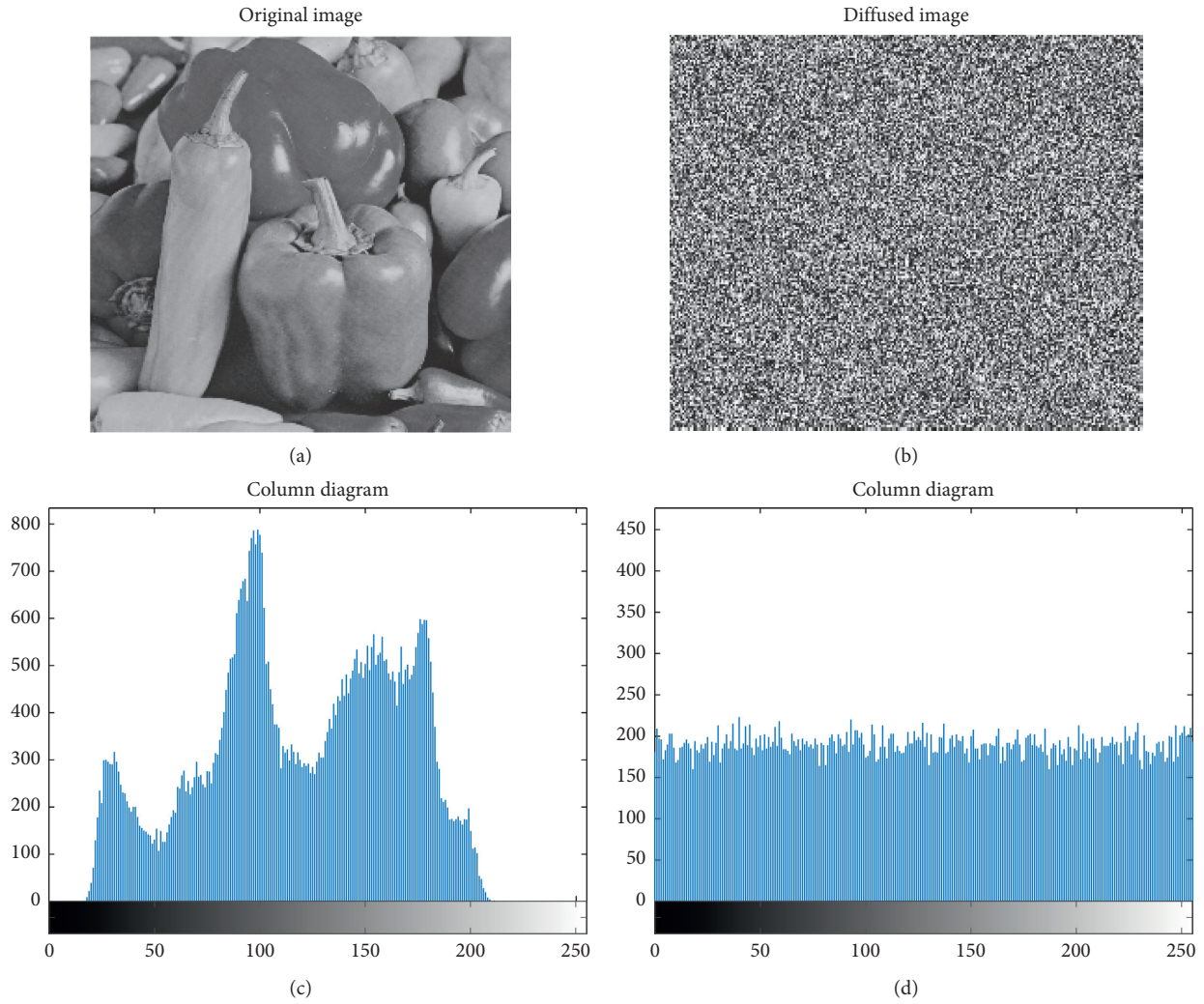


Figure 6: Histogram of original and encryption image: (a) original image, (b) cipher image, (c) histogram of plaintext image, (d) and histogram of cipher text image.

Table 2: Information entropy of encrypted images.

Entropy	Compression ratio							
	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
Cipher image	7.9920	7.9936	7.9937	7.9954	7.9960	7.9965	7.9972	7.9970

The table lists the cipher text entropies under the influence of salt-and-pepper noise and Gaussian noise with different parameters. It shows that the entropy value of the image after encryption in this study is close to 8, which can achieve effective encryption.

The correlation between adjacent pixels in an image can reflect the degree of diffusion of pixels in the image. The correlation between adjacent pixels in an encrypted image should be close to zero. In [33], a fractional-order Mellin transform is used to compress the image from two directions to obtain the encrypted image. Meanwhile, in [37], a discrete fractional-order random measurement matrix is used to encrypt the image from orthogonal directions. In this study, the correlation of adjacent pixels is compared with the above two studies to prove the effectiveness of this algorithm. Table 5 shows the correlation of adjacent pixels under the influence of salt-and-pepper noise and Gaussian noise, respectively.

Figure 10 shows the adjacent pixel correlation distribution between the plaintext image and the encrypted image when the original signal is polluted by salt-and-pepper noise with a noise intensity of 0.02. From the figure, we can see that the plaintext image has a high degree of correlation, while the adjacent pixels in the cipher text image are evenly distributed in the pixel interval, and the correlation is very weak. Therefore, according to the data and image results, it can be seen that the algorithm in this study can still achieve a good encryption effect when the signal source is polluted by noise.

