Hindawi
Security and Communication Networks
Volume 2020, Article ID 6665702, 15 pages
https://doi.org/10.1155/2020/6665702

Research Article

Secure and Efficient Image Compression-Encryption Scheme Using New Chaotic Structure and Compressive Sensing

Yongli Tang,[1] Mingjie Zhao ,[1] and Lixiang Li [2]

[1]*School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China*
[2]*Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunication, Beijing 100876, China*

Correspondence should be addressed to Lixiang Li; lixiang@bupt.edu.cn

Received 9 October 2020; Revised 6 November 2020; Accepted 8 December 2020; Published 29 December 2020

Academic Editor: Lingwei Xu

The rapid development of the Internet leads to a surge in the amount of information transmission and brings many security problems. For multimedia information transmission, especially digital images, it is necessary to compress and encrypt at the same time. The emergence of compressive sensing solves this problem. Compressive sensing can compress and encrypt at the same time, which can not only reduce the transmission bandwidth of the network but also improve the security of the system. However, when using compressive sensing encryption, the whole measurement matrix needs to be stored, and the compressive sensing can be combined with a chaotic system, so only the generation parameters of the matrix need to be stored, and the security of the system can be further improved by using the sensitivity of the chaotic system. This paper introduces a secure and efficient image compression-encryption scheme using a new chaotic structure and compressive sensing. The chaotic map used in the scheme is generated by our new and universal chaotic structure, which not only expands the chaotic range of the chaotic system but also improves the performance of the chaotic system. After analyzing the performance comparison of traditional one-dimensional chaotic maps and some existing methods, the image compression-encryption scheme based on a new chaotic structure and compressive sensing has a good encryption effect and large keyspace, which can resist brute force attack and statistical attack.

1. Introduction

With the advent of the fifth-generation mobile networks (5G) era, the amount of information transmission is gradually increasing, and the requirements for transmission speed are also increased significantly, which requires more effective compression sampling methods to achieve higher sampling rates and signal processing speeds. Due to the security problems of the network itself, multimedia data are vulnerable to various attacks in the process of storage and secure transmission in the network, so it is particularly important to ensure the security of media information data [1, 2]. In order to carry out multimedia communication more effectively, the original image must be compressed and encrypted at the same time, and the emergence of compressive sensing can solve this problem. In 2006, Donoho [3] and Candès et al. [4] formally proposed the theory of compressive sensing (CS). Compressive sensing is an improvement on the Nyquist sampling, which can sample sparse signals nonuniformly with the number of samples far less than Nyquist sampling law and recover the original data with the reconstruction performance lower than Nyquist sampling. It is widely used in wireless sensor networks, image encryption, image data hiding, etc.

Due to the use of compressive sensing for encryption, the whole measurement matrix needs to be stored, which requires a large amount of storage space. However, it is possible to use the chaotic system that only needs to store the generation parameters of the measurement matrix, instead of storing the characteristics of the whole measurement matrix to reduce the storage space. Because of their chaotic characteristics, such as sensitivity to initial values and parameters [5, 6], ergodicity [7, 8], and uncertainty [9, 10], chaotic systems have been widely used in encryption fields

[11–13]. Therefore, researchers have designed many image encryption algorithms that combine compressive sensing with chaotic systems [14–16].

Peng et al. [14] proposed a security and energy-saving scheme in wireless body area networks, which can solve both energy-saving and data security problems. Compared with the traditional encryption scheme, which only used one matrix to encrypt, they use any one of Chebyshev map, Logistic map, and Tent map to generate two chaotic matrices to encrypt at the same time, which increased the security and solved the security problem in a wireless volume domain network. Wang et al. [15] proposed a visual security image encryption scheme with parallel compressive sensing and designed a visual security encryption scheme with parallel compressive sensing counter mode and embedding technology. In order to achieve a higher security level, the Logistic-Tent chaotic system and 3D Cat map are introduced to construct the measurement matrix, and Zigzag confusion is used for interference. Chai et al. [16] proposed an image encryption method based on the combination of a magnetically controlled memristive chaotic system and compressive sensing. This scheme uses the technologies of a magnetically controlled memristive chaotic system, Secure Hash Algorithm- (SHA-) 512, and cellular automata. In this scheme, cellular automata are used in the diffusion stage to enhance the security of the encryption system, and SHA-512 is used to calculate the initial value of the chaotic system and further generate a measurement matrix, which makes the measurement matrix used in encrypting different types of data. This scheme can improve the correlation between the original image and the algorithm and resist known plaintext attacks and selected plaintext attacks. Chanil et al. [17] proposed a chaotic structure and applied a Logistic map and Sine map into their structure. In order to verify the performance of the proposed chaotic structure, they proposed a new bit-level color image encryption scheme. Through simulation analyses of the bifurcation diagram and Lyapunov exponent, it was proved that their chaotic structure was correct and the range of chaotic parameters was expanded.

We propose a secure and effective image compression-encryption scheme using the new chaotic structure and compressive sensing. The chaotic map used in the compression-encryption scheme is to apply the commonly used traditional one-dimensional chaotic maps to the new and general chaotic structure proposed by us. In this encryption scheme, compressive sensing is used for sampling, which can reduce storage space and transmission bandwidth. The chaotic system only needs to store matrix generation parameters, which can further reduce transmission bandwidth. Arnold interference technology and the SHA-256 function are also used, and the SHA-256 function makes different original images have different keys. Firstly, the Discrete Wavelet Transform (DWT) is used to sparse the original image, and then Arnold interference is applied to the sparse image. The interference parameters of Arnold interference are generated by the SHA-256 function. Then, compressive sensing is used to compress and sample the interference images. Finally, a chaotic sequence is used to perform row and column cyclic shift interference on the compressed and sampled image. Simulation results show that the compression-encryption scheme has a large parameter space and keyspace, which can prevent the statistical attack and brute force attack.

The rest of this paper is arranged as follows. Section 2 introduces the related basic knowledge. Section 3 describes the proposed chaotic structure and chaotic map under a new structure. Section 4 describes our encryption and decryption scheme. Section 5 simulates and evaluates our encryption scheme. Section 6 summarizes the research content carried out in this paper.

2. Fundamental Knowledge

This section gives a brief introduction to the traditional one-dimensional chaotic maps and compressive sensing.

2.1. Chaotic Maps. The commonly used traditional one-dimensional chaotic systems are the Sine map, Logistic map, Chebyshev map, and Tent map.

(1) Sine map

Sine map is a very simple and commonly used chaotic system [18]. Sine map is denoted as

$$s_{n+1} = r_s \times \sin(\pi \times s_n), \tag{1}$$

where r_s is the chaotic parameter of the Sine map, and $s_n \in [0, 1]$ is the Sine chaotic sequence.

The bifurcation diagram and Lyapunov exponent diagram of the traditional Sine map are shown in Figures 1(a) and 2(a). The Lyapunov exponent indicates that the chaotic system must have at least one positive Lyapunov exponent. When the Lyapunov exponent is positive, the chaotic characteristics of the system can be quantified; that is, a chaotic system is sensitive to initial conditions. The larger the Lyapunov exponent is, the more sensitive to initial values the chaotic system is. As can be seen from Figures 1(a) and 2(a), the Sine map has chaotic behaviors when the chaotic parameter r_s is in the range $r_s \in [0.867, 1]$.

(2) Logistic map

The logistic map is also a very simple but widely used chaotic system [19]. Its performance is similar to that of a Logistic map, and it is defined as

$$l_{n+1} = r_l \times l_n \times (1 - l_n), \tag{2}$$

where r_l is the chaotic parameter of the Logistic map, and $l_n \in [0, 1]$ is the Logistic chaotic sequence.

The bifurcation diagram and Lyapunov exponent diagram of the traditional Logistic map are shown in Figures 1(c) and 2(c). As can be seen from Figures 1(c) and 2(c), the Logistic map has chaotic behaviors when the control parameter r_l is in the range $r_l \in [3.5, 4]$.

