Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5598009, 13 pages
https://doi.org/10.1155/2021/5598009

Research Article

Secure and Efficient Image Transmission Scheme for Smart Cities Using Sparse Signal Transformation and Parallel Compressive Sensing

Hui Wang,[1] **Yong Wu**,[2] **and Huantian Xie**[1]

[1]*School of Mathematics and Statistics, Linyi University, Linyi 276005, Shandong, China*
[2]*School of Information Science and Engineering, Linyi University, Linyi 276005, Shandong, China*

Correspondence should be addressed to Hui Wang; 990381049@qq.com and Huantian Xie; xht0539@qq.com

Received 1 March 2021; Revised 18 June 2021; Accepted 19 July 2021; Published 10 August 2021

Academic Editor: Mohammad R. Khosravi

With the evolution of smart cities, images are used in a wide range of services such as smart healthcare and surveillance. How to ensure that images are transmitted and shared securely is of paramount importance for smart cities. To this end, a secure and efficient scheme for image transmission is proposed in this paper, which uses sparse signal transformation (SST) and parallel compressive sensing (CS). The primary employed techniques are sparse signal transformation (SST), parallel CS, and diffusion-permutation operation. The compression performance is achieved by parallel CS, whereas the encryption performance is derived from SST, parallel CS, and diffusion-permutation procedure. SST is exploited to change energy information before CS sampling and incorporated into diffusion-permutation framework, which not only balances the security and the efficiency of the algorithm, but also improves the transmission efficiency of the cipher image. We introduce chaotic system to generate the measurement matrix, SST matrix, and diffusion matrix to improve security. Furthermore, numerical simulation results and theoretical analyses confirm the security performances and effectiveness of the proposed scheme.

1. Introduction

For the residents of smart cities, images play an important role in their information exchange. In order to improve the quality of life of residents, various optimization algorithms for image application need to be further proposed [1–6]. If there is no suitable method to share the image, the resident interests may be threatened. How to ensure that the image can be transmitted securely and efficiently is crucial for smart cities [7]. Some image encryption schemes have been designed based on cryptographic features, such as the chaos theory [8, 9], DNA coding [10], and other techniques. It is worth noting that the aforementioned algorithms can achieve security performance, but they cannot further compress the cipher images.

The compressive sensing (CS) can be considered as an encryption model of symmetric cryptography, which was firstly presented as a remarkable signal processing breakthrough in [11]. What is more, a sparse or compressible signal can be computed with overwhelming probability using some reconstruction algorithms, which has been studied in [12–14]. Consequently, image encryption scheme based on CS for smart cities can perform encryption and compression simultaneously. Based on the inherent characteristics of CS, it has been popularly employed in wireless sensor networks and image cryptosystem [15]. In terms of computational secrecy, Rachlin and Baron[16] point out that the CS-based cryptosystem can achieve computational secrecy when it suffers from cipher only attack and brute force attack. Additionally, the CS security has been evaluated in many papers [17–19]. It is worth noting that the above discussed security is limited to the condition that the plain image only can be obtained according to the corresponding cipher image, and the attackers have no right to access many pairs of plain images and cipher images.

Some encryption schemes are designed in [20–26], which incorporates CS with other cryptographic techniques. These methods can be divided into two categories. The first kind of methods employs the permutation technique to scramble the measurement value matrix [22, 23] or to scramble the coefficient matrix before encoding the plain image [24, 25]. Another kind of methods mainly combines the double random phase encoding technique with CS to obtain the complicated cryptosystem [21, 26]. However, neither of the above two kinds of methods can resist chosen plain attack (CPA) if the measurement matrix is reused in the encoding process. The most essential cause of the above problem is that the measurement matrix can be calculated by means of launching chosen plain attack (CPA) under the condition of many pairs of plain images, and cipher images can be intercepted by an adversary, which has been pointed out in [27]. But, it is appealing if a large number of plain images can be sampled by the same measurement matrix with the view of engineering. The straight forward way to solve the above problem is to encrypt the measurement value matrix using traditional cryptographic method. However, some traditional methods are not efficient enough, such as AES and DES. Thus, it is necessary to design cryptosystem based on CS with higher efficiency under the condition that the measurement matrix is reused. Subsequently, countermode in block cipher is introduced to the CS framework in [28]. Theoretically, the cryptosystem based on CS can resist CPA if each plain image can be encoded by refreshing different measurement matrices. Based on this knowledge, Hu et al. [29] proposed an effective image encryption algorithm using parallel CS and countermode to void CPA. In [27], another novel approach constructs measurement matrix without satisfying restricted isometry property (RIP) by making full use of the secret key-related sparsifying basis. Based on this basis, a cryptosystem is designed in [30] by performing gyrator transform and double random phase followed by the CS encoding procedure. However, the decryption efficiency will be reduced as the measurement matrices need to be updated for different columns of the coefficient matrix. Apart from the above methods, other efficient techniques are also introduced to CS framework. For example, an image encryption scheme based on CS framework combined with wavelet packet transform was designed in [31]. However, the cipher image is not quantified, which results in reduced transmission efficiency. Chai et al. [32] presented a novel image encryption scheme by introducing cellular automata to CS framework, where the resistance to CPA owes the SHA-512 hash value of the plain image. But it is worth noting that the hash value of the original image must be transmitted to the decoder every time for different plain image, which may result in poor practicability.

In order to balance the efficiency and security of the cryptosystem under the premise that the measurement matrix can be reused, an efficient image encryption scheme using sparse signal transformation (SST) and parallel CS (SST-PCS) is presented in this paper, which includes two stages: the first one is SST-PCS sampling procedure for plain image and the second stage is diffusion-permutation procedure. Furthermore, based on the theory that the quality of reconstruction image will be improved if the coefficient matrix is evenly distributed, zigzag scrambling is applied on the transformed coefficient matrix with the selected start location before CS sampling. As pointed out in [33], it is theoretically feasible to construct the measurement matrix with chaotic sequence. In CS sampling procedure, every column of the final transformed coefficient matrix is encoded via parallel CS by adopting the same measurement matrix, which is constructed by the chaotic system to protect the security of the measurement matrix. What is more, compared to [29, 30], both encryption and decryption efficiency can be improved as the measurement matrix does not need to be updated.

The contributions of this paper can be summarized as follows: (i) the transformation function is employed to change energy information of the coefficient matrix before CS sampling, which is beneficial for improving the security of the cryptosystem; (ii) as SST is linear operation, SST is introduced to cryptosystem without adding computational complexity; (iii) the characteristic of SST is exploited and incorporated into diffusion-permutation framework to balance the efficiency and security of the cryptosystem; and (iv) the proposed algorithm can guarantee resistance against CPA with the help of SST, CS, and diffusion-permutation operation.

The rest of this paper is organized as follows. Section 2 introduces the preliminaries including CS and the chaotic map employed in this paper. Then, we detail the proposed scheme in Section 3, and the simulations and security analysis are discussed in Section 4. Finally, Section 5 gives the concluding remarks.

2. Preliminaries

2.1. Parallel Compressive Sensing. For traditional CS, suppose that $X = [x_1, x_2, \ldots, x_N]^T$ is a discrete signal, X is regarded as k-sparse signal if $S = \Psi X$, where S is a signal of length N with $\|S\|_0 = k$ and Ψ denotes an orthogonal matrix of size $N \times N$. CS theory states that S can be reconstructed by only M $(k < M \leq N)$ linear measurements via reconstruction algorithms [13]. The sampled process can be formulated as follows:

$$y = \Phi S, \tag{1}$$

where Φ represents measurement matrix of size $M \times N$ and satisfies the restricted isometry property (RIP) of a certain order k if there exists a constant $\delta_k \in [0, 1]$ such that

$$(1 - \delta_k)\|S\|_2^2 \leq \|\Phi S\|_2^2 \leq (1 + \delta_k)\|S\|_2^2, \tag{2}$$

for all k-sparse signals S, which can be recovered by solving the following optimization problem:

$$\begin{aligned} &\min \quad \|S\|_0 \\ &\text{subject to} \quad y = \Phi S, \end{aligned} \tag{3}$$

and the convex form of problem (3) can be transformed as

$$\begin{aligned} &\min \quad \|S\|_1 \\ &\text{subject to} \quad y = \Phi S, \end{aligned} \tag{4}$$

(or in noisy condition: $\|\Phi S - y\|_2 \le \varepsilon$).