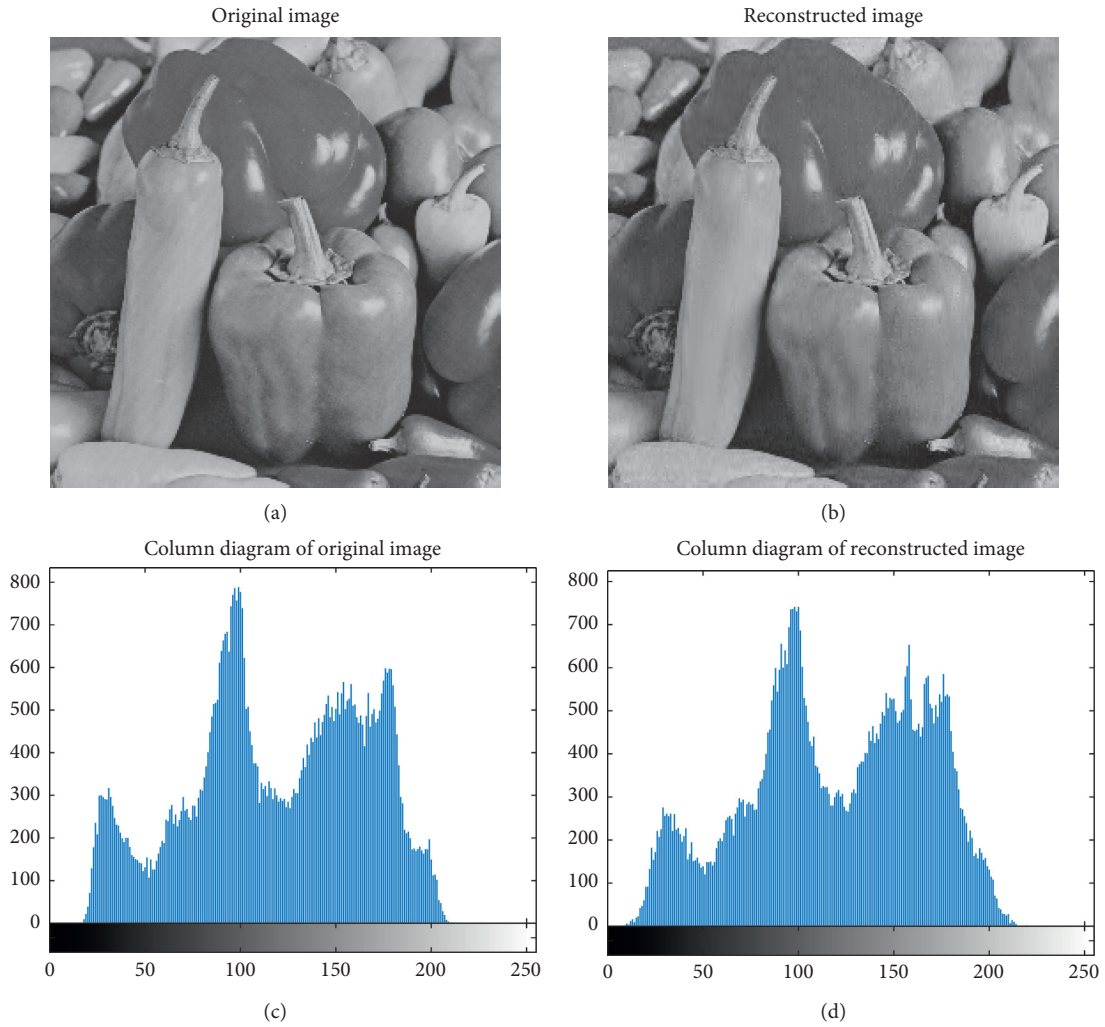


Figure 7: Histogram of original and reconstructed image: (a) original image, (b) reconstructed image, (c) histogram of original image, and (d) histogram of reconstructed image.

Table 3: Structural similarity between original image and reconstructed image.

SSIM	Compression ratio							
	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
Reconstructed image	0.4528	0.6356	0.7761	0.8592	0.9059	0.9453	0.9607	0.9813
Cipher image	0.0025	0.0034	0.0043	0.0055	0.0066	0.0070	0.0079	0.0092

Structural similarity is an index that can measure the similarity of two images. The structural similarity of natural images is very high, which is reflected in the strong correlation between the pixels of images. The value range of structural similarity is 0 to 1. When the similarity is close to 1, the more similar the two pictures, the more different the two pictures. Table 6 shows the structural similarity between the encrypted image and the original image under the influence of salt-and-pepper noise and Gaussian noise.

As can be seen from the table, the structural similarity of cipher text images affected by any noise is less than 0.2, which can achieve a satisfactory encryption effect.

4.3. Decryption (Reconstruction) Performance Analysis. The peak signal-to-noise ratio (PSNR) refers to the ratio between the maximum possible power of a signal and the destructive noise power that affects its signal accuracy. It can be defined by the mean square error (MSE), and its expression is shown as follows:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{L^2}{\mathrm{MSE}}\right), \tag{12}$$

where L is the value range of grayscale in the image. For the 8 bit image, $L = 256$. In general, the higher the PSNR, the lower the distortion.