(3) Chebyshev map

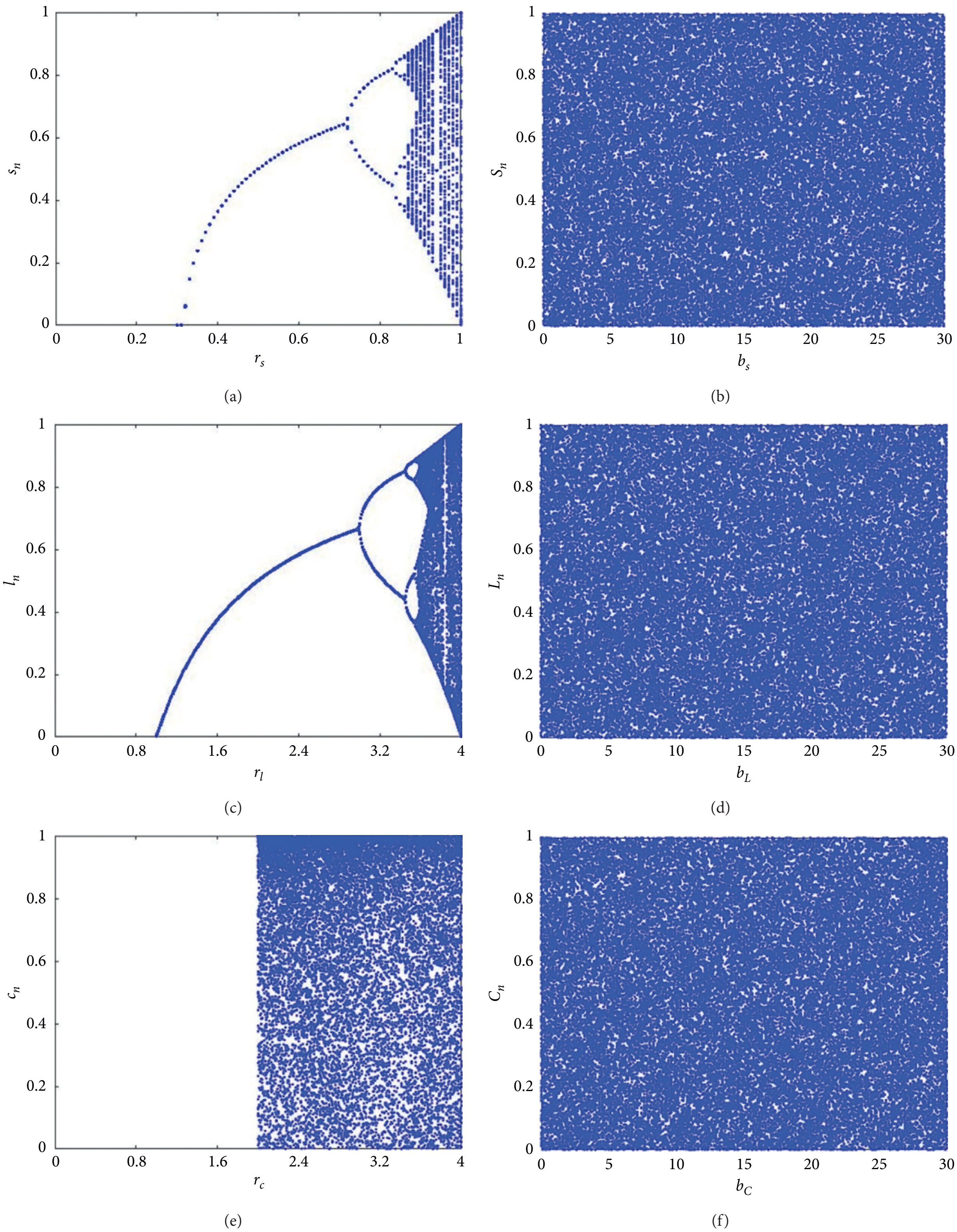
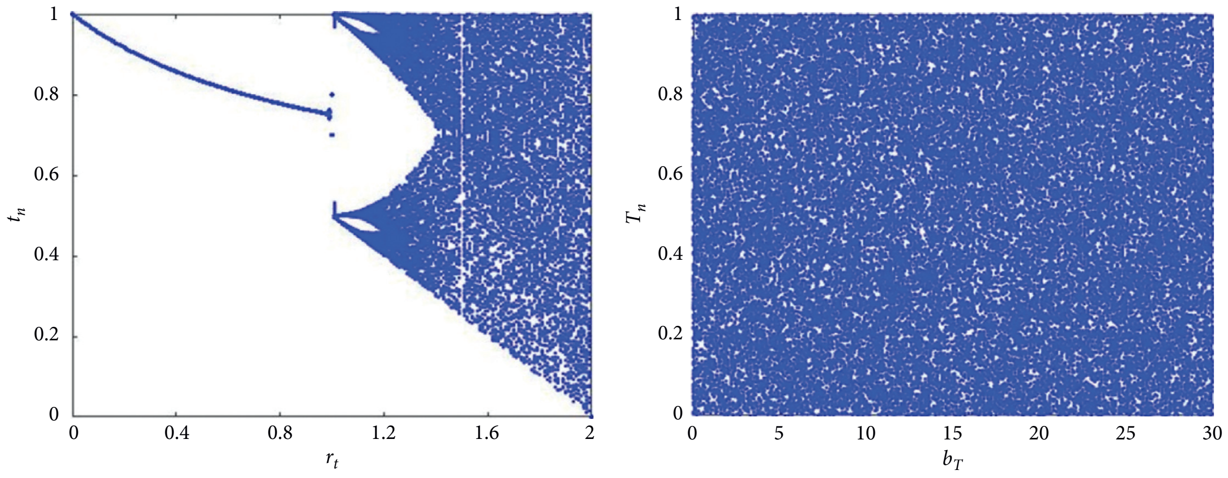


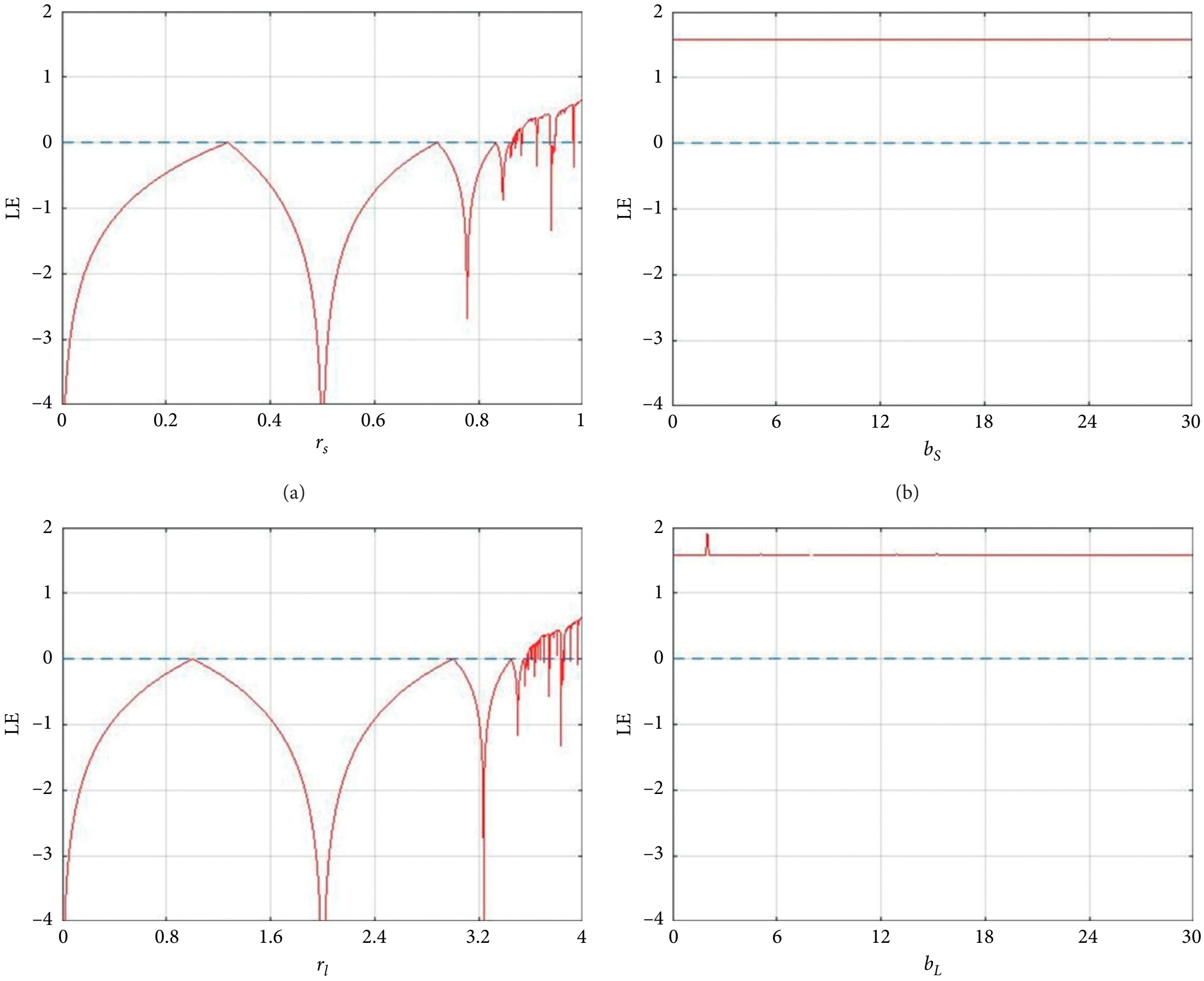
Figure 1: Continued.