However, for traditional CS, only the one-dimensional signal can be directly encoded; that is to say, the multidimensional signal needs to be rearranged to a one-dimensional signal before performing CS sampling process. The above operation will make the computational complexity become larger, as well as the storage space, as the size of measurement matrix becomes large. Subsequently, the block CS [34, 35] is proposed to solve the above problem. In general, the block CS firstly divides the plain image to many small blocks, which are reshaped to corresponding one-dimension vector individually and then sampled by CS, respectively. But for the decoder, in theory, the computational complexity is not reduced since the all small blocks need to be assembled to recover the plain image.

For encoding and decoding, what we are concerned about is whether there is a cryptosystem based on CS with relatively low complexity. To this end, parallel CS is proposed. The main idea of the parallel CS is to convert the original signal into the corresponding 2D matrix, and its each column is then encoded via CS by adopting the same measurement matrix. The encoding process of parallel CS for the image P with the size $N \times N$ can be defined as follows:

$$y_i = \Phi \Psi p_i, \quad (i = 1, 2, \ldots, N), \tag{5}$$

where Ψ is an orthonormal sparsifying basis and p_i, y_i represent the i-column of the image P and the corresponding measurement value matrix, respectively. It is obvious that the required size of the measurement matrix can be reduced significantly compared to the traditional CS. What is more, decoding also can be computed individually for every column in parallel CS.

2.2. Logistic-Tent System. In our work, Logistic-Tent system is utilized to generate the transformation matrix, measurement matrix, and diffusion matrix. As pointed out in [29], compared with Logistic map and Skew Tent map as presented in equations (6) and (7), respectively,

$$z_{n+1} = \mu z_n (1 - z_n), \tag{6}$$

$$z_{n+1} = \begin{cases} \dfrac{z_n}{q}, & 0 < z_n < q, \\ \dfrac{1 - z_n}{1 - q}, & q \le z_n < 1, \end{cases} \tag{7}$$

where the initial value $z_0 \in (0, 1)$ and the control parameter of Logistic map $\mu \in [3.57, 4]$ and the control parameter of Skew Tent map $q \in (0, 1)$. Logistic-Tent system exhibits superior performances in terms of chaotic range and other chaotic characteristics, which is described as follows:

$$z_{n+1} = \begin{cases} (r z_n (1 - z_n) + 0.5 z_n (4 - r)) \bmod 1, & z_n < 0.5, \\ (r z_n (1 - z_n) + 0.5 (1 - z_n)(4 - r)) \bmod 1, & z_n \ge 0.5, \end{cases} \tag{8}$$

when the initial value $z_0 \in (0, 1)$ and the control parameter of chaotic system $r \in (0, 4]$, Logistic-Tent system is chaotic.

3. The Proposed Scheme

In this part, the complete encryption scheme using SST-PCS is presented. The encryption procedure mainly consists of two primary stages: the SST-PCS sampling process and the following measurement value matrix quantization and diffusion-permutation process. The measurement value matrix is obtained by applying SST-PCS to sample the plain image. The decryption procedure is the inverse of the encryption procedure.

3.1. The Encryption Procedure. In this section, the encryption procedure is depicted, as shown in Figure 1. In our scheme, the pairs $(z_i, r_i)(i = 1, 2, 3)$, which are the initial values and control parameters of Logistic-Tent system, are adopted as the secret keys.

3.1.1. The SST-PCS Sampling Process. In this process, SST and zigzag scrambling are carried out on the coefficient matrix to calculate its scrambled version denoted final transformed coefficient matrix. All the entries of the transformation matrix and the measurement matrix are governed by Logistic-Tent system.

Step 1: (DWT transform) for a plain image P of size $N \times N$, the coefficient matrix CM is calculated by applying the discrete wavelet transform on the plain image, formulated as

$$\mathrm{CM} = \Psi \times P \times \Psi', \tag{9}$$

where Ψ denotes the orthogonal wavelet matrix and Ψ' denotes the transpose operation of Ψ.

Step 2: (generation transformation matrix) set the initial value $z_1 \in (0, 1)$ and the control parameter $r_1 \in (0, 4]$, and iterate chaotic system $N^2 d + n_1$ times to generate the chaotic sequence $T_1(r_1, z_1, d)$: $= \left\{ z^1_{n_1 + jd} \right\}_{j=1}^{N^2}$, where $d \in [1, 10]$ denotes the sampling interval of chaotic sequence. The transformation matrix OB can be calculated according to the following equation:

$$\begin{aligned} \mathrm{OB}(i) = &\left(2 \times \mathrm{round}\left(z^1(i)\right) - 1\right) \\ &\times \left(\mathrm{floor}\left(\mathrm{mod}\left(z^1(i) \times 10^{14}, 2\right)\right)\right) + 1. \end{aligned} \tag{10}$$

In this equation, the first "round" part and the second "mod" part will be subsequently used to change the sign and the energy of the sparse coefficient, respectively.

Step 3: (SST) reshape the transformation matrix OB to the matrix of size $N \times N$ and apply it to the coefficient matrix CM to produce the transformed coefficient matrix TCM as follows:

$$\mathrm{TCM} = \mathrm{OB}. \times \mathrm{CM}, \tag{11}$$

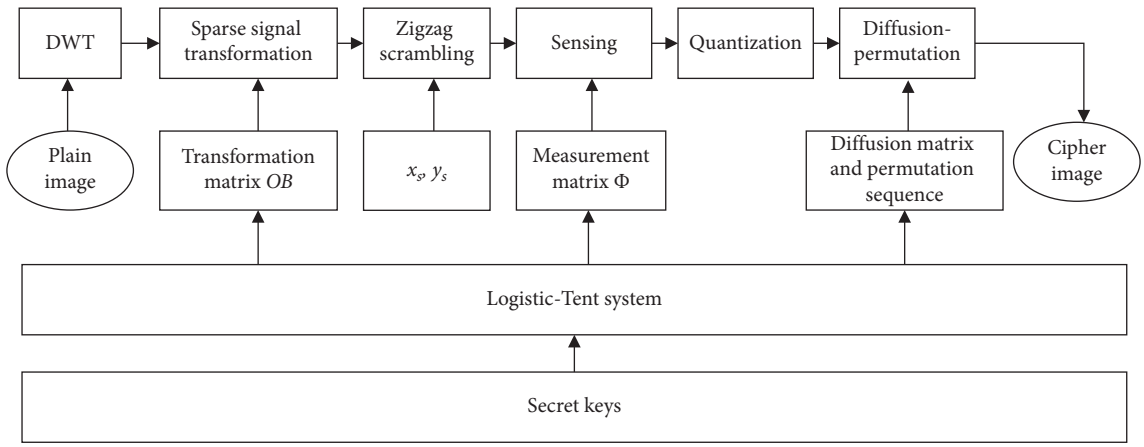


Figure 1: Architecture of the proposed encryption process.

where ".×" denotes the product of the corresponding components of two matrices having the same size.

Step 4: (zigzag scrambling) scan the transformed coefficient matrix in a zigzag mode from the start location (x_s, y_s) to obtain the final coefficient matrix FCM, where (x_s, y_s) serves as the secret key. Enforce a part of elements of FCM to be zero under the condition that their values are smaller than threshold T.