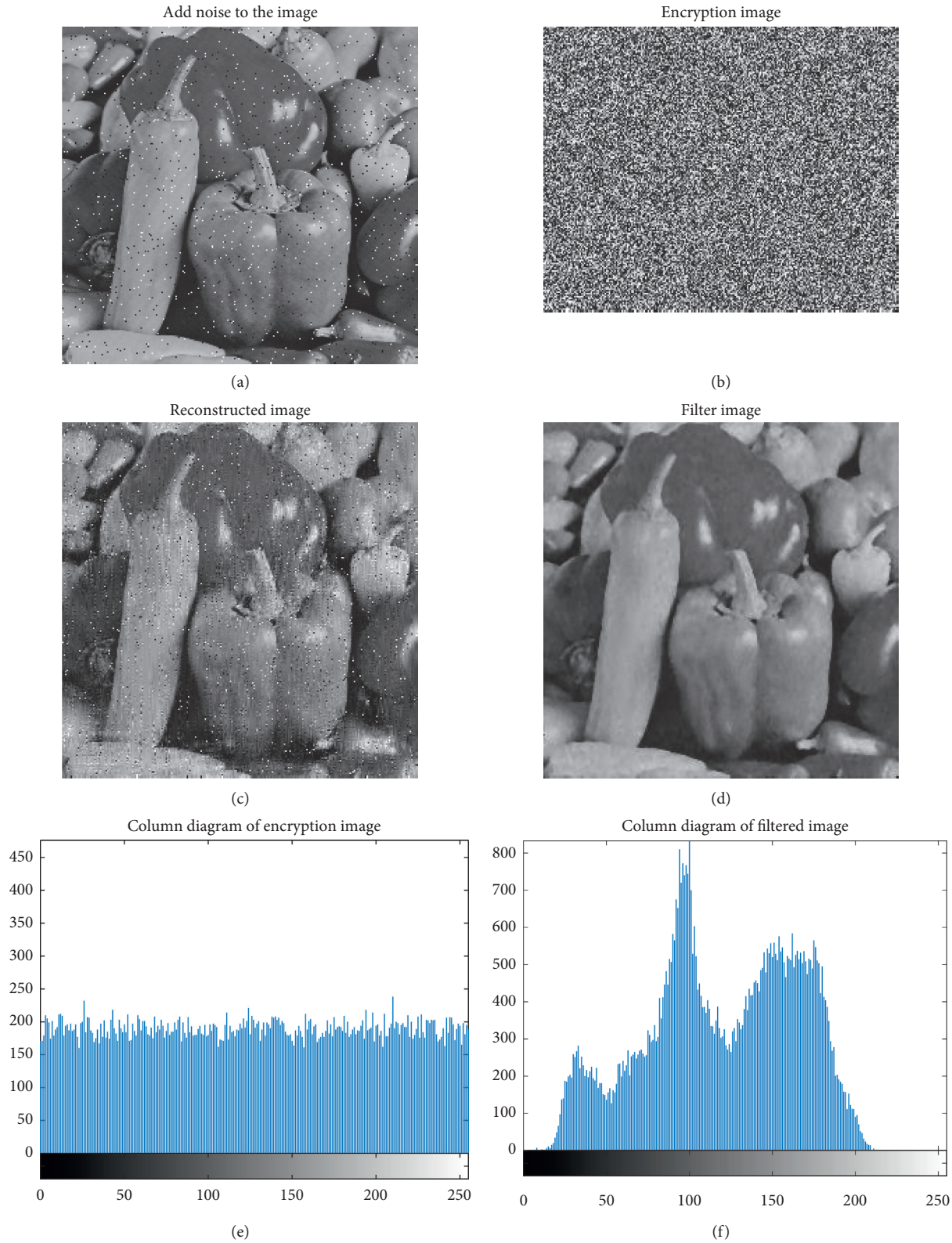


Figure 8: Encryption and reconstruction of noisy images: (a) image with noise, (b) cipher image, (c) reconstructed image, (d) filtered image, (e) histogram of cipher text image, and (f) histogram of filtered image.