(g)

(h)

Figure 1: Bifurcation diagrams of the traditional one-dimensional chaotic maps and the corresponding new one-dimensional chaotic maps under our chaotic structure: (a) the traditional Sine map, (b) Sine map under our chaotic structure, (c) the traditional Logistic map, (d) Logistic map under our chaotic structure, (e) the traditional Chebyshev map, (f) Chebyshev map under our chaotic structure, (g) the traditional Tent map, and (h) Tent map under our chaotic structure.



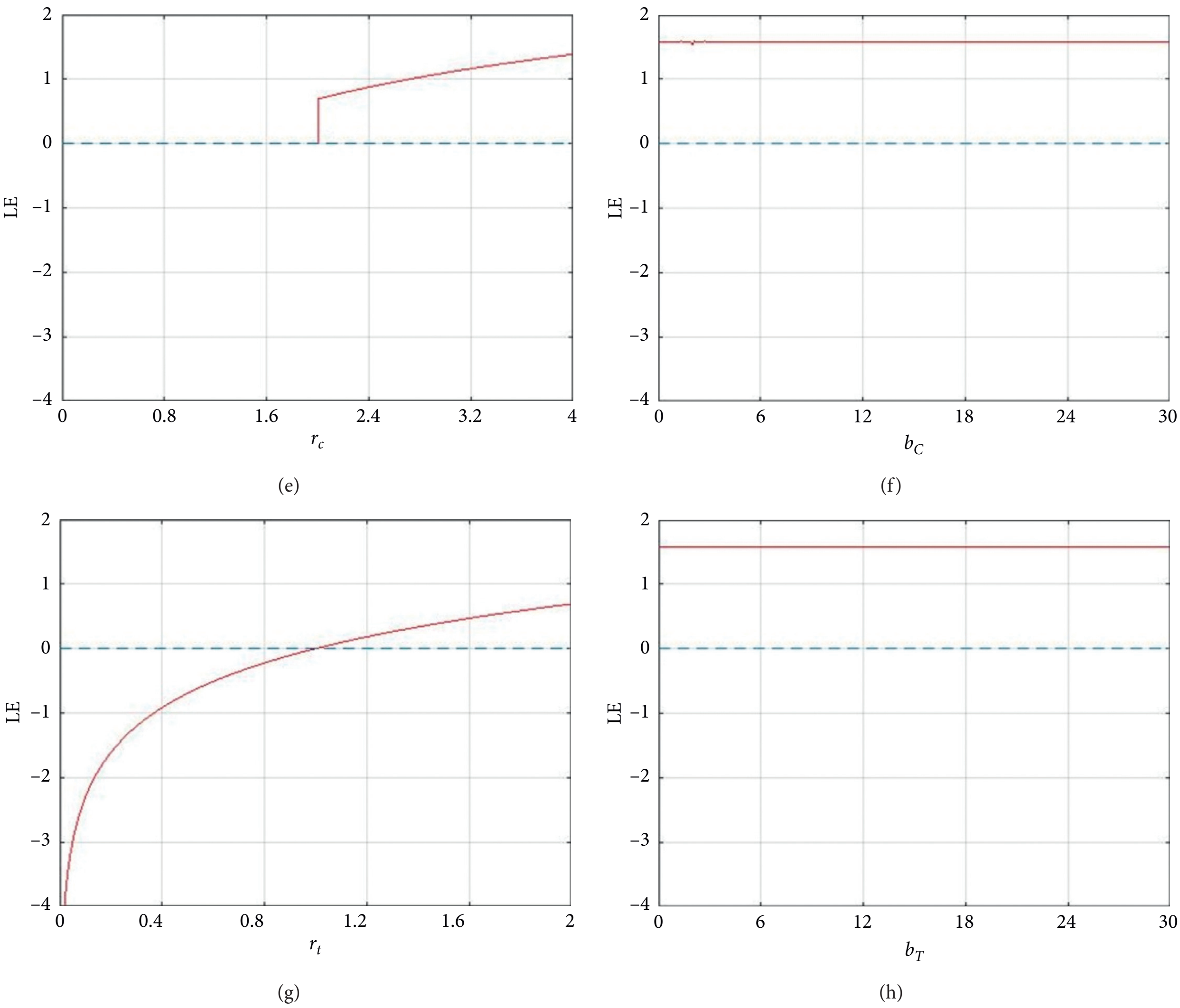
(a)

(b)

(c)

(d)

Figure 2: Continued.



(e)

(f)

(g)

(h)

Figure 2: Lyapunov exponent diagrams of the traditional one-dimensional chaotic maps and the corresponding new one-dimensional chaotic maps under our chaotic structure: (a) the traditional Sine map, (b) Sine map under our chaotic structure, (c) the traditional Logistic map, (d) Logistic map under our chaotic structure, (e) the traditional Chebyshev map, (f) Chebyshev map under our chaotic structure, (g) the traditional Tent map, and (h) Tent map under our chaotic structure.

Like the Logistic map and Sine map, the Chebyshev map is also a commonly used one-dimensional chaotic map [20], and it is defined as follows:

$$c_{n+1} = \cos\left(r_c \times \arccos c_n\right), \tag{3}$$

where r_c is the chaotic parameter of the Chebyshev map, and $c_n \in [-1, 1]$ is the Chebyshev chaotic sequence.

The bifurcation diagram and Lyapunov exponent diagram of the traditional Chebyshev map are shown in Figures 1(e) and 2(e). Chebyshev map has chaotic behaviors when the chaotic parameter r_c takes values in the range $r_c \in [2, 4]$.

(4) Tent map

Tent map is defined as follows [21]:

$$t_{n+1} = 1 - r_t \times \left|t_n - 0.5\right|, \tag{4}$$

where r_t is the chaotic parameter of the Tent map, and $t_n \in [0, 1]$ is the chaotic sequence of the Tent map.

The bifurcation diagram and Lyapunov exponent diagram of the traditional Tent map are shown in Figures 1(g) and 2(g). Tent map has chaotic behaviors when the chaotic parameter r_t is in the range $r_t \in (1, 2]$.

2.2. Compressive Sensing. Candès et al. [22] proposed that if $\mathbf{x} \in R^N$ is an unknown vector, which is sparse or compressible on a set of orthogonal bases, the unknown vector $\mathbf{x}$ can be accurately recovered by fewer random measured values $\mathbf{y}$. And this sampling process can be described by a mathematical model as follows:

$$\mathbf{y} = \mathbf{\Phi x}, \tag{5}$$

where $\mathbf{\Phi}$ is the matrix is of size $M \times N$, $M < N$, and $\mathbf{y} \in R^M$ is the sampling value.

This mathematical representation is also a description of the standard framework of compressed perception which is a special case of underdetermined linear equations. Since there are infinitely many solutions in equation (5), the original signal $\mathbf{x}$ cannot be recovered directly from the sampled value $\mathbf{y}$. However, if $\mathbf{x}$ reflects sparsity in the sparse dictionary $\mathbf{\Psi}$ [23], that is,

$$\mathbf{x} = \mathbf{\Psi}\mathbf{a}, \tag{6}$$

where $\mathbf{a}$ is K-sparse and is denoted as $\mathbf{a} \in \Sigma_K$, so we have

$$\mathbf{y} = \mathbf{\Phi}\mathbf{x} = \mathbf{\Phi}\mathbf{\Psi}\mathbf{a} = \boldsymbol{\theta}\mathbf{a}, \tag{7}$$

where $\boldsymbol{\theta} = \mathbf{\Phi}\mathbf{\Psi}$ is the measurement matrix in compressive sensing. So we can recover $\mathbf{x}$ from $\mathbf{y}$. $\mathbf{a}$ is recovered by

$$\min_{\mathbf{a}} \|\mathbf{a}\|_{l_0}, \quad \text{where}, \mathbf{y} = \boldsymbol{\theta}\mathbf{a}. \tag{8}$$

Equation (8) is a l_0 optimization problem. Under certain conditions, the l_0 optimization problem can be transformed into a l_1 optimization problem. The typical conditions include Null Space Property (NSP) and Restricted Isometry Property (RIP). And the equivalent solution can be obtained by [24]

$$\min_{\mathbf{a}} \|\mathbf{a}\|_{l_1}, \quad \text{where}, \mathbf{y} = \boldsymbol{\theta}\mathbf{a}. \tag{9}$$

For the measurement matrix, spark property should be satisfied, that is, the minimum number of linear correlation of the columns of the measurement matrix, and the formula is

$$\operatorname{spark}(\boldsymbol{\theta}) = \min_{\mathbf{a} \neq 0} \|\mathbf{a}\|_0, \quad \text{where}, \boldsymbol{\theta}\mathbf{a} = 0. \tag{10}$$

Donoho [25] pointed out that if $\operatorname{spark}(\boldsymbol{\theta}) > 2K$, for any vector $\mathbf{y} \in R^M$, there is at most one signal $\mathbf{a} \in \Sigma_K$ that makes $\mathbf{y} = \boldsymbol{\theta}\mathbf{a}$.