Step 5: (measurement matrix construction) set the initial value $z_2 \in (0,1)$ and the control parameter $r_2 \in (0,4]$, and iterate chaotic system $MNd + n_2$ times to generate the chaotic sequence $T_2(r_2, z_2, d) := \left\{z^2_{n_2+jd}\right\}_{j=1}^{MN}$, where $d \in [1,10]$ denotes the sampling interval of chaotic sequence. Then, regularize $z^2_{n_2+jd}$ to $\omega_j^2 = 1 - z^2_{n_2+jd}$, $\omega_j^2 \in (-1,1)$. Finally, the measurement matrix Φ is obtained by multiplying the factor $\sqrt{2/M}$ in a column-wise manner.

Step 6: (sensing) utilize the measurement matrix Φ to sample the final coefficient matrix FCM to acquire the measurement value matrix (MVM).

3.1.2. Measurement Value Matrix Quantization and Diffusion-Permutation Process. To enhance the security level, the quantization and diffusion-permutation operations are applied on the measurement value matrix. The detailed steps can be elaborated as follows:

Step 1: (quantization) quantize the entries of measurement value matrix (MVM) to the range of $[0, 255]$, and then the quantized measurement value matrix (QM) can be subsequently calculated according to the following equation:

$$\mathrm{QM} = \mathrm{floor}\left[\frac{255\,(\mathrm{MVM} - \min)}{(\max - \min)}\right], \tag{12}$$

where $\mathrm{floor}(x)$ denotes the largest integer not exceeding x, while max and min denote the maximum value and minimum value within the matrix MVM, respectively.

Step 2: (diffusion-permutation) the specific procedure is as follows:

Step 2.1: set the initial state value $z_3 \in (0,1)$ and the control parameter $r_3 \in (0,4]$, and iterate chaotic system $MNd + n_3$ times to generate the chaotic sequence $T_3(r_3, z_3, d) := \left\{z^3_{n_3+jd}\right\}_{j=1}^{MN}$, where $d \in [1,10]$ denotes the sampling interval of chaotic sequence. The diffusion matrix DM can be calculated according to the following equation:

$$\mathrm{DM}(i) = \mathrm{mod}\left(\mathrm{floor}\left(z^3(i) \times 10^{14}\right), 256\right). \tag{13}$$

Step 2.2: reshape the matrix QM to the matrix of size $MN \times 1$, and then the matrix EC can be calculated with the diffusion matrix as follows:

$$\mathrm{EC}(i) = \mathrm{QM}(i) \oplus \mathrm{DM}(i) \oplus \mathrm{EC}(i-1), \tag{14}$$

where "⊕" is XOR operator and $\mathrm{EC}(0) \in [0, 255]$ is the given secret value.

Step 2.3: obtain the cipher image C by scrambling the matrix EC using index sequences generated by chaotic sequence T_3. Then, reshape the matrix C to the matrix of size $M \times N$.

3.2. The Decryption Procedure. As illustrated in Figure 2, the image decryption procedure is the inverse of the image encryption process. The detailed steps can be summarized as follows:

Step 1: (inverse diffusion-permutation) reshape the cipher image C to the matrix of size $MN \times 1$. Implement step 2.1 in Section 3.1.2 to acquire diffusion matrix DM, perform inverse permutation process using index sequences to obtain the matrix DEC, and then obtain the decrypted quantized measurement value matrix DQM by calculating the following equation:

$$\mathrm{DQM}(i) = \mathrm{DEC}(i) \oplus \mathrm{DEC}(i-1) \oplus \mathrm{DM}(i), \tag{15}$$

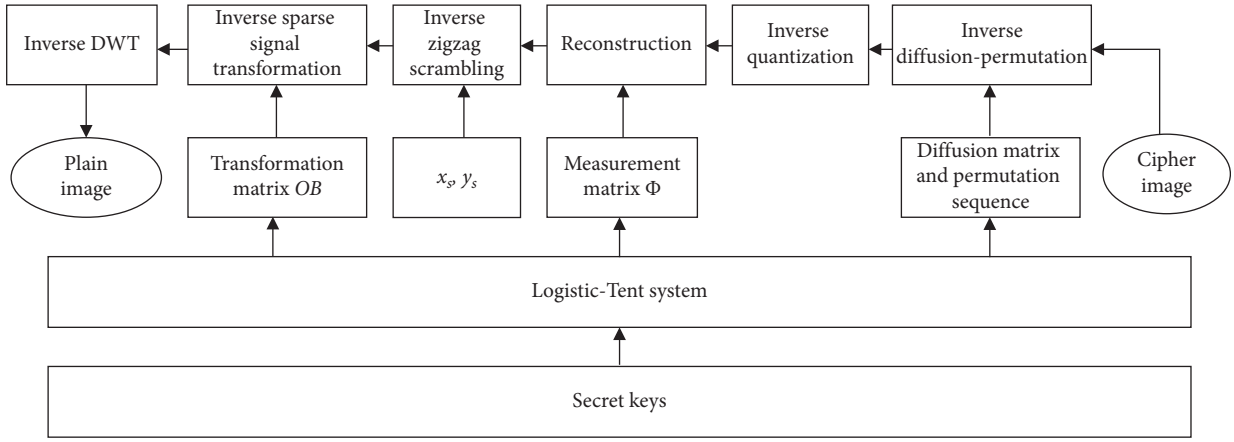


Figure 2: Architecture of the decryption process.

where "⊕" is XOR operator and DEC(0) is equal to EC(0).

Step 2: (inverse quantization) reshape DQM to the matrix of size $M \times N$. Inversely quantize the entries of matrix DQM to obtain the decrypted measurement value matrix DVM as follows:

$$\mathrm{DVM} = \frac{\mathrm{DQM} \times (\max - \min)}{255} + \min. \tag{16}$$

Step 3: (reconstruction)employ orthogonal matching pursuit (OMP) algorithm to recover the decrypted transformed coefficient matrix DTM with the measurement matrix Φ generated by performing step 5 in Section 3.1.1.

Step 4: (inverse zigzag scrambling) inversely scan the decrypted transformed coefficient matrix DTM with the secret key to obtain the matrix DFM.

Step 5: (inverse SST) perform step 2 in Section 3.1.1 to acquire the transformation matrix OB, and subsequently calculate the decrypted coefficient matrix according to the following equation:

$$\mathrm{DCM} = \mathrm{DFM}./\mathrm{OB}, \tag{17}$$

where "./" denotes the quotient of the corresponding component of two matrices having the same size.

Step 6: (inverse DWT transform) calculate the decrypted image DI with the orthogonal wavelet matrix by performing the following equation:

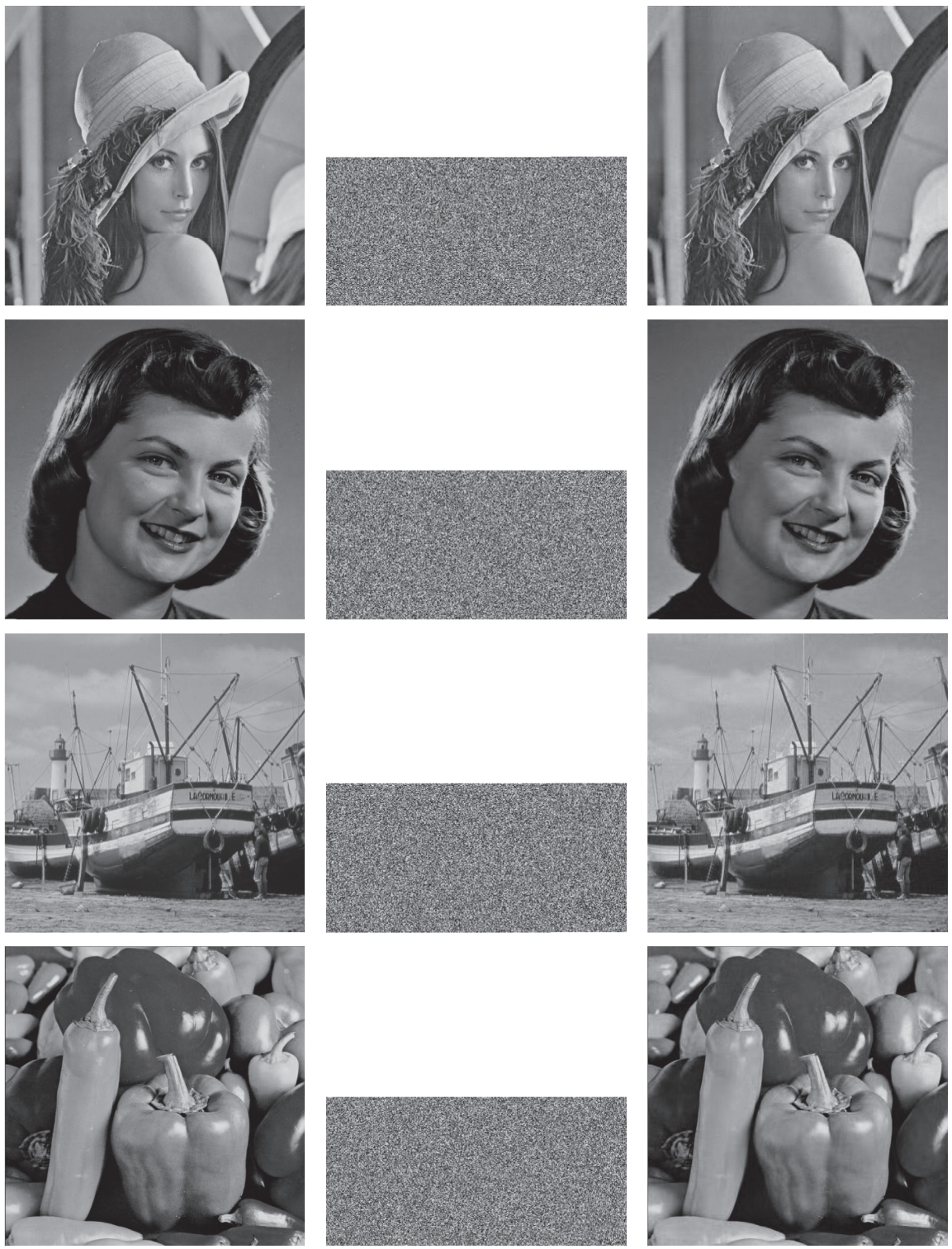
$$\mathrm{DI} = \Psi^T \times \mathrm{DCM} \times \Psi. \tag{18}$$

4. Simulations and Security Analyses

Numerical simulations and security analyses of the proposed algorithm are presented in this section. The 512×512 sized Lena, Girl, Boat, Barbara, and Peppers and the 256×256 sized Finger, Lena256, are chosen as test images in this paper. Set $z_1 = 0.417230953482913$, $r_1 = 2.31856720874261$, $z_2 = 0.51837265098274$, $r_2 = 3.41767202302761$, $z_3 = 0.61837265098274$, and $r_3 = 3.19385472819119$ as the secret keys to encrypt the original image. OMP is adopted as the reconstruction algorithm to recover the plain image.

4.1. Effectiveness Evaluation of Encryption and Compression. In this subsection, suppose that the compression rate is set to be 0.5, and some simulation experiments are presented to verify the effectiveness of proposed image encryption scheme in terms of encryption, compression, and quality of the reconstruction image, respectively. The simulation experiments result is presented in Figure 3, where the first to third columns represent the plain images, the cipher images, and the decrypted images with the secret keys, respectively. From the perspective of encryption performances, we cannot obtain useful information from the cipher images presented in the second column. Obviously, the volume of the cipher image is only half of the plain image, and the storage space is significantly reduced. The performances of both encryption and compression have been well illustrated. Then, the performances of reconstruction quality are further evaluated according to numerical simulations. Here, peak signal-to-noise ratio (PSNR) [36] is adopted as the metric to evaluate the quality of the decrypted image. As can be observed, the quality of the decrypted image is akin to the corresponding plain image from the visual perspective. Additionally, from top to bottom in the third column, the reconstructed image is with PSNRs of 34.1402(db), 35.4414(db), and 33.9282(db), respectively. Such numerical simulations indicate that the proposed encryption scheme can satisfactorily achieve encryption and compression simultaneously.

We also compare the quality of reconstructed image of the proposed scheme with other existing encryption schemes based on CS [6, 32, 37]. Table 1 presents the image reconstruction performance on test image Lena256 of size 256×256 when the compression rate is 0.5. As can be observed, the PSNRs of the decrypted images in [6, 32, 37] are less than our scheme, which indicates that our proposed scheme exhibits image superior reconstruction performance.



(a) (b) (c)

Figure 3: Effectiveness evaluation of the proposed scheme: (a) the plain images, (b) the cipher images, and (c) the decrypted images, respectively.

4.2. Key Space. As pointed out in [38], the cryptosystem can resist brute-force attack if the key space, which is composed of the all secret keys used in cryptosystem, is larger than 2^{100}. In our paper, the pairs $(z_i, r_i)(i = 1, 2, 3)$ are adopted as the secret keys. As the computational precision of the double precision number is about 10^{-15}, so the key space of the proposed algorithm is $(10^{15})^6 = 10^{90} \approx 2^{298}$, which indicates that the proposed scheme can resist brute-force attack.

Table 1: PSNR(db) comparison of image Lena256 reconstruction performance.

Algorithm	PSNR(db)
[6]	29.2337
[32]	29.82
[37]	<26
Proposed	30.25

4.3. Correlation Analysis. The correlation among adjacent pixels is an important evaluation index to evaluate the cryptosystem. Since the values among adjacent plain image pixels are similar, the plain image correlation coefficients are usually high. An effective encryption scheme should ensure that the correlation coefficients of cipher images are sufficiently low. To calculate the correlation coefficients of the images, 5000 adjacent pixels from the plain image Lena and its corresponding cipher image are randomly selected in horizontal, vertical, and diagonal directions, respectively. The correlation coefficients in horizontal, vertical, and diagonal directions are calculated by the following equation:

$$r_{xy} = \frac{n\sum_{i=1}^{n}(x_i y_i) - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{\left(n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2\right)\left(n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2\right)}}. \tag{19}$$

The simulation results are depicted in Figure 4 and Table 2. From Figure 4, we can observe that the correlations among adjacent pixels of plain image are dramatically reduced. As presented in Table 2, all listed algorithms exhibit satisfactory cipher image correlations, but compared to [29, 39], the proposed algorithm exhibits superiority in horizontal direction.

4.4. Histogram Analysis. Histogram is an evaluation index to assess the distribution of pixel values. An effective image encryption scheme can make the histogram of the cipher image equally distributed. Simulation results of histograms are presented in Figure 5. The plain image Lena and the corresponding cipher image are shown in Figures 5(a) and 5(c), respectively, and their corresponding histograms are shown in Figures 5(b) and 5(d). As we can see, the histogram of cipher image is uniformly distributed, which indicates that the redundancy of plain image is successfully removed.

4.5. Key Sensitivity Analysis. In order to assess the key sensitivity of cryptosystem performance, some simulation experiments are presented. An effective image encryption scheme will produce two different cipher images when tiny different secret keys are employed to encrypt the same plain image, and the cipher images will not be decrypted correctly when the correct key is changed slightly.

4.5.1. Key Sensitivity Analysis in the Encryption Process. The number of pixels change rate (NPCR) and unified average change in intensity (UACI) are introduced to evaluate the difference between two images of the same size, which are described as follows:

$$\begin{aligned} \mathrm{NPCR} &= \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \\ \mathrm{UACI} &= \frac{\sum_{i,j} \left|C_1(i,j) - C_2(i,j)\right|}{255 \times M \times N} \times 100\%, \end{aligned} \tag{20}$$

where $D(i,j) = 1$ if $C_1(i,j) = C_2(i,j)$; else $D(i,j) = 0$. Consequently, if two images are completely different, NPCR equals 1. In this test, suppose that the compression rate is set to be 0.75, and Lena is selected as the plain image. To test key sensitivity in the encryption process, a tiny change 10^{-14} is sequentially added to one of the parameters with others unchanged to obtain corresponding cipher images. The values of NPCR and UACI for the cipher images are 99.65%, 33.27%, 99.65%, 33.88%, 99.61%, 33.49%, 99.56%, 33.25%, 99.62%, 33.44%, 99.56%, and 33.37% with $z_1 + 10^{-14}$, $r_1 + 10^{-14}$, $z_2 + 10^{-14}$, $r_2 + 10^{-14}$, $z_3 + 10^{-14}$, and $r_3 + 10^{-14}$, respectively.