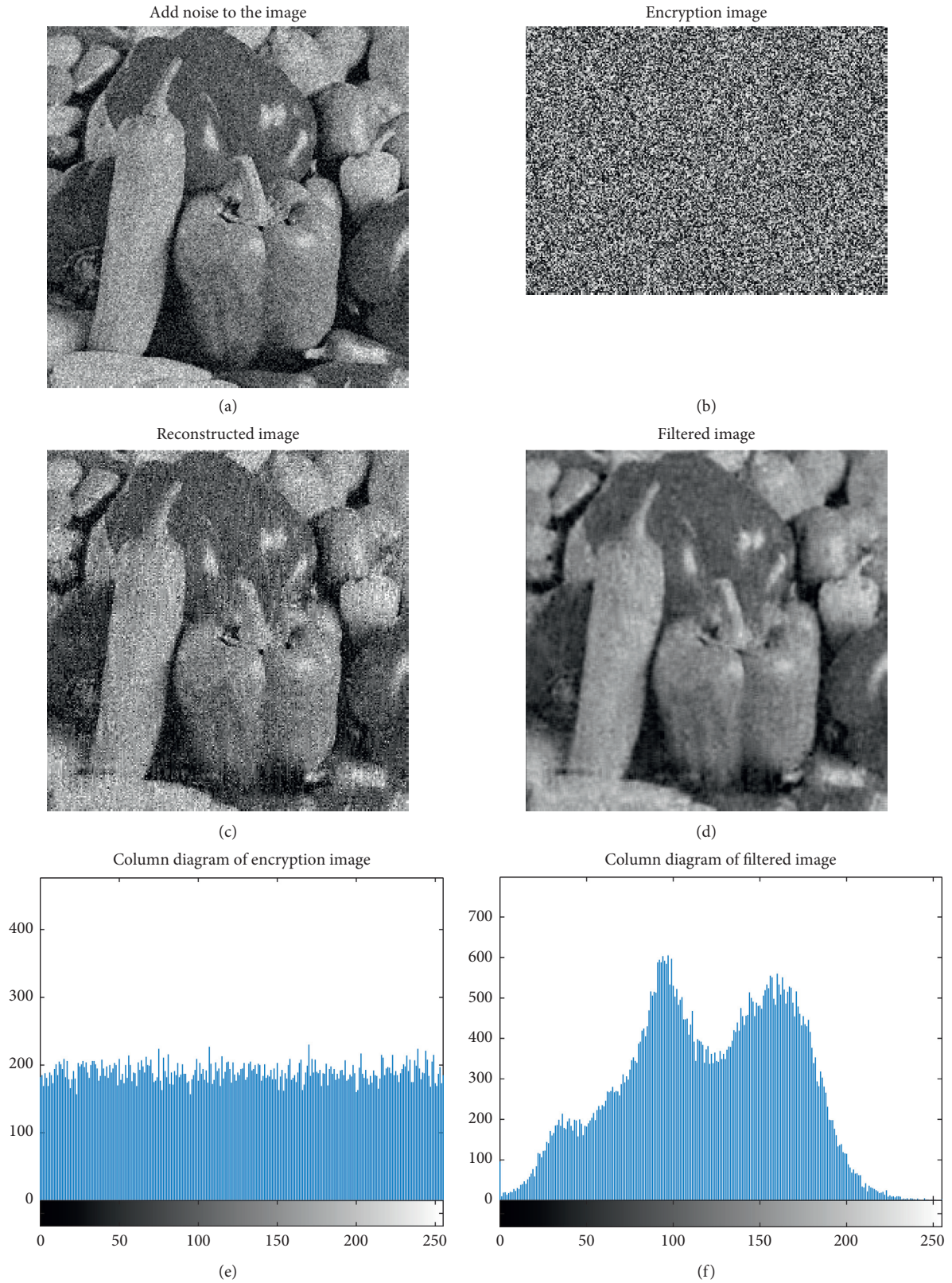


Figure 9: Encryption and reconstruction of noisy images: (a) image with noise, (b) cipher image, (c) reconstructed image, (d) filtered image, (e) histogram of cipher text image, and (f) histogram of filtered image.

Table 4: Information entropy of encrypted images.

Entropy		Compression ratio						
		0.3	0.4	0.5	0.6	0.7	0.8	0.9
Salt-and-pepper noise	$I = 0.02$	7.9918	7.9934	7.9948	7.9948	7.9962	7.9964	7.9970
	$I = 0.05$	7.9913	7.9933	7.9936	7.9955	7.9957	7.9966	7.9971
	$I = 0.1$	7.9921	7.9930	7.9944	7.9962	7.9957	7.9965	7.9971
Gaussian noise	$M = 0,\ V = 0.01$	7.9902	7.9939	7.9951	7.9954	7.9962	7.9955	7.9970
	$M = 0,\ V = 0.02$	7.9901	7.9928	7.9946	7.9956	7.9962	7.9969	7.9967
	$M = 0.2,\ V = 0.01$	7.9901	7.9925	7.9950	7.9951	7.9960	7.9961	7.9971

Table 5: Correlation between adjacent pixels of cipher text image.

Algorithm	Horizontal direction	Vertical direction	Diagonal direction
Proposed algorithm (impulse noise)	0.0498	−0.0035	0.0032
Proposed algorithm (Gaussian noise)	−0.0398	0.0051	0.0042
Reference [30]	0.0586	−0.0021	0.0269
Reference [25]	0.0597	0.0766	0.0083

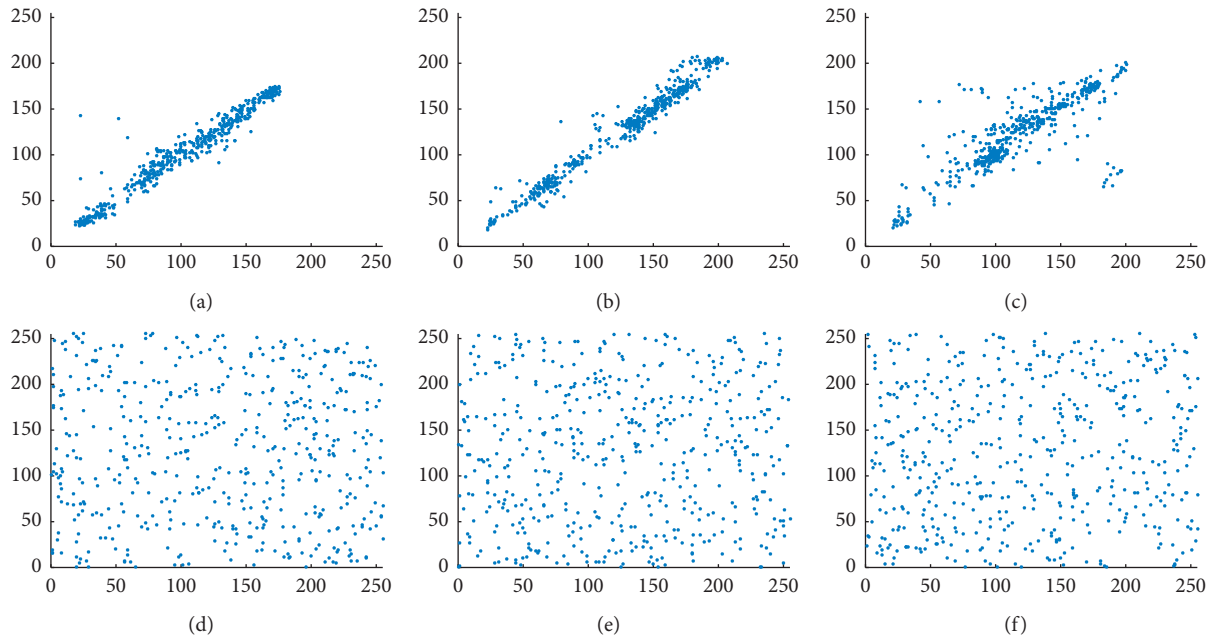


Figure 10: Distribution of adjacent pixels: (a) plaintext horizontal adjacent pixels, (b) plaintext vertical adjacent pixels, (c) plaintext diagonal adjacent pixels, (d) cipher text horizontal adjacent pixels, (e) cipher text vertical adjacent pixels, and (f) cipher text diagonal adjacent pixels.

Table 6: Structural similarity between original image and cipher image.