Because solving a sparse solution is an NP-hard problem, it is impractical to solve the measurement matrix $\boldsymbol{\theta}$ that satisfies this condition from the perspective of computation [26]. In order to recover sparse signals in reality, Candès et al. [4] introduced the RIP that there is a constant $\delta_K \in (0, 1)$. Equation (11) holds true for all $\mathbf{a} \in \Sigma_K$.

$$(1 - \delta_K)\|\mathbf{a}\|_2^2 \leq \|\boldsymbol{\theta}\mathbf{a}\|_2^2 \leq (1 + \delta_{\mathbf{K}})\|\mathbf{a}\|_2^2. \tag{11}$$

Although RIP provides a theoretical guarantee for recovering K-sparse signals, it is relatively complex to verify that a measurement matrix $\boldsymbol{\theta}$ meets RIP characteristics. Therefore, in many cases, it is necessary to use the correlation $\mu(\boldsymbol{\theta})$ of the measurement matrix $\boldsymbol{\theta}$ to provide a more specific recovery guarantee. Correlation $\mu(\boldsymbol{\theta})$ refers to the maximum value of the normalized inner product of two columns randomly selected in $\boldsymbol{\theta}$ [27], namely,

$$\mu(\boldsymbol{\theta}) = \max_{1 \leq i \neq j \leq N} \frac{\left|\langle \boldsymbol{\theta}_i, \boldsymbol{\theta}_j \rangle\right|}{\left\|\boldsymbol{\theta}_i\right\|_2 \left\|\boldsymbol{\theta}_j\right\|_2}, \tag{12}$$

where $\boldsymbol{\theta}_i$ is the i-th column of $\boldsymbol{\theta}$. For any vector $\mathbf{y}$, if $\mu(\boldsymbol{\theta}) \leq 1(2K - 1)$, there is at most one signal $\mathbf{a} \in \Sigma_K$, making $\mathbf{y} = \boldsymbol{\theta}\mathbf{a}$.

Common recovery algorithms include Matching Pursuit (MP) algorithm [28], Orthogonal Matching Pursuit (OMP) algorithm [29], Orthogonal Matching Pursuit (StOMP) algorithm [30], and Compressive Sampling Matching Pursuit (CoSaMP) algorithm [31].

3. New Chaotic Structure

In this section, we firstly describe a new chaotic structure in detail, and secondly, we describe the new chaotic maps generated by applying the Sine map, Logistic map, Chebyshev map, and Tent map to the new chaotic structure.

3.1. New Chaotic Structure. The new chaotic structure is given as follows:

$$\mathbf{y}_{n+1} = F(b, \mathbf{y}_n, k) = \operatorname{mod}\left(\left(F_{\text{chaos}}(b, \mathbf{y}_n) - \frac{\mathbf{y}_n^2}{3}\right) \times 2^k, 1\right), \quad k \geq 0, \tag{13}$$

where $F_{\text{chaos}}(b, \mathbf{y}_n)$ is the traditional one-dimensional chaotic map mentioned in Section 2, $F(b, \mathbf{y}_n, k)$ is a new chaotic map generated under our new chaotic structure, $\mathbf{y}_n \in [0, 1]$ is the chaotic sequence, b is the chaotic parameter of the proposed chaotic structure, and b can take any value. mod is a modulus function, which ensures that the values of the generated chaotic sequence are in the range $[0, 1]$. 2^k is an adjustment function about the iteration parameter k, which is iterated through adjustments to eliminate the transient effect. The values of b, k in this chaotic structure should be specifically analyzed according to the embedded map; that is to say, when different chaotic maps are applied to the proposed chaotic structure, the values of b, k will have different value ranges.

3.2. Application and Analysis of Our New Chaotic Structure. In this subsection, we give the detailed analyses of new chaotic maps generated by our new chaotic structure.

(1) New Sine map under our new chaotic structure

The new Sine map under our new structure is defined as follows:

$$S_{n+1} = \operatorname{mod}\left(b_S \times \sin(\pi \times S_n) - \frac{S_n^2}{3}\right) \times 2^{k_S}, 1), \tag{14}$$

where $S_n \in [0, 1]$ is the new Sine chaotic sequence which is generated by our new chaotic structure, and S_0 is the initial value of the new Sine chaotic sequence. b_S is the chaotic parameter of this new Sine map, and k_S is the iterations parameter of the new Sine map.

The bifurcation diagram and Lyapunov exponent diagram of the new Sine map under our new structure are shown in Figures 1(b) and 2(b). It can be seen from Figures 1(b) and 2(b) that the new Sine map under our new structure has a much larger chaotic parameter range than the traditional Sine map and the Lyapunov exponent that are all positive numbers, which proves the superiority of the proposed Sine map. When $k_S \in [6, 28]$ and $b_S \in [0, 30]$, the state of the new Sine map under our new structure is fully chaotic.

(2) New Logistic map under our new chaotic structure

The new Logistic map generated by our new chaotic structure is presented as follows:

$$L_{n+1} = \operatorname{mod}\left(\left(b_L \times L_n \times (1 - L_n) - \frac{L_n^2}{3}\right) \times 2^{k_L}, 1\right), \tag{15}$$

where $L_n \in [0, 1]$ is the new Logistic chaotic sequence which is generated by our new chaotic structure, and L_0 is the initial value of the new Logistic chaotic sequence. b_L is the chaotic parameter of the new Logistic map, and k_L is the iterations parameter of the new Logistic map.

The bifurcation diagram and Lyapunov exponent diagram of the new Logistic map under our new structure are shown in Figures 1(d) and 2(d). Like the new Sine map under our new structure, its chaotic range and performance are much better than the traditional Logistic map. When $k_L \in [7, 21]$, $b_L \in [0, 30]$, the Logistic map under our new structure is in a fully chaotic state.

(3) New Chebyshev map under our new chaotic structure

The new Chebyshev map under our new structure can be expressed as follows:

$$C_{n+1} = \operatorname{mod}\left(\left(\cos\left(b_C \times \arccos\left(C_n\right)\right) - \frac{C_n^2}{3}\right) \times 2^{k_C}, 1\right), \tag{16}$$

where $C_n \in [0, 1]$ is the new Chebyshev chaotic sequence which is generated by our new chaotic structure, and C_0 is the initial value of the new Chebyshev chaotic sequence. b_C is the chaotic parameter of this new Chebyshev map, and k_C is the iterations parameter of the new Chebyshev map.

The bifurcation diagram and Lyapunov exponent diagram of the new Chebyshev map under our new structure are shown in Figures 1(f) and 2(f). When $k_C \in [8, 29]$ and $b_C \in [0, 30]$, the state of the Chebyshev map under our new structure is fully chaotic.

(4) New Tent map under our new chaotic structure

The new Tent map under our new structure is defined as follows:

$$T_{n+1} = \operatorname{mod}\left(\left(\left(1 - b_T \times \left|T_n - 0.5\right|\right) - \frac{T_n^2}{3}\right) \times 2^{k_T}, 1\right), \tag{17}$$

where $T_n \in [0, 1]$ is the new Tent chaotic sequence which is generated by our new chaotic structure, and T_0 is the initial value of the new Tent chaotic sequence. b_T is the chaotic parameter of the new Tent map, and k_T is the iterations parameter of the new Tent map.

The bifurcation diagram and Lyapunov exponent diagram of the new Tent map under our new structure are shown in Figures 1(h) and 2(h). The Tent map under our new chaotic structure is fully chaotic when $k_T \in [5, 21]$, $b_T \in [0, 30]$.

4. The Proposed Compression-Encryption Scheme

In this section, a secure and effective image compression-encryption scheme is proposed by using the new chaotic map under a new structure and compressive sensing.