4.5.2. Key Sensitivity Analysis in the Decryption Process. Key sensitivity performance in the decryption procedure is also tested. Lena is chosen as the plain image, and the cipher image is obtained with the secret keys, as shown in Figure 6(a). The cipher images are sequentially decrypted with the correct key and the wrong keys constructed by adding a tiny change 10^{-14} to one of the parameters with others unchanged, namely, $z_1 + 10^{-14}$, $r_1 + 10^{-14}$, $z_2 + 10^{-14}$, $r_2 + 10^{-14}$, $z_3 + 10^{-14}$, and $r_3 + 10^{-14}$. The corresponding decrypted images are presented in Figures 6(b)–6(h). The differences between the corresponding decrypted images and the decrypted image with correct keys are 99.81%, 99.77%, 99.80%, 99.82%, 99.91%, and 99.90%, respectively. The simulation results show that the proposed scheme has extreme key sensitivity.

4.6. Efficiency Analysis. For the proposed image encryption algorithm, the time consumption mainly comes from the workloads of generating the measurement matrix and the sort of the chaotic sequence. The complexity is as low as $O(MN + MN\log MN)$ based on the sort algorithm. In many applications, encryption time is also an important index to evaluate the performance of the algorithm. The encryption time of different test images is presented in Table 3, from which one can see that the encryption time changes slightly when the compression ratio (CR) is varying from 0.25 to 0.75 for a same plain image. As shown in Table 3, the encryption time of image Finger varies from 0.2646s to 0.3484s when compression ratio changes from 0.25 to 0.75. We can observe that the encryption time increases as the size of plain image becomes larger. We also compare the encryption time of the proposed scheme with other existing encryption schemes [40]. The simulation results are depicted in Table 4. As a result, the proposed scheme can be applicable in practical applications.

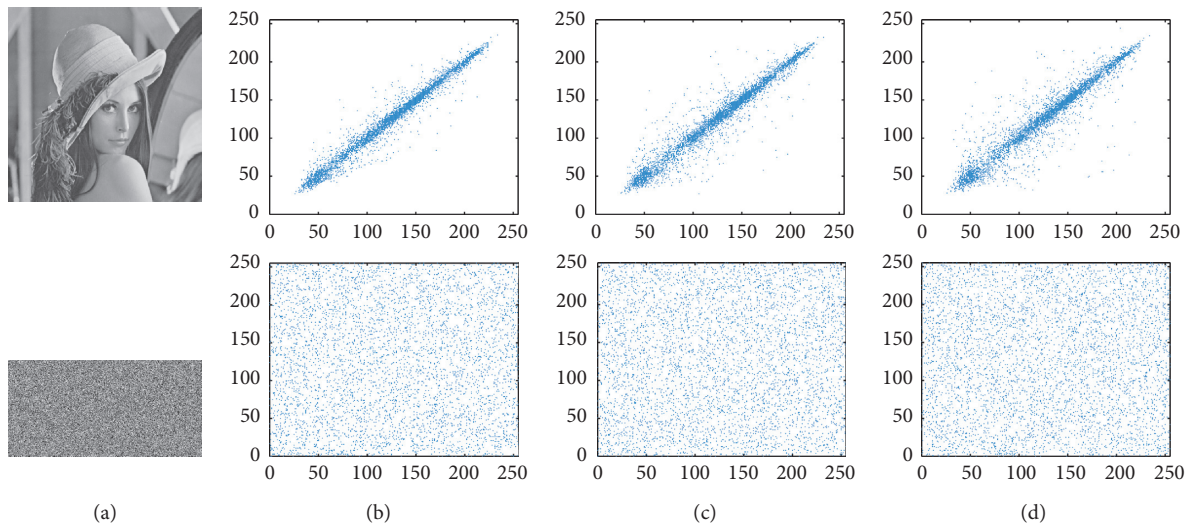


Figure 4: Correlation analysis. (a–d) The image and the correlation in horizontal, vertical, and diagonal directions, respectively.

Table 2: Comparison of adjacent pixel correlation.

Algorithm	Horizontal	Vertical	Diagonal
Plain image	0.9859	0.9729	0.9630
[29]	0.0036	0.0012	0.0005
[39]	0.0018	0.0014	0.0034
Proposed	0.0016	0.0048	−0.0046

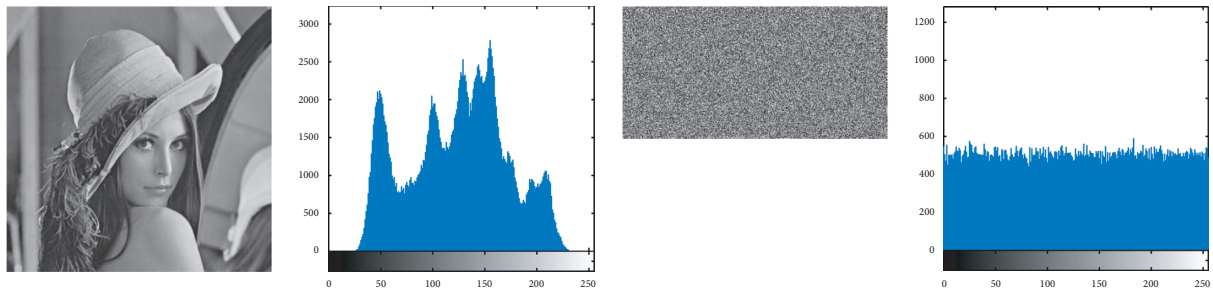


Figure 5: Histogram analysis: (a) plain image; (b) histogram of (a); (c) cipher image; (d) histogram of (c).

4.7. Chosen Plaintext Attacks. Since the CS process can be regarded as the linear projection, based on the knowledge of [27], the measurement matrix can be revealed essentially by choosing an identity matrix and obtaining the corresponding measurement value matrix. However, in the proposed scheme, the parallel CS output result of an identity matrix is no longer the measurement matrix because the identity matrix has been transformed and scanned in a zigzag mode before sampled by parallel CS.

To illustrate the above argument, some experiments have been done, and the results are shown in Figure 7, where Lena is selected as the test image. Set CR to be 0.5. Here, the CS-based image scheme without considering zigzag scrambling and SST (called the original CS scheme) is introduced and compared. The cipher images produced by the original CS scheme and the proposed scheme are presented in Figures 7(a) and 7(d), respectively. Then, Figures 7(b) and 7(e) represent the measurement value matrices MVM 1 and MVM 2 generated by the original CS scheme and the proposed scheme when the identity matrix is regarded as the plain image under the condition of without applying DWT on the identity matrix. Figure 7(c) is the decrypted image obtained by applying the decryption process of the original CS scheme in Figure 7(a) with the secret key z_2, r_2, z_3, r_3 and treating MVM 1 as the measurement matrix. Similarly, Figure 7(f) is the corresponding decrypted image obtained by applying the decryption process of our proposed SST-PCS scheme on Figure 7(d) with the secret key $z_2 r_2$, z_3, r_3