SSIM (cipher image)		Compression ratio						
		0.3	0.4	0.5	0.6	0.7	0.8	0.9
Impulse noise	$I = 0.02$	0.0042	0.0044	0.0064	0.0085	0.0071	0.0067	0.0074
	$I = 0.05$	0.0024	0.0018	0.0049	0.0036	0.0041	0.0047	0.0052
	$I = 0.1$	0.0020	0.0026	0.0020	0.0035	0.0074	0.0066	0.0076
Gaussian noise	$M = 0,\ V = 0.01$	0.0.017	0.0024	0.0031	0.0054	0.0053	0.0113	0.0104
	$M = 0,\ V = 0.02$	0.0022	0.0020	0.0041	0.0031	0.0051	0.0063	0.0120
	$M = 0.2,\ V = 0.01$	0.0023	0.0022	0.0039	0.0068	0.0089	0.0112	0.0063

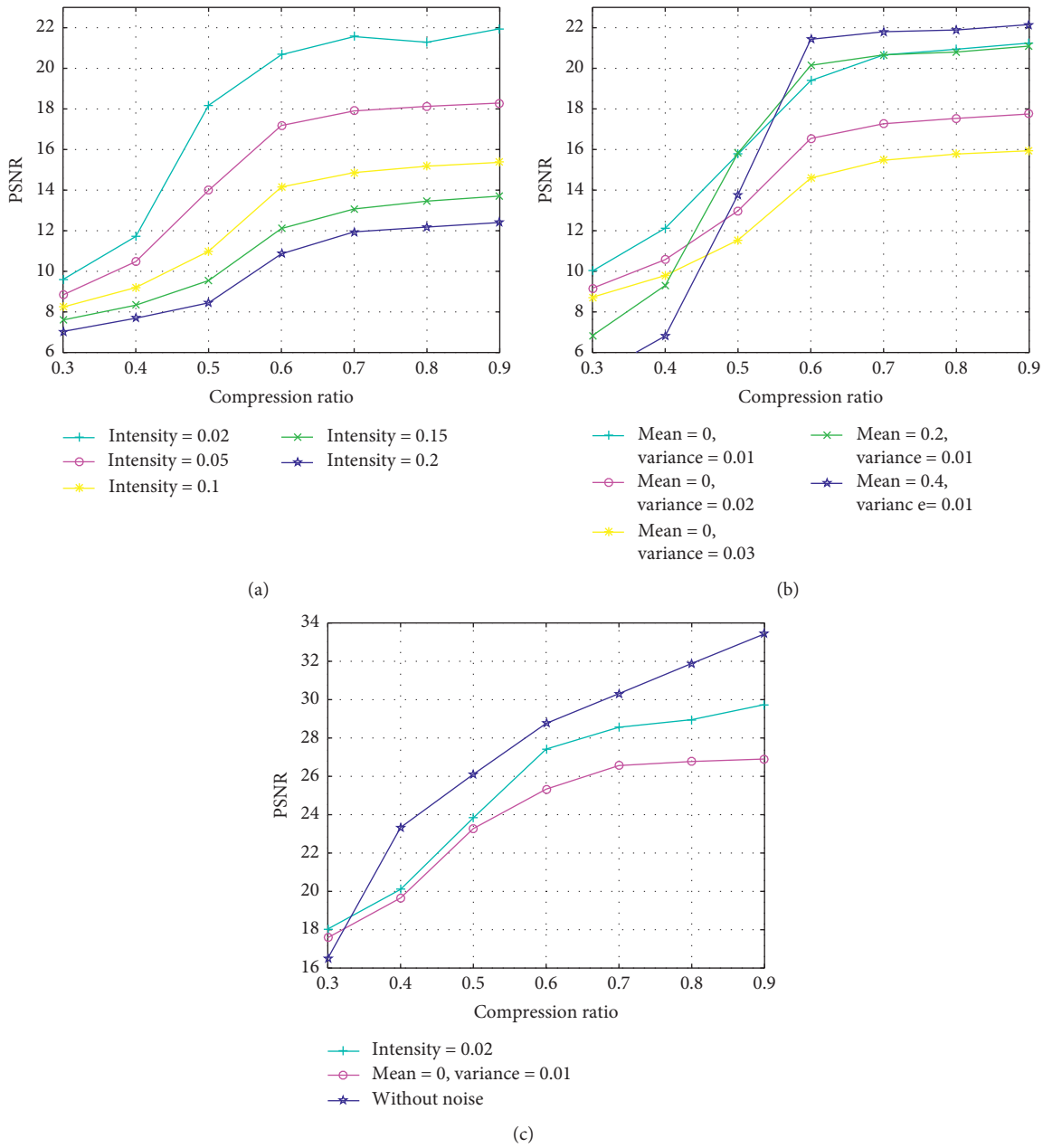


Figure 11: PSNR of reconstructed image: (a) PSNR of impulse noise, (b) PSNR of Gaussian noise, and (c) PSNR of filtered image.

Figure 11 shows a line chart of the peak signal-to-noise ratio of the restored picture under the salt-and-pepper noise with different noise intensities and Gaussian noise pollution with different mean variances.

It can be seen from Figure 11(a) that the PSNR of the reconstructed image increases with the reduction of salt-and-pepper noise intensity, and the curve trend in the figure is relatively consistent. In Figure 11(b), there are two variables (mean value and variance), and the curve in the figure has a large fluctuation. Since it has not been filtered, the reconstructed image still contains noise. When calculating PSNR, the noise in the image will have a certain impact on the calculated value. The PSNR value after filtering can be improved effectively. It can be seen from the performance analysis of encrypted images in Tables 4–6 that the images encrypted by the algorithm in this paper can meet the encryption requirements of images. In Figure 11(c), PSNR values under the condition of filtering salt-and-pepper noise, filtering Gaussian noise, and no noise are given, respectively, and it can be seen that the image quality has been significantly improved after filtering. In Figure 11(c), the curve at the top represents the PSNR value of the proposed algorithm under the circumstance of no noise. When processing the image without noise, the peak signal noise is higher, which can meet the safety requirements.

In reference [38], Zhou et al. proposed an algorithm based on hyperchaotic system and 2D compressive sensing without any noise. Table 7 shows the comparison results

Table 7: Comparison of PSNR.