4.1. Key Generation

(1) The generation of the Arnold interference parameters k_1, k_2 and the interference number k_3: calculate the 256-bit hash value H according to the original image X with SHA-256 function, then divide H into two blocks, and three initial values $n_0, \mathbf{a}_0, b_0$ are randomly selected. SHA-256 function can be used to calculate the key according to the original image, and different original images have different Arnold interference effects and different chaotic sequence parameters, so as to achieve different effects of original images and different measurement matrix. The specific formula of SHA-256 function can be expressed as follows:

$$\begin{aligned} H &= h_1, h_2, \ldots, h_{31}, h_{32}, \\ k_1 &= n_0 + \left(h_1 \oplus h_2 \oplus \cdots \oplus h_{15} \oplus h_{16}\right), \\ k_2 &= k_1 + \mathbf{a}_0 \times \left(h_{17} \oplus h_{18} \oplus \cdots \oplus h_{31} \oplus h_{32}\right), \\ k_3 &= \left(k_1 \oplus k_2\right) + b_0. \end{aligned} \tag{18}$$

(2) The generation of two improved chaotic sequences z_0, z_1: we use the new chaotic maps proposed in this paper to generate chaotic sequences. Two improved chaotic sequences are generated according to the initial values z_0', z_1' and control parameters u_0, u_1. Take a new Tent map and new Chebyshev map as examples:

$$\begin{aligned} z_0 &= \operatorname{mod}\left(\left(\cos\left(u_0 \times \arccos\left(z_0'\right)\right) - \frac{z_0^{\prime 2}}{3}\right) \times 2^{16}, 1\right), \\ z_1 &= \operatorname{mod}\left(\left(\left(1 - u_1 \times \left|z_1' - 0.5\right|\right) - \frac{z_1^{\prime 2}}{3}\right) \times 2^{16}, 1\right). \end{aligned} \tag{19}$$

(3) Calculate the cyclic sequence bitRow in the row direction. Randomly select the cycle number keyRow of the cyclic shift in the row direction, and generate LogisticRow according to the initial value

LogisticRow′ and control parameter ω_0. The steps can be expressed as follows:

$$\begin{aligned}
\text{LogisticRow} &= \text{zero}\,(\text{keyRow}, \text{Rows}),\\
\text{bitRow} &= \text{zero}\,(\text{keyRow}, \text{Rows}),\\
\text{for}\, i &= 2\text{: keyRow: Rows},\\
\text{LogisticRow}\,(i) &= \omega_0 \times \text{LogisticRow}\,(i-1)\\
&\quad \times (1 - \text{LogisticRow}\,(i-1)),\\
\text{bitRow}\,(i) &= \text{rem}\,(\text{round}\,(\text{LogisticRow}\,(i)\\
&\quad \times 100,000), \text{Columns}),\\
\text{end},&
\end{aligned} \tag{20}$$

where LogisticRow is the traditional Logistic map which is used to interfere with the sequence in the row direction, Rows is the numbers of rows, and Columns is the numbers of columns. The number of cycles on the row is once per row, so it needs Rows time. The interference in the row direction is performed according to the cycle number keyRow of the cyclic shift in the row direction. Since the number of interference in the row direction will not be greater than the number of Columns, the number of cycles can be set to Columns.

(4) Calculate the cyclic sequence bitColumn in the column direction. Randomly select the cycle number keyColumn of the cyclic shift in the column direction, and generate LogisticColumn according to the initial value LogisticColumn′ and control parameter ω_1. The steps can be expressed as follows:

$$\begin{aligned}
\text{LogisticColumn} &= \text{zero}\,(\text{keyColumn}, \text{Columns}),\\
\text{bitColumn} &= \text{zero}\,(\text{keyColumn}, \text{Columns}),\\
\text{for}\, i &= 2\text{: keyColumn: Columns},\\
\text{LogisticColumn}\,(i) &= \omega_1 \times \text{LogisticColumn}\,(i-1)\\
&\quad \times (1 - \text{LogisticColumn}\,(i-1)),\\
\text{bitColumn}\,(i) &= \text{rem}\,(\text{round}\,(\text{LogisticColumn}\,(i)\\
&\quad * 100,000), \text{Rows}),\\
\text{end},&
\end{aligned} \tag{21}$$

where LogisticColumn is the traditional Logistic map which is used to interfere with the sequence in the column direction. Similarly, the number of cycles on the column is one for each column, so it takes Columns time. Interference in the column direction is performed according to the number of cycles keyColumn of cyclic shift in the column direction. Since the number of interference in the column direction will not be greater than the number of Rows, the number of cycles can be set to Rows.

4.2. Compression-Encryption Scheme. The chaotic map proposed in this paper is used to construct the measurement matrix for compression and encryption. Specific encryption steps can be described as follows:

Step 1: firstly, an original image X with the size of $m \times n$ is obtained.

Step 2: the original image X is sparse by Discrete Wavelet Transform (DWT), and the sparse image X_1 with the size $m \times n$ is obtained.

Step 3: Arnold interference is carried out on a sparse image X_1 according to Arnold interference parameters k_1, k_2 and interference number k_3. The interference image is represented by X_2 with size $m \times n$.

Step 4: according to the z_0, z_1 chaotic sequences, two measurement matrices are obtained. One measurement matrix is represented by $\mathbf{\Phi}_1$ and the size is $p \times q$. p is a random number as the number of rows of the measurement matrix. The number of columns of the measurement matrix is the same as the number of rows of the measured image, that is $q = m$, which is used for compression and sampling, and the other measurement matrix is represented by $\mathbf{\Phi}_2$, whose size is $p \times q$. The compression and sampling process using compressive sensing is expressed as follows:

$$X3 = \mathbf{\Phi}_1 \times X2 + \mathbf{\Phi}_2, \tag{22}$$

where X_3 is the image after compressed sampling, and its size is $p \times n$.

Step 5: then perform cyclic shift encryption in the row direction to obtain the encrypted image X_4 in the row direction, wherein the size is $p \times n$, and the encryption steps in the row direction are expressed as follows:

$$\begin{aligned}
&\text{for}\, r\,\text{times} = 1\text{: keyRow},\\
&\quad \text{for}\, i = 1\text{: } p,\\
&X_4\,(i, :\,) = \text{circshift}\big(X_3\,(i, :\,), [0 \quad \text{bitRow}\\
&\qquad - (r\,\text{times}, i)]\big),\\
&\quad \text{end},\\
&\quad \text{end},
\end{aligned} \tag{23}$$

where r times is the number of bit cycles to be performed in all row directions for the control as a whole. circshif function has two parameters, one to control the row and the other to control the column. Now, as long as the column is operated, circshif function is set to $[0 \quad \text{bitRow} - (r\,\text{times}, i)]$.

Step 6: then, perform cyclic shift encryption in the column direction to obtain the encrypted image Y in the column direction with size $p \times n$, and the encryption steps in the column direction are expressed as follows:

$$\begin{aligned}
&\text{for}\, c\,\text{times} = 1\text{: keyColumn},\\
&\quad \text{for}\, i = 1\text{: } q,\\
&Y\,(i, :\,) = \text{circshift}\big(X_4\,(i, :\,), [\text{bitColumn} - (c\,\text{times}, i)\; 0]\big),\\
&\quad \text{end},\\
&\quad \text{end},
\end{aligned} \tag{24}$$

where c times is the number of bit cycles to be performed in all column directions for the control as a whole. Now, as long as the row is operated, so the circshif function is set to [bitColumn− (c times, i) 0].

4.3. Decryption Scheme. The decryption scheme is actually the reverse operation of the encryption scheme, and its principle is the same as that of the encryption scheme. The specific decryption steps can be described as follows:

Step 1: first obtain the encrypted image, which is represented by Y' and size is $p \times n$.

Step 2: according to the cycle number keyColumn of the cyclic shift in the column direction sent by the encryption party, a bit cyclic sequence bitColumn for decryption in the column direction is constructed.

Step 3: decrypt the encrypted image with a cyclic shift in column direction according to keyColumn and bitColumn and obtain the cyclic shift in the column direction to decrypt image $X_{4'}$, with size $p \times n$. The steps are as follows:

$$\begin{aligned}
&\text{for } c \text{ times} = 1\text{: keyColumn,}\\
&\quad \text{for } i = 1\text{: } q,\\
&X_{4'}(:,i) = \text{circshift}(Y\prime(:,i), [p - \text{bitColumn}(c \text{ times}, i) \quad 0]),\\
&\quad \text{end,}\\
&\quad \text{end,}
\end{aligned} \tag{25}$$

Step 4: according to the cycle number keyRow of the cyclic shift in the row direction sent by the encryption party, construct the bit cyclic sequence bitRow used for encryption in the row direction.

Step 5: perform cyclic shift decryption on the cyclic shift decrypted image $X_{4'}$ in the column direction according to the cycle number c_0 of cyclic shift encryption in the row direction sent by the encrypting party to obtain the cyclic shift decrypted image $X_{3'}$ in the row direction with size $p \times n$. The steps are as follows:

$$\begin{aligned}
&\text{for } r \text{ times} = 1\text{: keyRow,}\\
&\quad \text{for } i = 1\text{: } p,\\
&X_{3,}(:,i) = \text{circshift}\left(X_{4'}(:,i), [0 \quad q - \text{bitColumn}(r \text{ times}, i)]\right);\\
&\quad \text{end,}\\
&\quad \text{end.}
\end{aligned} \tag{26}$$

Step 6: generate the improved chaotic sequence according to the improved chaotic sequence initial values u_0, ω_0 sent by the encryption party to construct the random measurement matrix, which is used for decompression sampling. And $X_{3'}$ is recovered by the OMP algorithm to obtain a decompressed image, which is represented as $X_{2'}$ with size $m \times n$.

Step 7: Arnold inverse interference is performed on $X_{2'}$ according to Arnold interference parameters k_1, k_2 and interference number k_3 sent by the encryption party, and the image after inverse Arnold interference is represented as $X_{1'}$ with size $m \times n$.

Step 8: image $X_{1'}$ is subjected to inverse sparsity processing by Inverse Discrete Wavelet Transform (IDWT), and the final decrypted image X' with size $m \times n$ is obtained.