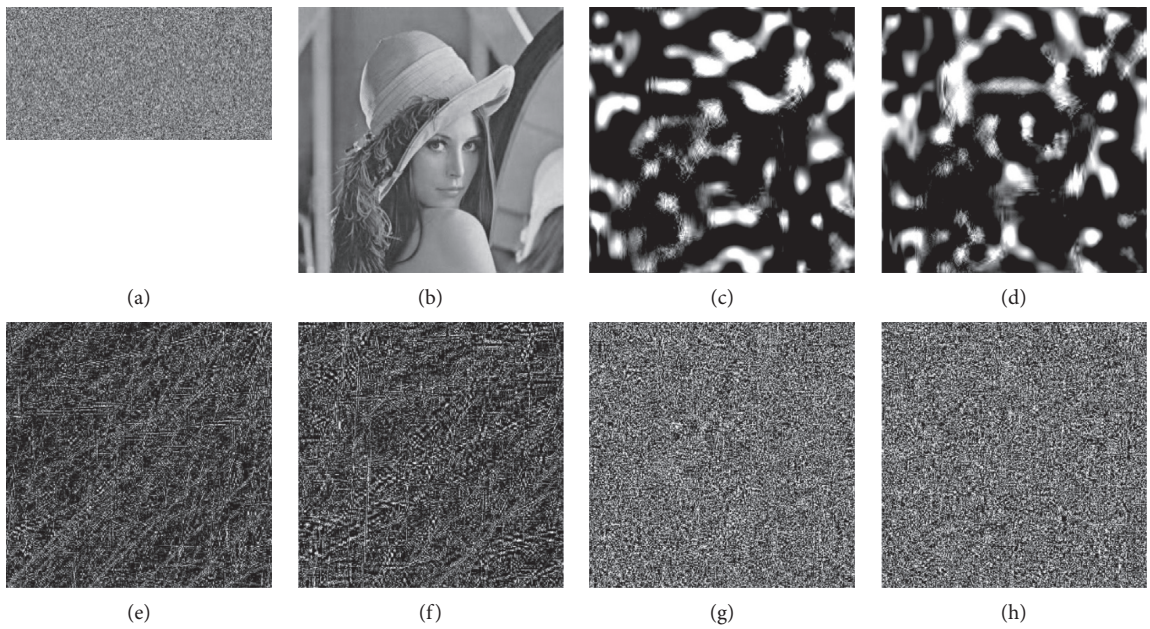


Figure 6: Key sensitivity analysis in the decryption process: (a) cipher image; (b) the decrypted image with correct key; (c) the decrypted image with z_1+10^{-14}; (d) the decrypted image with r_1+10^{-14}; (e) the decrypted image with z_2+10^{-14}; (f) the decrypted image with r_2+10^{-14}; (g) the decrypted image with z_3+10^{-14}; (h) the decrypted image with r_3+10^{-14}.

Table 3: Encryption time (seconds).

Images	Finger	Lena256	Girl	Boat	Peppers	Lena
CR = 0.25	0.2646	0.2768	0.5426	0.5545	0.5296	0.6602
CR = 0.5	0.3074	0.2888	0.6719	0.7034	0.6724	0.6816
CR = 0.75	0.3484	0.3423	0.8248	0.8220	0.8213	0.8213

Table 4: Comparison of encryption time (seconds).

Size	[40]	Proposed
256 ∗ 256	0.3085	0.2707
512 ∗ 512	0.5368	0.5717

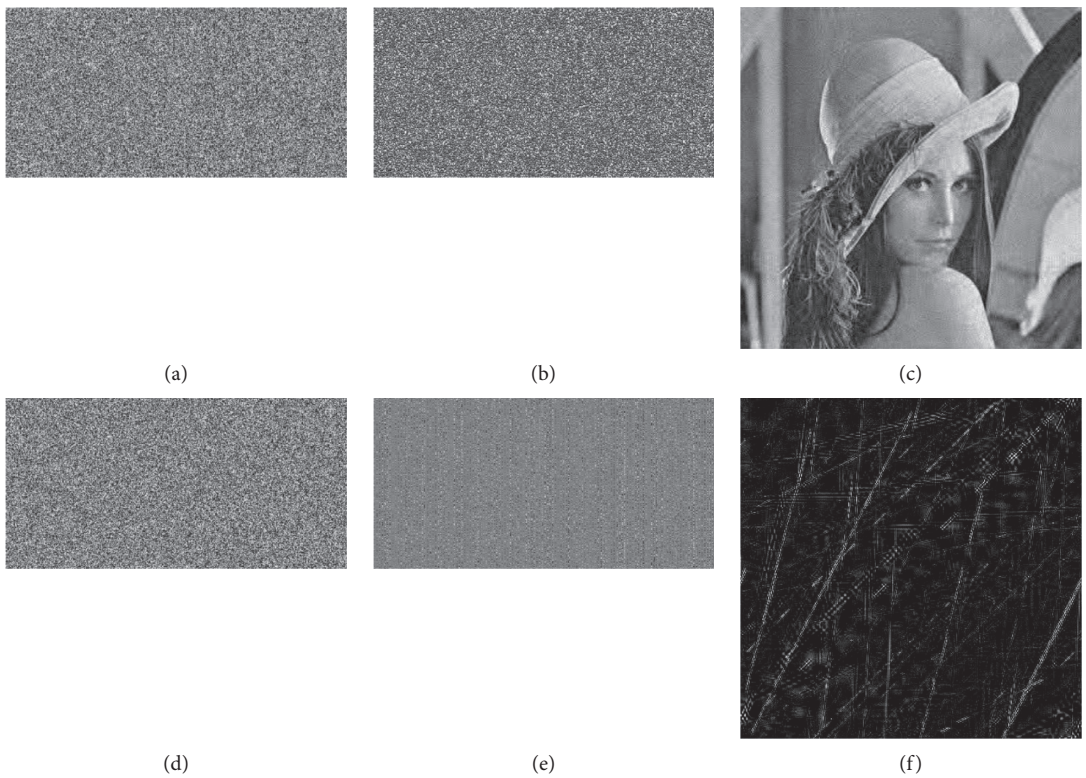
and treating MVM 2 as the measurement matrix. From Figure 7(f), one can see that the parallel CS output result of an identity matrix is no longer the measurement matrix.

What is more, the obtained measurement value matrix will be subsequently encrypted by diffusion process, so the probability of extracting the measurement matrix is zero. Consequently, the attacker cannot retrieve the plain image by launching CPA. In the light of the above analysis and experiments, it is impossible to retrieve the plain image by launching CPA.

4.8. Robustness Analysis

4.8.1. Robustness Evaluation against Noise. As the cipher image will be contaminated during the transmission process, robustness against noise attack is an evaluation index for an effective image encryption scheme. To assess the robustness against noise attack, the quality of corresponding decrypted images will be evaluated if the cipher image is contaminated with salt and pepper noise, Gaussian noise, and speckle noise with different intensities. In this test, the image Girl shown in Figure 3 is selected as the plain image, and its corresponding cipher image will be contaminated with noise. As shown in Figure 8, the cipher images with salt and pepper noise intensities 0.1%, 0.3%, 0.5%, and 0.7% are presented in the first row, the ones with Gaussian noise having different intensities 0.0001%, 0.0003%, 0.0005%, and 0.0007% are presented in the third row, and the ones with speckle noise having different intensities 0.0001%, 0.0003%, 0.0005%, and 0.0007% are presented in the fifth row, while the second row, fourth row, and sixth row denote the corresponding decrypted images of the first row, the third row, and the fifth row, respectively. As we can see, the decrypted images are still visually meaningful in the case of the cipher images contaminated.