	Proposed algorithm		Reference [38]	
	Impulse noise $I = 0.02$	Gaussian noise $M = 0,\ V = 0.01$	Picture 1	Picture 2
PSNR	28.5603	26.5630	30.6881	26.3460

between the algorithms in this paper and those in the literature [38] for which the compression rate is 76.5625%.

The PSNR of the two pictures in reference [38] is 30.6881 and 26.3460, respectively. In the algorithm in this paper, when the noise type is pepper-and-salt noise, the PSNR is 28.5603. When the noise type is Gaussian noise, the PSNR is 26.5630. It can be seen from the comparison that the image encrypted by the algorithm in this paper can also achieve effective decryption under the influence of noise.

In practical application, noise parameters are selected according to the size of the compression rate. From the figure above, we find that although this algorithm can recover the original image at the receiving end owing to the noise at the source, the effect of image reconstruction is still affected to some extent. In this paper, we think we can use compression rate as a measure of throughput. As can be seen from Table 3 and Figure 11, the similarity coefficient and PSNR of reconstructed images will increase with the increase of compression rate. However, when the compression rate reaches about 70%, the performance of reconstructed images can be stable. When the compression rate is more than 70%, the growth curve is relatively flat. Therefore, in the process of encryption and decryption, a better reconstruction effect can be achieved by setting the compression rate at around 60%–70%. Table 8 shows the structural similarity between the reconstructed image and the original image under the influence of noise of different parameters when the compression ratio is 74.2%.

It can be seen from Table 8 that under the influence of different parameter noises, the receiving end can reconstruct the original signal and can subjectively determine the effective information in the restored image. The structural similarity under each parameter mostly exceeds 0.5, indicating that the algorithm in this study can effectively recover the effective information of the signal when processing the signal polluted by noise and has the certain ability to resist the source noise.

4.4. Key Sensitivity and Key Space Analysis. Because the encryption algorithm is highly sensitive to the key, when the key changes slightly, this leads to the failure of decryption and other processes. Key sensitivity refers to the degree to which the cipher text changes when the initial key changes slightly. Owing to the sensitivity of the initial value of the chaotic system, we can verify the key sensitivity of this algorithm based on this characteristic. When the chaotic system changes initial value slightly, the reconstructed image will be greatly different. This section studies whether the original signal has good key sensitivity after being encrypted by the algorithm in this study. The superimposed noise in the original signal is salt-and-pepper noise with a noise intensity of 0.02, and the compression rate in the image encryption process is 74.2%. Figure 12(a) is the recovery image when the key changes by an order of magnitude of 10^{-14}, Figure 12(b) is the recovery image when the key changes by 10^{-15}, and Figure 12(c) is the recovery image when the key changes by 10^{-16}. It can be seen that although the initial value changed only very slightly, the reconstructed image could not recognize any effective information, proving that the algorithm has good key sensitivity.

In the process of image encryption, the size of the key space reflects the difficulty and complexity of attacking the cryptographic system. The above experiments on key sensitivity verification also show that the encryption algorithm needs to have a strong dependence on the key. When the decryption key changes slightly, the decrypted image will be very different from the original image. As an important reference to evaluate the encryption algorithm, the key space directly determines whether the algorithm can resist exhaustive attacks. For the algorithm proposed in this study, without considering the diffusion process or scrambling, only the following are considered: a measurement matrix to decrypt, nine-chaotic-sequence signal generator, and the control parameters of the system. According to the international standard IEEE 754, in order to simplify the comparison, a positive indices section is represented. The double-precision floating-point type of valid number is 52. Table 9 lists the key spaces of the algorithm in this study and the key spaces of different schemes proposed by others. It can be seen from the table that the key space in this study is at least $2^{52*9} = 2^{468}$. In other words, the attacker needs 2^{468} attacks to build the correct matrix, so the image encryption algorithm proposed in this study is safe enough to resist brute-force attacks.

The sensitivity intensity of the plaintext can determine the ability to resist differential attacks. The parameters used to measure the sensitivity of the encryption algorithm to plaintext can be described by either the number of pixels change rate (NPCR) or the unified average changing intensity (UACI). The calculation formulas of NPCR and UACI are as follows:

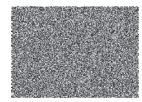
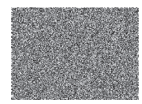
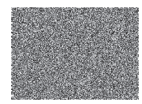
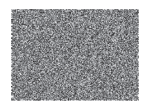
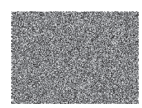
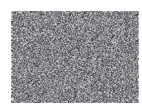
$$\mathrm{NPCR} = \frac{1}{N \times M} \sum_{i=1}^{M} \sum_{j=1}^{N} E(i, j) \times 100\%, \tag{13}$$

$$\mathrm{UACI} = \frac{1}{N \times M} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left| M_1(i, j) - M_2(i, j) \right|}{255} \times 100\%, \tag{14}$$

where M and N are the number of rows and columns of the image pixel and n is the color bit depth of the image. The NPCR and UACI of the encrypted image are listed in Tables 10 and 11, respectively, and are compared with the critical value.

In [42], the key generated through chaos is used as the index of row and column replacement in the image encryption process, and the encryption method of row and column replacement is adopted to encrypt the image. In [43], a hyperchaotic system based on closed-loop modulation is used to replace image pixels. In [44], piecewise linear chaotic mapping is used to exchange binary elements in the original image sequence with a chaotic sequence to scramble and encrypt the image. Table 12 shows a comparison

Table 8: Structural similarity between original image and decryption image.