This allows the receiver to decrypt the encrypted image and retrieve the original message. The flow chart of encryption and decryption is shown in Figure 3.

5. Simulation Result and Discussion

In this section, we simulate and evaluate the safe and effective image compression-encryption scheme, using MATLAB R2018a to simulate. The size of the selected image is 256 × 256, and the size of the constructed random measurement matrix is 230 × 256. And $n_0 = 4, \mathbf{a}_0 = 3, b_0 = 2$, the initial values of all chaotic sequences are set to 0.3, and $u_0 = 0.3, u_1 = 0.4, \omega_0 = 3.87, \omega_1 = 3.95$. The cycle number of row cyclic shift encryption is keyRow = 6, and the cycle number of column cyclic shift is keyColumn = 5. DWT is used to perform the sparse operation, and the OMP algorithm is used for recovery.

5.1. Encryption Effect. We select "Lena," "Boom," "Moon," and "Rice" images for encryption to analyze the encryption and decryption effect. We use four new chaotic maps proposed in this paper to perform chaotic encryption. The encryption effect is shown in Figure 4.

It can be seen from Figures 4(a) and 4(c) that the original image becomes disorganized and irregular after encryption, and the data of the original image cannot be identified, which proves that the encryption scheme proposed in this paper has a good encryption effect.

5.2. Histogram Analysis. The histogram represents the distribution of the pixel intensity of digital images in a graphical way, which can intuitively show the pixel distribution states of the original image and the encrypted image. When the pixel distribution is not uniform, it may cause the loss of image details. The histogram of the original image is unique and vulnerable to statistical attack. To prevent this attack, the histogram of the encrypted image must be relatively uniform and different from that of the original image.

From Figures 4(b) and 4(d), the histograms of the original images are not uniformly distributed, while the encrypted histograms are uniformly distributed. It can be seen that the proposed chaotic maps applied to the encryption field have a strong resistance to statistical attack.

5.3. Key Sensitivity Analysis. We use the proposed Logistic map under our new structure for testing. Firstly, we give a set of encryption keys to encrypt the original image and then decrypt it with the same key. We randomly use a set of keys

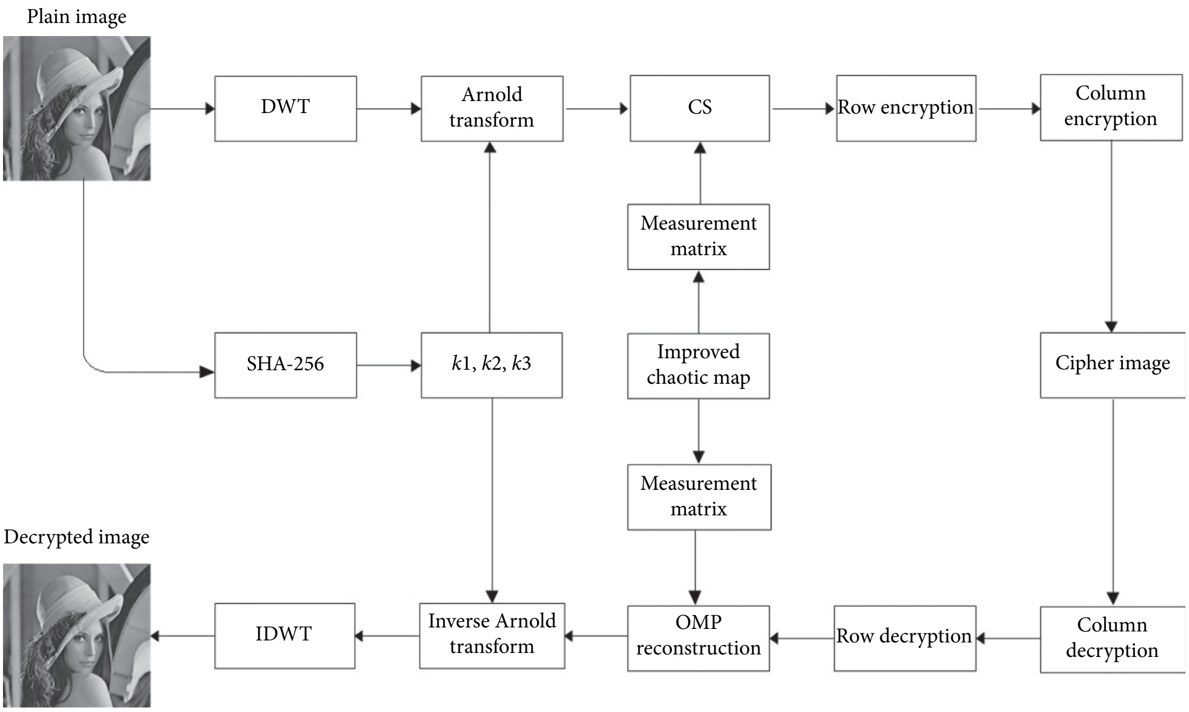


Figure 3: Flow chart of encryption and decryption.

$[0.568\ \ 0.265\ \ 1.25\ \ 23.26\ \ 456.2\ \ 256.2\ \ 2\ \ 1]$ to encryption. When we use $[0.568\ \ 0.265\ \ 1.25\ \ 23.26\ \ 456.2\ \ 256.2\ \ 2\ \ 1]$ to decrypt, we can get the decrypted image. But when we use $[0.568\ \ 0.265\ \ 1.25\ \ 23.26\ \ 456.2\ \ 256.2\ \ 2.0000000000000001\ \ 1]$ to decrypt, we could not get the decrypted image. As shown in Figure 5, even if the decryption keys differ by 0.0000000000000001, the decrypted image cannot be obtained; thus, the useful information cannot be obtained, which shows that new chaotic maps have high sensitivity.

5.4. Keyspace Analysis. A good encryption scheme should make the keyspace greater than 10^{30} in order to resist a brute force attack. There are 14 keys in our encryption scheme, which are $k, n_0, \mathbf{a}_0, b_0, u_0, u_1, z_0', z_1', \omega_0, \omega_1$, keyRow, LogisticRow$'$, keyColumn, and LogisticColumn$'$. If the accuracy is set to 10^{-14}, then the keyspace of our encryption scheme is 10^{196}. This shows that the keyspace of our encryption scheme is large enough to resist a brute force attack.

5.5. PSNR and SSIM Analysis. In order to further verify whether the encryption algorithm is safe and reliable, the quality of the images before and after encryption is analyzed. The quality of the restored images can be evaluated using the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM). PSNR can be expressed as

$$\mathrm{PSNR} = 10 \log \frac{255^2}{\left(\left(1/N^2\right) \sum_{i=1}^{N} \sum_{j=1}^{N} \left[P(i,j) - P'(i,j)\right]^2\right)}, \tag{27}$$

where $P(i,j)$ is the pixel value at the (i,j) position of the original image, $P'(i,j)$ is the pixel value at the (i,j) position of the restored image, N is the size of the image selected for the experiment, and 255 is the maximum value of the 8-bit representation. Generally, when the value of PSNR is lower than 28, the difference in image quality is greater. The smaller the PSNR, the greater the difference in image quality. The greater the PSNR, the less distortion the original image.

SSIM is used to measure the similarity between the original image and the restored image, which can be expressed as

$$\mathrm{SSIM} = \frac{\left(2\mu_X\mu_Y + C_1\right)\left(2\sigma_{XY} + C_2\right)}{\left(\mu_X^2 + \mu_Y^2 + C_1\right)\left(\sigma_X^2 + \sigma_Y^2 + C_2\right)}, \tag{28}$$

where $C_1 = 0.01 \times (2^8 - 1), C_2 = 0.01 \times (2^8 - 1)$, μ_X is the mean value of the original image, and μ_Y is the mean value of the restored image. σ_X^2 is the variance of the original image, σ_Y^2 is the variance of the restored image, and σ_{XY} is the covariance of the original image and the restored image. The range of structural similarity is $[-1, 1]$. In general, the larger the SSIM values, the better the overall quality of the reconstructed images. When the original image and the restored image are identical, the value of SSIM is 1.

Table 1 lists the analysis results of PSNR and SSIM. It can be seen from Table 1 that the PSNR and SSIM of our encryption scheme are the largest, indicating that the encryption and decryption effect proposed in this paper is good.

5.6. Information Entropy Analysis. Information entropy is used to measure the confusion of the image and the distribution of gray values. The larger the entropy of the images is, the more consistent the gray distribution of the images is.