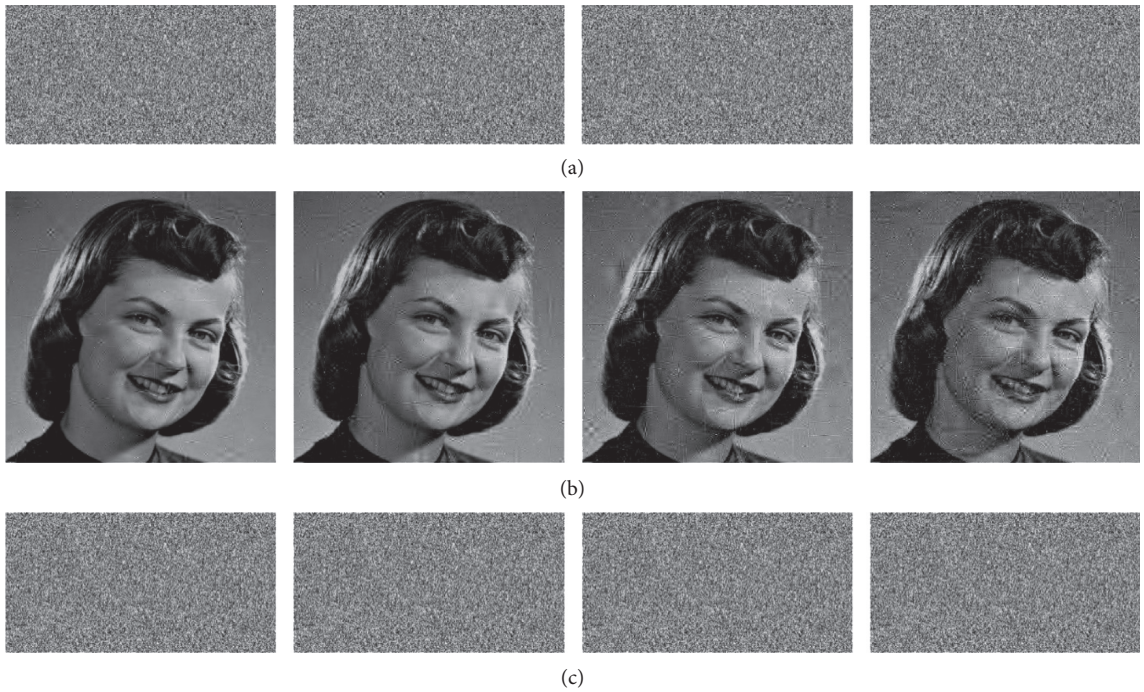
4.8.2. Robustness Evaluation against Occlusion. Robustness against occlusion of the proposed scheme is also tested in this paper. The image Girl is chosen as the plain image, and its corresponding cipher images will be occluded 32×32 in the upper left corner, the bottom left corner, the upper right corner, the bottom right corner, and the central directions, as shown in the first row of Figure 9. The decrypted



(a) (b) (c)

(d) (e) (f)

Figure 7: (a) The cipher image generated by the original CS scheme; (b) the measurement value matrix generated by the original CS scheme; (c) the decrypted image of (a); (d) the cipher image generated by the proposed SST-PCS scheme; (e) the measurement value matrix produced by the proposed SST-PCS scheme; (f) the reconstructed image of (d).

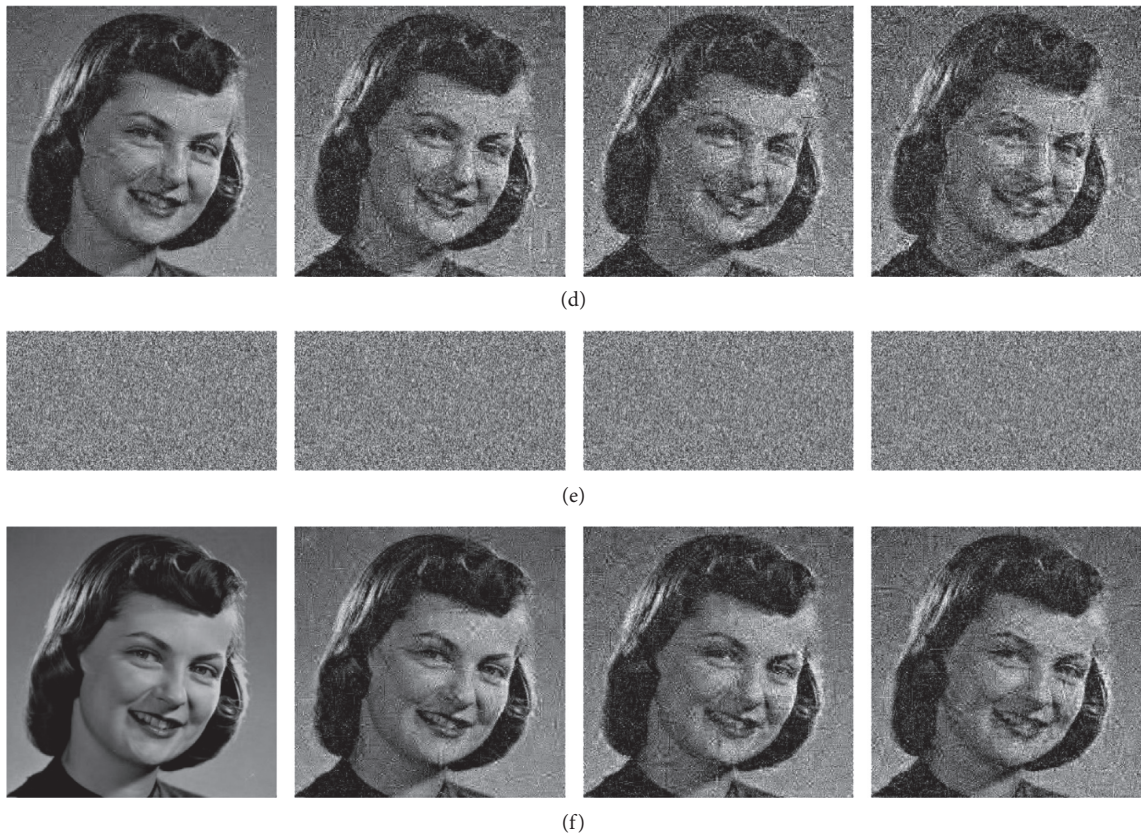


(a)

(b)

(c)

Figure 8: Continued.

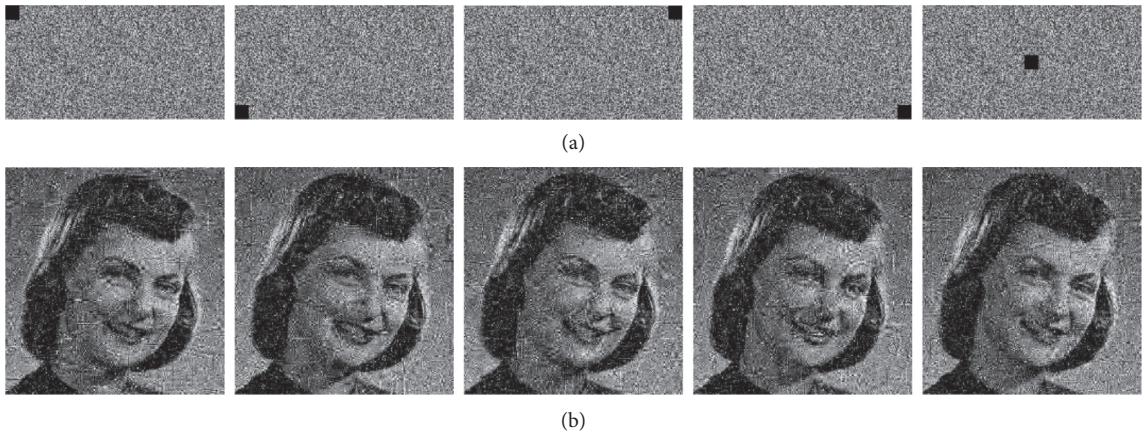


(d)

(e)

(f)

Figure 8: Robustness evaluation against noise: (a) sequentially cipher images with salt and pepper noise intensities 0.1%, 0.3%, 0.5%, and 0.7%, respectively; (c) sequentially cipher images with Gaussian noise intensities 0.0001%, 0.0003%, 0.0005%, and 0.0007%, respectively; (e) sequentially cipher images with speckle noise intensities 0.0001%, 0.0003%, 0.0005%, and 0.0007%, respectively; (b, d, f) the decrypted images corresponding to (a, c, e), respectively.



(a)

(b)

Figure 9: Robustness against occlusion analysis: the first column to the fifth column in (a) are sequentially the cipher images with occlusion in the upper left corner, the bottom left corner, the upper right corner, the bottom right corner, and the central directions, respectively; (b) the decrypted images corresponding to (a).