Original image	Image with noise	Noise parameter	Cipher image	Decrypted image	SSIM
 (impulse noise)		$I = 0.02$			0.7433
		$I = 0.05$			0.5275
		$I = 0.1$			0.3981
 (Gaussian noise)		$M = 0$ $V = 0.01$			0.5895
		$M = 0$ $V = 0.02$			0.4853
		$M = 0.2$ $V = 0.01$			0.5883

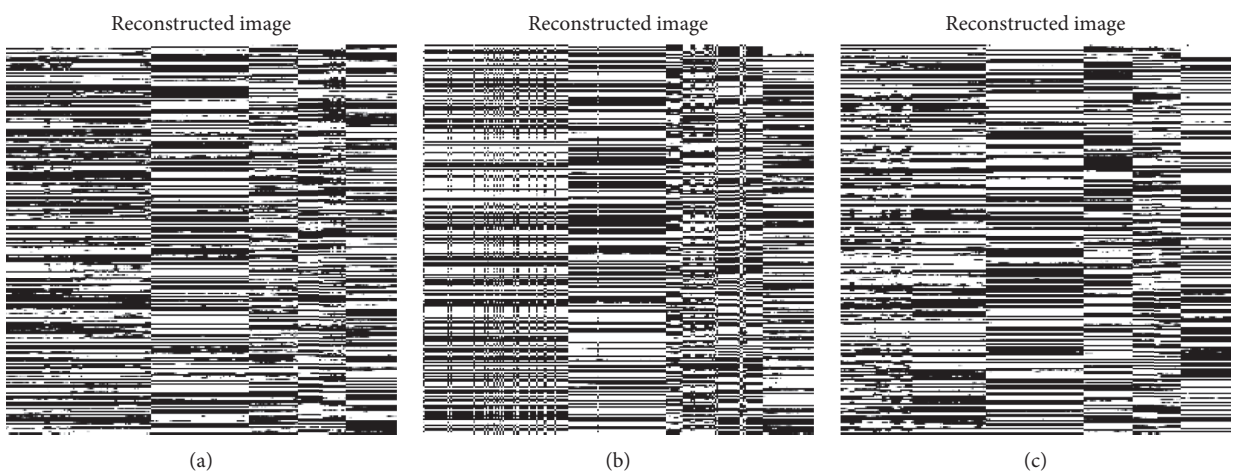


Figure 12: Key sensitivity analysis: (a) initial value change of 10^{-14}, (b) initial value change of 10^{-15}, and (c) initial value change of 10^{-16}.

Table 9: Comparison of key spaces.

Algorithm	Proposed algorithm	Reference [12]	Reference [39]	Reference [40]	Reference [41]
Key space	2^{468}	2^{16}	2^{78}	2^{128}	2^{96}

Table 10: NPCR analysis of test image.

NPCR (%)	Ideal NPCR critical values		
	$N^*_{0.05} = 99.5693\%$	$N^*_{0.01} = 99.5527\%$	$N^*_{0.001} = 99.5341\%$
99.6085	Pass	Pass	Pass

Table 11: UACI analysis of test image.

UACI (%)	Ideal UACI critical values		
	$U^{*-}_{0.05} = 33.2824\%$ $U^{*+}_{0.05} = 33.6447\%$	$U^{*-}_{0.01} = 33.2255\%$ $U^{*+}_{0.01} = 33.2016\%$	$U^{*-}_{0.001} = 33.1594\%$ $U^{*+}_{0.001} = 33.7677\%$
33.4632	Pass	Pass	Pass

Table 12: NPCR and UACI.

Index	Our scheme	Reference [42]	Reference [43]	Reference [44]
NPCR (%)	99.6094	99.6075	99.6063	97.6198
UACI (%)	33.4635	33.4195	33.3437	32.8014

between the NPCR and UACI obtained by the algorithm in this study and the above studies. The evaluation criteria of NPCR and UACI are given in [45].

The results show that the encrypted image can reach the threshold standard, which verifies that the compression and encryption algorithm proposed in this study can resist a differential attack to some extent.

5. Conclusions

In this study, the parallel encryption technology of a sequence generator and chaos measurement matrix based on noisy images is proposed. The purpose is to solve how to combine compressed sensing technology with chaotic cryptography for image encryption in actual hardware encryption. At the same time, due to the flexibility of the hardware circuit in this algorithm, the key in the encryption process is easy to change, which enhances the security of the encryption algorithm to a greater extent. This combines a compressed sensing algorithm with the random characteristics of chaotic signals from the perspective of security and efficiency of information transmission. Because chaotic signals are sensitive to initial values, this algorithm can greatly expand the key space and effectively resist violent attacks. Through a simulation, the feasibility of the algorithm was verified. The algorithm can still achieve effective encryption and decryption under the condition that the original information contains noise. In Section 4, the experimental results were analyzed in detail. Through the analysis, it could be seen that the algorithm proposed in this study has a very high key sensitivity, and the encryption effect of the image is ideal. In the process of restoring the original image, it was found that this algorithm can resist a certain degree of source noise pollution and effectively recover the original signal. In terms of operational efficiency, the algorithm encryption process needs 0.24 s, and the use of common compression perception algorithm encryption requires about 1 s. The decryption algorithm in this study requires 8 s and the ordinary compression perception algorithm decryption needs about 10 s, so the algorithm in this study using parallel transmission can effectively improve the efficiency of information transmission. In the following research, we will focus on whether the algorithm can resist the influence of channel noise and realize the image encryption and effective decryption.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (nos. 61571181 and 61801173) and the Natural Science Foundation of Heilongjiang Province, China (no. LH2019F048).

References

[1] A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map," *Optik*, vol. 184, pp. 205–213, 2019.

[2] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Optics & Laser Technology*, vol. 62, pp. 152–160, 2014.

[3] G. Hu, D. Xiao, Y. Wang, and T. Xiang, "An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications," *Journal of Visual Communication and Image Representation*, vol. 44, pp. 116–127, 2017.

[4] R. Gao, "A novel track control for Lorenz system with single state feedback," *Chaos, Solitons and Fractals*, vol. 122, pp. 236–244, 2019.

[5] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018.

[6] R. Ponuma and R. Amutha, "Compressive sensing based image compression-encryption using Novel 1D-Chaotic map," *Multimedia Tools and Applications*, vol. 4, pp. 1–26, 2017.