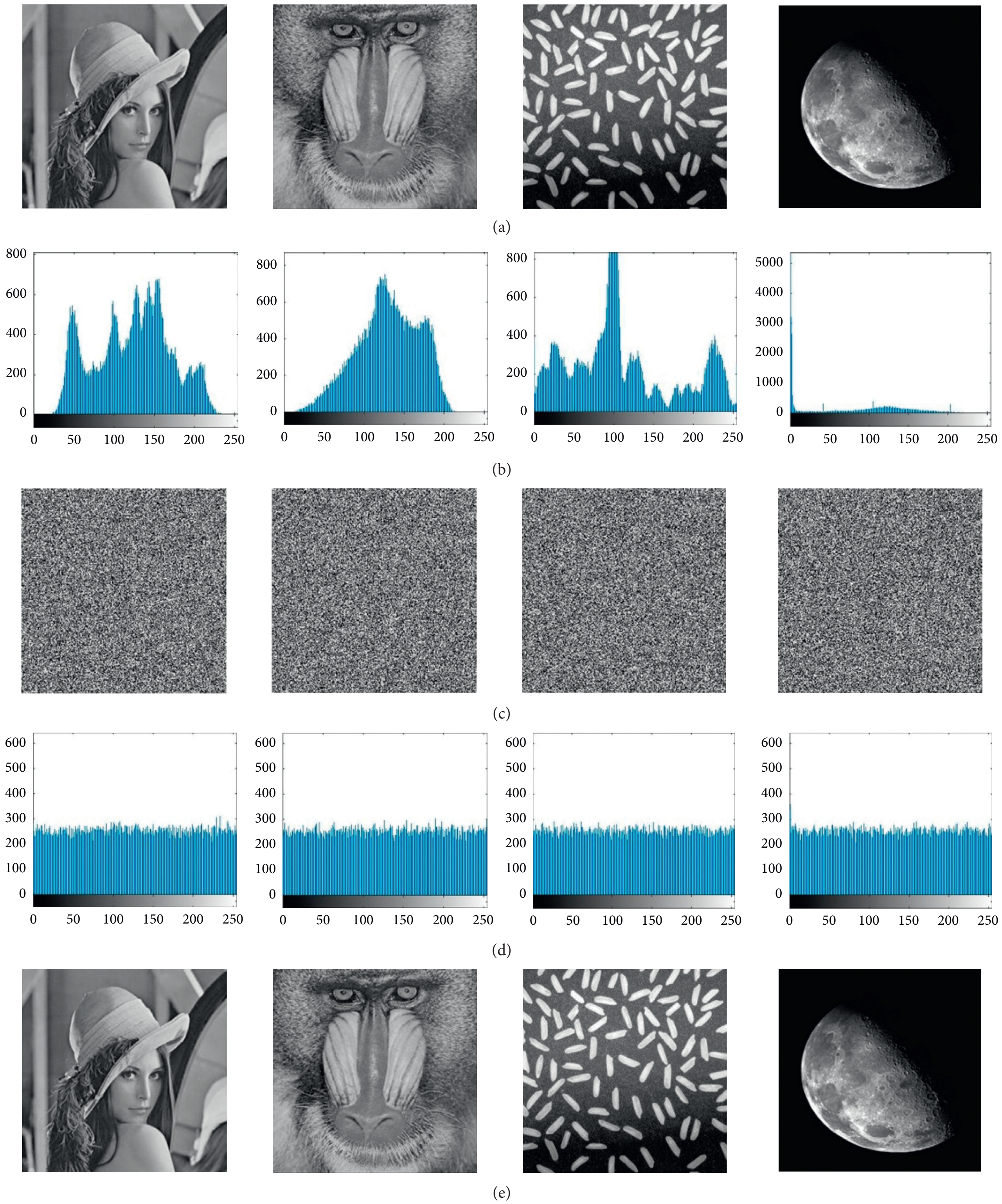
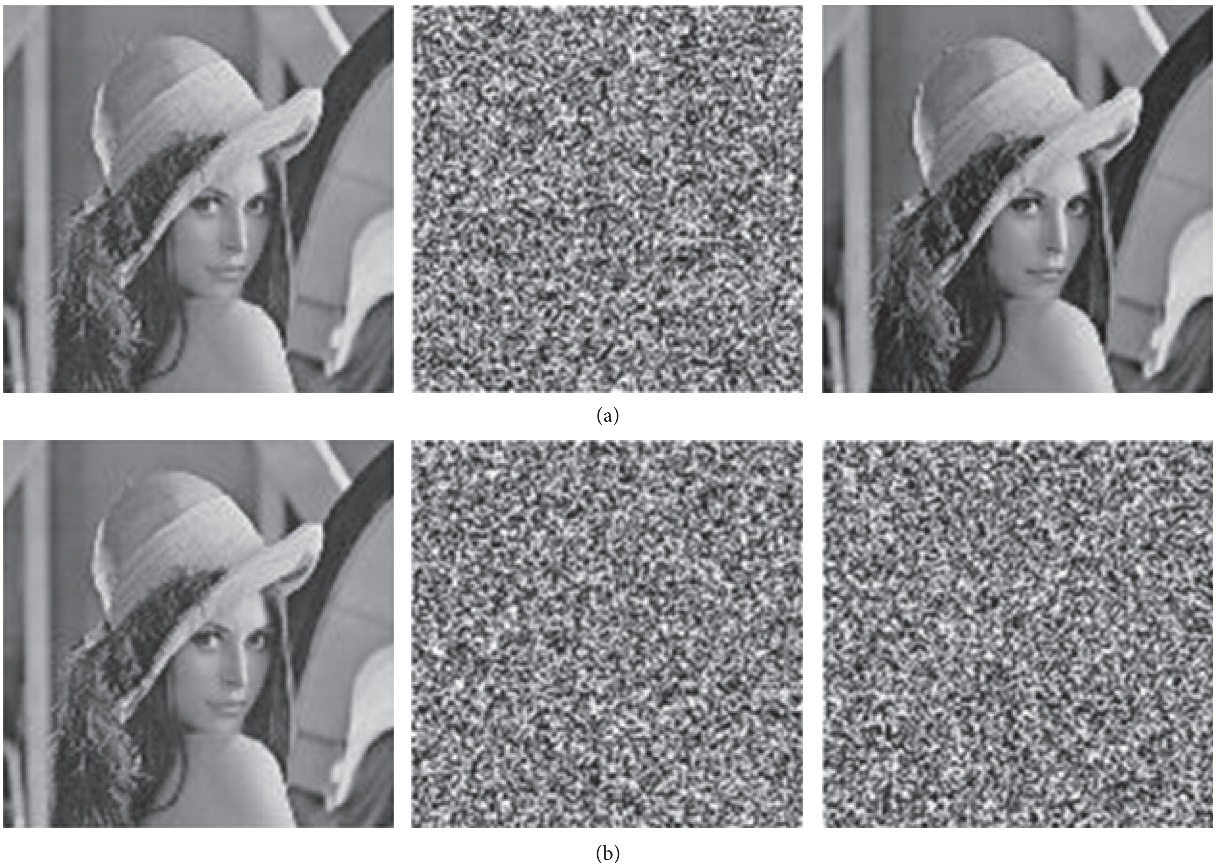


Figure 4: (a) Original image, (b) original image histogram, (c) encrypted image, (d) encrypted image histogram, and (e) decrypted image.

For a gray image of size 256 × 256, the theoretical value of information entropy is 8. An effective encryption algorithm should make the information entropy of the encrypted image close to the theoretical value. The information entropy can be expressed as

$$H(m) = -\sum_{i=1}^{L\times L} P(m_i)\log_2 P(m_i), \tag{29}$$

where $P(m_i)$ is the probability of the gray value m_i, and L is the gray level.



(a)

(b)

Figure 5: Key sensitivity analysis. The encryption key is [0.568 0.265 1.25 23.26 456.2 256.2 2 1]. (a) decryption key is [0.568 0.265 1.25 23.26 456.2 256.2 2 1] and (b) decryption key is [0.568 0.265 1.25 23.26 456.2 256.2 2.0000000000000001 1].

Table 1: PSNR and SSIM analysis.

	Chaotic map	CS scheme [14]			Our scheme		
		Lena	Boom	Average	Lena	Boom	Average
PSNR	Chebyshev + Tent [14]	32.2193	23.3287	**27.7740**	34.7032	26.9524	**30.8278**
	Our-Chebyshev + our-Tent	32.3556	23.4894	**27.9225**	35.4272	27.1717	**31.2995**
	Sine + Logistic [17]	32.2724	23.0829	**27.6777**	35.1394	26.5448	**30.8421**
	Our-Sine + our-Logistic	32.2654	23.5357	**27.9006**	35.3708	26.9977	**31.1843**
SSIM	Chebyshev + Tent [14]	0.7517	0.6227	**0.6872**	0.8118	0.7872	**0.7995**
	Our-Chebyshev + our-Tent	0.7528	0.6394	**0.6961**	0.8184	0.7971	**0.8078**
	Sine + Logistic [17]	0.7538	0.6450	**0.6994**	0.8164	0.7883	**0.8024**
	Our-Sine + our-Logistic	0.7512	0.6664	**0.7088**	0.8194	0.7955	**0.8075**

Table 2 lists the results of information entropy analysis. As can be seen from Table 2, the information entropy of the encrypted image is higher than that of the original image, which proves that the gray distribution of the encrypted image is more uniform than that of the original image.