Table 5: Comparison of entropy.

Image	Image entropy	[41]	Proposed
Lena	7.4474	7.9992	7.9993
Barbara	7.4664	7.9993	7.9993
Peppers	7.3967	7.9993	7.9992

images corresponding to the first row are shown in the second row in Figure 9. From Figure 9, one can still obtain most of the image information from the decrypted image. The simulation results show that the proposed scheme exhibit robustness against occlusion to some extent.

4.9. Entropy Analysis. The entropy is an important evaluation index to evaluate the cryptosystem. To calculate the entropy of the proposed scheme, Lena, Barbara, and Peppers are selected as the plain images. The entropy is calculated by the following equation:

$$H(x) = -\sum_{i=1}^{N} p(x_i)\log_2\ p(x_i), \tag{21}$$

where $p(x_i)$ is the probability of appearance of pixel x_i and the maximum value of H is 8. We also compare the entropy of the proposed scheme with other existing encryption schemes [41]. The simulation results are depicted in Table 5. We can observe that the entropy of the cipher image is closer to 8, which indicates that the proposed image encryption scheme has high security.

5. Conclusion

In this paper, a scheme for image secure and efficient transmission in smart cities using SST and CS has been presented. Many recent works have investigated how to incorporate CS with other efficient cryptographic primitives to ensure confidentiality of the image. However, since CS sampling is a linear projection, those compound encryption methods can be translated to matrix multiplication, which cannot resist CPA. What is more, for smart cities, security issue is the most important. In our proposed scheme, by incorporating SST into the framework of CS and subsequently performing diffusion-permutation procedure followed by parallel CS, an efficient image simultaneous encryption and compression model with resistance against CPA is realized. Particularly, encryption and decryption can be computed individually for every column in parallel CS. It is practicable and reliable, with high potential to be adopted for CS measurement matrix reuse circumstance. Theoretical analyses and performance evaluations have verified the security and robustness of the proposed scheme.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the Shandong Provincial Natural Science Foundation (no. ZR2020QF014) and the Shandong Provincial Key Research and Development Program (Major Science and Technological Innovation Project, no. 2019JZZY010134).

References

[1] E.-S. M. El-Kenawy, M. M. Eid, M. Saber, and A. Ibrahim, "MBGWO-SFS: modified binary grey wolf optimizer based on stochastic fractal search for feature selection," *IEEE Access*, vol. 8, no. 99, pp. 107635–107649, 2020.

[2] A. Ibrahim and E. El-Kenawy, "Image segmentation methods based on superpixel techniques: a survey," *Journal of Computer Science and Information Systems*, vol. 1, no. 6, pp. 01–10, 2020.

[3] A. Ibrahim and E. El-Kenawy, "Applications and datasets for superpixel techniques: a survey," *Journal of Computer Science and Information Systems*, vol. 1, no. 6, pp. 11–16, 2020.

[4] E.-S. M. El-Kenawy, A. Ibrahim, S. Mirjalili, M. M. Eid, and S. E. Hussein, "Novel feature selection and voting classifier algorithms for Covid-19 classification in ct images," *IEEE Access*, vol. 8, pp. 179317–179335, 2020.

[5] E.-S. M. El-Kenawy, S. Mirjalili, A. Ibrahim et al., "Advanced meta-heuristics, convolutional neural networks, and feature selectors for efficient Covid-19 x-ray chest image classification," *IEEE Access*, vol. 9, pp. 36019–36037, 2021.

[6] 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.

[7] L. Jones, "Securing the smart city," *Engineering & Technology*, vol. 11, no. 5, pp. 30–33, 2016.

[8] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[9] J. Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

[10] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[11] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: universal encoding strategies?" *IEEE Transactions on Information Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[12] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2004.

[13] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[14] Z. Gao, C. Xiong, L. Ding, and C. Zhou, "Image representation using block compressive sensing for compression applications," *Journal of Visual Communication and Image Representation*, vol. 24, no. 7, pp. 885–894, 2013.

[15] R. Hemalatha, S. Radha, and S. Sudharsan, "Energy-efficient image transmission in wireless multimedia sensor networks using block-based compressive sensing," *Computers & Electrical Engineering*, vol. 44, pp. 67–79, 2015.

[16] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proceedings of the 2008 Allerton*

Conference on Communication, Control, and Computing, pp. 813–817, Monticello, IL, USA, September 2008.

[17] A. Masoum, N. Meratnia, and P. J. M. Havinga, "A distributed compressive sensing technique for data gathering in wireless sensor networks," *Procedia Computer Science*, vol. 21, no. 4, pp. 207–216, 2013.

[18] Z. Yang, W. Yan, and Y. Xiang, "On the security of compressed sensing-based signal cryptosystem," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 3, pp. 363–371, 2015.

[19] T. Bianchi, V. Bioglio, and E. Magli, "On the security of random linear measurements," in *Proceedings of the 2014 IEEE International Conference on Acoustic, Speech and Signal Processing*, pp. 4020–4024, Florence, Italy, May 2014.

[20] B. Deepan, C. Quan, Y. Wang, and C. J. Tay, "Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique," *Applied Optics*, vol. 53, no. 20, pp. 4539–4547, 2014.

[21] J. Li, J. Sheng Li, Y. Yang Pan, and R. Li, "Compressive optical image encryption," *Scientific Reports*, vol. 5, pp. 10374–10, 2015.

[22] L. Zeng, X. Zhang, L. Chen, Z. Fan, and Y. Wang, "Scrambling-based speech encryption via compressed sensing," *Eurasip Journal on Advances in Signal Processing*, vol. 2012, no. 1, pp. 1–12, 2012.

[23] X. Huang, G. Ye, H. Chai, and O. Xie, "Compression and encryption for remote sensing image using chaotic system," *Security and Communication Networks*, vol. 8, no. 18, pp. 3659–3666, 2016.

[24] Y. Zhang, J. Zhou, F. Chen et al., "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, no. C, pp. 472–480, 2016.

[25] X. Wu, S. Tang, and P. Yang, "Low-complexity cloud image privacy protection via matrix perturbation," 2014, https://arxiv.org/abs/1412.5937.

[26] B. Kim, B. Lee, G. Situ, I. Muniraj, and N. Rawat, "Compressive sensing based robust multispectral double-image encryption," *Applied Optics*, vol. 54, no. 7, pp. 1782–1793, 2015.

[27] 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.

[28] R. Fay and C. Ruland, "Compressive sensing encryption modes and their security," in *Proceedings of the 11th International Conference for Internet Technology and Secured Transactions*, pp. 119–126, Barcelona, Spain, December 2016.

[29] 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.

[30] G. Hu, D. Xiao, Y. Wang, T. Xiang, and Q. Zhou, "Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes," *Optics and Lasers in Engineering*, vol. 98, pp. 123–133, 2017.

[31] X. Lv, X. Liao, and B. Yang, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28633–28663, 2018.

[32] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[33] L. Lei Yu, J. P. Barbot, G. Gang Zheng, and H. Hong Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Processing Letters*, vol. 17, no. 8, pp. 731–734, 2010.

[34] Y. Zhang, J. Zhou, F. Chen et al., "A block compressive sensing based scalable encryption framework for protecting significant image regions," *International Journal of Bifurcation and Chaos*, vol. 26, no. 11, pp. 1234–1247, 2016.

[35] Z. Chen, X. Hou, X. Qian, and C. Gong, "Efficient and robust image coding and transmission based on scrambled block compressive sensing," *IEEE Transactions on Multimedia*, vol. 20, no. 7, pp. 1610–1621, 2018.

[36] J. Li, H. Li, J. Li, Y. Pan, and R. Li, "Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography," *Optics Communications*, vol. 344, pp. 166–171, 2015.

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

[38] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[39] 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.

[40] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, 2017.

[41] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a boolean network," *Information Sciences*, vol. 539, pp. 195–214, 2020.