[7] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, 2019.

[8] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Optics and Lasers in Engineering*, vol. 121, pp. 169–180, 2019.

[9] S. Hassanzadeh and A. Karami, "Compression and noise reduction of hyperspectral images using non-negative tensor decomposition and compressed sensing," *European Journal of Remote Sensing*, vol. 49, no. 1, pp. 587–598, 2017.

[10] D. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2016.

[11] Y. Gu and Y. D. Zhang, "Compressive sampling optimization for user signal parameter estimation in massive MIMO systems," *Digital Signal Processing*, vol. 94, pp. 105–113, 2019.

[12] A. Orsdemir, H. Altun, G. Sharma et al., "On the security and robustness of encryption via compressed sensing," in *Proceedings of the Military Communications Conference, 2008. MILCOM 2008*, IEEE, San Diego, CA, USA, November 2008.

[13] A. Schulz, L. Velho, and E. Silva, "On the empirical rate-distortion performance of compressive sensing," in *Proceedings of the IEEE International Conference on Image Processing*, IEEE, Cairo, Egypt, November 2009.

[14] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[15] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," *IETE Technical Review*, vol. 33, no. 3, pp. 310–322, 2015.

[16] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[17] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[18] L. Chen, G. Chang, B. He, H. Mao, and D. Zhao, "Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition," *Optics and Lasers in Engineering*, vol. 88, pp. 221–232, 2017.

[19] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[20] L. Gong, C. Deng, S. Pan, and N. Zhou, "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," *Optics & Laser Technology*, vol. 103, pp. 48–58, 2018.

[21] L. Zhang, Y. Zhou, D. Huo, J. Li, and X. Zhou, "Multiple-image encryption based on double random phase encoding and compressive sensing by using a measurement array preprocessed with orthogonal-basis matrices," *Optics & Laser Technology*, vol. 105, pp. 162–170, 2018.

[22] G. Wang, R. Zhou, and Y. Zou, "Research on image optimization technology based on compressed sensing," *Journal of Electronics & Information Technology*, vol. 42, pp. 222–233, 2020.

[23] A.-A. Khennaoui, A. Ouannas, S. Bendoukha, G. Grassi, R. P. Lozi, and V.-T. Pham, "On fractional-order discrete-time systems: chaos, stabilization and synchronization," *Chaos, Solitons & Fractals*, vol. 119, pp. 150–162, 2019.

[24] L. Li, G. Wen, Z. Wang, and Y. Yang, "Efficient and secure image communication system based on compressed sensing for IOT monitoring applications," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 82–95, 2020.

[25] K. Zhou, J. Fan, H. Fan, and M. Li, "Secure image encryption scheme using double random-phase encoding and compressed sensing," *Optics and Laser Technology*, vol. 121, Article ID 105769, 2020.

[26] W. Shi, F. Jiang, S. Liu, and D. Zhao, "Image compressed sensing using convolutional neural network," *IEEE Transactions on Image Processing*, vol. 29, pp. 375–388, 2020.

[27] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Optics & Laser Technology*, vol. 99, pp. 238–248, 2018.

[28] L. Weizhi, L. Weiyu, K. Kpalma, and J. Ronsin, "Compressed sensing performance of random Bernoulli matrices with high compression ratio," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1074–1078, 2015.

[29] L. Zeng, X. Zhang, L. Chen, T. Cao, and J. Yang, "Deterministic construction of toeplitzed structurally chaotic matrix for compressed sensing," *Circuits, Systems, and Signal Processing*, vol. 34, no. 3, pp. 797–813, 2014.

[30] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Transactions on Multimedia*, vol. 18, no. 9, pp. 1720–1732, 2016.

[31] H. Jiang, Y. Liu, Z. Wei, and L. Zhang, "A new class of three-dimensional maps with hidden chaotic dynamics," *International Journal of Bifurcation and Chaos*, vol. 26, no. 12, Article ID 1650206, 2016.

[32] T. Zhang, S. Li, R. Ge, M. Yuan, and Y. Ma, "A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci-Lucas transform," *Mathematical Problems in Engineering*, vol. 2016, Article ID 7683687, 15 pages, 2016.

[33] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform," *Optics Communications*, vol. 343, pp. 10–21, 2015.

[34] E. F. Doungmo Goufo, "On chaotic models with hidden attractors in fractional calculus above power law," *Chaos, Solitons & Fractals*, vol. 127, pp. 24–30, 2019.

[35] H. Jahanshahi, A. Yousefpour, Z. Wei, R. Alcaraz, and S. Bekiros, "A financial hyperchaotic system with coexisting attractors: dynamic investigation, entropy analysis, control and synchronization," *Chaos, Solitons & Fractals*, vol. 126, pp. 66–77, 2019.

[36] J. Yu, S. Guo, X. Song, Y. Xie, and E. Wang, "Image parallel encryption technology based on sequence generator and chaotic measurement matrix," *Entropy*, vol. 22, no. 1, p. 76, 2020.

[37] J. Deng, S. Zhao, Y. Wang, L. Wang, H. Wang, and H. Sha, "Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 10097–10117, 2017.

[38] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[39] R. Huang and K. Sakurai, "A robust and compression-combined digital image encryption method based on compressive sensing," in *Proceedings of the Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Dalian, China, October 2011.

[40] S. George and D. Pattathil, "A secure LFSR based random measurement matrix for compressive sensing," *Sensing and Imaging*, vol. 15, no. 1, pp. 85–240, 2014.

[41] S. N. George, N. Augustine, and D. P. Pattathil, "Audio security through compressive sampling and cellular automata," *Multimedia Tools and Applications*, vol. 74, no. 23, pp. 10393–10417, 2014.

[42] X. Wang, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," *Nonlinear Dynamics*, vol. 79, no. 2, pp. 1141–1149, 2015.

[43] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[44] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

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