5.7. Correlation Analysis. Correlation analysis mainly analyzes the correlation between pixels in adjacent locations. The correlation between adjacent pixels of the original image is very high, while the correlation between encrypted cryptographic images after an effective secure encryption system should be

Table 2: Information entropy analysis.

Chaotic map		CS scheme [14]			Our scheme		
		Lena	Boom	Average	Lena	Boom	Average
Information entropy	Chebyshev + Tent [14]	7.2172	7.2735	**7.2454**	7.6397	7.8880	**7.7639**
	Our-Chebyshev + our-Tent	7.5729	7.5738	**7.5734**	7.9820	7.9895	**7.9858**
	Sine + Logistic [17]	7.2750	7.2735	**7.2743**	7.6658	7.6945	**7.6802**
	Our-Sine + our-Logistic	7.5612	7.5940	**7.5776**	7.9812	7.9840	**7.9826**

Table 3: Correlation analysis.

Image		Direction	Correlation coefficient of plain image	Correlation coefficient of cipher image			
				Chebyshev + Tent [14]	Our-Chebyshev + our-Tent	Sine + Logistic [17]	Our-Sine + our-Logistic
CS scheme [14]	Lena	Horizontal	0.9343	−0.0407	0.0098	−0.0568	−0.0251
		Vertical	0.9715	−0.0549	−0.0324	0.0943	0.0107
		Diagonal	0.9271	0.0343	−0.0047	0.0633	0.0624
	Boom	Horizontal	0.8544	−0.0195	−0.0011	0.0521	0.0372
		Vertical	0.8311	0.0402	0.0287	−0.0149	−0.0236
		Diagonal	0.7576	−0.0608	0.0293	0.0459	−0.0438
	Average	**Horizontal**	**0.8944**	**−0.0301**	**0.0044**	**−0.0024**	**0.0061**
		Vertical	**0.9013**	**−0.0074**	**−0.0019**	**0.0397**	**−0.0065**
		Diagonal	**0.8424**	**−0.0133**	**0.0123**	**0.0546**	**0.0093**
Our scheme	Lena	Horizontal	0.9278	0.0393	−0.0058	−0.0010	0.0012
		Vertical	0.9688	0.0352	0.0197	0.0428	−0.0306
		Diagonal	0.9031	0.0140	0.0246	−0.0023	−0.0197
	Boom	Horizontal	0.8685	−0.0125	−0.0105	−0.0123	−0.0126
		Vertical	0.8247	−0.0278	−0.0156	−0.0814	0.0181
		Diagonal	0.7623	−0.0173	−0.0149	0.0226	0.0344
	Average	**Horizontal**	**0.8982**	**0.0134**	**−0.0082**	**−0.0067**	**−0.0057**
		Vertical	**0.8968**	**0.0037**	**0.0021**	**−0.0193**	**−0.0063**
		Diagonal	**0.8327**	**−0.0017**	**0.0049**	**0.0102**	**0.0074**

relatively low, with the correlation coefficient close to 0. The correlation calculation can be expressed as

$$
\begin{aligned}
r_{xy} &= \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}},\\
\operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]\left[y_i - E(y)\right],\\
D(x) &= \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]^2,\\
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i,
\end{aligned}
\tag{30}
$$

where x and y represent the gray values of two adjacent pixels.

Table 3 lists the correlation coefficient analysis results of the safe and effective image encryption scheme. It can be seen from Table 3 that, compared with the correlation coefficient of the original image, the correlation coefficient of the encrypted image is greatly reduced and close to 0, which indicates that the abovementioned security theoretical scheme has a good encryption effect.

6. Conclusion

We propose a safe and effective image compression-encryption scheme based on a new chaotic structure and compressive sensing. This scheme uses a new chaotic structure proposed by ourselves and applies the commonly used traditional one-dimensional chaotic maps to the proposed chaotic structure to generate corresponding new one-dimensional chaotic maps. The proposed new chaotic maps not only keep the advantages of simple structure and easy implementation of a traditional one-dimensional chaotic map but also expands the parameter range space of traditional one-dimensional chaotic maps. It is useful whenever chaotic digital sequences are needed. In addition, compressive sensing is used for sampling in this encryption scheme, which can reduce the storage space and transmission bandwidth. The chaotic system only needs to store matrix generation parameters, which can further reduce the bandwidth. Simulation results show that the proposed chaotic structure and chaotic maps have a good chaotic effect and high chaotic intensity, and the output sequence has strong chaos in a very large area of parameter space and can prevent phase space reconstruction. It can be applied to the image encryption scheme in this paper and has a large parameter space and keyspace, which can prevent brute force attacks and statistical attacks.

Data Availability

The data used to support the findings of this study are available from the first or corresponding author upon request.

Conflicts of Interest

The authors declare there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was fully supported by the National Natural Science Foundation of China (nos. 61972051 and 62032002), the Support Plan of Scientific and Technological Innovation Team in Universities of Henan Province (no. 20IRTSTHN013), the Henan Key Laboratory of Network Cryptography Technology (no. LNCT2019-A04), and the Research Foundation of Young Core Instructor in Henan Province (no. 2018GGJS058).

References

[1] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Information Sciences*, vol. 396, pp. 97–113, 2017.

[2] J.-x. Chen, Z.-l. Zhu, C. Fu, H. Yu, and L.-b. Zhang, "An efficient image encryption scheme using gray code based permutation approach," *Optics and Lasers in Engineering*, vol. 67, pp. 191–204, 2015.

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

[4] E. J. Candès, 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, 2006.

[5] D. Wang, B. Zhang, D. Qiu, and F. Xie, "On the Super-Lorenz Chaotic model for the virtual synchronous generator," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 4, pp. 511–515, 2018.

[6] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759–765, 2005.

[7] X. Li, C. Li, and I.-K. Lee, "Chaotic image encryption using pseudo-random masks and pixel mapping," *Signal Processing*, vol. 125, pp. 48–63, 2016.

[8] K. W. Wong, Q. Lin, and J. Chen, "Simultaneous arithmetic coding and encryption using chaotic maps," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 2, pp. 146–150, 2010.

[9] C. Zhou, W. Hu, L. Wang, and G. Chen, "Turbo trellis-coded differential chaotic modulation," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 2, pp. 191–195, 2018.

[10] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.

[11] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[12] K. Cho and T. Miyano, "Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 2, pp. 478–487, 2015.

[13] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, 2010.

[14] H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, and D. Wang, "Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 11, no. 3, pp. 558–573, 2017.

[15] H. Wang, D. Xiao, M. Li et al., "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Processing*, vol. 155, pp. 218–232, 2017.

[16] 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.

[17] P. Chanil, A. Kwangil, J. Paeksan et al., "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 12027–12042, 2019.

[18] R. Lan, J. He, S. Wang, Y. Liu, and X. Luo, "A parameter-selection-based chaotic system," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 3, pp. 492–496, 2019.

[19] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013.

[20] X. Li, L. Bao, D. Zhao et al., "The analyses of an improved 2-order Chebyshev chaotic sequence," in *Proceedings of the International Conference on Computer Networks and Inventive Communication Technologies*, pp. 24–26, Harbin, China, 2011.

[21] R. Ponuma and R. Amutha, "Compressive sensing based image compression-encryption using novel 1D-chaotic map," *Multimedia Tools and Applications*, vol. 77, no. 15, pp. 19209–19234, 2018.

[22] E. J. Candès 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.

[23] K. J. Persohn and R. J. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation finite precision floating-point representation," *Chaos, Solitons & Fractals*, vol. 45, no. 3, pp. 238–245, 2012.

[24] H. Zhang, W. Yin, and L. Cheng, "Necessary and sufficient conditions of solution uniqueness in 1-norm minimization," *Journal of Optimization Theory and Applications*, vol. 164, no. 1, pp. 109–122, 2015.

[25] D. L. Donoho and M. Elad, "Optimally sparse representation in general (nonorthogonal) dictionaries via 1 minimization," *Proceedings of the National Academy of Sciences*, vol. 100, no. 5, pp. 2197–2202, 2003.

[26] M. A. Hanson, H. C. Powell, A. T. Barth et al., "Body area sensor networks: challenges and opportunities," *Computer*, vol. 42, no. 1, pp. 58–65, 2009.

[27] J. A. Tropp, "Greed is good: algorithmic results for sparse approximation," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2231–2242, 2004.

[28] S. G. Mallat and Z. Zhifeng Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3397–3415, 1993.

[29] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[30] D. L. Donoho, Y. Tsaig, I. Drori, and J.-L. Starck, "Sparse solution of underdetermined systems of linear equations by stagewise orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1094–1121, 2012.

[31] D. Needell and J. A. Tropp, "CoSaMP: iterative signal recovery from incomplete and inaccurate samples," *Applied and Computational Harmonic Analysis*, vol. 26, no. 32, pp. 301–321, 2009.